INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA STIINȚIFICĂ STUDENȚEASCĂ
CONFERENCE PROCEEDINGS

VOLUMUL 4
2025

Editura Academiei Naționale de Informații
„Mihai Viteazul”

INTELLIGENCE
ȘI CULTURA DE SECURITATE

nr. 4 – 2025

– Conferința Științifică Studențească –

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

Bucureşti, 2025

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”
© ANIMV
Bucureşti, 2025
Telefon: 0377720.000/1216
Fax: 0377721.134; 0377721.125
ISSN 2972 – 1350 ISSN-L 2971 – 8139

CUPRINS

CRIMINALITATEA DE MEDIU ŞI SECURITATEA GLOBALĂ

Livia MANDU*
Cornel RACOVEANU**

Abstract:

Environmental organized crime represents a significant challenge to global security, with severe implications for ecosystems, economies and vulnerable communities. This paper explores the complex relationship between environmental science and the illegal activities carried out by organized criminal networks, analyzing their impact and the institutional and technological responses developed to counter them.

First, the paper addresses the main types of environmental crime, such as wildlife trafficking, illegal deforestation and improper management of hazardous waste, highlighting their effects on biodiversity and the degradation of natural resources. Through relevant case studies, the scope and complexity of these activities are illustrated, as well as the global networks facilitating them.

The analysis then focuses on the ecological and socio-economic consequences of organized environmental crime. These include habitat loss, severe pollution and the intensification of climate change, which, in turn, exacerbate food insecurity and regional conflicts. The selected case studies reveal the connection between environmental crime and public health issues, as well as the negative impact on local communities dependent on natural resources.

Also, the paper examines legal and institutional responses to environmental crime, emphasizing the international legislative framework and the role of global organizations such as INTERPOL and the UN. The limitations of current policies are analyzed in depth, as well as the need for stronger public-private partnerships.

Another central aspect is the use of emerging technologies and environmental science in combating illegal activities. Satellite imagery, drones and artificial intelligence are essential tools for detecting and preventing organized environmental crime, with their applicability illustrated through relevant case studies.

Finally, the paper underscores the interdependence between global security and environmental protection, demonstrating how climate change amplifies illegal activities and how environmental crime constitutes a major transnational threat. The recommendations focus on strengthening legislation, promoting international cooperation and actively involving local communities in environmental protection efforts.

* doctorand, Şcoala Naţională de Studii Politice şi Administrative, Bucureşti, livia.mandu@gmail.com

** doctorand, Şcoala Naţională de Studii Politice şi Administrative, Bucureşti, cornel.racoveanu@yahoo.com

This research highlights the need for an integrated approach that combines expertise in environmental science with firm measures against organized criminal networks to ensure the sustainability of ecosystems and global security.

Cuvinte-cheie: *securitate, schimbări climatice, criminalitate organizată, criminalitate de mediu.*

Introducere

În ultimele secole, relația dintre mediul natural și activitățile umane a devenit tot mai complexă, pe fondul presiunilor economice, sociale și tehnologice, iar răspunsul la provocările generate în acest context s-a intensificat progresiv. Criminalitatea organizată, deși tradițional asociată cu domenii precum traficul de droguri, arme sau persoane, a evoluat rapid, extinzându-și sfera de influență și către domeniul protecției mediului. Această expansiune a avut consecințe profunde nu doar asupra ecosistemelor, ci și asupra securității globale, sănătății publice și stabilității socio-economice (Nellemann et al., 2016). Înțelegerea acestei intersecții între știința mediului și criminalitatea organizată este esențială pentru elaborarea unor politici eficiente și pentru protejarea resurselor naturale indispensabile vieții.

Criminalitatea de mediu reprezintă una dintre cele mai profitabile forme de criminalitate transnațională, generând venituri anuale estimate între 91 și 258 miliarde de dolari (INTERPOL & UNEP, 2016). Această formă de criminalitate include activități diverse, precum exploatarea forestieră ilegală, comerțul ilicit cu specii sălbatice, gestionarea frauduloasă a deșeurilor periculoase și pescuitul ilegal. Spre deosebire de infracțiunile clasice, criminalitatea de mediu implică adesea rețele complexe și bine organizate, capabile să corupă oficiali, să eludeze reglementările internaționale și să opereze dincolo de granițele naționale (UNODC, 2020).

Degradarea mediului cauzată de astfel de activități are efecte în lanț asupra ecosistemelor, generând pierderea biodiversității, intensificarea schimbărilor climatice și destabilizarea resurselor naturale vitale. Defrișările masive, poluarea apelor și aerului, precum și distrugerea habitatelor naturale conduc la insecuritate alimentară, migrații forțate și conflicte regionale (Brisman & South, 2020). În mod particular, comunitățile vulnerabile, care depind în mod direct de resursele naturale, sunt cele mai afectate, fiind adesea capturate într-un cerc vicios al sărăciei și marginalizării sociale.

Deşi răspunsurile internaţionale la criminalitatea de mediu s-au intensificat în ultimele decenii, cadrul legislativ şi eforturile de aplicare a legii rămân adesea fragmentate şi insuficient adaptate la complexitatea fenomenului. Organizaţii internaţionale precum INTERPOL, UNEP şi ONU au dezvoltat iniţiative majore pentru combaterea criminalităţii de mediu, însă impactul lor este limitat de lipsa resurselor, de fragmentarea jurisdicţiilor şi de colaborarea ineficientă între state (Nellemann et al., 2016). În acest context, tehnologiile emergente, precum imagistica satelitară, dronele şi inteligenţa artificială, oferă noi oportunităţi pentru detectarea şi prevenirea activităţilor ilegale, îmbinând progresele din ştiinţa mediului cu măsuri de securitate avansate.

Această lucrare îşi propune să analizeze relaţia dintre ştiinţa mediului şi criminalitatea organizată, concentrându-se pe tipologiile principale de criminalitate de mediu, impactul ecologic şi socio-economic al acestora, răspunsurile instituţionale dezvoltate şi utilizarea tehnologiilor moderne în combaterea fenomenului. Printr-o abordare interdisciplinară, cercetarea evidenţiază importanţa integrării cunoştinţelor din domeniul mediului în politicile de securitate şi justiţie penală, subliniind necesitatea unor soluţii inovatoare şi a unei cooperări internaţionale consolidate pentru a răspunde acestei provocări majore.

Prin această cercetare, se subliniază importanţa adoptării unei viziuni integrate care să recunoască conexiunile profunde dintre protecţia mediului şi securitatea internaţională, într-o lume tot mai interdependentă şi expusă unor riscuri complexe.

Metodologia de cercetare

Studiul de faţă utilizează o abordare calitativă, interdisciplinară, având ca obiectiv principal analiza relaţiei dintre criminalitatea organizată şi protecţia mediului, cu accent pe impactul ecologic, socio-economic şi asupra securităţii internaţionale. Alegerea metodei calitative se justifică prin complexitatea fenomenului investigat, care necesită o înţelegere aprofundată a contextelor sociale, politice, juridice şi de mediu în care criminalitatea de mediu se manifestă (Creswell, 2014).

În cadrul cercetării a fost utilizată metoda analizei documentare, prin examinarea critică a literaturii de specialitate, a rapoartelor oficiale elaborate de organizaţii internaţionale precum INTERPOL, UNEP, UNODC sau Europol, precum şi a legislaţiei relevante la nivel naţional, european şi internaţional. Această metodă a permis identificarea

principalelor forme de criminalitate de mediu, a rețelelor implicate și a consecințelor asupra mediului și securității (Bowen, 2009).

O atenție deosebită a fost acordată raportului dintre criminalitatea de mediu și schimbările climatice, degradarea biodiversității și insecuritatea alimentară, utilizând date statistice, studii de caz și analize comparative. De asemenea, au fost consultate lucrări din domeniul criminologiei verzi, securității internaționale și politicilor publice de mediu, pentru a construi un cadru conceptual solid care să susțină analiza (White, 2013).

Metoda studiului de caz a fost aplicată pentru a exemplifica modul concret în care grupările de criminalitate organizată operează în domeniul mediului, utilizând exemple documentate privind traficul de deșeuri, exploatarea forestieră ilegală și comerțul cu specii sălbatice protejate. Studiile de caz au fost selectate pe baza relevanței lor pentru tematica cercetării și a disponibilității informațiilor verificate în surse de încredere.

În procesul de analiză, s-a utilizat și metoda comparativă, prin care s-au examinat diferențele și asemănările dintre politicile și strategiile de combatere a criminalității de mediu în diverse regiuni ale lumii. Această abordare a permis evidențierea bunelor practici, dar și a lacunelor persistente în sistemele de răspuns existente (Yin, 2018).

Selecția surselor s-a realizat conform unor criterii riguroase de relevanță, actualitate și credibilitate, fiind preferate publicațiile din ultimii zece ani și materialele elaborate de instituții recunoscute la nivel internațional. În plus, au fost utilizate baze de date științifice precum Scopus, Web of Science și Google Scholar pentru a identifica articole de cercetare relevante.

Limitările metodologice ale studiului derivă în principal din dificultatea obținerii unor date exacte privind dimensiunea reală a criminalității de mediu, fenomen care, prin natura sa clandestină, este adesea subraportat sau mascat. De asemenea, lipsa unei abordări unificate la nivel global în clasificarea și măsurarea criminalității de mediu a impus o atenție sporită în analiza comparativă a datelor provenite din surse diferite.

În pofida acestor limitări, metodologia adoptată oferă o bază solidă pentru înțelegerea profundă a interacțiunii dintre criminalitatea organizată și mediul înconjurător și permite formularea unor concluzii relevante pentru îmbunătățirea politicilor de prevenire și combatere a acestui fenomen complex.

Rezultatele cercetării

Capitolul I: Tipologii de criminalitate organizată de mediu

Criminalitatea organizată specializată în activităţi ilegale legate de mediu sau criminalitatea de mediu constituie una dintre cele mai profitabile şi mai puţin riscante forme de activitate ilegală la nivel global, fiind în acelaşi timp una dintre cele mai subestimate în ceea ce priveşte impactul său asupra ecosistemelor şi societăţii. Această formă de criminalitate implică reţele transnaţionale bine structurate, care exploatează resursele naturale, încalcă reglementările de protecţie a mediului şi adesea corup oficiali locali şi internaţionali pentru a-şi perpetua activităţile.

Defrişările ilegale reprezintă o ameninţare critică pentru pădurile tropicale, în special în regiunile Amazonului, Asiei de Sud-Est şi bazinului Congo. Aceste activităţi sunt adesea facilitate de companii paravan, documente falsificate şi reţele care implică intermediari locali şi actori politici corupţi. Potrivit unui raport al INTERPOL şi al Programului Naţiunilor Unite pentru Mediu (UNEP, 2016), defrişările ilegale sunt responsabile pentru până la 90% din toate tăierile de pădure tropicală, generând venituri estimate la 30–100 de miliarde de dolari anual.

Consecinţele acestor activităţi nu se limitează la pierderea biodiversităţii, ci includ şi destabilizarea solului, perturbarea ciclurilor hidrologice şi accentuarea emisiilor de gaze cu efect de seră. În Brazilia, reţelele criminale de exploatare forestieră au reuşit să influenţeze decizii politice, reducând astfel eficienţa măsurilor de conservare (Kaimowitz, 2015).

Traficul de specii sălbatice este o altă manifestare a criminalităţii de mediu organizate, cu efecte devastatoare asupra biodiversităţii globale. Această activitate implică capturarea, transportul şi comercializarea ilegală de animale şi plante, uneori ameninţate cu dispariţia. Raportul Wildlife Crime Initiative arată că traficul cu specii sălbatice valorează anual între 7 şi 23 de miliarde de dolari (UNODC, 2020).

Animalele sunt adesea vândute ca animale de companie exotice, trofee de vânătoare sau ingrediente pentru medicina tradiţională. De exemplu, traficul de fildeş şi corn de rinocer a devastat populaţiile de elefanţi şi rinoceri africani. Această practică nu doar că ameninţă existenţa unor specii întregi, ci contribuie şi la destabilizarea ecosistemelor locale, afectând lanţurile trofice şi serviciile ecosistemice de care depind comunităţile umane.

Gestionarea necorespunzătoare a deșeurilor periculoase constituie o altă dimensiune importantă a criminalității de mediu. Aceste activități implică transportul, depozitarea și eliminarea ilegală a deșeurilor toxice, adesea în țările în curs de dezvoltare, unde reglementările sunt mai permisive sau mai ușor de eludat. În unele cazuri, deșeurile industriale din Europa sunt exportate ilegal către Africa sau Asia de Sud, unde sunt abandonate fără măsuri adecvate de protecție a mediului sau sănătății umane (Nellemann et al., 2016). Consecințele asupra mediului includ contaminarea apei, solului și aerului, afectând culturile agricole, resursele de apă potabilă și biodiversitatea locală. În plus, expunerea comunităților locale la substanțe toxice a dus la creșterea incidenței bolilor respiratorii, canceroase și neurologice (UNEP, 2018).

Un exemplu al modului în care rețelele de criminalitate organizată operează în domeniul exploatării forestiere ilegale este situația din Asia de Sud-Est. În Myanmar, Cambodgia și Laos, pădurile tropicale sunt sistematic devastate de grupări care transportă ilegal lemn de esență prețioasă, cum ar fi tecul sau palisandrul, către piețele din China și alte părți ale lumii. Raportul Environmental Investigation Agency (EIA, 2019) arată că aceste activități sunt sprijinite de rețele care corup oficialii locali, falsifică acte de transport și folosesc rute comerciale complexe pentru a masca originea ilegală a lemnului.

În Africa, comerțul ilegal cu fildeș și alte părți ale animalelor a atins proporții alarmante. Deși interdicțiile internaționale asupra comerțului cu fildeș au fost introduse prin Convenția CITES, rețelele de crimă organizată au reușit să mențină piețele ilegale active, alimentate de cererea crescută din Asia (UNODC, 2020). Activitățile acestor rețele nu numai că afectează biodiversitatea, ci contribuie și la finanțarea grupărilor armate și a conflictelor regionale, exacerbând instabilitatea politică și economică.

Capitolul II: Impactul criminalității de mediu asupra ecosistemelor și comunităților

Criminalitatea organizată constituie una dintre cele mai insidioase amenințări la adresa echilibrelor naturale și a stabilității socio-economice globale. Prin natura sa, criminalitatea de mediu afectează și comunitățile umane care depind de resursele naturale pentru supraviețuire. De la pierderea habitatelor naturale până la intensificarea fenomenelor climatice extreme, efectele criminalității de mediu sunt profunde, de durată și, adesea, ireversibile.

În ceea ce priveşte ecosistemele, impactul activităţilor ilegale, precum defrişările masive, braconajul sau poluarea industrială neautorizată, se manifestă printr-o accelerare semnificativă a pierderii biodiversităţii. Habitatul natural este fragmentat sau complet distrus, afectând capacitatea speciilor de a supravieţui şi de a se reproduce (Nellemann et al., 2016). Această dinamică alterează reţelele ecologice, slăbind reziliența ecosistemelor în faţa schimbărilor climatice şi a altor presiuni antropice. De exemplu, defrişările ilegale din bazinul Amazonului conduc nu doar la pierderea masivă de arbori seculari, ci şi la declinul alarmant al speciilor dependente de acele habitate, afectând atât lanţurile trofice, cât şi funcţiile ecologice vitale, precum stocarea carbonului şi reglarea regimurilor hidrologice (UNODC, 2020).

Pe lângă degradarea fizică a mediului, criminalitatea de mediu amplifică poluarea globală a apei, aerului şi solului. Deversările ilegale de deşeuri toxice în cursuri de apă sau depozitarea clandestină a substanţelor periculoase în zone rurale afectează direct sănătatea comunităţilor locale. Numeroase studii au arătat o corelaţie între proximitatea faţă de siturile contaminate ilegal şi incidenţa crescută a bolilor respiratorii, cancerului şi tulburărilor de reproducere (Robinson et al., 2021). În plus, poluarea atmosferică rezultată din arderea ilegală a pădurilor nu se limitează la regiunile afectate, ci contribuie la degradarea calităţii aerului la scară transfrontalieră, provocând episoade de smog sever în oraşe aflate la sute de kilometri distanţă (INTERPOL & UNEP, 2016).

Un alt efect indirect, dar extrem de grav, este intensificarea schimbărilor climatice. Defrişările şi arderea vegetaţiei naturale eliberează volume masive de gaze cu efect de seră în atmosferă, reducând simultan capacitatea biosferei de a capta şi stoca carbonul (FAO, 2022). Din nefericire, resursele naturale distruse de grupările infracţionale erau tocmai acelea care ofereau cea mai eficientă barieră împotriva schimbărilor climatice. Pierderea pădurilor tropicale sau a zonelor umede accelerează procesele de deşertificare, schimbă regimurile pluviale şi destabilizează ecosistemele de coastă, afectând astfel securitatea alimentară şi disponibilitatea resurselor de apă potabilă.

Impactul asupra comunităţilor umane este la fel de sever. Criminalitatea de mediu contribuie la marginalizarea economică a comunităţilor locale, care, private de resursele naturale vitale, sunt forţate să îşi abandoneze modurile tradiţionale de viaţă. De exemplu, comunităţile indigene din Amazon sau din Africa Centrală sunt printre cele mai afectate de defrişările ilegale şi braconaj, pierzând accesul la surse esenţiale de hrană, medicamente tradiţionale şi materiale

de construcție (WWF, 2020). Această degradare a mediului devine, astfel, un factor determinant al migrației forțate și al tensiunilor sociale, în special în regiunile în care statul de drept este slab sau inexistent.

Mai mult, criminalitatea de mediu amplifică inegalitățile economice și sociale, în condițiile în care profiturile generate de exploatarea ilegală a resurselor naturale ajung în mâinile unor rețele criminale transnaționale, în timp ce comunitățile locale suportă costurile ecologice și sanitare. Lipsa unui cadru legislativ eficient, combinată cu corupția endemică în multe dintre regiunile afectate, face ca aceste comunități să rămână vulnerabile, lipsite de mijloace reale de protecție sau de compensare.

Într-un studiu de caz reprezentativ, degradarea zonelor umede din America Latină, provocată de activități ilegale precum extracția necontrolată de resurse sau braconajul, a dus nu doar la declinul biodiversității locale, ci și la o criză socio-economică gravă în rândul comunităților indigene (UNEP, 2018). Pescuitul excesiv, poluarea apei și distrugerea habitatelor naturale au afectat securitatea alimentară și sănătatea publică, generând migrație rural-urbană și sporind presiunea asupra infrastructurii urbane deja fragile.

Capitolul III: Răspunsuri juridice și instituționale la criminalitatea de mediu

În fața intensificării criminalității de mediu, comunitatea internațională, guvernele naționale și organizațiile neguvernamentale au dezvoltat un arsenal de instrumente juridice și instituționale menite să contracareze acest fenomen complex. Deși eforturile depuse au înregistrat progrese semnificative, provocările persistă, reflectând dificultățile inerente în aplicarea normelor de protecție a mediului și în consolidarea cooperării internaționale.

La nivel internațional, răspunsurile juridice au fost, în principal, articulate prin tratate, convenții și acorduri multilaterale care stabilesc standarde și obligații pentru protecția mediului. Printre cele mai relevante instrumente se numără Convenția de la Basel privind controlul mișcărilor transfrontaliere ale deșeurilor periculoase și al eliminării acestora (1989), Convenția CITES privind comerțul internațional cu specii de faună și floră sălbatică periclitate (1973) și Convenția de la Stockholm privind poluanții organici persistenți (2001). Aceste cadre normative stabilesc nu doar reguli de protecție, ci și mecanisme de monitorizare și sancționare a încălcărilor (Basel Convention, 2022; CITES, 2023).

Totuşi, un obstacol major în aplicarea acestor instrumente îl reprezintă natura transnaţională a criminalităţii de mediu. Reţelele criminale profită de diferenţele legislative dintre state şi de slăbiciunile instituţionale pentru a-şi desfăşura activităţile ilicite cu risc minim. În acest context, cooperarea internaţională devine esenţială, iar iniţiative precum reţeaua INTERPOL – Environmental Crime Programme sau parteneriatele facilitate de UNODC urmăresc să întărească schimbul de informaţii, coordonarea anchetelor şi armonizarea măsurilor represive (INTERPOL, 2021).

Pe lângă tratatele internaţionale, organizaţiile regionale au dezvoltat propriile lor mecanisme de combatere a criminalităţii de mediu. Uniunea Europeană, de exemplu, a introdus Directiva 2008/99/CE privind protecţia mediului prin dreptul penal, care impune statelor membre să incrimineze o serie de acţiuni ce aduc prejudicii grave mediului (European Parliament, 2008). Această directivă marchează un moment important, recunoscând faptul că sancţiunile administrative nu mai sunt suficiente pentru a combate eficient infracţiunile de mediu şi că măsurile penale trebuie integrate în arsenalul de protecţie a mediului.

Instituţional, numeroase state au creat agenţii specializate sau au desemnat unităţi de aplicare a legii dedicate investigării infracţiunilor de mediu. În Statele Unite, Environmental Protection Agency (EPA) dispune de o divizie de aplicare a legii care colaborează îndeaproape cu FBI în cazurile majore de poluare ilegală sau trafic cu specii protejate (EPA, 2022). În Europa, Europol a dezvoltat programul EnviCrimeNet, o reţea informală care facilitează cooperarea între poliţiile de mediu ale statelor membre.

Cu toate acestea, eforturile la nivel naţional şi internaţional sunt adesea limitate de constrângeri financiare, lipsa de expertiză tehnică şi nivelul variabil al angajamentului politic. Unele state, în special cele în curs de dezvoltare, nu dispun de resursele necesare pentru a implementa legislaţia de mediu sau pentru a combate reţelele infracţionale bine organizate. În plus, corupţia endemică în anumite regiuni subminează grav eficacitatea măsurilor de combatere a criminalităţii de mediu (UNEP, 2018).

Un alt aspect esenţial al răspunsului instituţional îl reprezintă implicarea sectorului non-guvernamental. Organizaţiile neguvernamentale internaţionale, precum Greenpeace sau Environmental Investigation Agency, joacă un rol destul de important în monitorizarea încălcărilor, realizarea de investigaţii sub acoperire şi „obligarea" autorităţilor pentru aplicarea mai riguroasă a legii. Prin cercetări independente şi campanii

de conştientizare, aceste organizaţii contribuie la aducerea în atenţia publică a dimensiunii reale a criminalităţii de mediu şi la mobilizarea opiniei publice în sprijinul măsurilor de protecţie (EIA, 2022).

În ultimii ani, au fost înregistrate şi evoluţii semnificative în ceea ce priveşte justiţia penală internaţională. Conceptul de „ecocid" – distrugerea pe scară largă a mediului – câştigă teren ca posibilă incriminare la nivelul Curţii Penale Internaţionale (CPI). Deşi, în prezent, Statutul de la Roma nu include ecocidul ca infracţiune distinctă, există iniţiative importante pentru extinderea mandatului CPI în această direcţie, recunoscând impactul devastator al crimelor ecologice asupra securităţii globale (Higgins, Short & South, 2019).

În paralel, au fost dezvoltate mecanisme inovatoare de responsabilizare a corporaţiilor implicate direct sau indirect în criminalitatea de mediu. Litigiile strategice împotriva companiilor multinaţionale, utilizarea standardelor de due diligence ecologică şi presiunile investitorilor instituţionali pentru implementarea principiilor ESG (Environmental, Social, Governance) reprezintă instrumente suplimentare în lupta împotriva criminalităţii de mediu (OECD, 2021).

Un exemplu remarcabil de cooperare internaţională reuşită este Operaţiunea Thunder, coordonată de INTERPOL şi Organizaţia Mondială a Vămilor. În perioada 2017-2021, această iniţiativă globală a dus la arestarea a mii de suspecţi şi la confiscarea unor cantităţi semnificative de animale şi plante sălbatice traficate ilegal, demonstrând că răspunsul coordonat şi susţinut poate avea un impact semnificativ asupra reţelelor criminale (INTERPOL, 2021).

Din analiza studiilor de caz prezentate reiese faptul că răspunsurile juridice şi instituţionale la criminalitatea de mediu s-au diversificat şi întărit considerabil în ultimele decenii, reflectând o conştientizare crescândă a gravităţii acestei forme de infracţionalitate. Cu toate acestea, eficienţa acestor răspunsuri depinde de factori esenţiali precum voinţa politică, capacitatea instituţională, cooperarea internaţională şi implicarea societăţii civile.

Capitolul IV: Tehnologia și știința mediului în lupta contra criminalității de mediu

În contextul intensificării criminalităţii de mediu, tehnologia şi ştiinţa mediului au devenit aliaţi indispensabili în eforturile de prevenire, detectare şi combatere a infracţiunilor ecologice. Dezvoltarea rapidă a unor instrumente inovatoare, precum imaginile satelitare, inteligenţa artificială, analiza ADN-ului pentru specii de faună şi floră, precum şi tehnicile avansate de monitorizare a poluării, a deschis

noi fronturi în lupta împotriva reţelelor criminale care ameninţă ecosistemele globale.

Una dintre cele mai eficiente aplicaţii ale tehnologiei moderne este utilizarea imaginilor din satelit pentru detectarea defrişărilor ilegale, a mineritului neautorizat şi a altor activităţi distructive. Programele precum Global Forest Watch, susţinute de World Resources Institute, folosesc date satelitare în timp real pentru a monitoriza modificările în pădurile tropicale şi pentru a alerta autorităţile asupra intervenţiilor ilegale (Hansen et al., 2013). Astfel de instrumente nu doar că permit o reacţie rapidă, dar oferă şi dovezi incontestabile în procedurile judiciare.

Inteligenţa artificială (IA) şi învăţarea automată (machine learning) aduc un alt nivel de sofisticare în analiza datelor de mediu. Algoritmi specializaţi pot procesa volume imense de informaţii, detectând modele suspecte de transport de resurse naturale sau identificând pieţele online unde sunt comercializate ilegal produse din specii protejate (Joppa, 2017). În plus, reţelele neuronale convoluţionale sunt utilizate pentru recunoaşterea automată a speciilor în pericol pe baza imaginilor capturate de camerele de supraveghere amplasate în păduri sau în zone de conservare.

O altă inovaţie majoră o reprezintă tehnologia de analiză genetică. ADN-ul ambiental (eDNA) este colectat din sol, apă sau aer şi permite identificarea speciilor prezente într-un ecosistem fără a fi necesară capturarea sau observarea directă a organismelor (Deiner et al., 2017). Această tehnică s-a dovedit esenţială în detectarea comerţului ilegal cu specii rare, dar şi în monitorizarea biodiversităţii în zone vulnerabile la intervenţii criminale.

Tehnologia blockchain este, de asemenea, explorată pentru trasabilitatea produselor naturale. Prin înregistrarea fiecărei tranzacţii într-un registru digital imuabil, blockchain-ul poate ajuta la prevenirea certificării false a lemnului, a peştelui sau a altor resurse naturale extrase ilegal (FAO, 2021). Această abordare este promiţătoare în special în sectoare unde lanţurile de aprovizionare sunt complexe şi greu de monitorizat în mod tradiţional.

În paralel, senzorii de monitorizare a calităţii aerului, apei şi solului joacă un rol important în detectarea poluării ilegale. Senzorii mobili şi reţelele de senzori conectaţi la internet (Internet of Things – IoT) pot transmite date în timp real autorităţilor de mediu, permiţând localizarea rapidă a surselor de poluare şi intervenţia eficientă (Kumar et al., 2015). Astfel, tehnologiile IoT aduc un nivel sporit de transparenţă şi capacitate de răspuns în protejarea mediului.

O altă direcție promițătoare este utilizarea dronelor pentru supravegherea zonelor izolate sau greu accesibile. Datorită costurilor relativ scăzute și a capacității lor de a furniza imagini de înaltă rezoluție, dronele sunt folosite pentru a documenta activități ilegale de tăiere a pădurilor, pescuit ilegal și extragere neautorizată de resurse (Chabot & Bird, 2015). Utilizarea dronelor combinată cu analiza IA maximizează eficiența operațiunilor de patrulare și de investigație.

Știința mediului contribuie nu doar prin instrumente tehnologice, ci și prin expertiză analitică în reconstrucția impactului infracțiunilor de mediu. Specialiștii în ecologie, hidrologie, chimie ambientală sau biologie aplicată joacă un rol central în evaluarea daunelor produse și în fundamentarea cazurilor judiciare împotriva infractorilor de mediu. Rapoartele științifice devin, astfel, probe-cheie în instanță, ajutând la cuantificarea prejudiciului și la stabilirea responsabilității juridice.

În acest sens, evaluările de impact ecologic sunt instrumente esențiale nu doar în prevenirea daunelor, dar și în documentarea intervențiilor ilegale. Prin compararea datelor istorice și actuale, experții pot identifica tendințe de degradare asociate activităților criminale și pot furniza autorităților elemente concrete pentru anchetă (Glasson et al., 2013).

Totodată, platformele de participare civică asistată de tehnologie, cum ar fi aplicațiile mobile de raportare a infracțiunilor de mediu, democratizează accesul la procesul de protecție a mediului. Cetățenii pot transmite în timp real informații despre suspiciuni de activități ilegale, contribuind astfel la extinderea capacității de supraveghere a autorităților (Wilson et al., 2019). Însă, utilizarea tehnologiei în lupta împotriva criminalității de mediu ridică și o serie de provocări. Protecția datelor personale, riscul de abuz tehnologic și costurile ridicate ale implementării unor sisteme avansate sunt doar câteva dintre obstacolele care necesită o reglementare atentă și o strategie clară. De asemenea, în regiunile cu infrastructură tehnologică precară, pot apărea decalaje semnificative în capacitatea de aplicare a noilor tehnologii.

În ciuda acestor dificultăți, potențialul tehnologiei și al științei de a transforma fundamental modul în care comunitatea globală răspunde criminalității de mediu este incontestabil. Combinația dintre progresele tehnologice, colaborarea interdisciplinară și mobilizarea civică deschide perspective promițătoare pentru un viitor în care mediul să fie protejat mai eficient și în mod sustenabil.

Capitolul V: Criminalitatea de mediu şi securitatea globală

Criminalitatea de mediu nu mai poate fi privită doar ca o problemă ecologică sau economică izolată. În ultimele decenii, aceasta a devenit o ameninţare tot mai serioasă la adresa securităţii globale, influenţând stabilitatea politică, economică şi socială a numeroase regiuni. Dimensiunea transnaţională a fenomenului, conexiunile cu reţelele de criminalitate organizată şi impactul său devastator asupra resurselor naturale esenţiale pentru supravieţuirea umană au determinat includerea infracţiunilor de mediu pe agenda actorilor internaţionali de securitate.

În primul rând, criminalitatea de mediu afectează securitatea alimentară şi resursele de apă, piloni fundamentali ai securităţii umane. Tăierile ilegale de păduri contribuie la eroziunea solului, pierderea biodiversităţii şi schimbări climatice accelerate, afectând capacitatea comunităţilor de a-şi susţine sistemele agricole (Nellemann et al., 2016). De asemenea, poluarea apelor prin deversări industriale ilegale sau traficul cu deşeuri toxice compromite accesul la apă potabilă sigură, cu efecte directe asupra sănătăţii publice şi stabilităţii socio-economice.

În al doilea rând, reţelele de criminalitate de mediu sunt adesea implicate în finanţarea altor forme de criminalitate transfrontalieră, inclusiv terorismul. În anumite regiuni, profiturile obţinute din traficul de lemn, minerale rare sau faună sălbatică sunt utilizate pentru a sprijini grupări insurgente sau paramilitare (UNEP, 2018). Astfel, există o legătură clară între degradarea mediului, perpetuarea conflictelor armate şi destabilizarea guvernanţelor locale.

Dimensiunea economică a securităţii globale este, de asemenea, afectată de criminalitatea de mediu. Estimările arată că aceasta generează anual venituri de ordinul a sute de miliarde de dolari, ceea ce o plasează printre cele mai profitabile forme de criminalitate organizată, după traficul de droguri, de persoane şi de arme (Nellemann et al., 2016). Efectele economice includ pierderi masive de venituri fiscale pentru state, deformarea pieţelor legitime şi subminarea statului de drept.

Pe lângă efectele directe, criminalitatea de mediu accentuează riscurile generate de schimbările climatice, accelerând degradarea ecosistemelor critice. Distrugerea pădurilor tropicale, poluarea marilor oceane sau degradarea terenurilor agricole reduc capacitatea planetei de a amortiza impactul fenomenelor climatice extreme, cum ar fi inundaţiile, secetele şi uraganele (IPCC, 2022). Prin urmare, criminalitatea ecologică nu doar agravează schimbările climatice, ci şi amplifică efectele lor negative asupra securităţii globale.

În plan social, degradarea mediului cauzată de activități ilegale contribuie la migrații forțate și conflicte pentru resurse. Comunitățile afectate de pierderea mijloacelor de subzistență sau de contaminarea resurselor naturale sunt adesea forțate să migreze, alimentând crize umanitare și tensiuni geopolitice (Brown, 2008). Conform rapoartelor internaționale, zonele vulnerabile, cum ar fi Africa Subsahariană sau regiunea Sahelului, sunt deosebit de expuse acestor efecte combinate ale criminalității de mediu și schimbărilor climatice.

Instituțiile internaționale de securitate au început să recunoască această amenințare complexă. Consiliul de Securitate al Națiunilor Unite a abordat în mai multe rânduri legătura dintre degradarea mediului și riscul de conflicte armate, subliniind necesitatea unor abordări integrate în politicile de securitate (UN Security Council, 2018). De asemenea, INTERPOL și Programul Națiunilor Unite pentru Mediu (UNEP) au lansat inițiative comune pentru combaterea criminalității de mediu, evidențiind importanța colaborării între agențiile de aplicare a legii, organizațiile de protecție a mediului și organismele de securitate națională.

Un exemplu de abordare integrată îl reprezintă conceptul de „securitate ecologică" (ecological security), care propune extinderea conceptului tradițional de securitate națională pentru a include protecția ecosistemelor vitale (Dalby, 2002). Această paradigmă recunoaște interdependența dintre sănătatea mediului și stabilitatea politică, economică și socială, pledând pentru politici publice care să abordeze criminalitatea de mediu ca o amenințare strategică.

În același timp, securitatea globală este vulnerabilizată de dificultățile de aplicare a legislației internaționale în domeniul protecției mediului. Lipsa unui cadru juridic global unitar pentru criminalitatea de mediu, diferențele între regimurile de reglementare naționale și resursele insuficiente ale agențiilor de aplicare a legii facilitează expansiunea rețelelor criminale (Bruch et al., 2019). Această situație subliniază necesitatea unei cooperări internaționale mai strânse și a unei armonizări a normelor juridice pentru combaterea eficientă a fenomenului.

Pe viitor, integrarea combaterii criminalității de mediu în strategiile globale de securitate devine imperativă. Abordări precum consolidarea capacităților de monitorizare și investigare, sancționarea eficientă a infracțiunilor de mediu și dezvoltarea unor parteneriate între sectoarele public, privat și societatea civilă sunt esențiale pentru protejarea securității globale. În plus, educația ecologică și sensibilizarea opiniei publice sunt factori cheie pentru crearea unei culturi a responsabilității și respectului față de mediul înconjurător.

Concluzii şi recomandări

În urma analizei impactului şi provocărilor generate de criminalitatea de mediu, este evident că această formă de criminalitate reprezintă o ameninţare majoră pentru securitatea globală. Prin activităţile sale ilegale, reţelele de criminalitate organizată contribuie la degradarea rapidă a ecosistemelor, pierderea biodiversităţii, poluarea mediului şi agravarea schimbărilor climatice. Această formă de criminalitate nu doar că subminează sănătatea publică şi economia globală, dar exacerbează şi inegalităţile sociale, afectând în mod disproporţionat comunităţile vulnerabile, care depind direct de resursele naturale pentru supravieţuire.

O concluzie fundamentală a lucrării este că problemele legate de criminalitatea de mediu nu pot fi abordate doar la nivel naţional sau regional. Dimensiunea globală a acestei activităţi ilegale necesită o coordonare multilaterală mai eficientă şi o colaborare între state, organizaţii internaţionale şi sectorul privat. Criminalitatea de mediu este, într-adevăr, o ameninţare transfrontalieră, care afectează nu doar statele de origine ale activităţilor ilegale, dar şi regiunile vulnerabile care pot deveni destinaţii pentru resursele furate sau pentru deşeurile toxice.

Mai mult, impactul acestor activităţi este profund legat de dinamica schimbărilor climatice şi de securitatea mediului, iar complexitatea acestora impune nu doar un răspuns juridic şi instituţional, ci şi un angajament din partea comunităţii internaţionale de a promova dezvoltarea durabilă.

În lumina concluziilor formulate, combaterea eficientă a criminalităţii de mediu necesită o abordare diferenţiată, adaptată nivelurilor de guvernanţă şi actorilor implicaţi. Recomandările de mai jos sunt structurate implicit în funcţie de responsabilităţile instituţionale, fără a recurge la enumerări rigide, şi urmăresc să depăşească caracterul general al documentelor programatice existente.

La nivelul statelor naţionale, se impune integrarea criminalităţii de mediu în strategiile de securitate naţională şi în politicile de combatere a criminalităţii organizate. În multe cazuri, infracţiunile de mediu continuă să fie tratate ca abateri administrative sau delicte minore, ceea ce reduce capacitatea autorităţilor de a le investiga în profunzime. Prin urmare, este necesară armonizarea legislaţiei penale interne cu standardele internaţionale, inclusiv prin incriminarea explicită a infracţiunilor grave de mediu şi prin stabilirea unor sancţiuni proporţionale cu impactul real al acestora asupra mediului, sănătăţii

publice și economiei. Totodată, consolidarea capacității instituționale a parchetelor, poliției și autorităților de mediu, inclusiv prin formare specializată, reprezintă o condiție esențială pentru aplicarea efectivă a cadrului normativ existent.

În ceea ce privește organizațiile internaționale și regionale, precum Organizația Națiunilor Unite, INTERPOL, Europol sau Uniunea Europeană, este necesară trecerea de la un rol predominant normativ și de coordonare la unul mai operațional. Aceste organisme pot juca un rol central în facilitarea schimbului de informații, în dezvoltarea unor baze de date comune privind criminalitatea de mediu și în sprijinirea investigațiilor transfrontaliere. În acest sens, consolidarea mecanismelor de cooperare judiciară internațională și sprijinirea statelor cu capacitate instituțională limitată devin priorități strategice. Criminalitatea de mediu trebuie tratată nu doar ca o problemă de protecție a mediului, ci ca o componentă a securității internaționale, comparabilă cu alte amenințări transnaționale.

Un rol din ce în ce mai important revine comunității științifice și sectorului tehnologic, în special în contextul utilizării tehnologiilor emergente. Instituțiile de cercetare, universitățile și companiile din domeniul tehnologiei pot contribui semnificativ la dezvoltarea și aplicarea unor instrumente avansate de monitorizare, precum imagistica satelitară, inteligența artificială sau sistemele de analiză a datelor de mediu. Pentru a maximiza eficiența acestor soluții, este necesară o colaborare instituționalizată între cercetători, autorități publice și agenții de aplicare a legii, astfel încât datele științifice să fie integrate direct în procesele decizionale și operaționale.

În același timp, sectorul privat, în special companiile implicate în exploatarea resurselor naturale, transport, comerț internațional și managementul deșeurilor, trebuie să fie considerat un actor-cheie în prevenirea criminalității de mediu. Adoptarea unor mecanisme riguroase de due diligence, trasabilitate a lanțurilor de aprovizionare și raportare transparentă nu ar trebui să rămână doar la nivel voluntar, ci să fie încurajată și, acolo unde este necesar, reglementată. Implicarea sectorului privat este esențială pentru reducerea cererii de produse provenite din activități ilegale și pentru limitarea oportunităților economice exploatate de rețelele criminale.

La nivelul comunităților locale și al societății civile, recomandările vizează consolidarea educației de mediu și a participării publice. Comunitățile afectate direct de criminalitatea de mediu sunt adesea cele mai vulnerabile și, totodată, cele mai expuse riscului de a fi cooptate în

activităţi ilegale. Prin urmare, politicile publice trebuie să includă programe de educaţie, conştientizare şi dezvoltare alternativă, care să ofere populaţiei locale opţiuni economice sustenabile şi să reducă dependenţa de exploatarea ilegală a resurselor naturale.

Într-o perspectivă mai largă, se recomandă promovarea unui model integrat de dezvoltare durabilă, în care politicile de protecţie a mediului, combaterea criminalităţii organizate şi strategiile de securitate climatică să fie corelate. Criminalitatea de mediu nu poate fi separată de problemele structurale legate de sărăcie, guvernanţă deficitară şi schimbări climatice. Prin urmare, răspunsul la acest fenomen trebuie să depăşească logica reactivă şi să fie orientat spre prevenţie, rezilienţă şi sustenabilitate pe termen lung.

Această lucrare a subliniat complexitatea şi interdependenţa dintre criminalitatea de mediu şi securitatea globală. Prin urmare, este evident că o abordare integrată, care îmbină intervenţii juridice, tehnologice, economice şi educaţionale, este necesară pentru a combate cu succes această formă de criminalitate. Numai printr-o colaborare globală susţinută şi un angajament ferm al tuturor actorilor implicaţi se va putea asigura un viitor durabil pentru ecosistemele lumii şi pentru securitatea globală.

Bibliografie

1. Basel Convention. (2022). Text of the Basel Convention. https://www.basel.int/TheConvention/Overview/TextoftheConvention/tabid/1275/Default.aspx

2. Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

3. Brisman, A., & South, N. (2020). Green Criminology: Crime, Justice, and the Environment. Routledge.

4. Brown, O. (2008). Migration and Climate Change. International Organization for Migration (IOM). https://publications.iom.int/books/migration-and-climate-change

5. Bruch, C., Muffett, C., & Nichols, S. S. (2019). Governance, natural resources, and post-conflict peacebuilding. Routledge.

6. Chabot, D., & Bird, D. M. (2015). Wildlife research and management methods in the 21st century: Where do unmanned aircraft fit in? Journal of Unmanned Vehicle Systems, 3(4), 137–155. https://doi.org/10.1139/juvs-2015-0021

7. CITES. (2023). What is CITES? Retrieved from https://cites.org/eng/disc/what.php

8. Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

9. Dalby, S. (2002). Environmental Security. University of Minnesota Press.

10. Deiner, K., Bik, H. M., Mächler, E., Seymour, M., Lacoursière-Roussel, A., Altermatt, F., ... & Bernatchez, L. (2017). Environmental DNA metabarcoding: Transforming how we survey animal and plant communities. Molecular Ecology, 26(21), 5872–5895. https://doi.org/10.1111/mec.14350

11. Environmental Investigation Agency (EIA). (2022). About us. https://eia-international.org/about-us/

12. Environmental Protection Agency (EPA). (2022). Enforcement and Compliance History Online. https://echo.epa.gov/

13. Environmental Investigation Agency. (2019). Tainted Timber, Tarnished Temples: How the Illegal Timber Trade Funds Human Rights Abuses and Threatens Myanmar's Forests. https://eia-international.org

14. European Parliament. (2008). Directive 2008/99/EC on the protection of the environment through criminal law. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0099

15. FAO. (2021). Blockchain for Sustainable Supply Chains. https://www.fao.org/3/cb4373en/cb4373en.pdf

16. Food and Agriculture Organization of the United Nations (FAO). (2022). State of the World's Forests 2022: Forest pathways for green recovery and building inclusive, resilient and sustainable economies. FAO. https://doi.org/10.4060/cb9360en

17. Glasson, J., Therivel, R., & Chadwick, A. (2013). Introduction to Environmental Impact Assessment. Routledge.

18. Hansen, M. C., Potapov, P. V., Moore, R., Hancher, M., Turubanova, S., Tyukavina, A., ... & Townshend, J. R. (2013). High-resolution global maps of 21st-century forest cover change. Science, 342(6160), 850-853. https://doi.org/10.1126/science.1244693

19. Hansen, M. C., Potapov, P. V., Moore, R., Hancher, M., Turubanova, S., Tyukavina, A., ... & Townshend, J. R. (2013). High-resolution global maps of 21st-century forest cover change. Science, 342(6160), 850–853. https://doi.org/10.1126/science.1244693

20. Higgins, P., Short, D., & South, N. (2019). Protecting the planet: A proposal for a law of ecocide. Crime, Law and Social Change, 70(3), 251–266. https://doi.org/10.1007/s10611-018-9786-3

21. Intergovernmental Panel on Climate Change (IPCC). (2022). Sixth Assessment Report: Impacts, Adaptation, and Vulnerability. https://www.ipcc.ch/report/ar6/wg2/

22. INTERPOL. (2021). Global operation targets environmental crime. https://www.interpol.int/en/News-and-Events/News/2021/Global-operation-targets-environmental-crime

23. Interpol & United Nations Environment Programme (UNEP). (2016). The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security. UNEP. https://www.unep.org/resources/report/rise-environmental-crime

24. INTERPOL & UNEP. (2016). Strategic Report: Environment, Peace and Security – A Convergence of Threats. https://www.interpol.int/

25. Joppa, L. N. (2017). AI for Earth. Nature, 550(7675), 325–327. https://doi.org/10.1038/550325a

26. Kaimowitz, D. (2015). Forests and Governance: Lessons from Decentralization. Earthscan.

27. Kumar, P., Morawska, L., Martani, C., Biskos, G., Neophytou, M., Di Sabatino, S., ... & Britter, R. (2015). The rise of low-cost sensing for managing air pollution in cities. Environment International, 75, 199–205. https://doi.org/10.1016/j.envint.2014.11.019

28. Nellemann, C., Henriksen, R., Raxter, P., Ash, N., & Mrema, E. (2016). The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security. United Nations Environment Programme and INTERPOL.

29. Nellemann, C., Henriksen, R., Raxter, P., Ash, N., & Mrema, E. (Eds.). (2016). The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security. United Nations Environment Programme (UNEP) and RHIPTO Rapid Response–Norwegian Center for Global Analyses.

30. Nellemann, C., Henriksen, R., Raxter, P., Ash, N., & Mrema, E. (Eds.). (2016). The Environmental Crime Crisis: Threats to Sustainable Development from Illegal Exploitation and Trade in Wildlife and Forest Resources. United Nations Environment Programme.

31. Nellemann, C., Henriksen, R., Raxter, P., Ash, N., & Mrema, E. (Eds.). (2016). The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security. UNEP-INTERPOL Rapid Response Assessment.

32. Organisation for Economic Co-operation and Development (OECD). (2021). Due Diligence Guidance for Responsible Business Conduct. https://www.oecd.org/corporate/mne/due-diligence-guidance-for-responsible-business-conduct.htm

33. Robinson, E. J. Z., Kumar, A. M., & Albers, H. J. (2021). The economics of environmental crime: Applying economic models of crime to illegal logging and other environmental offences. Ecological Economics, 180, 106870. https://doi.org/10.1016/j.ecolecon.2020.106870

34. United Nations Office on Drugs and Crime (UNODC). (2020). World Wildlife Crime Report 2020: Trafficking in Protected Species. https://www.unodc.org/

35. United Nations Environment Programme. (2018). Waste Crime – Waste Risks: Gaps in Meeting the Global Waste Challenge. https://www.unep.org

36. United Nations Office on Drugs and Crime. (2020). World Wildlife Crime Report 2020: Trafficking in Protected Species. https://www.unodc.org

37. United Nations Office on Drugs and Crime (UNODC). (2020). World Wildlife Crime Report 2020: Trafficking in Protected Species. UNODC. https://www.unodc.org/unodc/en/data-and-analysis/wildlife.html

38. United Nations Environment Programme (UNEP). (2018). Environmental Rule of Law: First Global Report. https://www.unep.org/resources/report/environmental-rule-law-first-global-report

39. United Nations Environment Programme (UNEP). (2018). Environment, Peace and Security: A Convergence of Threats. https://www.unep.org/resources/report/environment-peace-and-security

40. UN Security Council. (2018). Report of the Secretary-General on the Protection of Civilians in Armed Conflict. Retrieved from https://undocs.org/S/2018/462

41. White, R. (2013). Environmental Harm: An Eco-Justice Perspective. Policy Press.

42. Wilson, K. A., Auerbach, N. A., Sam, K., Magini, A. G., Moss, A. S. L., Langhans, S. D., ... & Possingham, H. P. (2019). Conservation research is not happening where it is most needed. PLOS Biology, 17(3), e3000324. https://doi.org/10.1371/journal.pbio.3000324

43. World Wildlife Fund (WWF). (2020). Living Planet Report 2020: Bending the curve of biodiversity loss. WWF. https://livingplanet.panda.org/en-us/

44. Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). SAGE Publications.

CÂND ATACATORII DEVIN VICTIME: VULNERABILITĂȚILE GRUPĂRILOR DE CRIMINALITATE CIBERNETICĂ

Claudia-Alecsandra GABRIAN*

Abstract:

Ransomware groups represent a category of the cybercriminal landscape, they operate anonymously, through aliases and underground channels, but since 2022, when the war between Russia and Ukraine started, the cybercriminal ecosystem has seen some changes. Information leaks have shown that although these groups seem unstoppable, on the contrary, they are vulnerable and make mistakes. This article highlights vulnerabilities of cybercrime groups, based on the leak of internal data from two notable ransomware groups: Conti and Black Basta. The primary scope is to analyze how the leaks occurred, what they reveal about the internal operations of cybercriminal activities, and why such intelligence is highly valuable for cybersecurity research.

Conti was the first ransomware group that supported Russia in the context of the invasion in Ukraine, the leaks in 2022 revealed internal discussions, strategies, financial transactions, aliases, organizational structure, etc. After this major event, in 2025, another ransomware group was involved in a leak, Black Basta, that was highly active in this field since Conti shut down its activity. The leaks exposed critical operational details, names, chats, victims, transactions, etc. This article is relevant in this field because it represents a key topic about cybercrime vulnerabilities.

Conti and Black Basta leaks represent the two most important information leakage events within groups, and justify that cybercrime groups are also susceptible to the same exploits they exploit in others. The leaks offer valuable information and a unique opportunity to analyze cybercrime from the inside, their recruitment, and even internal conflicts. Knowing the weaknesses of cybercrime groups represents a significant way to understand how they think and organize their attacks.

Cuvinte-cheie: CONTI, BlackBasta, Telegram, leaks, cyber-attacks, ransomware

Introducere

Grupările de criminalitate cibernetică sunt considerate ca fiind foarte bine organizate, extrem de sofisticate şi de cele mai multe ori membrii grupărilor nu comit greşeli care să conducă la identificarea acestora. Pseudonimele şi tiparul pe care le folosesc sunt singurele care

* Universitatea Babeş-Bolyai, Facultatea de Istorie şi Filosofie, Departamentul de Studii Internaţionale şi Istorie Contemporană, Cluj-Napoca, claudia.gabrian@ubbcluj.ro.

pot să fie asociate cu o operaţiune specifică. În mediul de criminalitate cibernetică numărul grupărilor de ransomware active în prezent este de peste 60 de grupări, dintre care 16 au apărut după data de 1 ianuarie 2025 (Rapid7, 2025). Acest număr este foarte relevant, deoarece tendința de apariție a acestor tipuri de grupări este în continuă creștere. Mediul de ameninţări cibernetice devine unul foarte volatil şi complex, astfel, creşterea semnificativă poate fi atribuită şi faptului că există grupări care se rebranduiesc, în special după acţiuni de aplicare a legii împotriva acestora.

O tendinţă care este mai vizibilă din anul 2022 este aceea potrivit căreia unii dintre cei mai relevanţi actori de pe scena ameninţărilor cibernetice devin, la rândul lor, victime ale unor breşe de securitate, chiar probabil trădări interne, expuneri neintenţionate, sau chiar obişnuinţă, iar situaţia celor două grupări, Conti şi Black Basta confirmă acest paradox. Dacă se au în vedere scurgeri masive de date interne, conflicte între membrii sau erori operaţionale, aceste grupări de criminalitate cibernetică demonstrează faptul că nimeni nu este imun în faţa vulnerabilităţilor cibernetice, fie ele de natură umană sau tehnică, nici măcar cei care le exploatează zi de zi.

Scopul acestui articol este de analizare a modului în care publicarea informaţiilor din interiorul grupărilor poate să reprezinte un pas important în identificarea membrilor unei grupări. De asemenea, articolul îşi propune şi analizarea relevanţei pe care aceste scurgeri le au în domeniul cercetării ecosistemului de criminalitate cibernetică, prin înțelegerea dinamicii şi a fragilităţii acestor grupări. În cadrul cercetării se vor analiza documente interne şi discuţii între membrii grupării, rolul acestora fiind de a observa activitatea membrilor din aceste grupări de ransomware. Chat-uri interne ale grupărilor Conti şi Black Basta au fost postate pe X (fostul Twitter în 2022) şi pe canalul de Telegram (în 2025) şi pe Dark Web. Au fost utilizate aceste surse pentru a se înțelege mai bine modul de acţiune al acestor grupări, strategiile interne şi chiar posibilitatea asocierii unor nume adevărate cu aceste alias-uri şi parteneriate dintre aceste grupări şi servicii de informaţii din Rusia.

Prezenta cercetare investighează vulnerabilităţile interne ale grupărilor de criminalitate cibernetică, adresând un hiatus în literatura de specialitate prin valorificarea datelor provenite din scurgerile de informaţii din interiorul Conti şi Black Basta. Analiza acestor două incidente, considerate repere fundamentale în peisajul ameninţărilor actuale, fundamentează o nouă metodă de explorare a vulnerabilităţilor acestora, fiind cele mai relevante expuneri de informaţii care au fost

publicate vreodată. Analiza scurgerilor de date evidenţiază un proces critic de destabilizare operaţională şi structurală. În cazul Conti, fragmentarea a fost accelerată de disensiunile geopolitice interne, iar în cazul Black Basta, incidentul a fost precedat de încălcarea unui protocol intern de non-agresiune.

Metodologia utilizată în această cercetare este una calitativă, fiind bazată pe metoda netnografiei şi strategia studiului de caz. Prin metoda netnografiei s-au analizat scurgerile de informaţii publicate pe Telegram @ExploitWhispers; X (ex-Twitter) @ContiLeaks, cât şi interacţiunile online ale membrilor acestor grupări prin canale private, cum ar fi Matrix. Complementar, strategia studiului de caz a facilitat investigarea aprofundată şi contextualizată a grupărilor Conti şi Black Basta, corelându-se datele empirice cu dinamica lor organizaţională specifică. Prin aceste două metode, s-au identificat tipare comportamentale şi vulnerabilităţi structurale recurente.

Întrebarea de cercetare: În ce mod contribuie informaţiile provenite din breşele interne la procesul de deanonimizare a membrilor şi la înţelegerea structurii organizaţionale a grupărilor Conti şi Black Basta?

Rezultate

Criminalitatea cibernetică este un termen general care descrie multitudinea de activităţi infracţionale desfăşurate utilizând un computer, o reţea sau un alt set de dispozitive digitale. Există o gamă largă de activităţi ilegale pe care infractorii cibernetici le comit, dintre care se numără şi atacul de tip ransomware, printre multe altele. Criminalitatea cibernetică nu cunoaşte limite fizice, poate să ia multe forme şi evoluează încontinuu. Acest tip de ameninţare afectează atât persoanele fizice, companii şi entităţi guvernamentale, ceea ce poate duce la pierderi financiare semnificative. Activitatea lor se întinde pe diverse platforme şi tehnologii digitale, iar atacul de tip ransomware este un tip de malware care criptează datele critice ale victimelor, cerând o răscumpărare. Dacă această plată este făcută, victimele primesc o cheie de decriptare pentru a recupera accesul. Din punct de vedere financiar, atacurile ransomware duc la pierderi de date şi active. Există multe cazuri de ransomware care au avut succes, cele mai afectate sectoare sunt cele sănătate, educaţie, energie, transporturi etc. (ProofPoint, 2024).

Gruparea Conti

Gruparea Conti a fost una dintre cele mai sofisticate, agresive și eficiente operațiuni ransomware, vizând multe companii importante și organizații guvernamentale. Conti a apărut pentru prima dată la sfârșitul anului 2019, devenind una dintre operațiunile predominante de *ransomware-as-a-service* (RaaS). În urma analizării mai multor rapoarte despre această grupare, se sugerează o legătură cu un alt ransomware, cunoscut sub numele Ryuk, care era condus de un grup rusesc de criminalitate cibernetică cunoscut sub numele de Wizard Spider (CSO, 2022).

Conti deși opera ca un ransomware obișnuit, ceea ce îl diferenția de multe alte tipuri de ransomware era viteza sa de criptare, tehnicile avansate și utilizarea unui model de dublă extorcare, în care atacatorii nu numai că criptau fișierele, dar furau și datele sensibile, amenințându-i cu expunerea lor dacă nu se plătea răscumpărarea. În urma analizării discuțiilor dintre membrii, chiar dacă acea răscumpărare era plătită, ei nu asigurau integritatea datelor și nepublicarea lor online. Conti făcea parte din tendința crescândă a *ransomware-as-a-Service* (RaaS), care permitea afiliaților cu mai puțină expertiză tehnică să achiziționeze pachete de atac și să lanseze atacuri ransomware. Conti oferea acces la instrumentele și infrastructura lor în schimbul unei părți din plățile de răscumpărare. Acest model amplifica semnificativ numărul de atacuri efectuate de Conti, deoarece reducea barierele de acces pentru potențialii atacatori (Cyberly).

Motivul alegerii acestei grupări se datorează faptului că este prima grupare ransomware care a susținut invazia Rusiei în Ucraina. Aceasta și-a anunțat sprijinul deplin pentru guvernul rus și a amenințat cu atacuri cibernetice asupra infrastructurii critice a oricărei țări care va ataca Rusia. Astfel, în urma susținerii invaziei, au fost postate zeci de mii de mesaje, de către un cercetător în domeniul securității informatice care a avut acces la baza de date, oferind informații despre modul în care era condusă operațiunea, numele asociat membrilor, discuțiile cu victimele etc. După acest eveniment, membrii grupării au continuat să se implice în activități ilegale sub alte denumiri, cum ar fi o nouă operațiune ransomware numită Black Basta, care a reprezentat și continuarea activității acestora. Ca urmare, în 19 mai 2022, infrastructura Conti, inclusiv site-ul său oficial, au fost închise (CSO, 2022).

Gruparea Black Basta

Black Basta cunoscută pentru operațiunea de tip *ransomware-as-a-Service* (RaaS), a apărut în aprilie 2022 și este descendentul Conti și

Revil. A câştigat rapid notorietate pentru proliferarea sa rapidă, vizând peste 500 de organizaţii la nivel global în diverse sectoare de infrastructură critică, inclusiv în domeniul sănătăţii. Black Basta folosea un model de dublă extorcare, iar tacticile grupului vizau utilizarea instrumentelor legitime în scopuri rău intenţionate. Potenţialele legături cu Conti, au transformat gruparea într-o ameninţare semnificativă şi persistentă (TheSecMaster, 2025).

Apariţia acestei grupări a coincis cu declinul Conti, deşi o descendenţă directă nu a fost dovedită definitiv, poate fi posibil un rebranding sau o divizare a grupului. Mai mulţi factori sugerează o legătură puternică, cum ar fi asemănarea codului, multe dintre tacticile, tehnicile şi procedurile (TTP) ale Black Basta se aliniază cu cele utilizate de Conti, inclusiv dubla extorcare, direcţionarea unor industrii specifice şi utilizarea anumitor instrumente. Recrutarea de persoane din interior prin intermediul forumurilor de hacking (Exploit, XSS) relevă faptul că Black Basta îşi promova serviciile pe pieţele subterane ale criminalităţii cibernetice, indicând o operaţiune profesionistă care căuta mereu afiliaţi (TheSecMaster, 2025).

Originile exacte ale grupării sunt neclare, dar există mai multe indicii care relevă faptul că aceasta opera din Rusia sau din altă ţară din Europa de Est. Notele de răscumpărare şi alte comunicări ale grupării sunt în limba rusă sau conţin fragmente din limba rusă. O altă legătură relevantă, atât Conti, cât şi Black Basta folosesc bursa de criptomonede rusească Garantex pentru a spăla răscumpărările (Barracuda, 2024). Potrivit unei analize detaliate realizate de SentinelOne, operatorii Black Basta descurajează în mod activ atacurile asupra ţărilor din Comunitatea Statelor Independente (CSI), sau ţări prietene, care include majoritatea statelor din fosta URSS. Această practică este comună în rândul grupurilor de ransomware cu legături ruseşti, care evită să atace ţinte locale pentru a nu atrage atenţia autorităţilor (SentinelOne).

Chiar dacă s-a menţinut ca una dintre cele mai importante grupări de ransomware din ecosistemul de criminalitate cibernetică, scurgerea de informaţii din 11 februarie 2025 a expus vulnerabilitatea grupării, cât şi mecanismele interne, oferind o perspectivă concretă asupra tacticilor lor, la fel ca şi în cazul informaţiilor postate despre gruparea Conti (Kela, 2025). Colecţia de jurnale de chat interne utilizate de operatorii şi membrii Black Basta au fost cele mai relevante informaţii postate. Scurgerile conţineau aproximativ 200.000 de mesaje datate între 18 septembrie 2023 şi 28 septembrie 2024 (SRM, 2025).

Conti leaks

Informațiile din interiorul Conti au apărut pentru prima dată pe contul de Twitter numit „ContiLeaks" în data de 27 februarie 2022. Datele conţineau peste 60.000 de chat-uri interne de pe serverul privat de chat XMPP criptat şi Jabber, care se întind pe parcursul mai multor ani. Cel care a publicat informaţiile este de origine ucraineană, iar în urma analizei acestora, se identifică următoarele: structuri salariale, activităţi zilnice, structura grupului, adrese Bitcoin, fotografii ale serverelor de stocare şi un fişier ZIP protejat prin parolă care conţinea codul sursă pentru criptorul, decriptorul şi constructorul ransomware-ului Conti (Heimdal, 2024). Această divulgare de informaţii este considerată un eveniment notabil, în urma căreia se poate realiza o analiză concretă a operaţiunilor din interiorul unei grupări şi reprezintă un pas major prin care se poate atribui şi identifica membrii grupării (Trellix, 2022).

Jurnale Jabber postate sunt chat-uri individuale între fiecare doi membri. Prima parte conţine mesaje din 21 iunie 2020 până în 16 noiembrie 2020, în timp ce a doua parte conţine arhive din 29 ianuarie 2021 până în 27 februarie 2022, cu unele lacune. Scurgerea a inclus informaţii de la 6 servere Rocket.Chat diferite din perioada 31 august 2020 - 26 februarie 2022. În acest articol, s-au analizat conversaţiile membrilor extrase din jurnalele Jabber şi a folosit parţial conţinutul jurnalelor Rocket.Chat pentru a corobora constatările. La început, Jabber a fost folosit pentru mai multe tipuri de conversaţii, inclusiv atacuri continue. Spre 2021, majoritatea conversaţiilor tehnice (inclusiv piratarea anumitor companii, sarcini de codare etc.) au fost mutate pe Rocket.Chat (KELA, 2022).

În urma analizei chat-urilor interne în limba rusă, se identifică faptul că această grupare este organizată ca şi o companie obişnuită, având departamente pentru toate categoriile şi personal specializat (resurse umane, testeri, analişti OSINT, programatori, echipă de training, negociatori etc.). Aceştia îşi primesc salariul regulat în zilele de 15 şi 30 ale fiecărei luni, iar programul de lucru este între 10:00 şi 18:00, ora Moscovei, cinci zile pe săptămână (Trellix, 2022).

S-a identificat organigrama grupării, sunt 28 de membri, având toţi aliasuri: *Stern* este şeful principal, împreună cu *Tramp*. *Hof, Hors, Bentley, Starfall şi Zevs* sunt administratori de sistem, *Max* este developer Trickbot (botnet- platformă de distribuţie ransomware), *Revers* este hacker şi manager, *Swift şi Dollar* sunt hackeri şi *Reshaev* este hacker de top. *Professor, Bio şi Pumba* se ocupă de negocierile pentru plată răscumpărărilor din partea companiilor. *Buza* este developer şi

teamleader/cercetător OSINT, *Skippy* se ocupă de resursele umane şi de partea legală, *Many, Pin, Paranoik* şi *Cybergangster* lucrează la cryptolocker, decriptează datele pentru victime. *Salamandra*, *Kagas, Viper, Elvira şi Ford* se ocupă doar de partea de resurse umane, *Jaime* este developer şi *Mango* este manager tehnic (FORESCOUT, 2022).

Informaţiile regăsite în chat-urile interne ne ajută să identificăm mai multe tipare şi metode de activitate, astfel: *Stern* este şeful care supraveghează totul şi are 100 de persoane pe statul de plată. *Salmon* care este recrutor, afirmă faptul că weekend-urile şi vacanţele trebuie să fie respectate. *Bentley* care este manager, a lucrat acolo timp de un an, dar compania există de peste 10 ani. Există posibilele conexiuni guvernamentale potrivit lui *Angelo* care este tester/coder, *Stern* (un alt membru) este strâns afiliat cu FSB sau alte structuri şi lucrează pentru „Pu". Este important de menţionat faptul că *Basil* care este tester/coder a fost întrebat dacă este de la FSB, acesta a răspuns ulterior că are informaţii serioase legate de activitatea de la frontiera ucraineană. Această declaraţie a fost făcută cu şapte zile înainte de incursiunea Rusiei în Ucraina, ceea ce poate să sugereze faptul că gruparea are o relaţie apropiată cu guvernul rus şi/sau acţionează în interesul acestuia (Trellix, 2022). Unii membri ai grupului stăteau într-un birou din Rusia, pe baza conversaţiilor lor legate de comandarea mâncării şi întâlnirile într-un cadru real (KELA, 2022).

Printre alte departamente, Conti avea o echipă de apelanţi, un apelant trebuia să aibă cunoştinţe solide de limba engleză vorbită (nivel B2-C1) şi să aibă vârsta cuprinsă între 18 şi 25 de ani. Aceştia erau recrutaţi de echipa de resurse umane a Conti pentru a lucra de la distanţă pentru „un magazin online" în străinătate. Apelanţii câştigau mai mult în funcţie de succesul unui apel, programul de lucru era între 18:00-2:00, ora Moscovei (corespunzând programului obişnuit de lucru din emisfera occidentală) şi primeau concediu plătit, dar nu aveau încheiat niciun contract oficial conform Codului Muncii (Trellix, 2022).

Black Basta leaks

Scurgerile de informaţii Black Basta au avut loc pe 11 februarie 2025 şi au oferit o perspectivă profundă, nu doar asupra conflictelor interne ale grupului, ci şi asupra mecanismelor utilizate. S-a identificat faptul că există o tendinţă semnificativă care a fost verificată prin aceste jurnale de chat, aceea potrivit căreia grupările de ransomware reinvestesc răscumpărările plătite pentru a achiziţiona vulnerabilităţi zero-day (Rapid 7, 2025). O tehnică de atac zero-day este o eroare de

securitate pentru care furnizorul sistemului afectat nu a pus încă la dispoziția utilizatorilor afectați un patch pentru a remedia eroarea apărută (CSO, 2021).

Un administrator numit @ExploitWhispers al unui grup Telegram nou creat, „Шепот Басты" (Basta's Whisper) a distribuit conversațiile interne Matrix ale Black Basta, conținând peste 200.000 de mesaje. Administratorul a declarat că motivația din spatele scurgerii de informații a fost decizia unor membrii Black Basta de a „trece linia" atacând băncile ruseşti, o mişcare considerată inacceptabilă de către cel care a divulgat informațiile. Datele scurse au acoperit o perioadă cuprinsă între 18 septembrie 2023 și 28 septembrie 2024, în cadrul cărora au fost identificate informații sensibile, oferind o privire de ansamblu asupra funcționării interne Black Basta. Conținutul includea acreditări compromise, adrese IP, discuții operaționale interne, date despre victime, documente juridice, informații de plată, adrese de criptomonede și detalii despre infrastructura tehnică (KELA, 2025).

Deşi nu au fost identificate atacuri asupra băncilor ruseşti, identitatea și intenția lui @ExploitWhispers rămân neclare; ar putea fi un afiliat nemulțumit, un cercetător în domeniul securității sau un concurent al Black Basta RaaS. Potrivit lui @ExploitWhispers, liderul Black Basta, *GG, alias AA*, este un individ rus pe nume *Oleg Nefedov*. Pe baza cercetărilor din domeniul informațiilor open-source (OSINT), există un articol armean în care O. Nefedov a fost căutat de forțele de ordine din SUA și a fost reținut la Erevan pe 21.06.2024 și a scăpat în mod misterios de instanța armeană la două zile după arestarea sa (CIVILNET, 2024).

Prezentare generală a membrilor cheie și a dinamicii din cadrul BlackBasta este următoarea: *GG* (alias *Tramp)* este liderul de grup, *Lapa* este administrator cheie, *Cortes* este fost afiliat grupului Qakbot, *YY* este un alt administrator cheie al BlackBasta, *Bio* este un fost membru al lui Conti, iar când a lucrat cu Conti, Bio și-a schimbat porecla din „bio" în „pumba", dar de atunci a revenit la numele său original la BlackBasta. O altă descoperire relevantă are în vedere faptul că au fost identificate 533 de adrese IP din Rusia pentru atacurile lansate(FIRST, 2025). *Tinker* este implicat în acțiuni spam/vishing, este posibil să fi fost afiliat anterior și cu Conti. *Nickolas* este colaborator apropiat al lui *GG* în chat-ul „*talks.icu*". *N3auxaxl* este dezvoltator la distanță, posibil subordonat lui *YY*. *Ugway* este denumirea pentru operatori tehnici implicați în mai multe aspecte ale operațiunii, de la implementarea atacurilor, obținerea de acreditări, programe malware etc. (eSentire, 2025).

Cele mai relevante pasaje extrase din discuții arată că *GG* nu a trimis niciun mesaj între 20 iunie 2024 și 3 iulie 2024. Când *GG* și-a reluat

activitatea în chatul Matrix, a avut o conversaţie lungă cu un membru numit *Chuck*, discutând circumstanţele arestării sale, unde prietenii săi ruşi de la nivelul numărul 1 în stat au zburat imediat pentru a-l elibera. *Chuck* a întrebat dacă numărul 1 este „vvp" (potenţial V.V. Putin), însă nu a primit nicio confirmare sau infirmare. În plus, *Chuck* a menţionat o recompensă de 10 milioane de dolari pentru informaţii despre „tr" (posibil „-amp"), referindu-se posibil la recompensa americană pentru cinci membri cheie ai bandei Conti, inclusiv hackerul *Tramp*. În chat, *GG* a fost într-adevăr identificat drept *Tramp* (liderul Conti) prin „biografie" (cunoscut şi sub numele de „*pumba*", un alt membru Conti) (Trellix, 2025).

Mai mult, în timp ce discutau despre durata implicării lor în activităţi ilicite, *GG* şi *Chuck* au declarat că vor continua atât timp cât „bunicul" va trăi şi vor lucra până la încheierea Operaţiunii Militare Speciale (SMO), făcând referire la invazia Rusiei în Ucraina. Nu este clar la cine se referă „bunicul", însă ar putea fi o referire la o persoană de rang înalt care oferă protecţie liderilor Black Basta. *Chuck* a exprimat că SMO va dura o perioadă extinsă (Trellix, 2025). O altă descoperire este faptul că Black Basta utilizează ChatGPT pentru o varietate de scopuri, inclusiv compunerea de scrisori formale frauduloase în engleză, parafrazarea textului, rescrierea programelor malware şi colectarea datelor despre victime (Trellix, 2025).

Comunicarea ulterioară dintre *GG* şi *Chuck* se referă la un membru al grupului Conti/Trickbot, Fedor Andreev, care are Red Notice pe site-ul Interpolului. *GG* afirmă faptul că *Bentley*, unul dintre liderii Conti/ Trickbot, care este din Rusia, se presupune că lucrează pentru FSB. Din cauza unui atac legat de Black Basta RaaS, „biroul" îl căuta pe *GG*, acesta a răspuns întrebând „ce birou - FSB, FSO sau departamentul K?" (FSB: Serviciul Federal de Securitate, FSO: Serviciul Federal de Protecţie, Departamentul K: Departamentul Federal de Afaceri Interne care se ocupă de IT/criminalitate cibernetică). *Tinker* a dezvăluit că biroul era FSB. *GG* sub denumirea de "*usernamegg*" are două birouri în Moscova, unde îşi aveau sediul dezvoltatori şi operatori de programe malware (Trellix, 2025).

În urma analizării discuţiilor publicate online, au fost identificate următoarele elemente fundamentale referitoare la activitatea şi profilul operaţional al persoanei identificate sub pseudonimul *GG* (corelat cu identitatea lui *Tramp*, liderul grupării Conti). Primul element vizează beneficierea de o imunitate extrateritorială şi patronaj politic de nivel înalt, dedusă din capacitatea de a obţine un "coridor verde" pentru eliberarea sa rapidă în urma unei reţineri şi din referirile constante la protecţia oferită de figuri politice centrale. Al doilea element evidenţiază

alinierea ideologică și strategică la interesele geopolitice ale Federației Ruse, manifestată prin asumarea continuării operațiunilor până la finalizarea Operațiunii Militare Speciale și prin evitarea sistematică a vizării țărilor prietene. Al treilea element relavă o simbioză între structurile infracționale și agențiile de securitate statale (FSB, FSO), confirmată de prezența unor membri care activează dual sau sub supraveghere directă a "biroului".

Al patrulea element indică o instituționalizare fizică și logistică de tip corporativ, prin menținerea unor sedii administrative în Moscova, utilizarea unui personal auxiliar pentru securitatea transporturilor și implementarea unor protocoale stricte de acces și control ierarhic. Al cincilea element subliniază vulnerabilitatea strategică în fața contramăsurilor interne, reflectată prin eforturile de editare a mesajelor publice (de la pro-Rusia la pace) pentru a atenua represaliile internaționale. Toate aceste activități indică faptul că membrii grupării operează într-un cadru de criminalitate cibernetică hibridă, unde granița dintre infracționalitatea pură și obiectivele de securitate națională este deliberat ambiguizată (Interl417, 2025). Ca o evaluare, acest grad avansat de profesionalizare și protecție politică transformă gruparea dintr-un simplu actor de tip ransomware, într-o entitate de relevanță strategică, a cărei destabilizare este condiționată mai degrabă de dinamica politică internă a statului gazdă, decât de intervențiile tehnice ale agențiilor de securitate externe.

Interpretări

Analiza scurgerilor de informații despre chat-urile Conti și Black Basta a relevat potențiale conexiuni cu autoritățile ruse și colaborări cu alte operațiuni ransomware și malware. Chat-urile au arătat faptul că atât Black Basta, cât și Conti pot să fie localizate în Moscova, iar revizuirea scurgerilor de informații despre chat-urile Black Basta a demonstrat faptul că operațiunile nu s-au schimbat fundamental față de cele ale Conti. Conti și Black Basta au funcționat ca o companie bine organizată, cu mai multe locații fizice în Rusia, menținând diferite echipe de apelanți, negociatori, criptografi, coderi și spammeri. Aceste grupări au acționat sub convingerea că autoritățile ruse îi vor proteja de repercusiuni.

S-a observat faptul că unii afiliații Conti s-au alăturat Black Basta, astfel și legăturile au fost reconfigurate în noua grupare. De fiecare dată când are loc un rebranding pentru grupările ransomware, membrii se regrupează, învață din greșeli, dezvoltă instrumente inovatoare mai sofisticate (uneori datorită inteligenței artificiale) și continuă sub un

nume nou, atâta timp cât afacerea RaaS generează câştiguri financiare şi nu repetă ceea ce au făcut în trecut.

Chiar dacă operaţiunile grupării Conti au fost închise în 2022, continuarea activităţii infracţionale sub egida Black Basta este documentată prin analiza recentelor scurgeri de date, unde reiese faptul că le-a continuat. Acest caz relevă un proces extins de reflecţie internă asupra vulnerabilităţilor Conti, iar dezbaterile membrilor Black Basta privind infrastructura, reţelele de conexiuni şi instrumentele moştenite de la Conti, fundamentează ipoteza că noua entitate funcţionează ca un produs al evoluţiei organice a ecosistemului *ransomware-as-a-service* (RaaS). Aceste elemente relevă faptul că succesul operaţional al grupării este condiţionat de capacitatea de a asimila şi rectifica erorile strategice ale Conti, transformând informaţiile provenite din breşele interne, într-un potenţial spre reconfigurare structurală.

Analiza sugerează o constrângere majoră, abandonarea completă a paradigmelor operaţionale anterioare şi lansarea unui proiect RaaS complet autonom, rămân obiective dificil de atins, având în vedere că rădăcinile Black Basta sunt intrinsec legate de componentele tehnice ale grupării Conti. În secţiunea de interpretare, această dependenţă de parcurs, demonstrează faptul că grupările de criminalitate cibernetică nu pot opera o ruptură totală de propriul trecut organizaţional, fiind forţate să îşi reconstruiască reziliența pe aceeaşi arhitectură de bază, ceea ce menţine active direcţiile pentru cercetări viitoare.

O altă similaritate face referire la faptul că deşi infractorii cibernetici sunt motivaţi financiar şi au un istoric de colaborare transfrontalieră, adesea evitând implicarea în mediul politic, actualul conflict Rusia-Ucraina este menţionat în ambele chat-uri ale grupărilor şi nu trebuie să fie ignorat, mai ales faptul că în ambele grupări, membrii acestora menţionează faptul că au cunoştinţe de rang înalt din FSB. Deşi aceste afirmaţii nu au fost verificate independent, stabilirea unei legături directe între liderul unui grup ransomware şi serviciile secrete ruseşti ar fi o descoperire semnificativă. Statul rus oferă o impunitate controlată, atâta timp cât grupările nu vizează ţinte din interiorul Rusiei sau al CSI şi sunt dispuse să colaboreze cu serviciile de informaţii FSB, SVR la cerere, autorităţile în aceste condiţii pot ignora activitatea lor infracţională externă (DarkCovenant, 2023).

Cu toate acestea, presupusele legături ale liderului Black Basta cu serviciile secrete ruseşti ar putea sugera o relaţie mai profundă între grupările de ransomware şi serviciile de securitate ale statului, ridicând îngrijorări legate de securitatea naţională: în ce măsură a existat o colaborare între statul rus şi grupările Conti şi Black Basta? Aceasta

se justifică prin eliberarea lui *GG* din închisoare cu ajutor rusesc şi a discuţiilor purtate cu membrul *Chuck*, cât şi prin menţionarea instituţiilor de informaţii din Rusia şi legăturile dintre membrii grupărilor cu aceste instituţii. Întrebarea este relevantă, având în vedere istoricul grupării de a viza în mod explicit numeroase organizaţii de infrastructură critică din Europa. Conti şi Black Basta leaks au fost un rezultat direct al acestui conflict, deoarece au susţinut invazia Rusiei în Ucraina. Se poate concretiza o vulnerabilitate internă majoră, aceea potrivit căreia resursa umană reprezintă factorul care a declanşat închiderea definitivă a acestor două grupări.

Asemănările dintre Conti şi Black Basta sunt legate şi de faptul că ambele grupări au fost considerate printre cele mai sofisticate în perioada lor de ascensiune. Membrii păreau a fi veterani experimentaţi în ransomware şi criminalitate cibernetică, vorbitori de limbă rusă, scenariul demantelării operaţiunilor fiind aproape improbabil, chiar la doi ani diferenţă între ele.

Una dintre cele mai relevante informaţii regăsite, este legată de liderul grupării Black Basta, care este un cetăţean rus pe nume Oleg Evgenievich Nefedov, care a fost regăsit în cadrul grupării Conti, fiind asociat cu mai multe aliasuri *Tramp*, *Trump*, *GG* şi *AA*. Astfel, indică implicarea sa în grupări predecesoare majore, cum ar fi Conti. Deşi formarea de noi grupări este comună, iar cele deja închise apar adesea sub nume noi, aceste informaţii oferă dovezi suplimentare ale unor astfel de practici şi subliniază importanţa monitorizării comportamentelor afiliate în cadrul grupărilor ransomware.

Conexiunile între statul rus şi grupările de criminalitate cibernetică nu sunt neobişnuite, deoarece serviciile de informaţii ruseşti şi grupările de infractori cibernetici menţin în mod tradiţional relaţii de cooperare, primele bazându-se pe sprijin operaţional în cadrul unui acord *quid pro quo*: actorii clandestini îşi pot continua activitatea fără repercusiuni atâta timp cât cooperează cu statul. Fundamentul acestor relaţii este constrângerea infractorilor cibernetici să plătească bani în schimbul protecţiei, să participe la operaţiuni cibernetice organizate de stat, cum ar fi spionajul prin APT-uri sau furtul de date şi să susţină naraţiunile statului prin campanii hacktiviste sau de dezinformare.

Concluzii

Ransomware-ul reprezintă o ameninţare la adresa tuturor instituţiilor şi companiilor, iar Conti şi Black Basta reprezintă exemplele relevante pentru a justifica importanţa lor în ecosistemul de criminalitate

cibernetică. Grupările de ransomware sunt în continuă evoluţie, mai ales prin utilizarea inteligenţei artificiale, iar publicarea informaţiilor interne în cele două cazuri menţionate relevă importanţa studierii metodelor de atac şi a mentalităţii pe care aceşti atacatori o au. Utilizarea unui model de extorcare dublă, viteza de criptare şi tacticile sofisticate creează o variantă deosebit de periculoasă de ransomware.

Analiza datelor exfiltrate permite nu doar identificarea şi arestarea actorilor cheie din aceste grupări, ci şi clarificarea implicaţiilor şi motivaţiilor geopolitice. Sprijinul instituţional rus a ghidat activitatea acestor grupări pe parcursul ultimilor patru ani. Deşi succesiunea operativă de la Conti la Black Basta s-a încheiat formal la începutul anului 2025, riscul sistemic rămâne ridicat. Disoluţia unor astfel de organizaţii proliferează în realitate cu instabilitate, prin migrarea membrilor specializaţi către structuri emergente sau chiar prin reconfigurarea lor sub noi identităţi digitale.

Modelul RaaS, tacticile de dublă extorcare, adoptarea rapidă a noilor tehnici şi utilizarea instrumentelor legitime în scopuri rău intenţionate pot să reprezinte un punct de plecare în analizarea unei viitoare grupări de ransomware care va apărea sau care chiar a apărut în primăvara anului 2025, după închiderea activităţii Black Basta, conducând la identificarea unei noi organizări a membrilor Black Basta, ex-Conti. De asemenea, este important de urmărit dacă vor apărea alte scurgeri de informaţii care să ajute la identificarea membrilor grupării sau chiar să se analizeze modul în care aceştia vor fi mai precauţi cu membrii pe care îi acceptă.

Prin coroborarea datelor extrase din jurnalele de comunicaţii ale grupărilor Conti şi Black Basta, prezenta cercetare şi-a atins obiectivul fundamental, demonstrând faptul că publicarea informaţiilor din interiorul reţelelor de tip ransomware constituie un instrument critic în identificarea arhitecturii lor. Analiza a relevat faptul că aceste scurgeri de date nu sunt simple fragmente informaţionale, ci resurse strategice care permit cercetătorilor să cartografieze un ecosistem marcat de o fragilitate structurală surprinzătoare.

Răspunsul la întrebarea de cercetare indică faptul că breşele interne contribuie la procesul de deanonimizare şi înţelegere organizaţională prin trei mecanisme esenţiale: identificarea corelaţiilor dintre alias-uri (cum este cazul identificării lui *Tramp* ca lider central în ambele entităţi); expunerea fluxurilor financiare şi relevarea unei ierarhii de tip corporativ care mimează structurile comerciale legitime. Validarea empirică a acestor date confirmă faptul că înţelegerea structurii interne şi a motivaţiilor actorilor cheie oferă o perspectivă

unică asupra riscurilor hibride cu care se confruntă instituţiile de apărare şi securitate naţională.

Cercetarea demonstrează că operaţiunile acestor grupări nu sunt motivate exclusiv de profitul financiar, ci sunt profund influenţate de dinamica interpersonală complexă, presiunile politice externe şi simbioza cu serviciile de informaţii ale statului gazdă. Scurgerile de informaţii au permis creionarea unei organigrame detaliate, evidenţiind o specializare riguroasă a activităţii lor.

Lucrarea demonstrează că deşi grupări precum Conti şi Black Basta au părut invulnerabile în mediul digital, ele au funcţionat ca entităţi administrative cu vulnerabilităţi umane şi structurale majore, a căror transgresare a anonimatului prin breşe interne reprezintă cel mai eficient punct de acces pentru strategiile proactive de apărare şi deanonimizare a criminalităţii cibernetice organizate.

Direcţiile viitoare de cercetare se pot concentra pe investigaţii ştiinţifice aprofundate privind impactul acestor scurgeri de informaţii, asupra modului în care pot ajuta forţele de ordine să identifice persoanele care au stat în spatele atacurilor. În plan secund, este imperativă monitorizarea sistemică a ecosistemului infracţional, cât şi dinamica de reconfigurare a reţelelor emergente, analizând modul în care noile grupări de tip ransomware-as-a-service (RaaS) asimilează lecţiile învăţate din eşecurile Conti şi Black Basta pentru a-şi fortifica securitatea operaţională.

Contribuţia originală a prezentei lucrări rezidă în abordarea analitică a unui domeniu marcat de un deficit de date primare, propunând o perspectivă directă asupra dinamicii interne şi a interacţiunilor complexe din cadrul ecosistemelor de criminalitate cibernetică. Dezvoltarea unui cadru interpretativ a permis corelarea rezultatelor empirice cu identificarea vulnerabilităţilor structurale specifice grupărilor Conti şi Black Basta.

Bibliografie

1. Barracuda. 2024. „Black Basta's nasty tactics: Attack, assist, attack". Accesat în data de 04.04.2025, https://blog.barracuda.com/2024/05/18/black-basta-nasty-tactics

2. BlueVoyant. 2022. "Report CONTI Leaks 2022". Accesat în data de 04.04.2025, https://www.spirityenterprise.com/_files/ugd/f107e9_14108ba1522c4144b78f6672a598ebde.pdf?index=true

3. CIVILNET. 2024. „Ինչպես ԱՄՆ-ի կողմից հետախուզվող ՌԴ քաղաքացին փախավ Հայաստանի դատարանից". Accesat în data de 26.04.2025, https://www.civilnet.am/news/800556/%D5%AB%D5%B6%D5%B9%D5%BA%D5%A5%D5%BD-%D5%A1%D5%B4%D5%B6-%D5%AB-%D5%AF%D5%B8%D5%B2%D5%B4%D5%AB%D6%81-%D5%B0%D5%A5%D5%BF%D5%A1%D5%AD%D5%B8%D6%82%D5%A6%D5%BE%D5%B8%D5%B2-%D5%BC%D5%A4-%D6%84%D5%A1%D5%B2%D5%A1%D6%84%D5%A1%D6%81%D5%AB%D5%B6-%D6%83%D5%A1%D5%AD%D5%A1%D5%BE-%D5%B0%D5%A1%D5%B5%D5%A1%D5%BD%D5%BF%D5%A1%D5%B6%D5%AB-%D5%A4%D5%A1%D5%BF%D5%A1%D6%80%D5%A1%D5%B6%D5%AB%D6%81/

4. CSO. 2020. „TrickBot explained: A multi-purpose crimeware tool that haunted businesses for years". Accesat în data de 13.04.2025, https://www.csoonline.com/article/570169/trickbot-explained-a-multi-purpose-crimeware-tool-that-haunted-businesses-for-years.html

5. CSO. 2021. „Zero days explained: How unknown vulnerabilities become gateways for attackers". Accesat în data de 26.04.2025, https://www.csoonline.com/article/565704/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html

6. CSO. 2022. „Conti ransomware explained: What you need to know about this aggressive criminal group". Accesat în data de 26.03.2025, https://www.csoonline.com/article/571503/conti-ransomware-explained-and-why-its-one-of-the-most-aggressive-criminal-groups.html

7. Cyberly. „What is Conti ransomware, and how does it work?". Accesat în data de 26.03.2025, https://www.cyberly.org/en/what-is-conti-ransomware-and-how-does-it-work/index.html

8. Dark Covenant. 2023. "Connections Between the Russian State and Criminal Actors". Accesat în data de 29.01.2025, https://www.recordedfuture.com/research/russian-state-connections-criminal-actors

9. EMSISOFT. 2025. „The State of Ransomware in Q1 2025". Accesat în data de 25.03.2025, https://www.emsisoft.com/en/blog/46626/the-state-of-ransomware-in-q1-2025/?utm_source=chatgpt.com

10. ESentire. 2025. „Initial Takeaways from the Black Basta Chat Leaks". Accesat în data de 28.04.2025, https://www.esentire.com/blog/initial-takeaways-from-the-black-basta-chat-leaks

11. Firts. 2025. „Black Basta Ransomware Leak: Key Findings and Insights". Accesat în data de 28.04.2025, https://www.first.org/blog/20250321-black-basta-ransomware-leak

12. Flare. 2025. "Deciphering Black Basta's Infrastructure from the Chat Leak". Accesat în data de 23.03.2025, https://flare.io/learn/resources/blog/deciphering-black-bastas-infrastructure-from-the-chat-leak/

13. FORESCOUT. 2022. „Analysis of Conti Leaks".Accesat în data de 11.04.2025, https://www.forescout.com/resources/analysis-of-conti-leaks/

14. Heimdal. 2024. „All about Conti Ransomware. From $180 Million Yearly Revenue to Internal Data Leakage". Accesat în data de 09.04.2025, https://heimdalsecurity.com/blog/what-is-conti-ransomware/

15. Intel471. 2025. „An in-depth look at Black Basta's TTPs". Accesat în data de 23.03.2025, https://intel471.com/blog/an-in-depth-look-at-black-bastas-ttps

16. Intel471. 2025. „Black Basta exposed: A look at a cybercrime data leaks". Accesat în data de 27.04.2025, https://intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak

17. Kela. 2022. „Analysis of leaked Conti's Internal Data".Accesat în data de 11.04.2025, https://www.kelacyber.com/wp-content/uploads/2022/03/KELA-Intelligence-Report-ContiLeaks-1.pdf

18. Kela. 2025. „Inside the Black Basta Leak: How Ransomware Operators Gain Access". Accesat în data de 07.04.2025, https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%20Black%20Basta%20Leak_%20How%20Ransomware%20Operators%20Gain%20Access.pdf

19. PRODAFT. 2022. „CONTI Ransomware Group: In-depth Analysis". Accesat în data de 07.04.2025, https://resources.prodaft.com/conti-ransomware-group-report

20. ProofPoint, 2024, "Cyber Crime". Accesat în data de 29.01.2025, https://www.proofpoint.com/uk/threat-reference/cyber-crime

21. Qntinue. "Inside BlackBasta: What Leaked Conversations Reveal About Their Ransomware Operations". Accesat în data de 23.03.2025, https://www.ontinue.com/resource/inside-black-basta-leaked-coversations/

22. Rapid7. 2025. „2025 Ransomware: Business as Usual, Business is Booming". Accesat în data de 24.03.2025, https://www.rapid7.com/blog/post/2025/04/08/2025-ransomware-business-as-usual-business-is-booming/?utm_source=chatgpt.com

23. SentinelOne. „Black Basta". Accesat în data de 05.04.2025, https://www.sentinelone.com/anthology/black-basta/

24. SRM. 2025. „Cyber briefing note | The Black Basta leaks". Accesat în data de 08.04.2025, https://www.s-rminform.com/latest-thinking/the-blackbasta-leaks-cyber-briefing-note

25. TheSecMaster. 2025. „Black Basta Ransomware". Accesat în data de 30.03.2025, https://thesecmaster.com/blog/black-basta-ransomware

26. Trellix. 2022. „Conti Leaks: Examining the Panama Papers of Ransomware". Accesat în data de 10.04.2025, https://www.trellix.com/blogs/research/conti-leaks-examining-the-panama-papers-of-ransomware/

27. Trellix. 2025. „Analysis of Black Basta Ransomware Chat Leaks". Accesat în data de 27.04.2025, https://www.trellix.com/blogs/research/analysis-of-black-basta-ransomware-chat-leaks/

28. TrendMicro. 2022. „Black Basta". Accesat în data de 23.03.2025, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

NOUA ORDINE MONDIALĂ ÎN CONTEXTUL DIFUZIEI PUTERII – ÎNTRE IERARHIE ŞI DEZORDINE

Octavian-Alexandru-Ştefan BROŞTEANU*

Abstract:

The concept of global order has long constituted a central analytical framework within the field of international relations, traditionally grounded in realist assumptions emphasizing hierarchy, power maximization, and competition within an anarchic international system. During the Cold War and the subsequent unipolar moment, global politics was structured around the existence of a dominant hegemon, which provided relative stability and predictability. However, contemporary international dynamics are increasingly shaped by the diffusion of power, both among states and between state and non-state actors, challenging the classical understanding of hierarchical global order.

This article examines the structural implications of power diffusion for the configuration and functioning of the international system. It argues that the redistribution of power away from traditional centers toward emerging states and non-state actors erodes the foundations of hegemonic stability and contributes to the emergence of a more fragmented, fluid, and complex global order. The analysis is structured around two main dimensions: first, the transformation of state power, with a focus on the declining hegemonic capacity of the United States of America and the systemic constraints faced by emerging powers such as China, India, Russia, and the European Union; second, the expanding influence of non-state actors, including multinational corporations, non-governmental organizations, cyber-activists, terrorist networks, and private military companies.

By integrating these dimensions into a broader analytical framework, the article explores the evolving paradigms of polarity shaping contemporary international relations, assessing whether the emerging order can be best described as unipolar, multipolar, non-polar, or hybrid. Ultimately, it contends that the diffusion of power does not necessarily lead to systemic chaos, but rather to a reconfiguration of authority, governance, and cooperation mechanisms, wherein interdependence and transnational challenges increasingly condition global stability.

Keywords: *global order, power diffusion, polarity, hegemony, non-state actors, international system*

* Student doctorand în domeniul Ştiinţe Politice/Relaţii Internaţionale, în cadrul Şcolii Naţionale de Studii Politice şi Administrative din Bucureşti, absolvent al programului de master – „*Managementul Informațiilor de Securitate Națională*", promoţia 2023, din cadrul Academiei Naţionale de Informaţii „Mihai Viteazul" din Bucureşti, e-mail octavian.brosteanu@gmail.com.

Introducere

Problematica ordinii mondiale a constituit dintotdeauna un punct central de interes pentru teoreticienii şi practicienii din domeniul relaţiilor internaţionale, având la bază perspectiva realistă conform căreia statele se comportă asemenea indivizilor – într-o manieră egoistă, dominantă, cu scopul maximizării puterii, într-un mediu internaţional anarhic.

De-a lungul deceniilor trecute, s-a remarcat tendinţa constantă de clasificare a puterii fiecărui actor internaţional, pentru a identifica cine poate avea mai multă influenţă pe scena internaţională, dat fiind atât intervalul temporal corespondent Războiului Rece sau epocii ulterioare acestuia, în care sistemul internaţional a cunoscut un hegemon – Statele Unite ale Americii (SUA).

Cu toate acestea, începutul secolului al XXI-lea a adus transformări structurale profunde, care au subminat premisele stabilităţii unipolare. Globalizarea accelerată, revoluţia tehnologică, extinderea interdependenţelor economice şi apariţia unor noi centre de putere au contribuit la difuzia capacităţilor materiale şi simbolice în cadrul sistemului internaţional. Totodată, ascensiunea actorilor non-statali, de la corporaţii multinaţionale şi organizaţii neguvernamentale până la reţele transnaţionale de hackeri, grupări insurgente şi entităţi teroriste, a diminuat monopolul statului asupra exercitării puterii şi a controlului asupra spaţiilor politice, economice şi informaţionale.

În acest context, devine din ce în ce mai dificilă menţinerea unei perspective strict ierarhice asupra ordinii mondiale. Distribuţia puterii este caracterizată astăzi printr-un grad ridicat de fragmentare, mobilitate şi volatilitate, iar capacitatea actorilor tradiţionali de a impune reguli şi norme la scară globală este limitată de competiţia emergentă şi de constrângerile generate de interdependenţa complexă. În locul unei structuri piramidale, se conturează un sistem policentric, în care multiple niveluri de autoritate coexistă şi interacţionează într-un mod dinamic şi adesea imprevizibil.

Conceptul de „nouă ordine mondială”, deşi frecvent utilizat în discursul politic şi mediatic, este adesea marcat de ambiguitate semantică şi de conotaţii ideologice sau conspiraţioniste. Din perspectivă academică, trebuie înţeles ca un proces continuu de reconfigurare a relaţiilor de putere, a normelor şi a instituţiilor care structurează interacţiunile internaţionale. În acest sens, modificările generate de procesul difuziei puterii la nivel global conduc spre o redefinire profundă a acestui concept, apropiindu-ne, poate, de o formă a *dezordinii mondiale* – termen ce poartă o încărcătură negativă, însă nu întotdeauna justificată.

Astfel, în cadrul acestui articol am analizat impactul procesului de difuzie a puterii asupra structurii şi funcţionării sistemului internaţional contemporan, scopul fiind explicarea manierei în care difuzia puterii va afecta conceptul de ordine mondială. Demersul se axează pe două dimensiuni principale: transformările survenite în cadrul actorilor statali, respectiv ascensiunea şi consolidarea influenţei actorilor non-statali. În prima parte, sunt examinate limitele hegemoniei americane şi constrângerile structurale care împiedică statele emergente – în special China, India, Federaţia Rusă şi Uniunea Europeană – să preia un rol dominant la nivel global. În a doua parte, este analizată contribuţia unor actori non-statali relevanţi la remodelarea dinamicii globale, cu accent pe rolul corporaţiilor multinaţionale, organizaţiilor neguvernamentale, reţelelor cibernetice şi entităţilor paramilitare.

Rezultatele cercetării vor fi evidenţiate sub forma capitolului privind modalitatea în care ar putea arăta noua ordine mondială, în care voi dezvolta aspecte privind paradigma/paradigmele de polaritate în care ne vom afla – unipolar, multipolar, non-polar sau toate în acelaşi timp.

Viitorul sistemului internaţional din perspectiva actorilor statali

Aşa cum am evidenţiat anterior, transformările structurale ale ordinii mondiale contemporane sunt determinate de un proces complex de redistribuire a puterii, caracterizat prin erodarea avantajelor tradiţionale ale statelor occidentale şi ascensiunea relativă a actorilor emergenţi. În literatura de specialitate, acest fenomen este conceptualizat drept *difuzia puterii*, fiind corelat cu globalizarea, interdependenţa economică, revoluţia tehnologică şi democratizarea accesului la resurse strategice (Nye, 2012; Naím, 2015; Ikenberry, 2018).

Spre deosebire de tranziţiile hegemonice clasice, analizate în paradigma realistă prin prisma conflictului inevitabil dintre puterea dominantă şi challengerul emergent (Gilpin, 1981), redistribuirea actuală a puterii nu conduce automat la apariţia unui nou hegemon. Dimpotrivă, acumularea de resurse economice şi militare de către statele emergente este însoţită de constrângeri structurale, instituţionale şi geopolitice care limitează capacitatea acestora de a exercita o dominaţie sistemică durabilă.

În acest sens, ordinea internaţională contemporană tinde către o egalizare relativă a puterii, mai degrabă decât către o substituire clară a

hegemonului. Barry Buzan (2012) a susținut în cadrul unui discurs la TEDx Talks că sistemul internațional se îndreaptă către o configurație în care nu vor mai exista superputeri în sensul clasic al termenului, ci doar mari puteri cu influență regională și capacitate limitată de proiecție globală. Această perspectivă este confirmată și de raportul *Global Trends 2040* al comunității de intelligence americane, care anticipează o lume mai contestată, caracterizată prin competiție intensă, fragmentare și polarizare multipolară (National Intelligence Council, 2021).

Printre cauzele acestor transformări le putem identifica pe cele evidențiate de Moises Naim:

- revoluția cantității – mai mulți oameni, mai multe state, mai multe probleme;
- revoluția mobilității – oamenii pot călători mai mult, se emancipează și aduc în țările de origine idei, credințe, valori noi;
- revoluția mentalităților – schimbarea atitudinilor populației, în special a tinerilor, care contestă puterea și pun la îndoială autoritatea statelor (Naim, 2015).

În prezent, SUA reprezintă principalul pol de putere la nivel global, beneficiind de avantaje structurale semnificative în plan economic, militar, tehnologic și normativ. Cu un produs intern brut de aproximativ 27 de trilioane de dolari și un PIB pe cap de locuitor de peste 80.000 USD, SUA rămân cea mai performantă economie a lumii (World Bank, 2023). Din perspectivă militară, bugetul american de apărare depășește 900 de miliarde de dolari anual, situându-se net peste cel al următorilor competitori strategici, în special China și Rusia.

În pofida acestor avantaje, capacitatea SUA de a menține o hegemonie globală incontestabilă este tot mai limitată. Joseph Nye (2012) subliniază faptul că puterea contemporană nu mai poate fi evaluată exclusiv prin prisma resurselor materiale, ci trebuie analizată într-un cadru multidimensional, care include legitimitatea, capacitatea de coaliționare, influența normativă și atractivitatea culturală. În acest context, hegemonia americană se confruntă cu multiple constrângeri.

În plan intern, polarizarea politică accentuată, disfuncționalitățile instituționale și blocajele legislative afectează capacitatea administrațiilor succesive de a formula și implementa politici externe coerente și predictibile. De exemplu, sistemul politic învechit, bazat pe o constituție din secolul al XVIII-lea poate reprezenta o problemă, întrucât se întâmplă de multe ori să nu existe coeziune între deciziile președintelui și cele ale legislativului, care pot crea blocaje în luarea deciziilor, în special a celor urgente.

În plan socio-economic, fenomene precum dezindustrializarea, externalizarea producţiei şi adâncirea inegalităţilor sociale au erodat coeziunea internă şi au contribuit la diminuarea legitimităţii globale a modelului american. Datorită dezindustrializării şi a externalizării producţiei, în vederea maximizării profitului, către Asia de Est, în special către China, a consolidat poziţia acesteia în lanţurile globale de aprovizionare, diminuând avantajele competitive ale SUA şi ale aliaţilor occidentali (Baldwin, 2016).

Mai mult, există o serie de semnale actuale care relevă tendinţa leadershipului american de a-şi exercita puterea globală mai puţin *împreună cu alţii*, ci mai *mult asupra altora*, ceea ce va putea determina ca inclusiv statele aliate să se reorienteze către alţi parteneri. O altă tendinţă este relevată de redimensionarea doctrinei Monroe privind izolarea Americii din relaţiile internaţionale, iar adoptarea unei astfel de măsuri va putea determina sfârşitul influenţei SUA la nivel global, datorită faptului că principalul interes de securitate va avea în vedere protejarea teritoriului său naţional şi a proximităţii acestuia, ci mai puţin menţinerea unei dominaţii globale

Aceste constrângeri explică de ce supremaţia americană tinde să se transforme dintr-o hegemonie incontestabilă într-o primus inter pares, caracterizată prin leadership condiţionat şi capacitate limitată de impunere unilaterală. Astfel, deşi SUA vor rămâne, cel mai probabil, cel mai influent actor global în următoarele decenii, ele nu vor mai putea exercita un control sistemic deplin asupra ordinii internaţionale.

În plus, simpla dezvoltare economică, socială, politică şi militară a statelor care până în urmă cu câteva decenii nu reprezentau importanţă în afacerile globale vor determina ca SUA să piardă, cel puţin numeric, din *paritatea puterii* la nivel global, câştigată abia după sfârşitul Războiului Rece. De exemplu, dacă în anul 2000, SUA genera aproximativ 50% din cheltuielile militare de la nivel global (Nye, 2012), la nivelul anului 2023, deşi bugetul de apărare a continuat să crească, ponderea acestuia se situa la 37%.

Astfel, Barry Buzan, în acelaşi discurs evidenţiat anterior, aprecia că, deşi SUA îşi va păstra în următoarele decenii anumite avantaje pe care niciun alt stat sau alianţă nu le va putea egala, cum ar fi dezvoltarea tehnologiei de vârf sau puterea militară, America nu va mai fi un hegemon în relaţiile internaţionale, periferia globală urmând să recupereze o parte din decalaj până la o „nouă revoluţie industrială" (Buzan, 2012).

În mod automat, tendinţa de sorginte realistă ne determină să identificăm un viitor hegemon, care va domina competiţia sistemică în viitor. Mulţi tind să accentueze efectele transferului de putere şi să considere că între SUA şi China se va produce un transfer hegemonic, China urmând a deveni ţara care va domina lumea.

Într-adevăr, dezvoltarea Chinei reprezintă, fără îndoială, cea mai semnificativă transformare structurală a sistemului internaţional din ultimele decenii. Ritmul accelerat de dezvoltare economică, modernizarea capacităţilor militare şi expansiunea influenţei diplomatice au determinat numeroşi analişti să considere că asistăm la o tranziţie hegemonică inevitabilă, în cadrul căreia SUA vor fi înlocuite de China ca principal centru de putere globală (Mearsheimer, 2014; Allison, 2017). Cu toate acestea, o analiză sistemică aprofundată indică faptul că, în pofida progreselor remarcabile, China se confruntă cu o serie de constrângeri structurale, demografice, geopolitice şi instituţionale care îi limitează capacitatea de a exercita o hegemonie globală durabilă.

Din perspectivă economică, China a înregistrat una dintre cele mai spectaculoase traiectorii de creştere din istoria modernă. Între 1995 şi 2020, produsul intern brut al Chinei s-a multiplicat de peste zece ori, transformând statul asiatic în a doua economie a lumii şi principalul manufacturier global (World Bank, 2023). În pofida acestei dinamici impresionante, ritmul de creştere economică a cunoscut o decelerare semnificativă în ultimul deceniu, atingând un plafon structural determinat de maturizarea economiei, creşterea costurilor cu forţa de muncă şi reducerea avantajelor comparative tradiţionale (Eichengreen, 2018).

Mai mult, modelul de dezvoltare chinez rămâne profund dependent de investiţii publice masive, exporturi şi control statal e xtins, generând dezechilibre macroeconomice persistente, precum supraîndatorarea sectorului imobiliar, alocarea ineficientă a capitalului şi vulnerabilităţi sistemice în sectorul financiar (Lardy, 2019). Aceste disfuncţionalităţi structurale limitează capacitatea Chinei de a susţine pe termen lung un ritm de creştere suficient de ridicat pentru a rivaliza cu economia americană în termeni de inovaţie, productivitate şi dezvoltare tehnologică.

Din punct de vedere demografic, China se confruntă cu o tranziţie accelerată către o societate îmbătrânită, ca rezultat direct al politicii copilului unic şi al urbanizării rapide. Scăderea ratei fertilităţii şi reducerea populaţiei active exercită presiuni semnificative asupra sustenabilităţii creşterii economice şi asupra sistemelor de protecţie socială (United Nations, 2022). În acest sens, se consideră că ţara

va îmbătrâni înainte de a se îmbogăţi, ceea ce îi limitează potenţialul de acumulare a puterii materiale comparabil cu cel al Statelor Unite (Eberstadt, 2019).

Trebuie precizat şi că doar 10 din 31 de provincii au un venit mediu peste media naţională, respectiv că statul este pe locul doi în lume în ceea ce priveşte numărul de miliardari, aceştia însă devenind mai bogaţi „pe seama celor mai săraci din ţară" (McGregor, 2012).

Cu toate acestea, unul dintre principalele avantaje ale Chinei în lupta pentru dominaţia globală este populaţia – aproximativ 1.4 miliarde de oameni, ceea ce o clasează pe locul 1 în lume, la egalitate cu India, ţara beneficiind inclusiv de resurse naturale care o vor ajuta în consolidarea poziţiei de cea mai mare manufactură din lume. Puternica industrializare a Chinei a dovedit că întreaga *lume liberă* ar putea depinde de acest stat în asigurarea propriilor bunuri de consum, ceea ce ar spori influenţa statului în afacerile globale.

Din perspectivă militară, modernizarea forţelor armate chineze reprezintă un element central al strategiei naţionale de securitate. Bugetul apărării a crescut constant în ultimele două decenii, atingând aproximativ 300 de miliarde de dolari în 2023, ceea ce plasează China pe locul al doilea la nivel global (SIPRI, 2023). Cu toate acestea, diferenţa faţă de SUA rămâne semnificativă nu doar din punct de vedere cantitativ, ci şi calitativ. Capacitatea SUA de proiecţie globală a forţei, experienţa operaţională acumulată, reţeaua extinsă de alianţe şi superioritatea tehnologică în domenii-cheie precum inteligenţa artificială, aviaţia militară şi sistemele de comandă şi control conferă Washingtonului un avantaj strategic substanţial (Nye, 2015; Freedman, 2019).

Cu toate acestea, unul dintre cele mai mari dezavantaje care va face imposibilă proiectarea puterii Chinei la nivel mondial, cel puţin în cazul evitării capcanei lui Tucidide şi a menţinerii climatului relativ de pace, este poziţionarea sa geografică. Spre deosebire de SUA, care beneficiază de o poziţie geografică privilegiată şi de vecinătăţi stabile, China este înconjurată de o serie de state cu care întreţine relaţii tensionate sau conflicte latente: India, Japonia, Coreea de Sud, Vietnam şi Taiwan. Aceste rivalităţi regionale limitează capacitatea Beijingului de a-şi construi o sferă de influenţă coerentă şi stabilă, sporind costurile strategice ale ascensiunii sale. De asemenea, cu fosta Uniune a Republicilor Socialiste şi Sovietice (URSS) a avut diverse momente de conflict, existând chiar o potenţială tendinţă prin care China şi-ar putea dori în viitor să acapareze Siberia de la Federaţia Rusă.

Disputa privind statutul Taiwanului reprezintă, în acest context, principalul potențial declanșator al unui conflict sistemic major. Deși China revendică suveranitatea asupra insulei, sprijinul oferit Taiwanului de SUA și aliații săi transformă această problemă într-un punct semnificativ al competiției strategice globale. O eventuală escaladare militară în regiune ar genera costuri economice și politice enorme pentru Beijing, afectând sever legitimitatea și stabilitatea internă a regimului (Allison, 2017; Shambaugh, 2020).

În plus, la situația în cauză se adaugă și problemele interne, precum regimul autoritar, monitorizarea permanentă a populației și înlăturarea oricărei forme de opoziție la adresa guvernului care, coroborat cu influența stilului de viață sud-coreean sau japonez, respectiv cu cea a diasporei chineze din statele occidentale, ar putea duce în viitor la noi revolte pentru democratizare.

Prin urmare, deși China va continua să reprezinte principalul challenger strategic al Statelor Unite și va juca un rol esențial în configurarea ordinii internaționale, constrângerile economice, demografice, geopolitice și instituționale fac improbabilă transformarea sa într-un hegemon global comparabil cu SUA. Ascensiunea Chinei contribuie astfel mai degrabă la fragmentarea și pluralizarea centrelor de putere decât la instaurarea unei noi ordini unipolare.

Totuși, am putea aprecia că statul chinez își poate maximiza șansele de a obține hegemonia globală prin realizarea unei alianțe cu India, prin renunțarea la diferendele din prezent și realizarea de investiții în industrie/infrastructură etc., pentru a o transforma într-o *a doua China*, dacă va controla resursele naturale ale Rusiei și dacă și-ar putea atrage drept aliați, mizând pe valorile culturii asiatice comune, pe Coreea de Sud și Japonia. În acest caz, jumătate din populația planetei se va afla sub autoritatea Beijingului, iar China își va putea dezvolta orice ramură economică, și totuși va depinde de o altă mare amenințare la adresa securității globale: schimbările climatice.

De asemenea, există o tendință conform căreia India va depăși PIB-ul Chinei în următoarele decenii și va deveni cel mai important stat în sistemul internațional. Într-adevăr, India este văzută de mai mulți ani drept o „superputere prematură" (Nye, 2012) și beneficiază în termeni de putere relativă de o populație extrem de numeroasă, este o forță nucleară, având o armată clasată în primele 5 din lume, dezvoltă programe spațiale, au o importantă resursă de ingineri în IT, iar din perspectiva soft power, cultura indiană se poziționează printre cele mai atractive la nivel mondial, atât pentru gânditori, filozofi, cât și pentru marea masă a oamenilor.

Din perspectivă economică, deşi India a cunoscut o creştere susţinută în ultimele două decenii, nivelul dezvoltării rămâne relativ scăzut în raport cu marile economii globale. PIB-ul pe cap de locuitor, situat în jurul valorii de 2.500 USD, reflectă persistenţa sărăciei şi a inegalităţilor sociale, precum şi deficienţele sistemului educaţional şi infrastructural (World Bank, 2023). Rata analfabetismului, estimată la aproximativ 25%, şi performanţele modeste ale universităţilor indiene în clasamentele internaţionale limitează formarea capitalului uman necesar pentru susţinerea unei economii bazate pe inovare (Nye, 2015; UNDP, 2022).

În plan social, fragmentarea etnică, religioasă şi lingvistică a societăţii indiene generează tensiuni interne persistente, care afectează coeziunea naţională şi stabilitatea politică. Sistemul castelor, disparităţile regionale şi conflictele intercomunitare constituie factori structurali de vulnerabilitate, reducând capacitatea statului de a mobiliza resursele necesare pentru proiecţia puterii la nivel global (Varshney, 2014).

În plus, din perspectivă externă, India are probleme nerezolvate cu China, amintite anterior, dar şi cu Pakistan, un alt stat emergent, disputa fiind tot pentru trasarea graniţei comune, în provinciile Kashmir şi Jammu. De asemenea, în ciuda faptului că este stat fondator al Mişcării de Nealiniere, India nu face parte din Consiliul de Securitate al ONU ca membru permanent, în mod similar celorlalte state analizate în prezentul material.

Federaţia Rusă continuă să fie percepută ca unul dintre actorii majori ai sistemului internaţional, în principal datorită capacităţilor sale militare, arsenalului nuclear şi poziţiei sale geopolitice strategice. Cu toate acestea, o analiză sistemică relevă faptul că Rusia se confruntă cu un declin structural profund, care limitează semnificativ capacitatea sa de a exercita o influenţă globală durabilă şi de a aspira la un statut hegemonic.

Din perspectivă economică, economia rusă este caracterizată printr-un grad ridicat de dependenţă de exporturile de resurse naturale, în special hidrocarburi. Această structură mono-sectorială expune statul la volatilitatea pieţelor globale şi reduce capacitatea de inovare şi diversificare economică. PIB-ul Federaţiei Ruse, situat sub 2 trilioane USD, rămâne modest în raport cu marile economii globale, iar nivelul productivităţii şi al competitivităţii industriale este semnificativ inferior celui occidental sau est-asiatic (World Bank, 2023).

Din punct de vedere demografic, Rusia se confruntă cu un declin accentuat al populaţiei, cu o rată scăzută a natalităţii, speranţă de viaţă

redusă și migrație externă semnificativă. Aceste tendințe afectează grav sustenabilitatea creșterii economice și capacitatea de mobilizare militară pe termen lung (UN, 2022).

În plus, Federația Rusă este condusă de același lider de un sfert de secol, aspect ce a generat stabilitate pe termen scurt, dar a produs rigiditate instituțională, corupție endemică și lipsa mecanismelor de regenerare politică. Absența unei succesiuni politice clare și concentrarea excesivă a puterii pot spori riscul instabilității sistemice, în special în contextul presiunilor economice și sociale crescânde.

Agresiunea militară împotriva Ucrainei, declanșată în 2022, a accentuat dramatic aceste vulnerabilități structurale. Deși Rusia a demonstrat capacitatea de a mobiliza resurse militare considerabile, conflictul a scos în evidență deficiențe majore în plan logistic, operațional și tehnologic, precum și limitările industriei sale de apărare (Kofman & Lee, 2023).

În plus, pierderea influenței în spațiul ex-sovietic și în Orientul Mijlociu, precum și dependența strategică față de China, transformă Rusia dintr-un actor autonom într-un partener subordonat Chinei. Această dinamică reduce semnificativ marja de manevră geopolitică a Moscovei și îi limitează capacitatea de proiecție globală (Trenin, 2023).

Prin urmare, deși Rusia rămâne o putere militară relevantă, ea nu dispune de fundamentele economice, demografice și instituționale necesare pentru a deveni un hegemon sau chiar un pol stabil de conducere regională extinsă. Rolul său viitor va fi, cel mai probabil, cel de actor perturbator, capabil să genereze instabilitate, dar incapabil să construiască o ordine alternativă coerentă.

Uniunea Europeană reprezintă unul dintre cei mai importanți actori economici și normativi ai sistemului internațional, beneficiind de un produs intern brut agregat comparabil cu cel al Statelor Unite și de un nivel ridicat de dezvoltare tehnologică, socială și instituțională. Cu toate acestea, capacitatea sa de a acționa ca actor geopolitic unitar este profund limitată de fragmentarea politică internă și de lipsa unei identități strategice comune (Howorth, 2017).

Din perspectivă economică, Uniunea Europeană concentrează aproximativ 17% din PIB-ul global și domină comerțul internațional în multiple sectoare-cheie, inclusiv industrie, servicii financiare, tehnologie verde și reglementare normativă (European Commission, 2023). Conceptul de *putere normativă* (*normative power Europe*), formulat de Ian Manners (2002), subliniază capacitatea UE de a modela standarde globale prin instrumente juridice, comerciale și instituționale.

Cu toate acestea, fragmentarea decizională şi divergenţele strategice dintre statele membre limitează drastic capacitatea Uniunii de a acţiona ca actor geopolitic coerent. Politica externă şi de securitate comună rămâne marcată de consens dificil, reacţii lente şi lipsa unei voinţe strategice unitare, ceea ce reduce eficienţa UE în competiţia globală cu marile puteri (Hill, 1993).

Din punct de vedere militar, UE depinde structural de NATO şi, implicit, de SUA pentru garantarea securităţii colective. Lipsa unei capacităţi autonome de apărare şi a unei industrii militare integrate limitează sever autonomia strategică europeană, în pofida iniţiativelor recente privind cooperarea structurată permanentă (PESCO) şi Fondul European de Apărare.

În plan politic, ascensiunea curentelor eurosceptice, populiste şi naţionaliste afectează coeziunea internă şi subminează proiectul integrării europene. Crizele succesive, precum cea financiară, migraţionistă, pandemică şi geopolitică, au scos în evidenţă fragilitatea solidarităţii în interiorul uniunii şi dificultatea construirii unui leadership comun.

Prin urmare, deşi Uniunea Europeană dispune de resurse economice şi normative impresionante, deficitul de coeziune politică şi strategică îi limitează capacitatea de a deveni un pol hegemonic sau chiar un centru stabil de conducere globală. UE va rămâne, cel mai probabil, un actor major al guvernanţei globale, dar nu un hegemon în sens clasic.

Analiza comparativă a principalilor actori statali relevă o concluzie fundamentală: niciun stat nu deţine combinaţia necesară de resurse economice, militare, demografice, instituţionale şi normative pentru a exercita o hegemonie globală durabilă.

SUA îşi păstrează avantajele structurale, dar sunt constrânse de polarizare internă, suprasolicitare strategică şi erodarea legitimităţii globale. China dispune de masă critică economică şi demografică, dar este limitată de vulnerabilităţi interne şi constrângeri geopolitice. India, Rusia şi Uniunea Europeană se confruntă cu blocaje structurale majore care le împiedică să preia rolul de lider sistemic.

Prin urmare, difuzia puterii conduce nu către o tranziţie hegemonică, ci către o fragmentare sistemică, caracterizată prin multiplicitatea centrelor de influenţă şi competiţie permanentă între actori statali şi non-statali. Această dinamică transformă radical logica ordinii internaţionale, favorizând emergenţa unei structuri hibride, fluide şi policentrice.

Viitorul sistemului internațional din perspectiva actorilor non-statali

Așa cum am prezentat și în articolul „Difuzia puterii de la actorii statali la cei non statali", publicat în *Intelligence și Cultură de Securitate. Conferința științifică studențească. Proceedings* din anul 2023, un element de noutate în evoluția relațiilor internaționale contemporane îl constituie influența tot mai accentuată a actorilor non-statali asupra dinamicii globale și a configurării noii ordini mondiale, accentuată de redistribuirea puterii în contextul progresului tehnologic rapid. Acest aspect evidențiază dificultatea statelor de a menține controlul asupra domeniilor esențiale ale vieții sociale, economice, politice și securitare, zone gestionate în mod tradițional de state, dar în care își fac prezența treptat organizații și entități non-statale, care dobândesc o capacitate de acțiune din ce în ce mai mare.

Prin urmare, provocările internaționale nu mai sunt gestionate în mod exclusiv de statele suverane, ci includ tot mai frecvent organizații și grupuri care nu reprezintă interesele unui actor statal. Cei în cauză acționează autonom, urmăresc obiective proprii sau comune și beneficiază de sprijinul unor segmente semnificative ale populației. Influența lor este amplificată de accesul facil la tehnologie și de capacitatea de mobilizare rapidă a resurselor umane și financiare.

La nivel global se afirmă actori care profită de faptul că relevanța nu mai este condiționată exclusiv de dimensiune, forță militară sau statut. Printre acestea se numără companiile multinaționale, organizațiile teroriste, grupările insurgente, rețelele de hackeri și hacktiviști, organizațiile neguvernamentale, structurile de criminalitate transfrontalieră, indivizii cu notorietate globală sau mișcările sociale spontane. Acești actori utilizează o varietate de pârghii, de la influențarea procesului decizional politic până la confruntări directe sau indirecte cu statele, pentru a-și crește impactul în relațiile internaționale. Moises Naim îi definește pe acești actori drept „microputeri", subliniind capacitatea lor de a produce efecte disproporționate în raport cu dimensiunea lor formală (Naim, 2015).

Prezintă relevanță faptul că aceste „microputeri" pot acționa în mod unitar sau în convergență cu alți actori pe teritoriul aceluiași stat, în funcție de interesele divergente sau comune ale acestora. Gravitatea rezidă din suma capacității unor mai multe „microputeri" care acționează pe teritoriul aceluiași stat sau din gradul de repetabilitate a acțiunilor unei singure „microputeri", care acționează în mod individual.

Dintre actorii non-statali, companiile multinaţionale ocupă un rol central în arhitectura relaţiilor internaţionale actuale. Acestea nu mai pot fi considerate simple instrumente ale statelor de origine, ci devin actori autonomi, orientaţi spre urmărirea propriilor interese economice şi strategice. Activitatea lor contribuie la accentuarea tensiunii dintre logica politică şi cea economică, întrucât deciziile de investiţii pot genera beneficii financiare pe termen scurt, dar pot produce efecte geopolitice negative pe termen lung pentru statul de proveniență. Un exemplu relevant este reprezentat de investiţiile companiilor americane în China, care, deşi profitabile iniţial, pot sprijini ascensiunea economică şi strategică a acesteia în detrimentul SUA.

În prezent, companiile multinaţionale au capacitatea de a negocia direct cu guvernele naţionale prin intermediul propriilor reprezentanţi. Obiectivele acestora includ obținerea unor condiţii avantajoase pentru investiţii, accesul la resurse sau facilităţi fiscale. Totodată, ele pot exercita presiuni asupra politicii interne a statelor, promovând adoptarea unor legi favorabile intereselor proprii. În situaţii nefavorabile, companiile pot recurge la ameninţări precum reducerea forţei de muncă, relocarea producţiei sau suspendarea activităţilor economice. Există, de asemenea, cadre internaţionale în care aceste companii negociază între ele sau cu alţi actori non-statali, fără implicarea directă a statelor.

În anumite domenii strategice, capacitatea statului de a controla expansiunea multinaţionalelor este limitată, în special în sectorul tehnologiei informaţiei şi al inteligenței artificiale. Platforme precum WhatsApp, Telegram, Facebook, X sau TikTok funcţionează în spaţii digitale în care controlul statal este restrâns, fapt ce atrage atenţia asupra eficienței instituţiilor publice şi capacitatea acestora de a exercita autoritate asupra populaţiei. Conform lui Jaques Attali, pieţele globale tind să depăşească structurile politice limitate de frontiere geografice, iar rolul statului în economie este prognozat să se diminueze progresiv (Attali, 2023).

Pe lângă companii, organizaţiile neguvernamentale, activiştii civici şi alte persoane influente dobândesc tot mai mult soft power şi relevanţă economică. Prin promovarea unor cauze de interes general, precum protecţia mediului, apărarea drepturilor omului, conservarea patrimoniului cultural sau combaterea sărăciei, aceşti actori atrag sprijinul public şi îşi consolidează legitimitatea. Avansul tehnologic facilitează mobilizarea rapidă a susţinătorilor prin intermediul internetului şi al reţelelor sociale.

Numeroase organizații dispun astăzi de suficientă influență pentru a expune fraude, a retrage sprijin public sau a bloca inițiative guvernamentale, având capacitatea de a remodela peisajul politic intern prin afectarea imaginii partidelor politice (Naím, 2015). Un exemplu relevant este Greenpeace, care beneficiază de milioane de susținători la nivel global și exercită presiuni asupra guvernelor și actorilor economici pentru adoptarea unor politici sustenabile (Morari, 2015). Organizația recurge la proteste, dialog instituțional și propuneri concrete, aflându-se adesea în opoziție cu guvernele unor state precum Brazilia sau China.

Alte organizații importante includ Habitat for Humanity, UNICEF, Amnesty International, Médecins Sans Frontières, Save the Children sau Crucea Roșie, care reușesc să depășească limitele impuse de granițele statale și, în anumite situații, să influențeze sau să constrângă guvernele să adopte decizii conforme obiectivelor lor.

Hackerii și hacktiviștii reprezintă o categorie emergentă de actori non-statali care activează în spațiul cibernetic. Aceștia valorifică revoluția informațională pentru a influența agenda politică, exploatând vulnerabilități de securitate ale statelor și utilizând instrumente cibernetice legale sau ilegale în scopuri politice (Naím, 2015). Hacktiviștii sunt motivați ideologic și vizează infrastructuri digitale guvernamentale sau ale unor persoane influente, cu scopul de a le compromite. Un caz emblematic este cel al lui Julian Assange, fondatorul WikiLeaks, organizație specializată în publicarea de informații confidențiale, acțiuni care au afectat relațiile diplomatice ale Statelor Unite și imaginea acestora la nivel global.

Hackerii sunt mai puțin motivați de un scop politic anume, aceștia vizând în special obținerea unor beneficii din mediul online, având în vedere că din ce în ce mai multe activități se mută în această zonă. Din acest considerent, putem estima că infracțiunile informatice și atacurile cibernetice se vor înmulți, urmând a reprezenta unele dintre cele mai mari amenințări la adresa securității globale în următoarele decenii.

Activitatea organizațiilor teroriste și a companiilor militare private constituie una dintre cele mai relevante expresii ale procesului de privatizare a războiului (Nye, 2012) în sistemul internațional contemporan. Spre deosebire de perioada clasică westfaliană, în care utilizarea legitimă a forței era monopolul statului național, contextul actual este caracterizat de proliferarea unor actori non-statali capabili să conteste direct autoritatea statelor și să influențeze echilibrele regionale de securitate. Grupări precum Hamas sau Hezbollah demonstrează capacitatea organizațiilor teroriste de a combina tactici asimetrice cu

structuri cvasi-statale, beneficiind de sprijin social, resurse financiare externe şi control teritorial limitat. Această evoluţie subminează principiile suveranităţii şi stabilităţii internaţionale, transformând conflictul armat într-un fenomen fragmentat, persistent şi dificil de gestionat prin instrumentele tradiţionale ale securităţii colective (Kaldor, 2012).

În paralel, expansiunea companiilor militare private reflectă externalizarea funcţiilor fundamentale ale statului în domeniul securităţii şi apărării. Aceste entităţi, iniţial utilizate pentru activităţi auxiliare, au dobândit treptat capacitatea de a participa direct la operaţiuni armate, inclusiv în zone de conflict activ. Utilizarea armatelor private permite statelor să reducă costurile politice şi responsabilitatea directă asociată intervenţiilor militare, însă, în acelaşi timp, contribuie la erodarea normelor internaţionale privind utilizarea forţei şi responsabilitatea pentru crimele de război.

Deşi actorii non-statali nu au la momentul de faţă puterea să contrabalanseze forţa statelor naţionale şi a conceptelor stabilite ca urmare a sistemului westfalic, trebuie luate în considerare atunci când analizăm noua ordine mondială, întrucât acestea au posibilitatea de a deveni relevante în relaţiile internaţionale, iar atingerea unor scopuri globale, precum reducerea poluării şi protejarea mediului înconjurător, depinde de buna cooperare între state şi non-state.

Noua ordine mondială – în ce paradigmă de polaritate ne vom afla?

O modalitate eficientă privind reliefarea modalităţii în care va arăta noua ordine mondială este cea privind încadrarea sistemului global în paradigma polarităţii, care, deşi poate reprezenta un concept învechit, în maniera ce urmează a fi prezentată în continuare ne va releva o serie de aspecte inedite pentru viitorul curs al istoriei.

Secolul trecut a oferit lumii întregi evoluţii impresionante în termeni de polaritate, întrucât a debutat într-o manieră multipolară neechilibrată, ce a dus la izbucnirea Războaielor Mondiale, urmând ca, după anul 1945, să ne situăm într-o paradigmă bipolară, SUA şi URSS fiind principalii competitori. Ca urmare a destrămării URSS, SUA au rămas singura superputere, astfel sistemul internaţional a cunoscut un singur hegemon, într-o logică unipolară.

Aceasta a început să fie contestată în urma atentatelor teroriste din 11 septembrie 2001, când acţiunea teroriştilor islamici a condus către un Război în Irak foarte costisitor pentru SUA şi aliaţii occidentali. De asemenea, ca urmare a răspândirii internetului şi a accesibilităţii

tehnologiilor, actorii non-statali şi-au sporit influenţa, dobândind un loc la masa negocierilor în politica mondială, iar, în termeni de state, puterile emergente şi-au făcut simţită prezenţa mai ales în urma Crizei economice care a urmat anului 2008, acestea revenindu-şi mai rapid şi menţinând un trend de dezvoltare ascendent. În prezent, asistăm la o dezintegrare progresivă a unipolarităţii, fără ca aceasta să fie înlocuită de o structură multipolară clar definită (Ikenberry, 2018; Buzan & Lawson, 2015).

În acest context, Joseph Nye propune o conceptualizare inovatoare a ordinii mondiale contemporane, descriind-o ca un „joc de şah tridimensional" (2012). La primul nivel, cel militar, SUA îşi păstrează supremaţia incontestabilă, ceea ce sugerează menţinerea unei structuri unipolare. La al doilea nivel, cel economic, asistăm la o distribuţie multipolară a puterii, în care China, Uniunea Europeană, India şi alte economii emergente joacă un rol semnificativ. La al treilea nivel, cel al relaţiilor transnaţionale, puterea este profund difuză, fiind exercitată de o multitudine de actori non-statali, într-o configuraţie non-polară.

Această abordare evidenţiază faptul că sistemul internaţional contemporan nu poate fi încadrat într-o singură paradigmă de polaritate, ci funcţionează într-o logică hibridă, caracterizată simultan prin elemente unipolare, multipolare şi non-polare. Această complexitate structurală reflectă procesul mai amplu al difuziei puterii şi al fragmentării autorităţii globale.

În plan militar, menţinerea superiorităţii americane conferă sistemului o structură unipolară, însă capacitatea SUA de a acţiona unilateral este profund limitată de constrângerile economice, politice şi normative (Nye, 2012). Intervenţiile militare costisitoare din Irak şi Afganistan, precum şi dificultăţile de gestionare a conflictelor hibride contemporane, demonstrează limitele proiecţiei forţei într-un mediu strategic complex (Freedman, 2019).

În plan economic, distribuţia puterii este multipolară. SUA, China, Uniunea Europeană, India şi alte economii emergente deţin ponderi semnificative din PIB-ul global, iar lanţurile de producţie şi aprovizionare sunt profund interdependente. Multipolaritatea economică generează atât oportunităţi de cooperare, cât şi riscuri sporite de fragmentare, protecţionism şi competiţie strategică.

Pe ce-a de-a treia tablă de şah, putem observa o multitudine de actori care se extind dincolo de controlul sau de graniţele geografice ale statelor, în acest sector puterea fiind complet difuză. Actorii sunt diverşi, de la companii multinaţionale care fac tranzacţii ce depăşesc în valoare PIB-urile multor state considerate dezvoltate, ONG-uri care pot fi mai eficienţi decât statele în promovarea de politici, până la teroriști sau

grupări de infracţionalitate organizată, care ameninţă securitatea statelor, ori hackeri care pun în pericol spaţiul cibernetic. Proliferarea actorilor non-statali conduce la o non-polaritate structurală, caracterizată prin difuzia autorităţii şi imposibilitatea exercitării unui control centralizat. Problemele globale majore – schimbările climatice, securitatea cibernetică, pandemiile, migraţia, terorismul – nu pot fi gestionate eficient de state în mod izolat, necesitând formate extinse de cooperare multilaterală şi implicarea societăţii civile globale (Keohane & Nye, 2012).

Prin urmare, noua ordine mondială nu se configurează ca o structură clar delimitată, ci ca un sistem policentric, fragmentat şi fluid, în care stabilitatea depinde de capacitatea actorilor de a construi mecanisme flexibile de guvernanţă şi cooperare. Această realitate impune o redefinire a conceptelor clasice de putere, suveranitate şi securitate, precum şi o reconfigurare a instituţiilor internaţionale.

Concluzie

Date fiind argumentele menţionate anterior, putem concluziona că noua ordine mondială nu va fi dominată de niciun actor hegemonic. SUA îşi păstrează poziţia de lider relativ, însă constrângerile interne şi externe le limitează capacitatea de proiecţie globală. China, India, Rusia şi Uniunea Europeană dispun de resurse semnificative, dar se confruntă cu vulnerabilităţi structurale care împiedică emergenţa unui nou hegemon.

În paralel, ascensiunea actorilor non-statali transformă profund arhitectura puterii globale, erodând monopolul statului asupra autorităţii politice, economice şi militare. Această dinamică generează o fragmentare sistemică, caracterizată prin competiţie intensă, interdependenţă crescută şi dificultăţi sporite în realizarea consensului.

Cu toate acestea, noua ordine mondială nu trebuie interpretată ca o formă de dezordine globală. Interdependenţa economică, densitatea reţelelor transnaţionale şi costurile prohibitive ale conflictului militar major favorizează menţinerea unui climat relativ de stabilitate. În acest context, cooperarea internaţională, guvernanţa globală şi consolidarea instituţiilor multilaterale devin deosebit de importante.

Adevărata provocare a secolului XXI nu constă în evitarea unei confruntări hegemonice clasice, ci în gestionarea eficientă a problemelor transnaţionale sistemice, precum schimbările climatice, securitatea cibernetică, pandemiile şi inegalităţile globale, unde este necesară acţiunea tuturor actorilor din relaţiile internaţionale. Capacitatea acestora de a construi mecanisme incluzive şi flexibile de cooperare va determina viabilitatea şi stabilitatea noii ordini mondiale.

Bibliografie

1. Allison, G. (2017). Destined for War: Can America and China Escape Thucydides's Trap? Houghton Mifflin.
2. Baldwin, R. (2016). The Great Convergence. Harvard University Press.
3. Buzan, B. (2012). No More Superpowers. TEDx Talks.
4. Buzan, B., & Lawson, G. (2015). The Global Transformation. Cambridge University Press.
5. Eberstadt, N. (2019). China's Demographic Outlook. AEI Press.
6. Eichengreen, B. (2018). The Populist Temptation. Oxford University Press.
7. Freedman, L. (2019). Strategy: A History. Oxford University Press.
8. Gilpin, R. (1981). War and Change in World Politics. Cambridge University Press.
9. Howorth, B. (2014). Security and Defence Policy in the European Union. Palgrave Macmillan.
10. Hill, C. (1993) The capability – Expectations gap, or Conceptualizing Europe's International Role, Journal of Common Market Studies.
11. Ikenberry, G. J. (2018). The End of Liberal International Order? International Affairs.
12. Kaldor, M. (2012). New and Old Wars. Stanford University Press.
13. Keohane, R., & Nye, J. (2012). Power and Interdependence. Longman.
14. Lardy, N. R. (2019). The state strikes back: The end of economic reform in China? Cambridge University Press.
15. Kofman, M., & Lee, R. (2023). Russia's Military Performance in Ukraine. War on the Rocks.
16. Manners, I. (2002). Normative Power Europe. Journal of Common Market Studies.
17. McGregor, R. (2012), Party. The Secret World of China's Communist Rulers, Penguin Books, Londra.
18. Mearsheimer, J. (2001). The Tragedy of Great Power Politics. Norton.
19. Naím, M. (2015). The End of Power. Basic Books.
20. National Intelligence Council. (2021). Global Trends 2040.
21. Nye, J. (2012). The Future of Power. PublicAffairs.
22. Shambaugh, D. (2013). *China goes global: The partial power*. Oxford University Press.
23. SIPRI (2024). World Military Expenditure 2023. Stockholm.
24. Trenin D. (2023). Russia's New Worldview. Carnegie Endowment for International Peace.
25. United Nations Development Programme. (2022). Human development report 2021/2022: Uncertain times, unsettled lives.
26. Varshney, A. (2014). Battles Half Won: India's Improbable Democracy. Penguin.
27. World Bank (2023). Fişele individuale ale SUA, China, India şi Rusia.

ASTROTURFING ŞI RĂZBOIUL PSIHOLOGIC PE FACEBOOK: GRILE DE VERIFICARE A CONTURILOR FALSE

Cristian HAIDĂU*

Abstract:

Astroturfing is a sophisticated form of psychological warfare and informational manipulation, where coordinated networks of fake accounts create the illusion of genuine public support for specific political, economic, or social narratives. In the context of hybrid warfare, this strategy has become a crucial tool used by both state and non-state actors to influence public perceptions, destabilize societies, and undermine democratic processes. Its impact on national security is significant, as it erodes a population's ability to distinguish between real and fabricated information, thereby reducing resilience to manipulation and propaganda.

This study examines the impact of astroturfing on public opinion, identifies the psychological mechanisms exploited in such campaigns, and proposes a methodological framework for detecting suspicious accounts involved in these activities. Two identification grids for fake Facebook accounts have been developed: an extensive grid with 34 criteria for in-depth analysis and a simplified grid with 10 key indicators, designed for quick and accessible use by regular users. These grids are based on observable behavioral patterns and technical characteristics that may indicate potential manipulative activity. The application of these criteria to a set of suspicious accounts has validated the relevance of each indicator within the current digital ecosystem.

The paper highlights the crucial role of media literacy and appropriate regulations in combating this phenomenon but places particular emphasis on critical thinking as the primary means of resilience against manipulation. In an era where information warfare plays a central role in influence strategies, the ability of individuals to critically analyze and evaluate the information they consume is a key factor in national security and societal stability.

Keywords: *astroturfing, psychological warfare, national security, informational manipulation, fake accounts, social networks, disinformation*

Context şi importanţa subiectului

Fenomenul astroturfing-ului se manifestă într-un context socio-politic complex, marcat de creşterea influenţei tehnologiei şi

* Student doctorand, anul IV, Şcoala Doctorală, SNSPA, Bucureşti, domeniu de cercetare - ştiinţele comunicării, dezinformare şi manipulare în mediul digital, e-mail: Cristian.Haidau.21@drd.snspa.ro

a platformelor digitale asupra opiniei publice. Această metodă de manipulare, utilizată de entități statale și non-statale, exploatează emoțiile colective pentru a genera impresia unui sprijin autentic față de anumite idei, doctrine sau actori politici. România se află într-un context geopolitic extrem de tensionat, fiind aproape de prima linie a conflictului necombativ cinetic dintre Rusia și Ucraina. Această poziție strategică ne expune unor atacuri concertate de psihologie socială, menite să influențeze opinia publică și să servească intereselor Rusiei.

În prezent, informația a devenit o veritabilă armă de război (Roman 2024), utilizată în cadrul conflictelor moderne nu doar pentru propagandă, ci și pentru modelarea percepțiilor colective și influențarea deciziilor politice. Odată cu dezvoltarea rețelelor sociale și a comunicării ultra-rapide și în masă, războiul informațional a devenit un instrument strategic esențial, fiind exploatat intens de actorii ostili pentru a slăbi democrațiile din interior, folosindu-se de vulnerabilitățile lor intrinseci, precum libertatea de exprimare și diversitatea de opinii. Manipularea discursului public prin dezinformare și polarizare face ca societățile democratice să fie mai ușor de influențat, creând confuzie, neîncredere și diviziune.

Mai mult decât atât, succesul unei campanii de dezinformare nu depinde doar de strategia celor care o inițiază, ci și de predispoziția receptorului de a fi dezinformat. Oamenii tind să accepte mai ușor informațiile care le confirmă convingerile și să respingă cele care contravin sistemului lor de valori. Această tendință naturală de a filtra realitatea prin prisma propriilor credințe face ca dezinformarea să fie nu doar posibilă, ci și extrem de eficientă. În esență, un individ expus unui mesaj manipulator este vulnerabil în primul rând pentru că, fie conștient, fie inconștient, dorește să audă și să creadă acel mesaj (Stan 2021, 194).

Astroturfing-ul influențează percepția publică asupra realității, facilitând amplificarea artificială a unor mesaje coordonate strategic pe rețelele sociale. Această practică erodează fundamentul proceselor democratice prin alterarea percepțiilor și fragmentarea spațiului public. Ea contribuie la polarizarea societății, amplificând tensiunile existente și reducând coeziunea socială (Ghiurgiu 2024).

Astroturfing-ul reprezintă o vulnerabilitate strategică în contextul atacurilor hibride, fiind utilizat ca instrument de destabilizare în cadrul operațiunilor de influență desfășurate de actori ostili. În acest context, România este ținta unor operațiuni sofisticate de dezinformare, al căror scop este subminarea stabilității interne și promovarea narațiunilor care avantajează interesele geopolitice ale Rusiei. Aceste atacuri vizează atât

segmentul politic şi electoral, cât şi încrederea populaţiei în instituţiile statului, utilizând tehnici de propagandă şi manipulare psihologică fără precedent. Aceste campanii urmăresc influenţarea percepţiilor colective şi a deciziilor politice prin diseminarea dezinformării, subminarea încrederii în instituţiile statului şi promovarea unui climat de incertitudine, precum şi amplificarea diviziunilor sociale şi radicalizarea opiniilor prin utilizarea conţinutului provocator şi polarizant.

Impactul asupra securităţii naţionale este major, deoarece manipularea opiniei publice poate influenţa direct procesele decizionale critice, inclusiv cele din domeniul electoral, economic şi de apărare. Un exemplu concret este anularea alegerilor din România, o măsură extraordinară adoptată pentru protejarea procesului democratic în faţa unui atac de psihologie socială fără precedent, care ameninţa stabilitatea electorală şi funcţionarea instituţiilor statului. Această decizie a evidenţiat necesitatea unor mecanisme de apărare eficiente împotriva manipulării informaţionale şi a demonstrat vulnerabilitatea proceselor electorale în faţa unor operaţiuni coordonate de influenţă externă.

Scopul şi obiectivele acestui articol

Lucrarea de faţă îşi propune să ofere o înţelegere actualizată a fenomenului de astroturfing, punând accent pe instrumentele prin care utilizatorii obişnuiţi de Facebook pot identifica rapid şi cu o acurateţe rezonabilă conturile suspecte. În acest sens, articolul introduce două grile de analiză adaptate pentru nevoi diferite. Prima este o grilă detaliată, alcătuită din 34 de criterii, destinată unei analize amănunţite a conturilor suspecte, incluzând factori ce ţin de identitate, activitate, reţea socială şi tipare de interacţiune iar cea de-a doua este o grilă simplificată, cu doar 10 criterii esenţiale, concepută pentru a fi utilizată rapid şi intuitiv de către orice utilizator, fără a necesita un proces îndelungat de analiză sau cunoştinţe tehnice.

În 2025, state, organizaţii şi grupuri de interese recurg la tactici avansate de influenţare digitală, utilizând algoritmi de amplificare, conturi automatizate gestionate prin inteligenţă artificială şi conţinut generat automat pentru a crea iluzia unui sprijin popular autentic faţă de anumite idei, doctrine sau personalităţi publice. Aceste metode sofisticate de manipulare afectează capacitatea indivizilor de a distinge între opinia reală şi cea fabricată, având implicaţii majore asupra proceselor democratice şi a climatului social global. În faţa unei opinii prezentate ca fiind a „majorităţii", punctele de vedere individuale, chiar

dacă sunt corecte, își pot pierde din entuziasm și vizibilitate, fenomen descris în literatura de specialitate ca efectul conformismului sub presiunea socială (Dobrescu and Bârgăoanu 2003, 25).

Într-un peisaj digital tot mai influențat de inteligența artificială și de relaxarea regulilor de moderare pe marile platforme sociale, acest articol are ca scop informarea și educarea publicului despre mecanismele actuale ale astroturfing-ului și despre modul în care acesta influențează percepția socială. Obiectivul principal este de a crește nivelul de conștientizare cu privire la manipularea informațională, oferind utilizatorilor metode clare și accesibile pentru a identifica conturile false și activitățile coordonate de dezinformare.

În acest context, articolul analizează principalele resorturi psihologice exploatate în astroturfing și impactul acestora asupra utilizatorilor, alături de metodele tehnologice moderne utilizate pentru a amplifica mesajele artificiale. De asemenea, sunt abordate implicațiile inteligenței artificiale în generarea și gestionarea automată a conținutului, care complică și mai mult eforturile de combatere a dezinformării. Un element esențial al analizei este reprezentat de grila extinsă de identificare a conturilor suspecte, care detaliază fiecare criteriu și relevanța sa în actualul ecosistem digital. În completare, grila simplificată oferă o metodă rapidă prin care utilizatorii pot evalua autenticitatea unui cont de Facebook, fără a fi necesară o verificare complexă.

Prin această lucrare, se urmărește oferirea cititorilor a unor instrumente practice și actualizate pentru recunoașterea și combaterea manipulării informaționale. Totodată, se dorește încurajarea unei atitudini mai critice și mai analitice în evaluarea informațiilor din mediul online.

Definirea și explicarea fenomenului de astroturfing

Astroturfing-ul reprezintă o tactică sofisticată de manipulare informațională, utilizată de grupuri de interese sau entități cu agende ascunse pentru a influența opinia publică cu privire la un subiect, o știre, un personaj sau o inițiativă, fie prin crearea iluziei unui sprijin popular autentic, fie prin discreditarea și denigrarea adversarilor (Merriam-Webster 2023). Deși pare o reacție spontană a cetățenilor, acest fenomen este, în realitate, rezultatul unei strategii bine orchestrate, menite să modifice percepțiile colective și să creeze artificial un curent de opinie favorabil sau defavorabil unei cauze specifice. Astroturfing-ul nu este

folosit doar pentru a crea artificial sprijin în jurul unui mesaj sau al unei cauze, ci şi ca instrument de subminare a credibilităţii unei persoane, instituţii sau idei. Prin răspândirea sistematică a îndoielii şi amplificarea atacurilor orchestrate, aceste campanii reuşesc să erodeze încrederea publicului şi să compromită percepţia asupra legitimităţii unei figuri publice sau a unei iniţiative. Neincrederea este profund contagioasă (Georgescu 2024) şi, odată inoculată într-un grup social, aceasta se propagă rapid, afectând percepţiile colective şi generând o atmosferă de scepticism şi ostilitate. Astfel, astroturfing-ul nu doar modelează sprijinul artificial, ci şi slăbeşte în mod deliberat coeziunea socială prin inducerea neîncrederii generalizate. Acesta se manifestă atât online, prin comentarii, reacţii, distribuiri artificiale, generare de conţinut manipulator şi utilizarea trolilor şi boţilor digitali, cât şi offline, prin organizarea de proteste sau evenimente cu participanţi care fie sunt manipulaţi să participe pe baza unor informaţii înşelătoare, fie sunt recrutaţi şi motivaţi cu anumite beneficii. În unele cazuri, participanţilor li se prezintă un motiv iniţial de protest, care ulterior este deturnat către o altă agendă, fără ca aceştia să fie conştienţi de adevăratul scop al mobilizării.

Termenul "astroturfing" a fost introdus de senatorul texan Lloyd Bentsen în 1985, când a remarcat că o campanie intensă de scrisori adresate Congresului, aparent provenind de la cetăţeni preocupaţi de anumite schimbări legislative, era, de fapt, iniţiată de companii din industria asigurărilor. Denumirea provine de la "AstroTurf", un tip de gazon artificial, ilustrând astfel caracterul prefabricat al acestui tip de influenţă publică (CSMonitor 2009). Fenomenul a evoluat rapid, devenind o componentă cheie a operaţiunilor psihologice moderne şi fiind exploatat atât de actori politici, cât şi de corporaţii sau alte entităţi cu interese specifice.

Prin utilizarea unor metode din ce în ce mai avansate, inclusiv manipularea algoritmilor pentru amplificarea mesajelor pe platformele digitale, crearea automată şi gestionarea conturilor false cu inteligenţa artificială, precum şi utilizarea acesteia pentru generarea de conţinut şi coordonarea activităţilor acestora, astroturfing-ul devine un instrument extrem de eficient şi destul de ieftin în manipularea percepţiilor publice, fiind utilizat tot mai frecvent în conflictele asimetrice şi în cadrul războiului hibrid. Acesta permite actorilor non-statali sau statali să destabilizeze societăţi şi să influenţeze procesele decizionale fără a recurge la mijloace convenţionale de confruntare, folosind manipularea informaţională ca armă strategică. Cercetările arată că informaţiile false

din domeniul politic au un potenţial de viralizare de trei ori mai ridicat decât cele din alte domenii (Bârgăoanu 2018, 146). Această capacitate de diseminare rapidă permite manipularea opiniilor şi crearea unui climat social polarizat, reducând spaţiul pentru dezbaterea raţională.

Astroturfing-ul reprezintă o ameninţare majoră pentru procesele democratice, având potenţialul de a submina încrederea în instituţiile publice şi de a distorsiona mecanismele decizionale. Prin crearea unei percepţii false asupra sprijinului sau opoziţiei faţă de anumite politici sau lideri, acest fenomen poate influenţa alegerile, formularea politicilor publice şi dinamica socială generală.

Implicaţii etice şi legale ale astroturfing-ului

Astroturfing-ul pe Facebook și alte platforme sociale continuă să ridice preocupări etice şi legale, având un impact semnificativ asupra integrităţii discursului public şi a proceselor democratice. În ultimii doi ani, avansul tehnologiilor de inteligenţă artificială şi noile reglementări internaţionale au influenţat radical atât modul în care astroturfing-ul este utilizat, cât şi strategiile de combatere a acestuia.

Implicaţiile etice ale astroturfing-ului sunt multiple şi afectează direct modul în care opinia publică este formată şi influenţată.

Manipularea opiniei publice reprezintă una dintre principalele consecinţe, deoarece astroturfing-ul creează o aparenţă falsă de sprijin popular. Acest fenomen subminează autonomia şi libertatea de exprimare a individului, împiedicând o dezbatere autentică bazată pe fapte. În 2025, utilizarea AI-urilor generative pentru crearea de conturi false şi mesaje hiper-personalizate a amplificat problema, făcând manipularea şi mai greu de detectat sau combătut.

Înşelarea utilizatorilor este o altă problemă majoră, întrucât astroturfing-ul implică folosirea de conturi false, boţi avansaţi şi reţele coordonate pentru a induce iluzia unui sprijin sau a unei opoziţii autentice. Această practică contravine principiului onestităţii şi transparenţei, inducând în eroare publicul cu privire la sursa şi motivaţiile reale ale mesajelor politice. Noii algoritmi de detecţie dezvoltaţi de platformele digitale în 2024 încearcă să limiteze fenomenul, însă eficienţa acestora rămâne sub semnul întrebării.

Dezinformarea şi distorsionarea informaţiei completează tabloul implicaţiilor etice. Astroturfing-ul utilizează tehnici de manipulare a faptelor pentru a promova agende politice sau economice, iar în 2025 AI permite generarea automată de conţinut falsificat, sub forma unor

articole, comentarii şi videoclipuri deepfake. Acest fenomen contravine principiului acurateţei şi corectitudinii informaţiei, afectând capacitatea publicului de a lua decizii informate (Chan 2022). Reglementările Uniunii Europene privind dezinformarea digitală, adoptate în 2024, încearcă să combată această practică, însă aplicarea lor este încă în curs de perfecţionare.

Implicaţiile legale ale astroturfing-ului sunt complexe şi reflectă atât evoluţiile tehnologice recente, cât şi schimbările de reglementare din mediul digital.

Odată cu schimbările politice din 2024 şi reconfigurarea administraţiei americane, s-a conturat o nouă paradigmă legislativă, care privilegiază libertatea de exprimare în detrimentul moderării stricte a conţinutului. În acest context, intervenţia platformelor asupra discursului public, anterior criticată ca posibilă formă de cenzură partizană, a fost descurajată. Ca urmare, marile companii de tehnologie şi-au ajustat strategiile, reducând moderarea umană şi colaborarea cu organizaţiile de fact-checking, în favoarea unei abordări mai permisive, aliniate noilor orientări de reglementare digitală. Deşi tehnologiile AI continuă să fie utilizate pentru identificarea reţelelor de dezinformare, lipsa verificării umane a dus la o creştere a eficienţei campaniilor de manipulare, inclusiv a fenomenului de astroturfing (Meta 2025).

Legislaţia privind protecţia datelor personale reprezintă un alt domeniu afectat de astroturfing, întrucât această practică poate implica colectarea şi utilizarea ilegală a datelor personale ale utilizatorilor, încălcând regulamentele internaţionale în vigoare. Conform noii Directive UE privind confidenţialitatea digitală (2024), utilizarea AI pentru extragerea şi profilarea automată a utilizatorilor în scopuri de manipulare politică sau comercială este interzisă. Sancţiunile au fost înăsprite, incluzând amenzi de până la 4% din cifra de afaceri anuală a companiilor implicate („GDPR" 2025).

Legislaţia electorală şi finanţarea politică au fost, de asemenea, afectate de fenomenul astroturfing-ului, care a devenit o problemă majoră în campaniile electorale. Utilizarea reţelelor false pentru influenţarea alegerilor a fost interzisă prin noile reglementări electorale din SUA şi UE, care prevăd monitorizarea şi sancţionarea entităţilor politice ce beneficiază de astfel de tactici. Noile legi impun şi transparenţă în publicitatea politică digitală, inclusiv dezvăluirea surselor de finanţare şi a metodelor de ţintire. Cu toate acestea, relaxarea reglementărilor privind moderarea conţinutului pe marile platforme sociale a generat un mediu în care entităţile politice şi economice

pot desfășura campanii de influenţă fără un control strict asupra autenticităţii şi veridicităţii informaţiilor distribuite (Autoritatea Electorală Permanentă 2024)

Astroturfing-ul rămâne o ameninţare serioasă la adresa democraţiei, iar evoluţiile tehnologice recente au complicat şi mai mult peisajul manipulării informaţionale. Creşterea utilizării AI şi noile reglementări fac ca detectarea şi prevenirea acestui fenomen să fie o provocare constantă pentru guverne, companii de tehnologie şi societatea civilă. În acelaşi timp, un nou trend promovat de figuri proeminente precum Donald Trump, Elon Musk şi Mark Zuckerberg susţine liberalizarea exprimării pe reţelele sociale, renunţarea la angajaţii responsabili cu moderarea conţinutului şi reducerea colaborării cu organizaţiile de fact-checking. Această tendinţă ridică întrebări legate de vulnerabilitatea crescută a platformelor la campanii de dezinformare şi manipulare, inclusiv la practici precum astroturfing-ul.

Principalele resorturi psihologice exploatate de astroturfing

Principiul mesianismului reprezintă una dintre strategiile eficiente utilizate pentru a influenţa şi manipula masele, bazându-se pe ideea că un lider carismatic poate deveni un mesia politic, un salvator al poporului, capabil să rezolve toate problemele şi să îndeplinească aspiraţiile acestuia (Bichir 2020). Acest principiu nu se limitează doar la un personaj uman, ci poate fi aplicat şi unei ţări, unei doctrine sau unei idei sociale ori politice.

Prin exploatarea acestui principiu, actorii implicaţi în manipulare şi modelare psihologică, inclusiv cei care utilizează tactici de astroturfing, urmăresc să obţină sprijinul şi loialitatea maselor, inducând ideea că liderul lor este un conducător providenţial. Strategia se bazează pe discursuri carismatice, promisiuni grandioase şi manipulare emoţională, având ca scop crearea unei iluzii a puterii şi speranţei în rândul populaţiei. De-a lungul istoriei, lideri precum Hitler, Mussolini, Stalin, Mao Zedong, Perón, Chávez şi Kim Il Sung au folosit acest principiu pentru a mobiliza masele, construindu-şi culturi ale personalităţii şi exploatând vulnerabilităţile sociale. Prin propagandă, retorică populistă şi demonizarea adversarilor, aceştia au obţinut loialitate necondiţionată şi control asupra opiniei publice.

Manipularea prin acest principiu este amplificată de reţelele sociale şi inteligenţa artificială, care permit distribuirea rapidă şi

automatizată a conţinutului propagandistic. Aceste tehnologii creează o imagine idealizată a liderului şi a agendei sale politice, influenţând percepţia publicului. Tendinţa naturală a maselor de a căuta un lider puternic şi carismatic le face susceptibile la astfel de tactici, facilitând instaurarea unui cult al personalităţii şi consolidarea controlului asupra opiniei publice. Acest proces asigură un nivel ridicat de influenţă asupra maselor şi permite exercitarea unui control sporit asupra acestora.

Un alt element esenţial în aplicarea principiului mesianic este identificarea unui inamic comun, perceput ca fiind sursa tuturor problemelor sociale şi economice. Manipulatorii folosesc această strategie pentru a demoniza adversarii politici şi a le atribui responsabilitatea pentru dificultăţile resimţite de populaţie. Crearea unei opoziţii binare între liderul providenţial şi adversarii săi întăreşte loialitatea maselor şi justifică măsuri radicale în numele binelui colectiv (Sturza 2021). Această dihotomie facilitează acceptarea unor acţiuni extreme şi contribuie la consolidarea poziţiei liderului, care devine singura alternativă percepută ca viabilă.

Principiul mesianic este astfel un instrument puternic de manipulare, utilizat pentru a controla opinia publică şi a obţine sprijinul necondiţionat al maselor. În contextul digital actual, reţelele sociale şi inteligenţa artificială facilitează diseminarea rapidă a acestui tip de influenţă, permiţând coordonarea eficientă a campaniilor de astroturfing şi consolidarea unui cadru favorabil războiului psihologic prin inducerea unor percepţii colective controlate artificial. Aplicarea sa în cadrul strategiilor de influenţă informaţională subminează gândirea critică şi reduce capacitatea indivizilor de a analiza obiectiv realitatea politică şi socială. Într-un mediu digital dominat de reţele sociale şi tehnici avansate de comunicare, acest principiu rămâne unul dintre cele mai eficiente mecanisme de mobilizare şi control al opiniei publice.

Principiul maniheismului şi principiul mesianismului sunt două concepte interconectate, utilizate frecvent în strategiile de influenţă şi manipulare a opiniei publice. Maniheismul reprezintă o strategie bazată pe dualitate, în care lumea este împărţită strict între bine şi rău, eliminând orice nuanţe intermediare. Această perspectivă dihotomică creează o delimitare rigidă între grupuri, prezentând unii actori ca fiind moralmente superiori, în timp ce adversarii sunt demonizaţi şi consideraţi principala sursă a problemelor societăţii.

Această diviziune artificială favorizează consolidarea unei imagini mesianice în jurul liderului, care este promovat ca singura soluţie

viabilă pentru redresarea naţiunii sau a grupului vizat. În astfel de cadre ideologice, greşelile liderului sau ale susţinătorilor săi sunt trecute cu vederea sau justificate, în timp ce orice opoziţie este aspru condamnată şi deseori prezentată ca o ameninţare existenţială. Acest tip de narativ rigid restrânge semnificativ capacitatea societăţii de a analiza critic situațiile complexe, reducând dezbaterea democratică și înlocuind-o cu loialitatea necondiționată față de figura centrală (Volkoff 2009, 126–27).

Impactul acestei manipulări prin maniheism este profund, având implicaţii asupra coeziunii sociale şi asupra mecanismelor democratice. Prin eliminarea nuanţelor şi impunerea unei perspective radicale, discursul critic şi dezbaterea raţională sunt marginalizate, conducând la polarizare, excludere şi, în unele cazuri, la radicalizare extremă. Această strategie este adesea utilizată în combinaţie cu tehnici moderne de propagandă, cum ar fi astroturfing-ul şi exploatarea algoritmilor şi grupurilor/camerelor de rezonanţă ale platformelor sociale, facilitând amplificarea mesajelor maniheiste şi crearea unor ecouri informaţionale menite să întărească percepţiile preexistente. Într-un context dominat de reţelele sociale şi de tehnologiile avansate de inteligenţă artificială, impactul maniheismului asupra societăţii contemporane devine o provocare majoră pentru securitatea informaţională şi stabilitatea politică.

Principiul validării sociale joacă un rol fundamental în tactici precum astroturfing-ul politic, unde opinia şi comportamentul sunt manipulate pentru a crea iluzia unei susţineri larg răspândite. Oamenii sunt predispuşi să fie influenţaţi spontan de cei din jur, iar pe măsură ce numărul acestora creşte, tendinţa de a accepta rapid şi fără o analiză critică opinia majorităţii devine mai pronunţată. Acest fenomen se explică prin dorința de a economisi timp și resurse cognitive, evitând procesul laborios al unei evaluări individuale (Chelcea 2006, 247–49).

Astroturferii exploatează această tendinţă prin utilizarea unui număr mare, dar artificial de susţinători, aprecieri şi redistribuiri pentru a sugera popularitatea şi legitimitatea unei anumite agende politice. Prin crearea unei impresii puternice de validare socială, aceştia influenţează utilizatorii să adopte şi să sprijine o anumită idee, bazându-se pe premisa că, dacă mulţi o susţin, aceasta trebuie să fie analizată corespunzător, verificată şi în consecinţă corectă şi/sau adevărată (Oprea 2021, 118).

Manipularea prin astroturfing se bazează astfel pe încrederea excesivă a indivizilor în opiniile celorlalţi, exploatând principiul conformismului şi al validării sociale pentru a distorsiona percepţia

publicului asupra unei cauze sau a unui lider. În era digitală, această strategie este amplificată de algoritmii reţelelor sociale, care favorizează conţinutul cu un nivel ridicat de angajament, indiferent de autenticitatea sa, contribuind astfel la consolidarea unor naraţiuni artificiale.

Principiul autorităţii joacă un rol esenţial în mecanismele de influenţă socială, fiind exploatat frecvent în cadrul strategiilor de astroturfing. Oamenii sunt educaţi să manifeste respect şi supunere faţă de autorităţi, ceea ce le poate diminua tendinţa de a pune sub semnul întrebării informaţiile primite din surse aparent credibile. Astroturferii utilizează această predispoziţie prin crearea de conturi false care par a fi deţinute de experţi sau persoane cu autoritate în domeniu (Chelcea 2006, 253–56).

Printre cele mai frecvent simulate identităţi se numără cadrele militare, medicale şi reprezentanţii bisericii. Aceste personaje sunt alese strategic pentru a spori credibilitatea mesajului şi a reduce scepticismul publicului. Prin prezentarea mesajelor drept fundamentate pe expertiză, cunoştinţe solide sau principii etice incontestabile, manipulatorii reuşesc să câştige încrederea utilizatorilor şi să îi influenţeze în direcţia dorită. Această tehnică este deosebit de eficientă în contextul reţelelor sociale, unde utilizatorii sunt bombardaţi cu informaţii şi rareori dispun de timpul sau resursele necesare pentru a verifica autenticitatea surselor.

În era digitală, inteligenţa artificială şi tehnologiile de deepfake facilitează şi mai mult utilizarea acestui principiu, permiţând generarea de conţinut vizual şi auditiv extrem de convingător. Astfel, fenomenul de astroturfing devine din ce în ce mai sofisticat, exploatând încrederea în autoritate pentru a influenţa percepţiile publice şi a modela opiniile colective.

Principiul fricii şi ameninţării reprezintă o tactică de manipulare eficientă, utilizată frecvent în strategiile de astroturfing pentru a influenţa percepţiile şi comportamentele publicului. Această tehnică se bazează pe exploatarea temerilor legate de aspecte precum securitatea naţională, imigraţia, terorismul, infracţionalitatea, problemele economice şi alte incertitudini, amplificând anxietăţile colective pentru a genera reacţii emoţionale puternice. Prin sublinierea pericolelor şi a consecinţelor negative asociate cu o anumită opţiune, manipulatorii urmăresc să inducă o stare de neliniște şi să stimuleze mecanismele de apărare şi conservare.

Astroturferii folosesc tehnici de amplificare a incertitudinii şi de exagerare a riscurilor pentru a canaliza atenţia publicului către soluţiile

pe care le promovează. Prin crearea unei imagini alarmiste asupra unei alternative, aceştia încearcă să direcţioneze susţinerea şi acceptarea către propria agendă politică sau ideologică. Manipularea emoțională bazată pe frică devine astfel un instrument esenţial pentru influenţarea maselor, determinând indivizii să acţioneze nu pe baza unei analize raţionale, ci ca reacţie la o ameninţare percepută (André 2004).

Această strategie este deosebit de eficientă în era digitală, unde reţelele sociale şi algoritmii platformelor online favorizează conţinutul care generează reacţii emoţionale intense. Astfel, frica şi ameninţarea devin factori determinanţi în modelarea opiniei publice, permiţând celor care folosesc aceste tactici să-şi impună naraţiunile şi să slăbească sprijinul pentru alternativele concurente sau să distragă atenţia de la subiecte incomode pentru propriile interese.

Principiul coeziunii sociale se referă la tendinţa oamenilor de a forma legături puternice şi de a se identifica cu grupurile sociale, generând solidaritate şi susţinere reciprocă (Roşca 2019). Acest principiu este exploatat în strategiile de astroturfing, unde manipulatorii creează comunităţi false (echo-chambers) pe platforme precum Facebook, aparent în sprijinul unei anumite cauze sau candidaţi (Bârgăoanu 2018, 120). Scopul este de a cultiva un sentiment puternic de apartenenţă şi loialitate faţă de aceste grupuri, influenţând utilizatorii să adere şi să susţină cauza promovată, având în vedere puterea şi influenţa pe care grupul le poate exercita asupra membrilor săi.

În paralel, manipulatorii pot utiliza teoria identităţii sociale pentru a cultiva sentimente de separare şi antagonism faţă de alte grupuri sociale, alimentând astfel conflicte şi diviziuni. Identitatea socială este un factor determinant în formarea opiniilor şi comportamentelor, întrucât indivizii îşi construiesc percepţia de sine în raport cu grupurile de apartenenţă (Boncu 2014). Astroturferii exploatează această tendinţă pentru a crea şi amplifica tensiuni, diminuând solidaritatea şi sprijinul faţă de grupurile sau cauzele opuse.

Acest principiu este strâns legat de **teoria conformismului social**, care evidenţiază tendinţa oamenilor de a se conforma normelor şi aşteptărilor sociale pentru a evita conflictele şi a obţine aprobarea celorlalţi (Lazarsfeld, Berelson şi Gaudet 2004, 205–6). De asemenea, **teoria autoclasificării** subliniază că indivizii tind să se categorizeze în anumite grupuri sociale şi să îşi construiască identitatea personală prin asociere cu acestea (Turner and Reynolds 2012).

Aceste teorii se completează şi oferă un cadru explicativ asupra modului în care identitatea socială poate fi influenţată şi manipulată pentru promovarea anumitor agende. Prin astroturfing, aceste efecte sunt amplificate, facilitând controlul naraţiunilor dominante şi slăbirea sprijinului pentru grupurile sau cauzele considerate opozante. Astfel, coeziunea socială devine un instrument puternic în strategii de influenţă informaţională, având implicaţii semnificative asupra comportamentului colectiv şi asupra stabilităţii sociale.

Metodologia de cercetare şi validarea instrumentelor propuse

Procesul de elaborare şi validare a grilelor de identificare a conturilor false s-a desfăşurat pe parcursul a aproximativ două luni, in intervalul ianuarie–februarie 2025. Demersul a urmat o abordare inductivă, construită treptat pe baza observaţiei directe şi a corelării tiparelor recurente identificate în mediul online. Punctul de plecare metodologic l-a constituit cadrul teoretic propus de studiul (McAfee 2022), care defineşte şase criterii de bază pentru detectarea profilurilor neautentice. Aceste repere au fost utilizate ca filtru iniţial, cercetarea având ca obiectiv adaptarea şi extinderea lor pentru a surprinde mai adecvat complexitatea actuală a fenomenului astroturfing.

În acest context, conturile false sau deturnate sunt instrumente deliberate, folosite fie pentru beneficii economice (inclusiv prin activităţi infracţionale), fie pentru campanii de influenţă precum astroturfing-ul. Ele contribuie la crearea artificială a validităţii sociale, la amplificarea mesajelor şi la polarizarea discursului public, inclusiv prin inducerea fricii, urii şi neîncrederii (Catrina 2024). Din această perspectivă, identificarea acestor conturi devine o etapă necesară pentru înţelegerea modului în care sunt construite şi propagate naraţiunile manipulative în spaţiul public digital.

În prima etapă a studiului, criteriile McAfee au fost utilizate pentru selectarea unui eşantion relevant de analiză. Procesul a presupus monitorizarea a patru pagini de Facebook active în spaţiul digital românesc, alese pe baza vizibilităţii ridicate şi a tendinţei de a disemina naraţiuni populiste şi polarizante. Din interacţiunile generate în jurul acestor pagini a fost extras un lot de 20 de conturi care îndeplineau cel puţin patru dintre cele şase criterii de bază. Acest prag a fost stabilit pentru a reduce riscul includerii accidentale a unor utilizatori legitimi, orientând analiza către profiluri cu o probabilitate mai ridicată de neautenticitate şi cu o prezenţă constantă în amplificarea mesajelor respective.

Etapa următoare a constat într-o examinare detaliată, realizată manual, a celor 20 de conturi selectate, vizând istoricul activității, structura rețelei de conexiuni și elementele tehnice vizibile. Această analiză a permis identificarea unor tipare comportamentale suplimentare, care nu erau acoperite de modelul inițial. Prin sistematizarea acestor observații, lista inițială de indicatori a fost extinsă la un total de 34 de criterii care stau la baza grilei extinse de analiză propusă în această lucrare.

Pornind de la grila extinsă, a fost elaborată ulterior și o versiune simplificată, limitată la 10 criterii esențiale. Selecția acestora a avut în vedere două principii: frecvența apariției în cadrul eșantionului analizat și gradul de accesibilitate pentru un utilizator normal. În timp ce frecvența a putut fi evaluată în mod obiectiv, criteriul accesibilității a fost stabilit printr-o apreciere subiectivă și asumată, din perspectiva unui utilizator obișnuit care are nevoie de o evaluare rapidă. Această opțiune metodologică reflectă intenția de a oferi un instrument practic, utilizabil în afara mediului academic, fără a impune o rigoare cantitativă excesivă într-un demers cu finalitate predominant educațională.

Pentru a verifica funcționarea grilelor, acestea au fost aplicate comparativ pe două eșantioane distincte. Primul a inclus cele 20 de conturi suspecte inițiale, reevaluate prin prisma grilei extinse pentru a observa consistența rezultatelor, iar al doilea eșantion, utilizat cu rol orientativ de control, a fost alcătuit din 20 de conturi autentice, selectate din cercul extins de cunoscuți, urmărindu-se o diversitate rezonabilă din punctul de vedere al vârstei, sexului, nivelului de educație și domiciliului. Această etapă a avut rolul de a observa potențialul de rezultate fals-pozitive și de a evalua măsura în care grilele pot diferenția între comportamente artificiale și activitatea obișnuită a utilizatorilor reali.

Din perspectiva resurselor implicate, testarea a evidențiat diferențe clare de timp între cele două instrumente. Aplicarea grilei extinse a necesitat, între 15 și 30 de minute per cont, în funcție de volumul și complexitatea activității analizate, în timp ce grila simplificată a permis o evaluare mai rapidă, cuprinsă între 3 și 7 minute. Această diferență susține utilizarea complementară a celor două instrumente: grila extinsă este adecvată pentru analiză aprofundată și cercetare, iar varianta restrânsă răspunde nevoii de orientare rapidă și igienă informațională cotidiană. Deși metodologia are limitele inerente unei abordări calitative, rezultatele oferă un cadru operațional coerent, adaptat realităților ecosistemului digital din anul 2025.

Tabelul nr. 1: Grilă extinsă de analiză a conturilor suspecte de Facebook.

	Grilă extinsă de analiză a conturilor suspecte de Facebook	
Nr.	**Criteriu**	**Bifat**
1.	**Nume atipic** - Combinarea de nume din culturi diferite sau alăturarea a două nume de familie prin generare aleatorie nepotrivită.	
2.	**Nume schimbat recent** - Link-ul contului nu corespunde cu numele actual, indicând posibilitatea unei reutilizări.	
3.	**Fără poză de profil/cover** - Lipsa unei imagini de profil poate indica un cont artificial.	
4.	**Poză de profil generică, generată cu AI, furată de pe internet sau de calitate foarte proastă** - Astfel, conturile false evită identificarea, mascându-şi identitatea reală şi creând o aparenţă de autenticitate fără a expune informaţii personale.	
5.	**Schimbări frecvente de poza de profil** - Indică încercări de a evita detectarea automată a contului fals.	
6.	**Cont fără informaţii personale –** Generarea automată de conturi false se îngreunează cu fiecare detaliu în plus şi din acest motiv de multe ori se alege cantitatea în detrimentul calităţii.	
7.	**Cont nou (<6 luni) sau schimbări bruşte de identitate**. - Conturile false sunt adesea create rapid pentru scopuri specifice.	
8.	**Cont fără activitate/conţinut** - Un cont real are postări şi interacţiuni, în timp ce unul fals poate fi gol sau cu puţine informaţii.	
9.	**Link cont nepersonalizat -** Link generat automat pentru a putea reutiliza mai uşor contul în alte campanii.	
10.	**Frecvenţă neregulată a postărilor** - Alternanţă între perioade de inactivitate şi activitate intensă, specifică conturilor automate.	
11.	**Activitate anormală** - Volum mare de postări fără interacţiuni reale. Poate indica un cont automatizat care distribuie conţinut.	
12.	**Postări 24/24** - Activitate constantă, inclusiv în intervale neobişnuite pentru fusul orar. Un utilizator real are pauze naturale de activitate.	
13.	**Postări fără descriere -** Distribuirea de conţinut fără explicaţii poate fi un semnal de automatizare.	
14.	**Trecerea bruscă de la conţinut personal la activitate suspectă -** Un cont furat încetează brusc să mai posteze conţinut personal şi începe să distribuie materiale specifice astroturfing-ului sau manipulării, indicând o posibilă preluare şi reutilizare.	
15.	**Descrieri scrise greşit/incoerent -** Textele pot fi traduse automat sau generate cu inteligenţa artificială.	

16.	**Conținut intens pe o temă -** Conturile false sunt adesea concentrate doar pe un subiect (ex: politică, conspirații etc).	
17.	**Conținut preponderent instigator -** Mesaje care promovează ură, divizare socială sau polarizare politică.	
18.	**Raport ciudat între numărul de prieteni și cel de interacțiuni -** Un cont cu mii de prieteni, dar fără interacțiuni, poate fi suspect.	
19.	**Prieteni cu conturi suspecte -** Conexiuni cu alte conturi care prezintă aceleași caracteristici suspecte.	
20.	**Prieteni dispersați geografic -** Conturile false au adesea conexiuni internaționale fără logică aparentă.	
21.	**Toți sau majoritatea prietenilor sunt adăugați recent –** Acest aspect poate indică o rețea artificială construită rapid pentru propagandă.	
22.	**Adaugă prieteni doar dintr-o anumită nișă -** Conturile false se infiltrează adesea în comunități specifice.	
23.	**Cerc social incoerent** - Discrepanțe sociale și culturale între profil și prieteni.	
24.	**Număr mic de prieteni (<250) -** Conturile false au adesea foarte puțini prieteni, deoarece este dificil să creeze rapid o rețea autentică de conexiuni.	
25.	**Tipar de distribuire în masă**- Distribuire masivă de conținut, fără comentarii proprii.	
26.	**Lipsa reacțiilor la propriile postări -** Poate indica lipsa unei audiențe reale.	
27.	**Nu răspunde la mesaje private/comentarii -** Un cont real în general interacționează cu ceilalți.	
28.	**Comentarii generice, scurte și repetitive** - Ex: „Adevărat!", „Fake news!", „Toată lumea știe", „Minciuni! Propagandă!" etc.	
29.	**Distribuire excesivă de link-uri suspecte -** Link-uri către site-uri obscure sau de propagandă.	
30.	**Legături cu alte conturi suspecte -** Își primește like-urile și comentariile doar de la aceleași conturi.	
31.	**Postări codificate -** Utilizarea deliberată a simbolurilor sau greșelilor ortografice pentru a evita detectarea automatizată a platformei.	
32.	**Comentarii cu link-uri ascunse –** Plasarea strategică a link-urilor in partea de text care nu se vede, *„blind spotul"* („punctul mort") - „Vezi mai mult".	
33.	**Schimbare bruscă a limbii utilizate în conținut –** Posibil semn de cont furat prin strategii de phishing.	
34.	**Diferențe între locația profilului și istoricul activității**- Contul pretinde că este din România, dar toate check-in-urile, evenimentele sau postările vechi sunt din altă țară. Acest lucru poate indica un cont furat.	
	TOTAL criterii îndeplinite	

Tabelul nr. 2: Niveluri de alarmare pentru un cont suspect pe grila extinsă.

Niveluri de alarmare pentru un cont suspect pe grila extinsă	
0-5 criterii -» **Cont probabil autentic**	Contul nu prezintă semne evidente de activitate suspectă.
6-10 criterii -» **Cont puţin suspect**	Există semnale de alarmă, dar nu suficient de multe pentru a bănui serios că este un cont fals sau parte dintr-o reţea de manipulare. Poate fi un cont nou sau al unei persoane care nu prea foloseste platforma. Se interpretează şi în funcţie de ce criterii bifează.
11-17 criterii -» **Cont suspect**	Contul prezintă suficiente semne de activitate problematică. Există o probabilitate mare ca acesta să fie un cont fals, utilizat pentru manipulare, propagandă şi/sau astroturfing.
18+ criterii -» **Cont foarte suspect**	Contul bifează multe criterii pentru a fi considerat fals sau furat, parte a unei reţele de dezinformare sau un cont utilizat pentru propagandă. Se recomandă raportarea la Facebook.

Tabelul nr. 3: Grilă restrânsă de analiză a conturilor suspecte de Facebook.

	Grilă restrânsă de analiză a conturilor suspecte de Facebook	
Nr.	**Criteriu**	**Bifat**
1.	**Fără poză de profil/cover** - Lipsa unei imagini de profil poate indica un cont artificial.	
2.	**Poză de profil generică, generată cu AI, furată de pe internet sau de calitate foarte proastă** - Astfel, conturile false evită identificarea, mascându-şi identitatea reală şi creând o aparenţă de autenticitate fără a expune informaţii personale.	

3.	**Cont nou (<6 luni) sau schimbări bruște de identitate**. - Conturile false sunt adesea create rapid pentru scopuri specifice.	
4.	**Tipar de distribuire în masa -** Distribuire masivă de conținut, fără comentarii proprii.	
5.	**Comentarii generice, scurte și repetitive** - Ex: „Adevărat!", „Fake news!", „Toată lumea știe", „Minciuni! Propagandă!" etc.	
6.	**Prieteni cu conturi suspecte -** Conexiuni cu alte conturi care prezintă aceleași caracteristici suspecte.	
7.	**Număr mic de prieteni (<250) -** Conturile false au adesea foarte puțini prieteni, deoarece este dificil să creeze rapid o rețea autentică de conexiuni.	
8.	**Conținut intens pe o temă -** Conturile false sunt adesea concentrate doar pe un subiect (ex: politică, conspirații etc).	
9.	**Legături cu alte conturi suspecte -** Își primește like-urile și comentariile doar de la aceleași conturi.	
10.	**Postări codificate -** Utilizarea deliberată a simbolurilor sau greșelilor ortografice pentru a evita detectarea automatizată a platformei.	
	TOTAL criterii îndeplinite	

Tabelul nr. 4: Niveluri de alarmare pentru un cont suspect pe grila restrânsă

Niveluri de alarmare pentru un cont suspect pe grila restrânsă	
0-3 criterii -» Cont probabil autentic	Contul nu prezintă suficiente semne evidente de activitate suspectă. Poate fi cont nou sau al unei persoane fără prea multă activitate.
4-6 criterii -» Cont suspect	Contul prezintă suficiente semne de activitate problematică. Există o probabilitate mare ca acesta să fie un cont fals, utilizat pentru manipulare, propagandă și/sau astroturfing.
7+ criterii -» Cont foarte suspect	Contul bifează multe criterii pentru a fi considerat fals sau furat, parte a unei rețele de dezinformare sau un cont utilizat pentru propagandă. Se recomandă raportarea la Facebook.

Explicarea criteriilor din grila de identificare a conturilor false din Facebook:

1. Nume atipic – Generarea automată a numelor pentru conturi false poate duce la discrepanțe evidente, cum ar fi combinarea a două

nume din culturi diferite sau formatarea incoerentă a prenumelui şi numelui. Un semnal puternic de alarmă este nepotrivirea dintre nume şi alte elemente ale contului, cum ar fi poza de profil sau regiunea geografică indicată. În 2025, algoritmii de generare sunt mai avansaţi, dar multe reţele de boţi continuă să folosească baze de date slabe, ceea ce face ca numele incoerente să rămână un indicator valid.

2. Nume schimbat recent – Poate indica reutilizarea unui cont, adesea parte dintr-o reţea de boţi sau pregătit pentru revânzare şi reutilizare în alte scopuri. Conturile vechi sunt mai valoroase, deoarece trec mai uşor de filtrele Facebook, iar schimbarea numelui este un prim pas în procesul de ascundere a activităţii anterioare. Deşi Facebook permite modificarea link-ului profilului, multe conturi suspecte nu o fac, din motive precum restricţiile platformei, graba operatorilor sau limitările de diverse resurse. Astfel, dacă link-ul contului conţine un nume diferit de cel actual, acesta poate fi un indiciu puternic al unui cont reciclat sau compromis.

3. Fără poză de profil/cover – Lipsa unei poze de profil sau a unui cover este frecventă la conturile false, în special cele generate rapid pentru scopuri de propagandă sau spam. Conturile automate simple sunt mai uşor şi mai rapide de creat fără a încărca imagini, evitând astfel verificările suplimentare şi economisind resurse. Această tactică ajută conturile false să evite atragerea atenţiei, deoarece utilizatorii reali tind să ignore sau să nu interacţioneze cu profiluri goale. În plus, boţii care generează şi controlează un număr mare de conturi pot avea limitări hardware, iar simplificarea conturilor reduce costurile.

4. Poză de profil generică, generată cu inteligenţă artificială, furată de pe internet sau de calitate foarte proastă – Conturile false folosesc frecvent poze de profil generice, fie imagini cu peisaje, flori sau animale, fie fotografii generate cu inteligenţă artificială, furate de pe internet sau de calitate foarte slabă. Scopul acestora este de a evita detectarea automată şi de a crea o aparenţă de autenticitate fără a expune informaţii personale. Unele conturi aleg imagini prea artistice pentru a părea atractive, iar altele folosesc poze reale, dar furate, ceea ce poate fi verificat prin căutări inverse. De asemenea, aceste conturi evită postarea de fotografii cu alte persoane reale, deoarece menţinerea unei identităţi credibile ar necesita interacţiuni constante.

5. Schimbări frecvente ale pozei de profil – Conturile false îşi pot schimbă frecvent poza de profil pentru a evita detectarea automată şi pentru a crea impresia unei activităţi autentice. Această practică este folosită de reţelele de boţi pentru a înşela algoritmii de moderare şi

pentru a împiedica utilizatorii să le recunoască. Uneori, schimbările sunt realizate între imagini generice, poze furate sau chiar fotografii generate cu AI. Dacă un cont își modifică imaginea neobișnuit de des, fără un motiv clar, poate fi un indiciu că încearcă să ascundă o identitate falsă sau că este parte dintr-o rețea artificială.

6. Cont fără informații personale – Cu cât se dorește crearea automată a unor conturi de Facebook mai complete și mai realiste, cu atât procesul devine mai dificil și mai expus detectării de către algoritmii platformei. Din acest motiv, administratorii rețelelor de boți preferă să genereze profiluri minimale, completând doar datele strict necesare pentru a trece de filtrele inițiale ale Facebook.

Atunci când se încearcă adăugarea unor informații mai detaliate, pot apărea incongruențe, precum nepotrivirea dintre vârstă și fotografia de profil, disonanțe între genul numelui și cel al pozelor sau contradicții între locul de naștere, nume și poza de profil. Pentru a evita aceste erori și pentru a minimiza riscul de identificare, conturile false rămân în general lipsite de detalii personale, permițând și reutilizarea lor în diverse campanii de manipulare.

7. Cont nou (<6 luni) sau schimbări bruște de identitate – Facebook își îmbunătățește constant algoritmii de detectare a conturilor false, ceea ce face ca durata de viață a acestora să fie, în general, scurtă. De aceea, majoritatea conturilor false utilizate în campaniile de manipulare sunt conturi noi, create rapid și în număr mare prin botnet-uri, automatizări și rețele proxy. Deși conturile furate sunt mai greu de detectat, utilizarea acestora este limitată, deoarece securizarea cu doi factori și procedurile de recuperare le fac mai greu de exploatat la scară largă. Astfel, schimbările bruște de identitate sau activitatea ridicată a unui cont recent creat pot fi indicatori eficienți ai unui profil suspect.

8. Cont fără activitate/conținut – Întrucât generarea automată de conținut autentic și convingător la scară largă este dificilă, multe conturi false aleg să nu posteze deloc sau să aibă un conținut minim, pentru a evita detectarea de către algoritmii Facebook. Lipsa activității este o strategie de camuflare folosită de rețelele de boți, care preferă să interacționeze prin like-uri, comentarii generice sau distribuiri automate, fără a publica postări proprii. Totuși, manipularea online este un fenomen dinamic, iar calitatea și strategia utilizării conturilor false variază în funcție de experiența și resursele celor care le gestionează.

9. Link cont nepersonalizat – Multe conturi false de Facebook folosesc link-uri generate automat, fie pentru că nu îndeplinesc cerinţele platformei pentru personalizare, fie pentru a fi mai uşor reutilizate în alte campanii, fie pentru că procesul de personalizare a URL-ului este omis intenţionat, fiind considerat inutil. Resursele sunt concentrate pe crearea unui număr mare de profiluri, iar schimbarea link-ului ar necesita programare suplimentară, consum de timp şi un risc mai mare de erori, ceea ce face ca reţelele de conturi false să evite acest pas şi să aleagă variantele cele mai simple şi rapide. În plus, link-urile personalizate pot servi drept indiciu pentru identificarea şi monitorizarea conturilor suspecte, motiv pentru care reţelele de dezinformare preferă să le lase generice, făcând conturile mai greu de urmărit şi detectat.

10. Frecvenţă neregulată a postărilor – Conturile false prezintă adesea o frecvenţă neregulată a postărilor, alternând între perioade lungi de inactivitate şi episoade de activitate intensă. Această oscilaţie este un indiciu al automatizării, deoarece boţii sau operatorii umani care le controlează acţionează în valuri organizate, în funcţie de necesităţile campaniilor de dezinformare, spam sau influenţă. Un cont real are, de obicei, o activitate constantă şi organică, în timp ce unul fals poate posta masiv într-un interval scurt, distribuind conţinut repetitiv, pentru ca apoi să dispară. Acest comportament este frecvent întâlnit în reţelele coordonate, unde conturile sunt activate doar în momente strategice, evitând detectarea şi restricţiile algoritmilor Facebook.

11. Activitate anormală – Conturile false sau automatizate pot prezenta activitate anormală, caracterizată printr-un volum mare de postări zilnice, fără a genera interacţiuni reale. Studiile arată că utilizatorii obişnuiţi postează, în medie, 1-2 postări pe zi, iar frecvenţe mai mari sunt specifice paginilor oficiale sau influencerilor. În schimb, un cont suspect poate posta de peste 4-5 ori pe zi, adesea conţinut distribuit automat, fără comentarii personalizate sau răspunsuri la interacţiuni.

Această strategie este utilizată de reţelele de astroturfing şi propagandă, care se bazează pe cantitate, nu pe engagement autentic. Lipsa reacţiilor naturale, cum ar fi like-uri sau comentarii de la prieteni reali, poate fi un indicator clar al unui cont fals.

12. Postări 24/24 – Un utilizator real are pauze naturale de activitate, reflectând orele de somn, muncă şi alte activităţi offline. În schimb, conturile false sau automatizate pot avea postări constante, 24/24, indiferent de fusul orar al ţării în care pretind că activează. Acest

tip de activitate nefirească este un indiciu puternic al utilizării de boți, al conturilor gestionate de echipe din alte zone geografice sau al rețelelor coordonate de dezinformare. Adesea, coordonatorii boților nu setează un ritm realist de postare, ceea ce face ca aceste conturi să fie active în timpul nopții, fără variații naturale. Deși utilizatorii reali pot avea activitate nocturnă ocazională, postările constante la ore atipice pot ridica suspiciuni, mai ales atunci când sunt combinate cu alte semnale de alarmă.

13. Postări fără descriere – Conturile false distribuie adesea postări fără descriere, deoarece generarea automată de texte coerente, relevante și corect scrise rămâne încă o provocare pentru rețelele de boți. În plus, Facebook utilizează algoritmi avansați care analizează conținutul textual pentru a detecta tipare suspecte. Prin urmare, lipsa unei descrieri poate fi o strategie folosită pentru a evita analiza lingvistică și a reduce riscul de detectare. Deși utilizatorii reali pot uneori să partajeze conținut fără comentarii, conturile false fac acest lucru constant, postând sau redistribuind materiale fără nicio explicație personalizată. Această lipsă de context și de interacțiune autentică este un indiciu bun de automatizare sau de activitate coordonată.

14. Trecerea bruscă de la conținut personal la activitate suspectă – Un cont real de Facebook are un tipar de activitate constant, postând ocazional conținut personal, actualizări despre viața utilizatorului sau interacțiuni autentice. În schimb, un cont furat încetează brusc să mai posteze astfel de informații și trece la distribuirea conținutului standardizat, adesea axat pe propagandă, dezinformare sau astroturfing. Această schimbare bruscă poate fi un semnal clar al reutilizării contului într-o rețea coordonată. Administratorii conturilor compromise evită uneori să șteargă istoricul postărilor pentru a menține o aparentă autenticitate, însă modifică tipul de conținut promovat. Dacă un profil își schimbă brusc stilul de postare, renunțând la interacțiuni personale în favoarea unui flux suspect de distribuiri, acesta trebuie analizat atent.

15. Descrieri scrise greșit/incoerent – Textele incoerente sau cu greșeli gramaticale pot indica utilizarea traducerilor automate, a generatoarelor de text slab optimizate sau a unor algoritmi care nu sunt adaptați la nuanțele limbii române. Deși inteligența artificială a evoluat semnificativ, unele rețele de boți încă folosesc sisteme mai puțin avansate, ceea ce duce la formulări rigide, structuri ciudate sau greșeli frecvente. Totuși, nu toate textele incorecte aparțin conturilor false și nu toate textele corect scrise sunt autentice. Un cont devine suspect atunci

când postează în mod constant mesaje cu erori recurente, traduceri nefireşti sau fraze care nu se potrivesc contextului conversaţional.

16. Conţinut intens pe o temă – Conturile false sunt adesea concentrate pe un singur subiect, reflectând agenda reţelei care le controlează. Acestea pot promova teme precum politică, conspiraţii, activism extremist sau dezinformare. Spre deosebire de utilizatorii reali, care abordează subiecte diverse şi au interacţiuni variate, conturile suspecte postează exclusiv conţinut legat de un singur domeniu, fără variaţii naturale. Acest tipar indică o posibilă implicare într-o campanie coordonată de astroturfing, menită să amplifice artificial un mesaj, să polarizeze opinia publică sau să creeze percepţia falsă că există un interes masiv pentru o anumită idee.

17. Conţinut preponderent instigator – Conturile false pot fi utilizate pentru a polariza discursul public, promovând mesaje care instigă la ură, divizare socială şi conflict. Aceste tactici sunt frecvent folosite în campanii de manipulare şi destabilizare, deoarece tensiunile sociale facilitează influenţarea opiniilor şi radicalizarea grupurilor. Astfel de conturi distribuie conţinut menit să exacerbeze diferenţele politice, culturale sau ideologice, amplificând teme controversate precum teorii ale conspiraţiei, naţionalism extrem, conflicte etnice sau sociale. De multe ori, postările sunt construite pentru a stârni emoţii puternice, cum ar fi furie sau indignare, generând reacţii rapide şi diminuând gândirea critică. Această strategie permite manipularea percepţiei colective şi crearea iluziei unei susţineri largi pentru idei extreme.

18. Raport ciudat între numărul de prieteni şi cel de interacţiuni – Un cont care are mii de prieteni, dar prezintă foarte puţine interacţiuni reale poate fi un indiciu al unui profil fals sau automatizat. În mod natural, un utilizator activ pe Facebook primeşte like-uri, comentarii şi reacţii la postările sale, în special de la prietenii apropiaţi. În schimb, conturile suspecte pot avea liste extinse de prieteni, dar fără ca aceştia să interacţioneze real cu postările lor. Această discrepanţă poate apărea deoarece mulţi boţi şi conturi cumpărate adaugă prieteni în masă, dar nu au un istoric autentic de conversaţii sau engagement.

19. Prieteni cu conturi suspecte – Conturile false de pe Facebook adoptă uneori strategii de interconectare între ele pentru a crea o aparentă autenticitate. Boţii sau conturile controlate manual din reţele de dezinformare se adaugă reciproc ca prieteni, îşi distribuie conţinutul, îşi dau like-uri şi comentarii între ele, încercând să genereze o impresie falsă de popularitate şi legitimitate.

Un indiciu al unui cont suspect este o listă de prieteni formată majoritar din alte conturi cu caracteristici similare. Acest tipar este des întâlnit în rețelele de propagandă, unde un grup de conturi suspecte se validează reciproc pentru a amplifica artificial mesajele și a crește vizibilitatea conținutului distribuit.

20. Prieteni dispersați geografic – Un utilizator real are, de obicei, o rețea de prieteni formată în mare parte din persoane din aceeași țară sau cu care împărtășește un context comun, precum școala, locul de muncă sau evenimente sociale. În schimb, conturile false prezintă frecvent prieteni dispersați geografic, adăugând utilizatori din zone fără nicio conexiune logică.

Acest tipar poate apărea în cazul conturilor automatizate care se adaugă între ele pentru a crea o aparență de autenticitate, dar și în cazul conturilor cumpărate, care sunt reutilizate pentru diverse scopuri. De exemplu, un cont aparent românesc, dar cu prieteni preponderent din Africa, Asia sau America de Sud, poate fi suspect. Rețelele de boți sau de propagandă globală folosesc această strategie pentru a-și întări artificial credibilitatea și pentru a evita detectarea rapidă de către algoritmii Facebook, însă această lipsă de coerență geografică rămâne un indicator bun al unui cont suspect.

21. Toți sau majoritatea prietenilor sunt adăugați recent – Un cont real își formează rețeaua de prieteni treptat, prin interacțiuni naturale. În schimb, un cont fals adaugă zeci sau sute de prieteni într-un timp foarte scurt, semn că face parte dintr-o rețea artificială. Unele conturi sunt create de la zero, iar altele sunt conturi furate prin phishing. Acestea își schimbă numele, poza de profil și lista de prieteni, ștergând conexiunile originale și adăugând rapid noi prieteni specifici scopului urmărit. Dacă un cont are multe conexiuni adăugate brusc, fără interacțiuni reale, este probabil un profil fals folosit într-o campanie coordonată.

22. Adaugă prieteni doar dintr-o anumită nișă – Conturile false sunt adesea create pentru a se infiltra în comunități specifice, precum grupuri politice, conspiraționiste, economice sau activiste. În loc să adauge prieteni în mod diversificat, acestea își formează rețeaua preponderent sau chiar exclusiv în jurul unei teme de interes, conectându-se cu utilizatori care împărtășesc aceeași ideologie sau preocupare. Această strategie ajută conturile suspecte să capete legitimitate, să amplifice mesaje coordonate și să influențeze mai ușor conversațiile din acea nișă. De multe ori, aceste profiluri sunt utilizate pentru propagandă, manipulare sau escrocherii, fiind concepute pentru

a răspândi dezinformări într-un anumit mediu. Dacă un cont are prieteni preponderent sau exclusiv dintr-o singură categorie (ex. activişti radicali, promotori ai unei/unor conspiraţii etc), fără variaţie socială, acest tipar poate fi un semnal de alarmă.

23. Cerc social incoerent – Un cont real are o reţea de prieteni logică, formată în mod natural. În schimb, conturile false pot prezenta discrepanţe evidente, fie din cauza unei construcţii artificiale, fie pentru că încearcă să exploateze principiul autorităţii, pretinzând că aparţin unor profesii de încredere, precum militari, doctori, profesori sau preoţi. Totuşi, astfel de profiluri ar trebui să aibă prieteni din acelaşi domeniu. Un medic fără conexiuni cu alţi doctori, un militar fără prieteni din armată sau un bancher bogat cu o reţea formată preponderent din persoane cu venituri mici pot ridica suspiciuni.

24. Număr mic de prieteni (<250) – În 2013, un studiu arăta că utilizatorii de Facebook aveau, în medie, 338 de prieteni, într-o perioadă în care platforma număra 1,23 miliarde de utilizatori activi lunar. De atunci, Facebook a crescut considerabil, ajungând în 2025 la peste 3 miliarde de utilizatori. Deoarece nu există studii recente care să ofere o medie actualizată a numărului de prieteni pe Facebook, estimez că această valoare a crescut proporţional cu expansiunea platformei. Dacă numărul de utilizatori s-a extins de aproximativ 2,5 ori, consider că şi numărul mediu de prieteni a crescut în mod similar, situându-se acum între 500 şi 700 de prieteni per utilizator activ.

Pentru a stabili pragul minim sub care un cont devine suspect, mă bazez pe analiza distribuţiei sociale. În orice reţea socială, utilizatorii tind să se încadreze în jurul mediei, iar cei care cad semnificativ sub acest prag sunt fie utilizatori ocazionali, fie conturi suspecte. Consider că un prag de 250 de prieteni este rezonabil, fiind situat între 30% şi 40% din media estimată, ceea ce înseamnă că un cont real ar trebui să depăşească acest număr pentru a nu ridica suspiciuni.

Conturile false au dificultăţi în acumularea prietenilor, fie din cauza lipsei unei identităţi credibile, fie din cauza restricţiilor Facebook, care limitează cererile de prietenie şi elimină automat conturile suspecte. Desigur, un număr mic de prieteni nu este singurul criteriu care defineşte un cont fals. Însă, pe baza acestei analize, consider că un profil cu mai puţin de 250 de prieteni poate ridica suspiciuni şi trebuie analizat în combinaţie cu alţi factori.

25. Tipar de distribuire în masa – Un utilizator autentic de Facebook îşi exprimă, de regulă, opiniile şi prin comentarii, reacţii şi

postări proprii. În schimb, conturile suspecte afișează un tipar de distribuire excesivă, în care singura sau preponderenta activitate este cea de distribuire masivă de conținut, fără comentarii sau explicații. Acest comportament sugerează că respectivul cont este folosit pentru propagare, nu pentru interacțiune, fiind un instrument folosit în campaniile de astroturfing. Astfel de conturi distribuie frecvent postări din aceleași surse, preponderent îndoielnice și concentrate pe un singur subiect. În contextul astroturfing-ului, acest model de distribuție este utilizat pentru a crea iluzia unui sprijin popular, amplificând artificial anumite mesaje, fie prin conținut politic, fie prin dezinformare strategică. Mai mult, distribuirea excesivă în grupuri multiple, într-un timp scurt, poate indica o tentativă de manipulare sau automatizare, caracteristici esențiale ale rețelelor de influență artificială.

26. Lipsa reacțiilor la propriile postări – Un utilizator real de Facebook primește, de regulă, reacții și comentarii la postările sale, fie de la prieteni, fie de la urmăritori cu interese comune. În schimb, conturile suspecte au o lipsă totală sau aproape totală de interacțiuni, ceea ce poate indica o audiență reală inexistentă. Acest tipar este comun în cazul conturilor automatizate folosite în campanii de astroturfing, unde scopul principal este de distribuirea a unui mesaj.

27. Nu răspunde la mesaje private și comentarii – Un cont real de Facebook interacționează în mod natural cu ceilalți utilizatori, răspunzând la comentarii și mesaje private, fie și ocazional. În schimb, conturile false sunt create în număr mare și gestionate automat sau parțial, ceea ce face dificilă monitorizarea și răspunsul personalizat la interacțiuni. Deoarece aceste conturi sunt utilizate pentru astroturfing, ele nu sunt concepute pentru conversații directe. Răspunsurile ar necesita resurse tehnologice și umane semnificative, ceea ce nu este eficient pentru administratorii acestor rețele. În plus, un răspuns neinspirat sau incoerent ar putea crește suspiciunile utilizatorilor reali.

28. Comentarii generice, scurte și repetitive – Un utilizator real tinde să lase comentarii variate, cu argumente, opinii sau reacții personalizate. În schimb, conturile suspecte folosesc mesaje scurte, generice și repetitive, precum „Adevărat!", „Minciuni!", „Fake news!", „Toată lumea știe!", „Trezirea!" etc. Acest tipar este comun în campaniile de astroturfing și manipulare, unde conturile false sunt folosite pentru a amplifica artificial anumite mesaje. Comentariile generice sunt preferate pentru că sunt simple, permit ușoare erori în interpretarea contextului și sunt ușor de generat automat.

29. Distribuire excesivă de link-uri suspecte – Conturile false distribuie constant link-uri de pe site-uri special create pentru manipulare, concepute să pară publicaţii autentice. Aceste platforme imită site-uri de ştiri cunoscute, folosind nume asemănătoare sau chiar denumiri ale unor publicaţii care nu mai există, pentru a părea surse legitime. În loc să partajeze conţinut diversificat, asemenea unui comportament uman normal, aceste conturi promovează în mod repetitiv aceleaşi surse obscure, cu informaţii manipulate, conspiraţii sau propagandă.

31. Legături cu alte conturi suspecte – Un cont autentic de Facebook primeşte interacţiuni diverse, de la prieteni reali cu opinii şi comportamente variate. În schimb, conturile suspecte funcţionează în reţele coordonate, unde like-urile, comentariile şi distribuirile provin mereu din aceleaşi surse, adesea alte conturi suspecte. Acest tipar poate indica o infrastructură artificială de amplificare a mesajelor, folosită în campanii de astroturfing, propagandă sau dezinformare. De multe ori, aceste conturi se susţin reciproc prin comentarii generice sau reacţii automate, fără o interacţiune autentică. Analizând profilurile care interacţionează frecvent cu un cont suspect, putem observa că multe dintre ele prezintă aceleaşi caracteristici artificiale, au activitate restrânsă la un singur subiect şi conexiuni limitate la alte conturi suspecte. Acest comportament poate indica o reţea organizată, menită să creeze falsa impresie de popularitate şi să manipuleze percepţiile publicului.

31. Postări codificate – Pentru a evita detectarea de către algoritmii Facebook, conturile suspecte folosesc uneori postări codificate, în care anumite cuvinte cheie sunt modificate deliberat prin simboluri, caractere speciale sau greşeli ortografice. Această tehnică încearcă să păcălească algoritmii, îngreunând identificarea şi ştergerea conţinutului care încalcă regulile platformei. De exemplu, în loc de „vaccin", se poate scrie „v@cc1n", iar în loc de „guvern", se foloseşte „g0vern" sau „gu vern min ciu nă". Unele postări încearcă să păcălească algoritmii şi prin scrierea fonetică greşită „guvărnul minchinos". Această metodă este des utilizată în campaniile de astroturfing şi dezinformare, unde este crucial ca mesajele să circule fără a fi blocate. Un cont care recurge frecvent la astfel de tactici, mai ales pe subiecte controversate, poate indica o încercare deliberată de manipulare sau evitare a moderării platformei.

32. Comentarii cu link-uri ascunse – O tehnică frecvent utilizată de conturile suspecte pentru a disemina conţinut manipulat

sau propagandistic este plasarea strategică a link-urilor în *„blind spotul”* („punctul mort”) Facebook, ascunzându-le sub butonul „Vezi mai mult” din comentarii. Această metodă este folosită în încercarea de a evita detectarea automată a link-urilor suspecte, deoarece Facebook analizează cu prioritate partea vizibilă a unui comentariu, din considerente de optimizare a resurselor hardware. Pentru a determina utilizatorul să dea click pe „Vezi mai mult” și ulterior să acceseze linkul, prima parte a mesajului este concepută în stil clickbait – un text scurt, care captează atenția, creează curiozitate și îl impulsionează să dea clic si pe link.

33. Schimbare bruscă a limbii utilizate în conținut – Un utilizator real își păstrează, de regulă, coerența în utilizarea limbii, chiar dacă poate interacționa ocazional în alte limbi. În schimb, un cont suspect poate prezenta o schimbare bruscă și completă a limbii în care postează și comentează, fără o explicație logică. Acesta este un posibil semn că respectivul cont a fost furat printr-o strategie de phishing și ulterior reutilizat pentru un alt scop, fără a fi resetat complet. Hackerii care operează astfel de conturi preferă uneori să păstreze istoricul profilului, deoarece acest lucru îl face mai credibil. De exemplu, un cont care anterior posta doar în sârbă și brusc, începe să posteze exclusiv în română, poate fi parte dintr-o rețea de astroturfing sau dezinformare.

34. Diferențe între locația profilului și istoricul activității – Un utilizator autentic are, de obicei, o activitate coerentă cu locația sa declarată, reflectată în check-in-uri, evenimente, postări și interacțiuni. În schimb, un cont suspect poate prezenta discrepanțe între țara pe care o afișează și istoricul activității sale. De exemplu, un profil care pretinde că este din România, dar are check-in-uri și postări vechi dintr-o altă țară, fără nicio explicație logică (ex. mutare, călătorii frecvente), poate fi un indiciu al furtului și reutilizării contului. Acest lucru este frecvent întâlnit în cazul conturilor compromise prin phishing, care sunt preluate și integrate în rețele de astroturfing și manipulare digitală.

Limitările studiului

Deși prezenta cercetare propune instrumente operaționale validate pentru identificarea conturilor implicate în campanii de astroturfing, aceasta prezintă anumite limitări metodologice. În primul rând, validarea grilelor a fost realizată pe un eșantion calitativ restrâns, format din 20 de conturi suspecte. Deși rezultatele susțin ipotezele

teoretice formulate, dimensiunea eşantionului limitează generalizarea statistică la nivelul întregului ecosistem digital.

În al doilea rând, analiza s-a concentrat exclusiv asupra platformei Facebook, cu particularităţile sale structurale şi algoritmice. Indicatorii de manipulare şi tipologiile de conturi false pot diferi semnificativ pe alte platforme, unde nivelul de filtrare, gradul de permisivitate şi formatele de conţinut sunt diferite.

Nu în ultimul rând, dinamica accelerată a tehnologiilor de inteligenţă artificială generativă (AI) reprezintă o provocare majoră. Capacitatea tot mai avansată a modelelor AI de a produce imagini hiperrealiste, texte corecte, coerente şi interacţiuni aparent autentice riscă să reducă în curând relevanţa unor indicatori vizuali sau lingvistici utilizaţi în prezent, ceea ce impune actualizarea periodică a criteriilor de detecţie.

Concluzii

Studiul de faţă arată că astroturfing-ul nu constituie o simplă problemă tehnologică, ci o formă complexă de influenţă psihologică, care exploatează vulnerabilităţi cognitive fundamentale pentru a distorsiona realitatea percepută. Analiza teoretică evidenţiază faptul că eficienţa acestor campanii este strâns legată de activarea unor mecanisme de psihologie socială: validitatea socială, care creează iluzia consensului, apelul la frică şi ameninţare, menit să inhibe gândirea critică, precum şi utilizarea schemelor maniheiste şi mesianice pentru polarizarea discursului public. În acest cadru, utilizatorul obişnuit este transformat din receptor pasiv într-un agent involuntar de diseminare a dezinformării.

Răspunsul operaţional propus şi testat în această cercetare constă în formalizarea procesului de detecţie prin cele două grile de evaluare a conturilor suspecte. Validarea empirică a demonstrat că, în pofida progresului tehnologic, conturile false continuă încă să lase urme comportamentale şi structurale identificabile. Grila extinsă s-a dovedit adecvată analizei aprofundate, în timp ce varianta simplificată oferă un instrument rapid, util pentru menţinerea unei minim scut în mediul digital.

Cu toate acestea, nici cele mai performante instrumente nu pot substitui complet factorul uman. Aşa cum a fost argumentat anterior, educaţia digitală şi alfabetizarea media reprezintă în contextul anului 2025, elemente centrale ale rezilienţei societăţii. Utilizatorii trebuie să fie

capabili nu doar să identifice conținutul manipulator, ci și să înțeleagă logica algoritmilor ce amplifică artificial anumite narațiuni. În mod complementar, securitatea cibernetică personală devine o componentă esențială, întrucât compromiterea conturilor legitime facilitează integrarea acestora în rețele de influență prin furt de identitate.

Un element suplimentar, preluat din practica jurnalistică clasică, rămâne esențial în procesul de evaluare critică a discursului public: întrebarea privind beneficiarul unei narațiuni. Analiza oricărui mesaj ar trebui să includă constant o reflecție asupra intereselor pe care acesta le servește, a actorilor care ar putea sta în spatele său și a efectelor urmărite la nivel social, economic sau politic. O astfel de abordare presupune depășirea reacțiilor emoționale imediate și plasarea informației într-un cadru mai larg, care permite o înțelegere mai lucidă a dinamicilor de influență.

În final, deși responsabilitatea individuală și cultivarea gândirii critice sunt indispensabile, combaterea eficientă a astroturfing-ului nu poate rămâne exclusiv la nivel individual. Cercetarea subliniază necesitatea unei cooperări între platformele digitale și autorități, în vederea dezvoltării unor mecanisme automatizate de detecție, fundamentate pe indicatorii identificați și a adaptării cadrului normativ la provocările generate de inteligența artificială. Doar prin convergența dintre utilizatorul informat, capabil de analiză calmă și critică și mecanismele instituționale de protecție poate fi menținută in limite rezonabile siguranța spațiului public digital în fața operațiunilor de influență hibridă.

Bibliografie

1. André, Christophe. 2004. *Psihologia fricii: temeri, angoase și fobii*. București: Editura Trei.

2. Autoritatea Electorală Permanentă. 2024. „Proiect de hotărâre privind aprobarea Ghidului finanțării campaniei electorale”. *Roaep.ro*. Accesat la 20 februarie 2025. https://www.roaep.ro/legislatie/wp-content/uploads/2025/02/PROIECT-HOTARARE-MATERIAL-PUBLICITATE-POLITICA.pdf.

3. Bârgăoanu, Alina. 2018. *#FAKENEWS. O nouă cursă a înarmării*. București: Evrika Publishing.

4. Bichir, Florian. 2020. „Conceptul de mesianism în geopolitică". *Geopolitica*, 2020. https://www.geopolitic.ro/wp-content/uploads/2020/02/GEOPOLITICA1.html.

5. Boncu, Ştefan. 2014. *Psihologie socială*. Iaşi: Editura Polirom.

6. Catrina, Geanina. 2024. „Legile internetului. Reacţii la ameninţările informaţionale". *Revista Intelligence*, 20 august 2024. https://intelligence.sri.ro/legile-internetului-reactii-la-amenintarile-informationale/.

7. Chan, Jovy. 2022. „Online Astroturfing: A Problem beyond Disinformation". *Philosophy & Social Criticism*, iunie, 01914537221108467. https://doi.org/10.1177/01914537221108467.

8. Chelcea, Septimiu. 2006. *Opinia publică. Strategii de persuasiune şi manipulare*. Bucureşti: Editura Economică.

9. CSMonitor. 2009. „The Time-Honored Practice of Astroturf Lobbying". *Christian Science Monitor*, 2009. https://www.csmonitor.com/USA/Politics/Decoder/2009/0903/The-time-honored-practice-of-Astroturf-lobbying.

10. Dobrescu, Paul şi Bârgăoanu, Alina. 2003. *Mass media şi societatea*. Bucureşti: Comunicare.ro.

11. GDPR. 2025. „General Data Protection Regulation in 2025". *ComplyDog*, 2025. https://complydog.com/blog/gdpr-in-2025.

12. Georgescu, Paul. 2024. „Vinovaţii fără vină. Diseminarea neintenţionată a mesajelor false". *Revista Intelligence*, 2024. https://intelligence.sri.ro/vinovatii-fara-vina-diseminarea-neintentionata-mesajelor-false/.

13. Ghiurgiu, Florin Mitruţ. 2024. „Infosfera şi ecourile realităţii virtuale". *Revista Intelligence*, 2024. https://intelligence.sri.ro/infosfera-si-ecourile-realitatii-virtuale/.

14. Lazarsfeld, Paul; Berelson, Bernard şi Gaudet, Hazel. 2004. *Mecanismul votului. Cum se decid alegătorii într-o campanie prezidenţială*. Bucureşti: Comunicare.ro.

15. McAfee. 2022. „How To Spot A Fake Facebook Account". *McAfee Blog*, 9 decembrie 2022. https://www.mcafee.com/learn/spot-fake-facebook-account/.

16. Merriam-Webster. 2023. „Definition of ASTROTURFING". *Merriam-Webster.com*. Accesat la 14 iulie 2023. https://www.merriam-webster.com/dictionary/astroturfing.

17. Meta. 2025. „Condiţiile de utilizare Meta". *Facebook.com*. Accesat în 2025. https://ro-ro.facebook.com/terms/.

18. Oprea, Bogdan. 2021. *Fake news şi dezinformare online: recunoaşte şi verifică*. Iaşi: Editura Polirom.

19. Roman, Dan. 2024. „Internetul, teatru de război. Militarizarea informaţiei". *Revista Intelligence*, 6 iunie 2024. https://intelligence.sri.ro/internetul-teatru-de-razboi-militarizarea-informatiei/.

20. Roşca, Tatiana. 2019. „Dinamica componentelor identităţii sociale în psihologia modernă". *Studia Universitatis Moldaviae*, nr. 9 (129).

21. Stan, Mircea. 2021. *Programul de măsuri active al KGB-GRU împotriva României (1964-1989)*. Bucureşti: Editura Militară.

22. Sturza, Cătălin. 2021. „Pericolele mesianismului politic". *Adevărul*, 27 august 2021. https://adevarul.ro/blogurile-adevarul/pericolele-mesianismului-politic-2116291.html.

23. Turner, J.C. şi Reynolds, Katherine. 2012. „Self-Categorization Theory". În *Handbook of Theories in Social Psychology*, 399-417. Londra: SAGE Publications.

24. Volkoff, Vladimir. 2009. *Tratat de dezinformare*. Bucureşti: Editura Antet.

FRANCE AND EUROPEAN STRATEGIC AUTONOMY: BETWEEN REGIONAL LEADERSHIP AND NATO COMMITMENTS

Daniel-Aurel BUCUR*

Abstract:

Amid escalating geopolitical tensions, France plays a pivotal role in shaping European security through its commitment to strategic autonomy while maintaining its NATO obligations. As one of Europe's most influential military powers, France has positioned itself as a regional leader, balancing its transatlantic commitments with its vision for a more sovereign European defence. France, a NATO founding member, has historically oscillated between transatlantic cooperation and the pursuit of an independent defence strategy. A defining moment in this regard was France's withdrawal from NATO's integrated command in 1966, under General de Gaulle, reflecting its ambition to maintain full sovereignty over its military decisions. This strategic posture, known as the Gaullo-Mitterrandism doctrine, continues to shape France's dual approach today. After decades of pragmatic cooperation, France officially rejoined NATO's integrated military structure in 2009 under President Nicolas Sarkozy, aiming to strengthen its influence within the alliance while continuing to advocate for a more self-reliant European defence.

The concept of European strategic autonomy, widely promoted by France, envisions a security framework that enables the European Union to act independently in matters of defence, economy, and technology. Initiatives such as PESCO, European Defence Fund and the Strategic Compass have been implemented to enhance Europe's military capabilities. Nevertheless, significant challenges persist: NATO remains the central pillar of security for many European Union member states, and the United States has expressed concerns about potential divergences in transatlantic defence cooperation.

Drawing on the 2022 National Strategic Review and key historical analyses, this paper examines France's dual approach—its deep-rooted commitment to NATO alongside its ambition for greater European defence autonomy. The findings highlight the inherent paradox in its strategy: while advocating for European sovereignty, France remains a key pillar of NATO's security architecture. Furthermore, the study evaluates whether France can effectively achieve its vision of a more independent European defence structure or if geopolitical realities – such as diverging strategic cultures within the European Union and controversies surrounding recent French declarations-will necessitate continued reliance on NATO. Finally, the paper assesses the long-term implications of this strategy for European security and transatlantic relations by 2030.

Keywords: *France, Gaullo-Mitterrandist doctrine, European strategic autonomy, EU-NATO relations, Defence policy.*

* PhD. student, Faculty of History and Philosophy, "Babeș-Bolyai" University, Cluj-Napoca, daniel.bucur@ubbcluj.ro

Research objectives

In this research paper, the main objective is to analyse France's role in promoting European strategic autonomy while maintaining its commitments to the North Atlantic Alliance. This dual positioning involves – reflects a long-standing tradition in French foreign policy known as Gaullo-Mitterrandism doctrine, which combines strong support for national and European sovereignty with pragmatic cooperation within NATO.

Based on this theoretical framework, the first objective is to define the concept of European strategic autonomy on the basis of the main recent theoretical and strategic contributions. A second objective is to analyse the historical and current role of France in promoting this concept, notably through its involvement in initiatives such as Permanent Structured Cooperation (PESCO), the European Defence Fund and the Strategic Compass. The third objective is to assess the main geopolitical challenges – including tensions in the Eastern Mediterranean, the war in Ukraine and internal divergences in the European Union – that may limit France's ability to promote an autonomous European defence. The final objective is to examine the implications of the French strategy for the future of European security and transatlantic relations, with a focus on the need for in-depth coordination with European partners in the context of new strategic developments and the adaptation of the EU-NATO relationship.

Research methodology

The research is based on the following methods:

1. The descriptive method is used to identify and present the strategic initiatives promoted by France in the field of European defence;
2. The analytical method is applied to examine the role of France within the European structures and NATO, as well as the relationships between these two strategic dimensions, using the Gaullo-Mitterrandist tradition as a conceptual lens for understanding France’s strategic posture;
3. The comparative method highlights the differences in vision between France and other EU Member States, such as Poland and the Baltic States, which adopt a more Atlanticist approach to security and express reservations about the idea of European strategic autonomy, preferring to base their defence on NATO commitments and the American presence in the region;

4. Documentary analysis is based on the study of primary sources (official documents of France, NATO and the European Union) and secondary sources (specialized literature, geopolitical analysis, academic and press articles).

This multi-method approach enables an integrated perspective on French strategic ambitions in a European context marked by multiple and dynamic challenges, while remaining anchored in France's unique strategic culture.

Introduction

"Allié mais non-aligné": the tradition of French strategic autonomy

France has long played a central role in promoting the idea of European strategic autonomy. This vision is part of a solid historical tradition of asserting sovereignty in the fields of defence and foreign policy, best illustrated by a doctrine known as Gaullism-Mitterrandism, formulated and theorized by Hubert Védrine, former diplomatic advisor to President François Mitterrand between 1981 and 1986, and one of the main architects of the concept of strategic autonomy applied to French foreign policy. It expresses the conviction that France must be a loyal ally, but never a subservient one. This approach presupposes a real capacity for autonomous strategic decision-making, based on its own resources, but also on political and technological influence at the European level. In the French conception, autonomy is not an isolated case, but an integral part of a geopolitical Europe that is better able to defend its interests outside the protective shadow of the United States. This was reflected in President Charles de Gaulle's decision in 1966 to withdraw France from NATO's integrated military command. This choice was based on the fundamental principle that France must retain complete freedom of judgment, decision, and action – the three dimensions that today define the concept of strategic autonomy promoted by Paris.

Strategic autonomy cannot be fully understood without first clarifying the fundamental role of sovereignty. In the European context, sovereignty refers to the ability of a state or the European Union to take autonomous decisions in areas such as defence, technology and foreign policy without undue external influence. It implies the ability to define and implement policies in accordance with its own internal priorities and strategic assessments, and not according to the agendas of other external actors.

From this perspective, strategic autonomy becomes more than a rhetorical ambition. It is the operational expression of sovereignty in a multipolar and competitive world. For France in particular, this link has deep historical roots, influenced by the Gaullist-Mitterrandist tradition, where sovereignty is not merely a legal status but a strategic necessity. European strategic autonomy implies not only institutional instruments and defence capabilities, but also a reaffirmation of Europe's capacity to act sovereign on the international stage.

This theoretical relationship between sovereignty and autonomy provides a conceptual key to understanding the rationale behind France's initiatives at the European level. It explains why autonomy, in the French vision, is inseparable from sovereignty: without the ability to decide and act independently, any aspiration to strategic autonomy remains structurally limited (Beaucillon, 2023; Védrin, 2012). This approach also highlights the internal tension in the current European Union security architecture, which is trying to balance transatlantic dependence with a growing desire to adopt an independent strategic posture.

This doctrinal continuity combines attachment to national and European sovereignty with pragmatic cooperation within NATO. This vision was taken up and consolidated in the post-Gaulle period. President François Mitterrand maintained France's doctrinal independence in the field of defence, reaffirming the importance of national nuclear deterrence and of a Europe capable of speaking with one voice. A key moment in this stance was his refusal to support the US "Star Wars program" (Strategic Defence Initiative) promoted by President Ronald Reagan in the 1980s. Unlike other US allies, Mitterrand opposed the idea of militarizing space and preferred a European strategy of balance and arms control. This gesture reinforced France's image as a sovereign actor, committed to cooperation but not automatically subject to US strategic will. Ultimately, the strategic autonomy proposed by Paris does not mean isolation or rivalry, but rather Europe's ability to face global challenges even when the transatlantic partnership is out of balance – a lesson learned from numerous tense episodes in Franco-American relations.

Later, in 2003, President Jacques Chirac refused to allow France to participate in the invasion of Iraq, expressing his veto in the UN Security Council against any resolution authorising military intervention. In a context where the United States was exerting major pressure on its NATO allies, this clear *"no"* to Washington and its allies forced them to act without international legal cover. This decision reaffirmed France's

commitment to international law and to the principle of decision-making autonomy within alliances.

In recent years, this strategic tradition has been revived under the presidency of Emmanuel Macron, who has claimed the Gaullist-Mitterrandist doctrine as his own since his 2017 election campaign. In his speech at the Sorbonne, he called for a *"sovereign, united, and democratic Europe"* capable of acting independently in the face of global challenges (Macron 2017). This vision was reinforced by strategic documents such as the Defence and National Security Strategic Review (DNSSR 2017) and National Strategic Review (NSR 2022), where strategic autonomy is presented not as a break with NATO, but as a necessary condition for the credibility and effectiveness of European action.

Even in the face of the controversy generated by his statements in 2023, following his official visit to China (Kauffmann 2023b), Macron reaffirmed his commitment to the idea that Europe must be a *"third pole"* of power, capable of deciding for itself on security and defence matters. In his view, strategic autonomy is not just a tactical option, but *"Europe's horizon"*, its historical meaning and the condition for its ability to act in a multipolar world.

This orientation was reaffirmed in March 2025, when President Macron proposed extending French nuclear deterrence to European partners, as well as deploying troops to support a peace agreement in Ukraine (Le Monde 2025). These recent initiatives show that the French vision of strategic autonomy is not limited to a discourse of principle, but seeks to be translated into political, military, and symbolic instruments, in line with a Europe capable of acting autonomously but in a coordinated manner in the face of global uncertainties.

Nevertheless, the vision promoted by France is not uniformly shared by the other members of the European Union. Countries such as Poland and the Baltic states, which are deeply attached to NATO and the US military presence, view with reservation the idea of strategic autonomy, which could be perceived as a step towards decoupling from the collective security provided by the North Atlantic Alliance.

Thus, the French vision of strategic autonomy remains both a project of European ambition and a test of political and strategic cohesion within the European Union. Its success depends not only on France's will, but also on the Union's ability to build a common vision that combines European sovereignty with transatlantic solidarity. European strategic autonomy is not a new idea, but a project of French origin that reflects a long tradition of sovereigntist geopolitical

thinking and a constant desire to strengthen Europe's ability to act independently on the international stage.

France's initiatives for European strategic autonomy

Permanent Structured Cooperation (PESCO)

France played a decisive role in the creation and development of Permanent Structured Cooperation (PESCO), which was officially established in December 2017. Alongside Germany, France was one of the main architects of this initiative, which was provided for in the Treaty of Lisbon but remained dormant for almost a decade. The activation of PESCO is a significant diplomatic victory for France, which, since the election of Emmanuel Macron, has stepped up its efforts to deepen European integration in the field of defence.

French diplomacy has worked hard to overcome the reluctance of some member states, particularly in Central and Eastern Europe, which feared that PESCO would duplicate NATO or weaken the transatlantic alliance. France had to negotiate a compromise between its initial vision of an ambitious and selective PESCO, reserved for states willing to engage in demanding projects, and the more inclusive approach advocated by Germany and other states (Calcara and Simón 2024). This compromise resulted in a two-tier PESCO: binding commitments for all participants and specific projects in which member states participate according to their capabilities and interests.

At the operational level, France is leading or participating in several strategic projects within PESCO. Among the most important are the ESSOR (European Secure Software Defined Radio) project, which aims to develop common technologies for secure military communications. France is also piloting the EURAS space surveillance project, which is essential for Europe's strategic autonomy in an increasingly contested domain. The Eurodrone project, developed in cooperation with Germany, Italy, Spain, and the Czech Republic, reflects France's ambition to equip Europe with independent surveillance and intelligence capabilities.

For France, PESCO is not just a cooperation mechanism, but a tool for gradually transforming European strategic cultures towards a more integrated vision of common defence, while maintaining compatibility with NATO – a delicate balance that reflects France's position as an *"ally but not aligned"* (Howorth 2002).

European Defence Fund (EDF)

The European Defence Fund is another major initiative in which France has had a decisive influence. Initially proposed by the European Commission in 2016, the EDF was strongly supported by Paris, which saw it as an essential tool for financing innovation and strengthening Europe's technological autonomy.

French diplomacy was particularly active in the negotiations on the EDF budget, initially supporting a budget of €13 billion for the period 2021–2027. The final allocation of €7.3 billion, although below France's desired level, nevertheless reflects concrete recognition at the European Union level of the need to invest collectively in strengthening capacity and technological autonomy in the field of defence. (European Commission, 2021).

France's influence can also be seen in the technological orientation of the EDF. Paris has actively promoted funding for sectors considered strategic: artificial intelligence applied to defence, autonomous systems, cybersecurity, and space technologies. This focus is in line with the priorities identified in French strategic documents and aims to fill European capability gaps in areas where technological dependence on the United States or other powers is considered problematic.

The industrial dimension of the EDF is particularly important for France. The rules for allocating funds, which favour transnational European consortia, are in line with the French vision of a more integrated and less fragmented European defence technological and industrial base (EDTIB). This approach reflects France's conviction that strategic autonomy necessarily requires industrial and technological sovereignty (Ianakiev, 2019).

Strategic Compass

Adopted in March 2022, the Strategic Compass is the first European defence white paper, providing a shared vision of threats and defining the European Union's strategic guidelines for the coming years. France played a leading role in its preparation, particularly during its Presidency of the Council of the European Union in the first half of 2022.

France's influence can be seen in several key aspects of the document. Firstly, the Strategic Compass explicitly takes up the concept of *"autonomous action"*, which is dear to France, and enshrines it as a political objective of the European Union. Second, it integrates the French approach to a European defence structured around four pillars: crisis management, resilience, defence capabilities, and strategic partnerships.

One of the most emblematic proposals in the Strategic Compass, with a particular focus on security in the Mediterranean and an opening towards the Indo-Pacific, a region of strategic interest to Paris due to its overseas territories. This maritime dimension illustrates France's ambition to extend the geographical scope of European strategic action beyond the continent's immediate neighbourhood.

Other significant initiatives

Beyond the institutional structures of the European Union, France has launched several complementary initiatives aimed at strengthening Europe's strategic autonomy. The European Intervention Initiative (EI2), proposed by President Emmanuel Macron in his speech at the Sorbonne in September 2017 and formalized in June 2018, is a significant example. Bringing together thirteen European states, including the post-Brexit United Kingdom, EI2 aims to develop a common strategic culture and facilitate joint military commitments, independently of the structures of the European Union or NATO (Ministry of the Armed Forces 2021).

In response to the war in Ukraine, France has been at the forefront of promoting the concept of a *"war economy"*. At the European Union Defence Conference held in Brussels in February 2023, President Emmanuel Macron called for a profound transformation of the European defence industry to drastically increase production capacity. This initiative, inspired by the EDIDP (European Defence Industrial Development Program), aims to remedy the structural weaknesses highlighted by the Ukrainian conflict: insufficient ammunition stocks, vulnerable supply chains, and limited production capacities (Macron 2017).

More recently, in March 2025, President Emmanuel Macron proposed extending France's nuclear deterrence to its European partners as part of a *"strategic dialogue"* on the role of France's strike force in defending the continent. This proposal, which echoes similar suggestions made during François Mitterrand's presidency, illustrates France's desire to assert its strategic leadership in Europe, building on its status as the European Union's sole nuclear power since Brexit (Melander and Rose 2025).

Analysis of French strategic documents

Strategic Analysis of National Defence and Security (2017)

Published a few months after Emmanuel Macron's election, the 2017 Strategic Analysis marks a turning point in the French conceptualization of European autonomy. The document establishes a

direct link between French national sovereignty and the construction of a more strategically autonomous Europe.

For France, the analysis defines Europe as a *"power multiplier"*, emphasizing that *"the defence of Europe also involves building European strategic autonomy, complementary to the Atlantic Alliance"* (DNSSR 2017). This nuanced wording reflects the balance that France is trying to maintain between its European commitment and its participation in NATO.

The analysis of transatlantic relations in this document is particularly revealing. Without questioning the fundamental importance of NATO for European security, the assessment highlights a strategic uncertainty linked to the evolution of US foreign policy, particularly since the election of Donald Trump and the start of his term in 2017. Perceived as unpredictable and sometimes critical of the Alliance, this new context has fuelled fears in France of a possible withdrawal of US commitment to Europe. Consequently, the document justifies the need to accelerate European efforts to strengthen its own defence capabilities as a form of insurance against possible repositioning by its transatlantic partner.

In terms of capabilities, the review identifies several priority areas that France will then promote within European initiatives: intelligence, cyber defence, missile defence, force projection, and resilience to hybrid threats. These priorities reflect the ambition for a comprehensive European defence capable of operating across the entire spectrum of contemporary threats.

Strategic update (2021) and national review (2022)

The 2021 strategic update, followed by the 2022 national strategic review, reflects an intensification of French discourse on European strategic autonomy in the face of an increasingly unstable international environment. These documents incorporate the lessons learned from several major crises: the COVID-19 pandemic, which exposed the vulnerabilities of strategic supply chains, and the Russian invasion of Ukraine, which marked the return of conventional warfare to Europe.

The 2022 review considerably broadens the concept of strategic autonomy, which is no longer limited to defence but now encompasses energy, technology, industry, and health. This holistic approach is presented as a necessity in the face of strategic competition between major powers, which *"is now taking place in all areas and involves all actors"* (NSR 2022).

The document also introduces a more pragmatic approach to EU-NATO relations. While the ambition for autonomy remains intact, France

recognizes that, in the short term, the Russian threat reinforces the importance of the US security umbrella for Europe. Strategic autonomy is therefore presented as a medium-term objective to be pursued in parallel with the strengthening of the European pillar of NATO.

The 2022 analysis attaches particular importance to contested spaces (cyberspace, space, the seabed) and critical technologies (semiconductors, artificial intelligence, quantum technology), identified as areas where European autonomy is particularly threatened. This analysis has had a direct influence on France's proposals at European level, particularly with regard to the orientation of EDF funding and the industrial defence strategy.

Assessment of the practical impact of France's proposals

Tangible achievements

The assessment of the practical impact of the initiatives promoted by France shows that, beyond the declaratory dimension, there is real progress towards European strategic autonomy. At the institutional level, the launch of PESCO and the operationalization of the EDF have strengthened the framework for defence cooperation, and France's role in shaping these instruments has been decisive.

From a strategic point of view, the adoption of the Strategic Compass marked an important step towards a common vision at European level. France has succeeded in incorporating its guidelines into this document, from the idea of "autonomous capacity to act" to the emphasis on the southern neighbourhood and the Indo-Pacific region. At the same time, the proposal for a European rapid reaction force by 2025 confirms the transition from principles to instruments.

On the industrial front, projects such as Future Combat Air System (FCAS) and Eurodrone—already mentioned above—reflect the desire to reduce dependence on non-European technologies. Even if these programs are marked by coordination difficulties, they remain a sign of the maturing of European cooperation in critical areas (Ianakiev 2019).

In terms of operational capabilities, France has demonstrated its ability to initiate and lead European missions in diverse contexts: in the Sahel, through Task Force Takuba, and in the Mediterranean, through the IRINI naval operation. Although not all of these have reached their intended scale, they demonstrate Europe's potential for strategic projection in its immediate neighbourhood.

The balance sheet is therefore mixed: French initiatives have catalysed a number of relevant changes in the European defence

architecture, but their implementation is often hampered by political resistance, budgetary constraints, and the lack of a robust strategic consensus at the EU level.

Constraints and obstacles

Despite this progress, several obstacles limit the impact of French initiatives. Considerable political resistance persists, particularly from member states that favour an Atlanticist approach to security. Poland and the Baltic states, in particular, are skeptical about the idea of European strategic autonomy, which they see as potentially weakening NATO's guarantees against the Russian threat.

In financial terms, the resources available are often disproportionate to the ambitions set. Although important instruments such as the European Defence Fund have been launched, the resources available do not, in their current form, allow for the desired qualitative leap in common strategic capabilities. In addition, most member states continue to fall short of the 2% of GDP target for defence spending, despite repeated calls from France.

There are also contradictions between rhetoric and practice: although France promotes the integration of the European defence industry, its arms exports often favour national interests. Similarly, simultaneous support for initiatives within and outside the EU framework – such as PESCO and the IEI – raises questions about Paris's strategic coherence.

Finally, Europe's structural dependence on US capabilities remains pronounced in key areas: reconnaissance satellites, strategic transport, and missile defence. This technical and operational reality objectively limits the full applicability of the concept of European strategic autonomy, even in its pragmatic version.

Partner perceptions

The reception of French initiatives varies considerably from one European partner to another. Germany, despite its strong attachment to the transatlantic framework, has gradually moved closer to the French position on the need for greater European autonomy, particularly since the Australian submarine crisis in 2021, which shook confidence in the American partnership.

On the other hand, Central and Eastern European countries, as well as some Nordic countries, continue to view with suspicion what they see as an attempt by France to impose its geopolitical vision on the Union as a whole. The proposal to extend France's nuclear deterrence, in

particular, has met with mixed reactions, with some considering it an inadequate alternative to US guarantees (Tisdall 2025).

On the American side, the Biden administration has adopted a more conciliatory approach than its predecessor towards European defence initiatives, expressing support for strengthening European capabilities as long as they remain compatible with NATO and contribute to a fair burden-sharing. Nevertheless, significant reservations remain regarding the industrial and technological dimension of strategic autonomy, which is sometimes perceived as protectionist and potentially contrary to US commercial interests (Besch 2021).

Internationally, Russia and China are closely monitoring the development of European strategic autonomy. For Moscow, these initiatives are generally seen as a means of reducing US influence in Europe, which could theoretically serve Russia's interests. Beijing, for its part, sees the emergence of a more autonomous Europe as a potential counterweight to American hegemony in a multipolar world, while expressing concern about a possible consolidation of the Western bloc (Sabanadze and al. 2024).

An interim assessment

The results of France's initiatives in favour of European strategic autonomy are mixed. On the one hand, Paris has undeniably succeeded in putting this concept on the European agenda and giving it substance through significant institutional progress (PESCO, EDF, the Strategic Compass). France's conceptual influence on the definition of European strategic guidelines has been considerably strengthened.

On the other hand, there is still a significant gap between stated ambitions and concrete achievements. Europe remains largely dependent on US security guarantees, particularly in the context of the Russian threat, and autonomous European capabilities are still in their infancy in many key areas.

Nevertheless, French initiatives have contributed to a European awareness of the need for greater strategic resilience. The war in Ukraine, Sino-US tensions, and political uncertainties in the United States have gradually convinced even the most Atlanticist member states that Europe must strengthen its capacity for autonomous action, at least as an "insurance policy" against geopolitical dangers.

In the short term, the dynamics seem to favour continued efforts toward greater strategic autonomy, but with a pragmatic approach that recognizes current constraints and the need to maintain a strong transatlantic partnership. Ultimately, this evolution fits quite well with

the French vision of autonomy "not against NATO, but within NATO" (Védrine 2012), reflecting the Gaullist principle of *being an ally, but not aligned.*

European reactions and differences

France's proposal on European strategic sovereignty has sparked contrasting reactions from member states, revealing divergent views on the security architecture of the European continent.

Mapping member states' positions

Member states' positions on strategic autonomy can be grouped into three broad categories.

The first group, in favour of a more autonomous Europe, includes France, Spain, Italy, and Greece. These Mediterranean states actively support the strengthening of European capabilities, given both the instability in their southern neighbourhood and their own security interests. Greece's position is emblematic: it supports the French vision of strategic autonomy, as demonstrated by the defence agreement signed with France on September 28, 2021. This agreement provides not only for deeper military cooperation, but also for the purchase of Belhara frigates and Rafale multi-role aircraft. Nevertheless, this European orientation coexists with a strengthened strategic partnership with the United States, as evidenced by the renewal of the bilateral defence agreement in 2019 and the expansion of the US military presence in Greece. This ambivalent position is largely explained by the perception of Turkey – a NATO member – as a direct threat to Greece's security. The Greek case thus illustrates how regional geopolitical considerations have a concrete influence on member states' positions on the idea of European strategic autonomy (Mitsotakis 2021).

An intermediate group, consisting of Germany, Belgium, and the Netherlands, takes a more nuanced position. These countries support the development of European capabilities while insisting on complementarity with NATO. Germany, in particular, embodies this ambivalence: despite announcing a "Zeitenwende" and an exceptional €100 billion defence fund in the wake of the Russian invasion of Ukraine, Berlin has largely focused its procurement on American equipment, notably the F-35 (Malté and al. 2022; Le Monde 2022).

A third group, consisting mainly of Poland, the Baltic states, and other countries in Central and Eastern Europe, strongly favours the transatlantic framework. For these nations, the American guarantee is

a vital insurance against Russian threats, and any initiative that could weaken NATO arouses instinctive mistrust.

Disagreements between the French vision and the Atlanticist approach

Several doctrinal rifts explain these disagreements. The very concept of relations with NATO pits the French vision of independent action against the fear of transatlantic decoupling among the most Atlanticist countries. President Emmanuel Macron's statements on the "brain death" of NATO in 2019 crystallized these tensions, provoking strong reactions in Central and Eastern Europe (The Economist 2019).

Strategic priorities also differ significantly: while countries on the eastern flank focus on deterring Russia, France has historically paid more attention to threats from the south (terrorism, regional instability). Although the war in Ukraine has partially reduced this divergence, priorities remain different.

Another point of difference is the industrial dimension. Countries with a big industrial and tech base in defence (France, Italy, Spain) have a direct interest in promoting European preference, unlike importing countries, which often prefer American equipment because of cost and immediate interoperability.

Case studies reveal

Poland is a perfect illustration of the reluctance to accept the French concept of strategic autonomy. After its historical experience with Russia, Warsaw considers the American guarantee to be non-negotiable. Poland has invested heavily in its defence (almost 4% of GDP), favouring US equipment such as F-35s, Patriot systems, Abrams tanks (The Economic Times 2023). Nevertheless, Poland participates pragmatically in certain European projects, such as the Permanent Structured Cooperation (PESCO), revealing a selective approach guided by its national interests.

Germany presents a different but equally revealing case. Berlin feels torn between its ambition to become a European leader and its dependence on the United States for security. This tension can be seen in the difficulties of the Future Combat Air System (FCAS) project with France, where industrial differences reflect different strategic conceptions. Germany currently favours a vision of open strategic autonomy, seeking to reconcile European consolidation with transatlantic solidarity (Major and Mölling 2020).

The Baltic states, despite their deep attachment to NATO, show some nuances. Estonia is particularly involved in discussions on European digital sovereignty, an area in which it has recognized expertise, while Lithuania actively supports the European military mobility initiative, which complements NATO's efforts (Wright 2021; Šešelgytė 2018).

Structural determining factors

These national positions are largely explained by deep-rooted structural factors. Historical legacy plays a decisive role: the experience of Soviet domination for Central and Eastern European countries contrasts with France's tradition of strategic independence. Geography also has a direct influence on these perceptions, with proximity to Russia naturally reinforcing the importance attached to the US guarantee.

National strategic cultures differ fundamentally: the French tradition of external intervention and global status differs considerably from the defensive territorial approach favoured by several member states. These conceptual differences transcend traditional political divisions and persist beyond changes of government.

Despite these differences, the war in Ukraine has encouraged the emergence of a renewed pragmatism. A minimal consensus is emerging around concrete projects such as military mobility and cyber defence, which allows progress to be made on the technical aspects of strategic autonomy while temporarily avoiding deeper conceptual disagreements. This gradual approach, which favours concrete achievements over major theoretical debates, characterizes the recent evolution of the European debate on strategic sovereignty.

Discussions

NATO-EU relations: complementarity or rivalry?

The relationship between NATO and the European Union is the real Gordian knot in the debate on European strategic autonomy. Far from being a mere technical and institutional issue, this relationship encapsulates the fundamental tensions between the aspiration for European sovereignty and the realities of transatlantic cooperation. France, the main promoter of strategic autonomy, consistently argues that this should not be a break with NATO, but rather a strengthening of Europe's ability to act when necessary. Nevertheless, for some member states and analysts, the French vision risks fuelling perceptions of

institutional rivalry with NATO, highlighting fundamental differences on the future of the continent's security architecture.

Analysis of the concept of "open strategic autonomy"

The concept of "strategic autonomy" has evolved significantly since its emergence. Initially limited to the military sphere in the 2010s, it has gradually expanded to encompass other dimensions. As highlighted in the article Toute l'Europe, "the Covid-19 pandemic has changed the rules of the game, exposing European dependencies" (Lictevout 2020), extending the concept to include health, technological, and economic aspects.

The addition of the adjective "open" in 2020, at the instigation of the German Presidency of the European Union, marks an attempt to reconcile French ambitions for independence with the concerns of the most Atlanticist countries. While this formulation has allowed a diplomatic convergence, it has also introduced ambiguity in defining the true extent of independence envisioned by France. This qualification explicitly signals that this autonomy is part of a partnership framework, particularly with NATO and the United States, and does not aim at strategic autarky. As High Representative Josep Borell stated, *„Enhancing our strategic autonomy goes hand in glove with the strengthening of our relations with partners."* (European Defence Agency 2020).

Nevertheless, there are inherent ambiguities in this compromise wording. For supporters of a classic French vision, it risks diluting the initial ambition of decision-making independence. For staunch Atlanticists, autonomy, even "open," continues to suggest a potential weakening of NATO's primacy. The polysemy of the term certainly allows for political progress, but at the cost of some conceptual confusion.

President Emmanuel Macron has linked this concept to that of *"European sovereignty," stating that "our Europe [...] must acquire greater strategic autonomy,"* (Macron 2024) particularly in the area of defence. This association between sovereignty and strategic autonomy reinforces the political dimension of the concept, beyond its military and capacity aspects.

Assessment of the compatibility of European initiatives with NATO

The compatibility of European defence initiatives with NATO is the subject of divergent assessments, reflecting underlying tensions related to strategic autonomy.

Permanent Structured Cooperation (PSC), although initially presented as complementary to NATO, has raised concerns about possible duplication. As a result, the first PSC projects were carefully selected to fill capability gaps identified by NATO, such as military mobility. The latter, dubbed the "military Schengen," illustrates the potential for complementarity: NATO defines infrastructure standards, while the European Union finances and develops cross-border road and rail networks.

The European Defence Fund (EDF), with a budget of €7.3 billion for the period 2021-2027, has become a focal point of debate: some present it as a tool to strengthen NATO's European pillar, while others fear that its rules – especially on "third countries" participations – overly favour the European defence industrial base and disadvantage transatlantic partners. (European Commission 2023; Santopinto 2025)

In its military dimension, European strategic autonomy generally refers to the EU's capacity to act autonomously in defence, while remaining able to cooperate with partners Damen 2022). Nevertheless, this ambition faces potential contradictions between the development of a European defence industrial and technological base and the imperatives of interoperability with NATO, where American standards prevail.

The American perception of French ambitions

The American perception of European initiatives for strategic autonomy has evolved considerably since the early 2000s, oscillating between mistrust and conditional encouragement.

The Bush administration expressed significant reservations about the first European defence initiatives, fearing the "3Ds": decoupling, duplication, and discrimination (towards allies outside the EU). This mistrust crystallized during the Iraq crisis in 2003, pitting the "old Europe" against the more Atlanticist "new Europe" (Hunter 2002).

The Obama administration adopted a more nuanced position, encouraging greater burden-sharing while maintaining reservations on certain industrial issues. Secretary of State Hillary Clinton made US support conditional on strategic autonomy that would strengthen NATO rather than compete with it.

Paradoxically, the arrival of Donald Trump has helped legitimize discussions on European strategic autonomy. His virulent criticism of NATO and his pressure on allies have reinforced the French argument for the need for strategic assurance. As President Macron pointed out*, "The paradox would be that, at the moment when we implement the elements of*

genuine European strategic autonomy, we start following US policy out of a kind of panic reflex." (Da Sois 2023).

The Biden administration has proposed a more sophisticated approach, verbally supported a strengthened European defence pillar while maintained precise "red lines." The letter sent by the Pentagon to the European Commission in 2021, expressing concern about US companies' access to the FED, illustrates this ambivalent position. Washington supports a more capable Europe militarily but remains vigilant on industrial and commercial issues.

Recent geopolitical developments, notably the war in Ukraine, have temporarily brought the transatlantic partners closer together around a common goal. Nevertheless, structural differences remain, fuelled by competing industrial interests and different visions of the international order.

The economic and industrial dimension of strategic autonomy, highlighted in the above-mentioned article *Toute l'Europe*, is currently a major point of divergence. The European Union is seeking to "protect European companies and strategic sectors" from potentially hostile foreign investment, in particular through the foreign investment screening mechanism adopted in 2019, which may come into tension with US economic interests in Europe.

This complex relationship between NATO and the EU reflects deeper questions about the future of the transatlantic link. European strategic autonomy thus lies at the intersection of geopolitical, economic, and identity considerations that go far beyond the technical aspects of defence. It fundamentally raises the question of the role Europe intends to play on the international stage and its relationship with its American ally in a rapidly changing multipolar world.

The structural challenges of European autonomy

The ambition for European strategic autonomy faces several fundamental obstacles that go beyond mere circumstantial considerations. These structural challenges, rooted in the industrial, cultural, and political realities of the continent, require a systematic approach to be overcome.

Industrial capabilities and constraints

Despite consolidation efforts, the European defence industrial landscape remains fragmented. This fragmentation leads to costly redundancies, with several countries developing similar systems without pooling resources. The absence of a genuine single defence market limits

economies of scale and undermines the competitiveness of European companies on global markets (Clapp and al. 2025).

Critical technological dependencies persist in strategic areas such as advanced semiconductors, certain weapon systems, and essential electronic components. These vulnerabilities compromise Europe's decision-making and operational autonomy, particularly in crisis situations. In addition, Europe lags far behind in disruptive technologies– artificial intelligence, quantum, advanced space – that will define tomorrow's military capabilities.

Insufficient interoperability between the equipment of different national armed forces is also a major obstacle to joint effectiveness, limiting the capacity for collective action in the face of threats.

Divergent strategic cultures

Europe is characterized by a mosaic of strategic cultures shaped by history, geography, and national experience. These differences can be seen even in the perception of priority threats: Eastern European countries generally consider Russia to be their main security concern, while Mediterranean countries are more concerned about instability in the Middle East and North Africa.

This heterogeneity is also reflected in attitudes toward NATO and the United States. Central and Eastern European countries often favour the American security guarantee, while others, led by France, advocate greater European autonomy. National traditions regarding the use of force differ profoundly: countries such as France and the United Kingdom have an interventionist strategic culture and extensive experience in foreign operations, while others take a more reserved approach to the use of military force. These conceptual differences complicate the emergence of a common strategic vision, which is essential for any real European autonomy.

Budgetary constraints and political will

Despite growing awareness of the need to invest in defence, accelerated by the conflict in Ukraine, overall European defence investment remains insufficient to support real strategic autonomy. There are considerable disparities between Member States, with some reaching or exceeding the NATO target of 2% of GDP, while others remain well below this target.

The mobilization of common resources to finance major capability programs faces deep-rooted political reluctance. National budgetary decisions often tend to favour other priorities perceived as

more urgent by public opinion. Defence is still largely considered a national prerogative, which makes it difficult to pool efforts.

These financial constraints come against a tense economic backdrop marked by post-pandemic debt and the challenges of the green transition, which are creating competition for limited resources. European strategic autonomy requires sustained political will that transcends electoral cycles, something that is still lacking in many Member States.

Outlook for 2030

Prospective analysis of possible developments

The evolution of strategic autonomy by 2030 could follow several trajectories, depending on internal and external factors. In short, the European Union appears to be committed to a gradual strengthening of its autonomous capabilities, driven by recent geopolitical tensions. The European Defence Fund and the European Peace Fund testify to an institutional determination to increase common resources.

Recent developments confirm this dynamic. In February 2025, the European Commission launched the first call for proposals under the European Defence Investment Program (EDIP), mobilizing €1.5 billion until 2027 for the joint production of high-priority military equipment. This initiative demonstrates an awareness of the crucial role of EU funding in complementing national efforts. It marks an important step towards the development of a more integrated and competitive European defence industry capable of meeting the capability needs of Member States.

Between now and 2030, there are three main paths forward. The first would be a substantial acceleration of defence integration, with the effective creation of a genuine European rapid reaction force and the implementation of major joint capability programs such as FCAS (Future Combat Air System) or NGCS (Main Ground Combat System). This development would enable Europe to assert itself as a coherent strategic actor.

The second, more modest trajectory would consist of "variable geometry autonomy," in which groups of member states would move forward together in specific areas while maintaining the current security architecture, which is largely dependent on NATO. This pragmatic approach could lead to the emergence of European "coalitions of the willing" on specific issues.

The third, more pessimistic trajectory would see European efforts fragment in the face of economic pressures and persistent strategic divergences, compromising ambitions for autonomy.

The factors determining the success of strategic autonomy

The degree of strategic autonomy achieved by Europe in 2030 will depend on several critical factors. First, the political coherence of Member States and their ability to define common strategic interests. Without a minimum consensus on priority threats and the means to respond to them, efforts will remain fragmented and ineffective.

The level of financial investment is a second determining factor. Joint European investments are beginning to materialize through flagship programs such as EDIP and the €1.5 billion for the period 2025-2027 to stimulate joint production of priority defence equipment. This initiative demonstrates an awareness of the crucial role of EU funding in complementing national efforts. Nevertheless, the scale of these investments will need to increase significantly in the coming years to meet the ambitions for strategic autonomy, particularly in the face of challenges related to technological innovation and the need to modernize Europe's armed forces.

The success of this quest for autonomy will also depend on strengthening Europe's defence technological and industrial base. The EDIP program aims precisely to address the critical defence capability shortfalls identified, while strengthening this industrial base. Without competitive and integrated industrial capabilities, Europe will remain dependent on external suppliers for critical equipment. Progress in emerging technologies (cyber, space, AI) will be particularly decisive.

A significant breakdown in transatlantic relations or increased instability at Europe's borders could act as a catalyst for autonomy efforts, while a strengthening of US engagement could, conversely, slow down the process.

Conclusions

European strategic autonomy is now not just a theoretical concept or a political aspiration, but a necessity imposed by an increasingly volatile international context. France, through its Gaullist-Mitterrandist tradition and the initiatives it has launched in recent decades, has established itself as the main promoter of this idea, succeeding in profoundly influencing the European Union's strategic agenda. From the

launch of PESCO and the EDF to the adoption of the Strategic Compass and the initiation of discussions on extended nuclear deterrence, Paris has consistently sought to transform Europe into an autonomous actor capable of responding to global challenges without relying exclusively on the American security umbrella.

Nevertheless, the road to autonomy is strewn with major structural and political obstacles: fragmentation of defence industries, cultural and strategic divergences between member states, budgetary hesitations, and the lack of a clear consensus on the future of the transatlantic relationship. Furthermore, the perception of partners – whether European, American or strategic rivals – remains ambivalent, oscillating between conditional support and suspicion.

In this complex equation, France plays an essential role, but not one that is sufficient on its own. The future of European strategic autonomy will depend on the Union's ability to move forward collectively, through concrete initiatives, sustained investment, and a shared vision of its role in the multipolar world of the 21st century. In this perspective, what is at stake is not only operational autonomy, but the definition of Europe's geopolitical identity in the coming decades.

Bibliography

1. Arteaga, Felix and al. 2016 Nov. Appropriate Level of European Strategic Autonomy #8. Report. Armament Industry European Research Group. https://www.iris-france.org/wp-content/uploads/2016/11/ARES-Group-Report-Strategic-autonomy-November-2016.pdf

2. Barré, Nicolas. 2023 Apr 11. L'autonomie stratégique doit être le combat de l'Europe ? Les Échos ; p. 6.

3. Beaucillon Charlotte. 2023. Strategic autonomy : a new identity for the EU as global actor. European Papers Vol. 8, 2023, No 2, pp. 417-428 (European Forum, 27 July 2023), pp. 417-428.https://www.europeanpapers.eu/europeanforum/strategic-autonomy-new-identity-eu-global-actor.

4. Beaucillon Charlotte. 2023. Strategic autonomy : a new identity for the EU as global actor. European Papers Vol. 8, 2023, No 2, pp. 417-428 (European Forum, 27 July 2023), pp. 417-428.https://www.europeanpapers.eu/europeanforum/strategic-autonomy-new-identity-eu-global-actor.

5. Bellouard, Patrick. 2021. La coopération européenne en matière d'armement, outil de l'autonomie stratégique de l'Europe. Administration, 272(4), 28-30. https://doi.org/10.3917/admi.272.0028.

6. Besch, Sophia. 2021 Dec 22. Rebooting the U.S. – EU Defense Relationship. Carnegie Endowment for International Peace. American-German Institute. https://americangerman.institute/publication/rebooting-the-u-s-eu-defense-relationship/

7. Boniface, Pascal. 2018. Why the Concept of Gaullo-Mitterrandism Is Still Relevant. Revue internationale et stratégique, No 109(1), p. 22-35. https://shs.cairn.info/journal-revue-internationale-et-strategique-2018-1-page-22?lang=en

8. Borrell, Josep. 2020 Dec 4. European Defence Agency: Remarks by the High Representative/Vice-President Josep Borrell at the annual virtual conference. https://www.eeas.europa.eu/eeas/european-defence-agency-remarks-high-representativevice-president-josep-borrell-annual-virtual_en?

9. Bozo, Frédéric. 1995. La France et l'Alliance: les limites du rapprochement. *Politique étrangère.* Vol. 60, No. 4 (HIVER 1995/1996), p. 865-877. www.jstor.org/stable/42675442

10. Calcara, Antonio, and Luis Simón. 2024. "Face to Face: France, Germany and the Future of the European Defence Industry."*Journal of European Public Policy*, June, p. 1–25. https://doi.org/10.1080/09662839.2025.2500296

11. Clapp, Sebastien and al. 2025 Sep 22. *Building a Common Market for European Defence.* EPRS-European Parliamentary Research Service Briefing – Brussels. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775924

12. Comité 1. 2022. Defence and European Strategic Autonomy: Harmonising The response capability Of nato And the eu. Revue Défense Nationale, No 849(4), p. 59-65. https://shs.cairn.info/journal-revue-defense-nationale-2022-4-page-59?lang=en

13. Comité 2. 2021. European Strategic Autonomy: How to Achieve Commitment to the Principle? Revue Défense Nationale, No 836(1), p. 21-25. https://shs.cairn.info/journal-revue-defense-nationale-2021-1-page-21?lang=en

14. Cour des comptes France. 2018 Apr 17. Rapport. La coopération européenne en matière d'armement. https://www.ccomptes.fr/fr/publications/la-cooperation-europeenne-en-matiere-darmement

15. Da Sois, Julien. 2023 Apr 12. Macron réaffirme l'importance de «l'autonomie stratégique» de l'Europe face à la Chine et aux États-Unis. Le Figaro. https://www.lefigaro.fr/conjoncture/macron-reaffirme-l-importance-de-l-autonomie-strategique-de-l-europe-face-a-la-chine-et-aux-etats-unis-20230409

16. Damen, Mario. 2022 Jul 08. *EU strategic autonomy 2013-2023. From concept to capacity.* EPRS-European Parliamentary Research Service Briefing-Brussels. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589

17. De Gliniasty, Jean. 2017. Autour du gaullo-mitterrandisme. Revue internationale et stratégique, 107(3), p. 175-179. https://doi.org/10.3917/ris.107.0175

18. Defence and National Security Strategic Review (DNSSR). 2017. https://www.defense.gouv.fr/sites/default/files/dgris/Defence%20and%20National%20Security%20Strategic%20Review%20-%202017.pdf

19. Deschaux-Dutard, Deplphine. 2023. Europe de la défense, un mirage stratégique? Politique étrangère, Automne (3), 49-60. https://doi.org/10.3917/pe.233.0049

20. Dumoulin, André. 2025. La France et l'OTAN : vers la normalisation ? https://shs.cairn.info/revue-courrier-hebdomadaire-du-crisp-2008-20-page-5.

21. European Commission. 2023. *European Defence Fund (EDF)*, Brussels. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

22. European Defence Agency. 2020. https://eda.europa.eu/publications-and-data/all-publications/annual-report-2020

23. Favin Lévêque, Jacques. 2021. Comment définir l'autonomie stratégique européenne? Revue Défense Nationale, 841(6), 129-132. https://doi.org/10.3917/rdna.841.0129

24. Giegerich, Bastian. 2019. Franco-German Cooperation in Security, Defense, And European Strategic Autonomy. Revue Défense Nationale, No 821(6), p. 43-49. https://shs.cairn.info/journal-revue-defense-nationale-2019-6-page-43?lang=en

25. Giegerich, Bastian. 2019. Franco-German Cooperation in Security, Defense, And European Strategic Autonomy. Revue Défense Nationale, No 821(6), p. 43-49. https://shs.cairn.info/journal-revue-defense-nationale-2019-6-page-43?lang=en

26. Giuliani, Jean-Dominique. 2022a. L'autonomie stratégique européenne. Dans Publication couronnée par J. Holeindre et J. Fernandez Annuaire français de relations internationales : 2022. p. 417-433. Éditions Panthéon-Assas. https://doi.org/10.3917/epas.ferna.2022.01.0417

27. Giuliani, Jean-Dominique. 2022b. Renforcer l'autonomie stratégique de l'Union européenne face aux défis sécuritaires d'aujourd'hui. Cahiers de la sécurité et de la justice, 55(2), p. 76-85. https://doi.org/10.3917/csj.055.0076.

28. Gouttefarde, Fabien. 2021 Nov 9. Défense : cinq and de plus pour l'ambition de l'autonomie stratégique. La Tribune no. 7263.

29. Grandin Jade, de l'Eprevier. 2023 Apr 13. Macron a-t-il flingué l'autonomie européenne ? L'Opinion ; p. 1,7.

30. Grieco, A. Kelly. 2024 Jul 2. Albright's 3Ds: Dependency, Dependency, Dependency. Stimson Center.https://www.stimson.org/2024/albrights-3ds-dependency-dependency-dependency/

31. Howorth, Jolyon. 2002. La France, l'OTAN et la sécurité européenne : statu quo ingérable, renouveau introuvable. *Politique étrangère*, HIVER 2002-

2003. Vol. 67, No. 4 (HIVER 2002-2003), p. 1001-1016. Published by : Instiut Français des Relations Internationales. www.jstor.org/stable/42676018

32. Hunter, E. Robert. 2002. The European Security and Defense Policy. NATO's Companion – or Competitor? Chapter Six – THE THREE *Ds*-AND A FOURTH, p. 33-44. Santa Monica, CA: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1463/RAND_MR1463.pdf

33. Ianakiev, Gueorgui. 2019 Nov 29. *The European Defence Fund: A Game Changer for European Defence Industrial Collaboration?* ARES Group Policy Paper no. 48, November 2019. Paris: IRIS. https://www.iris-france.org/wp-content/uploads/2019/11/ARES-48.pdf.

34. IHEDN. 2021. Union européenne et enjeux de défense: les défis de l'autonomie stratégique européenne. Revue Défense Nationale, 836(1), p. 7-11. https://doi.org/10.3917/rdna.836.0007

35. Kauffman, Sylvie. 2020a Dec 3. Sortir du piège de l'autonomie stratégique. Le Monde ; p.39.

36. Kauffman, Sylvie. 2023b Apr 9. Les clivages de l'autonomie stratégique. Le Monde ; p.28.

37. Lasserre, Isabelle. 2017 Jun 21. Emmanuel Macron au *Figaro*: «L'Europe n'est pas un supermarché ». Le Figaro. https://www.lefigaro.fr/international/2017/06/21/01003-20170621ARTFIG00333-emmanuel-macron-l-europe-n-est-pas-un-supermarche.php

38. Le Monde. 2022 Dec 16. *Germany struggles to modernize its army.* https://www.lemonde.fr/en/international/article/2022/12/16/germany-struggles-to-modernize-its-army_6008006_4.html

39. Le Monde. 2025 Mar 5. "Macron Says He Will Open Debate on Using French Nuclear Deterrence to Protect Europe." https://www.lemonde.fr/en/international/article/2025/03/05/macron-says-he-will-open-debate-on-using-french-nuclear-deterrence-to-protect-europe_6738859_4.html.

40. Lefebvre, Maxime et Simon, Édouard. 2021. L'autonomie stratégique européenne, nouveau projet commun ? Revue internationale et stratégique, 122(2), p. 95-103. https://doi.org/10.3917/ris.122.0095

41. Macron, Emmanuel. 2017 Sep 26. *Initiative for Europe: A sovereign, united, democratic Europe*. Speech delivered at the Sorbonne. https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe

42. Macron, Emmanuel. 2019 Nov 7. "*Emmanuel Macron warns Europe: NATO is becoming braind-dead".* The Economist. https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead

43. Macron, Emmanuel. 2024 Apr 25. *Speech on Europe*. Speech delivered at the Sorbonne. https://www.elysee.fr/en/emmanuel-macron/2024/04/24/europe-speech

44. Major, Claudia and Mölling Christian. 2020 Oct 13. *Europe Germany and defense: priorities and challenges of the german EU presidency and the way*

ahead for European Defense. Note no. 63/20. Paris : Fondation pour la Recherche Stratégique, 2020. https://www.frstrategie.org/en/publications/notes/europe-germany-and-defense-priorities-and-challenges-german-eu-presidency-and-way-ahead-european-defense-2020

45. Malté, Aylin and al., 2025. *Assessing the Zeitenwende: Implications for Germany, the United States, and Transatlantic Security* (Carlisle Barracks, PA: US Army War College Press, 2025), https://press.armywarcollege.edu/monographs/976

46. Maulny, Jean-Pierre. 2019. Vers une autonomie stratégique européenne. Revue Défense National n° 821.

47. Melander, Ingrid and Rose Michel. 2025 Mar 5. Reuters. "Macron will open debate about extending French nuclear protection to European allies." https://www.reuters.com/world/europe/frances-macron-address-nation-late-wednesday-2025-03-05/

48. Ministère des Armées. *Strategic Update 2021*. Paris: Ministère des Armées, 2021. https://archives.defense.gouv.fr/content/download/605304/10175711/file/strategic-update%202021.pdf.

49. Mitsotakis, Kyriakos, (2021). *Prime Minister Kyriakos' remarks after the signing of the Greece-France strategic partnership for defence and security*. Athens, 28 September 2021. https://www.primeminister.gr/en/2021/09/28/27610

50. National Strategic Review (NSR). 2022. https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf

51. Ouvry, Louis. 2022. La difficile « voie française » au sein de l'OTAN et ses enjeux. *DSI (Défense et Sécurité International)*, Mars-Avril 2022, No. 158 (Mars-Avril 2022), p. 88-91. www.jstor.org/stable/10.2307/48651840

52. Pszczel, Robert. 2024 Nov 15. Europe's security without America: an imperative of the moment or a dangerous idea? Center for Eastern Studies. https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-11-15/europes-security-without-america-imperative-moment-or-a

53. Sabanadze, Natalie and al. 2024 Jun 26. Report. China-Russia alignment: a threat to Europe's security. A report by MERICS, Chatham House and GMF. https://merics.org/en/report/china-russia-alignment-threat-europes-security

54. Santopinto, Frederico. 2025 Jun 17. *The involvement of Third-Country Entities in EU Defence Programmes.* Paris : IRIS/ARES. https://www.iris-france.org/en/the-involvement-of-third-country-entities-in-eu-defence-industrial-policies-and-the-european-design-authority-concept/

55. Scholz, Olaf. 2022 Dec 5. The Global Zeitenwende. *How to Avoid a New Cold War in a Multipolar Era*. Foreign Affairs [update Jan/Feb 2023]. https://www.foreignaffairs.com/germany/olaf-scholz-global-zeitenwende-how-avoid-new-cold-war?

56. Šešelgytė, Margarita. 2018 Sep 11. PESCO: The Lithuanian Perspective (IRIS 2018/2019). https://www.iris-france.org/117399-pesco-the-lithuanian-perspective/

57. Soare, R. Simona. 2020. Turning the tide. How to rescue transatlantic relations. EU Institute for Security Studies. Paris. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Transatlantic%20relations%20book.pdf

58. Soutou, Goerges-Henri. 2022. L'autonomie stratégique européenne. *DSI (Défense et Sécurité International)*, Mars-Avril 2022, No. 158 (Mars-Avril 2022), p. 82-85. www.jstor.org/stable/10.2307/48651838

59. Tellenne, Cédric. 2023. « L'OTAN est en état de mort cérébrale. » Idées reçues sur la géopolitique et la géoéconomie ; p. 211-221. Le Cavalier Bleu. https://shs.cairn.info/idees-recues-sur-la-geopolitique-et-la-geoeconomie--9791031806136-page-211?lang=fr

60. Testaferri, Sara. 2022. Les Débats Sur la Défense Commune Européenne Depuis la Crise des Euromissiles Jusqu'à la Présidence Française du Conseil de L'union Européenne. L'Europe en Formation, 395(2), 159-173. https://doi.org/10.3917/eufor.395.0159

61. The Economic Times. 2023 Aug 30. *"Poland to spend over 4% of GDP on defence in 2024"*. https://economictimes.indiatimes.com/news/defence/poland-to-spend-over-4-of-gdp-on-defence-in-2024/articleshow/103403076.cms?from=mdr

62. Tisdall, Simon. 2025 Feb 17. The Guardian. "As the US retreats, Europe must look out for itself - so is Macron's nuclear offer the answer?". https://www.theguardian.com/commentisfree/2025/feb/17/europe-france-uk-nuclear-shield-emmanuel-macron

63. Tobelem, Boran. 2022 Jan 31. Qu'est-ce que l'autonomie stratégique européenne ? Toute l'europe.eu Comprendre l'Europe [update 2025 Mar 14 by Verdes Juliette]. https://www.touteleurope.eu/l-ue-dans-le-monde/qu-est-ce-que-l-autonomie-strategique-europeenne/

64. Lictevout, Léo. 2020 Aug 13. *L'Europe face à la pandémie de Covid-19*. 2109-2023 – L'Europe face au Covid-19. Toute l'Europe. https://www.touteleurope.eu/societe/dossier-l-europe-face-a-la-pandemie-de-covid-19/

65. Vaïsse, Maurice. 2009. La France et l'OTAN : une histoire. *Politique étrangère,* Hiver(4), p. 861-872. https://doi.org/10.3917/pe.094.0861

66. Védrine, Hubert et al. 2007. Continuer l'Histoire. Éditions revue et augmentée. Libraire Arthème Fayard.

67. Védrine, Hubert. 2012 Nov 14. Rapport pour le président de la République française sur les conséquences du retour de la France dans le commandant intègre de l'OTAN, sur l'avenir de la relation transatlantique et les perspectives de l'Europe de la défense. https://otan.delegfrance.org/Le-rapport-Vedrine

68. Védrine, Hubert. 2021. L'illusion d'une autonomie stratégique européenne. Administration, 272(4), p. 22-23. https://doi.org/10.3917/admi.272.0022

69. Vicard, Vincent and Wibaux Pauline. 2022. L'économie mondiale 2023. Éditions La Découvert, collection Repères, Paris. Chapitre VI, De quoi l'autonomie stratégique ouverte est-elle le nom ? ; p. 87-101.

70. Wright, Helen. 2021 Mar 02. Estonia, EU countries propose faster 'European digital sovereignty'. https://news.err.ee/1608127618/estonia-eu-countries-propose-faster-european-digital-sovereignty

71. Zancarini-Fournel, Michelle and Delacroix, Christian. 2014 Oct 15. La France du temps présent (1945-2005) : Version compacte. Édition Belini. Paris. Chapitre 6. Mutation du politique (1958-1968). Sous-chapitre III. Une politique étrangère d'indépendance nationale. *La volonté d'autonomie stratégique face aux Américains.* p. 343-346.

MUTAREA CENTRULUI DE GREUTATE AMERICAN ÎN ASIA-PACIFIC: COMPETIȚIA SINO-AMERICANĂ ÎNTRE REALISM ȘI BLUF STRATEGIC

Paul-Alexandru SITEA*

Abstract:

This paper aims to analyze the geopolitical trends of the great power competition, and is based on the need to overcome the global crisis due to the signals of hegemonic regression coming from Washington in Europe, the deeper involvement of China in world politics, which aims to fill the security vacuums made vulnerable by the West. Using the analytical methodology of scenarios, the paper will be able to offer conclusive strategic directions about the avalanche of current events.

It will also assess the impact and priority of the Asia-Pacific region over European security and Middle Eastern stability from the perspective of the unpredictability of Arab-Israeli dynamics by practicing antagonistic policies concerning traditional and regional allies. Beyond this new realist paradigm, particularly competitive from an economic and military point of view, we can visualize a new Sino-Russian strategic game in their eastern and northern proximity, also targeting the vulnerabilities of the fragmented European bloc.

The article has the role of navigating the international chaos to design viable scenarios for the future systemic configuration, where imperialist actors and autocratic alliances such as BRICS will have a much more influential weight in global affairs. The emerging multipolarity has protectionism at the forefront, and multilateralism will be in the shadow of unilateral or bilateral approaches, small and medium-sized states will seek strategic repositioning, the growing chances of economic and military conflicts being directly proportional to the premises of multipolarity.

The conclusions will help decipher the future geostrategic coordinates of the great powers, the projections of the new American strategy being exposed to enormous risks, transforming it from a stabilizing hegemon into a destabilizing one.

Keywords: security vacuums, hegemonic regression, strategic repositioning.

Introducere

Complexitatea evoluției scenei internaționale creează precedentul unei noi paradigme geopolitice, anume o eră a ciocnirilor constante pe

* Student masterand la Universitatea „Lucian Blaga" din Sibiu, Facultatea de Științe Socio-Umane, Progam Securitate și Relații Internaționale, email: paulalexandru.sitea@ulbsibiu.ro.

plan mondial și regional. Competiția marilor puteri este dusă la un alt nivel, calculele strategice fiind greu de preconizat la prima vedere, direcția războiului din Ucraina, tensiunile ascendente din Orient, volatilitatea competitivității din Asia-Pacific, criza europeană profundă, toate fiind coordonate în raport cu schimbarea instabilă a polilor de putere.

Determinarea Washingtonului asupra proiecției în regiunea Asia-Pacific a fost redată încă din anul 2011, atunci când administrația Obama anunța strategia pivotării spre Asia. Deși emergența Beijingului a fost un factor central, viziunea Washingtonului a urmărit elemente economice și militare mai profunde, cum ar fi: containment-ul Coreei de Nord prin limitarea amenințărilor Phenianului, cooperarea multilaterală prin consolidarea relațiilor cu actori cheie precum Tailanda, Vietnam și Filipine, interoperabilitatea militară cu aliații regionali și aprofundarea legăturilor cu ASEAN și partenerii din proximitatea Oceanului Indian.

Această proiecție nu a marcat o retragere din Europa sau Orientul Mijlociu, ci a reprezentat o încercare de a extinde omniprezența strategică a SUA într-o formă mai sustenabilă pe termen lung (Janine Davidson, 2014, pp. 77-82).

Eșecul pivotării de atunci ne aduce în prezent într-o situație mult mai complicată, în care administrația Trump semnalează reconcilierea relațiilor cu Federația Rusă pentru a contracara China, Iranul sau Coreea de Nord, iar obiectivul unei astfel de strategii ar fi acela de a schimba fundamental status quo-ul internațional iar tratativele privind încheierea războiului din Ucraina, fără participarea directă a Ucrainei, sunt descrise de analiști ca o reinterpretare a strategiei diplomatice triunghiulare de tip Nixon–Kissinger în relația cu Republica Populară Chineză, dar invers aplicată, despărțirea binomului RPC–URSS având un succes extraordinar în anii ’70.

Acest tip de abordare poate aminti de tratate celebre, precum Westafalia - 1648, Utrecht - 1713 sau Viena - 1815, înțelegeri confidențiale precum Camp David - 1978, a administrației Carter, vizita lui Kissinger în 1971 sau probabil cea mai celebră încercare de reconciliere, cu cel mai dramatic impact asupra cursului istoriei din secolul 20 și până în prezent, Chamberlain - 1938, acordul de la Munchen.

Favorizarea asimetrică a Moscovei poate semăna semințele unui conflict extins, în condițiile în care economia sa este orientată exclusiv spre război, iar probabilitatea continuării conflictului pe termen lung în Europa este ridicată. Acțiunile destabilizatoare nu se vor opri odată cu eventualele garanții de securitate occidentale acceptate de Moscova în

Ucraina. În aceeaşi ecuaţie, războaiele hibride din Europa se află la apogeu, iar acţiunile cibernetice desfăşurate de Rusia sunt extrem de agresive, vizând ingerinţe în procesele electorale şi acte de sabotaj asupra infrastructurii critice.

Acordarea unui grad mai mare de încredere Federaţiei Ruse, dincolo de anumite limite strategice, de către Washington ar putea reprezenta o greşeală majoră pe termen mediu şi lung. Indiferent dacă Rusia intenţionează sau nu să continue cucerirea de teritorii ucrainene, obiectivele sale de recalibrare economică şi extindere a influenţei politice în Europa vor rămâne active prin strategii menite să reconstruiască o sferă de influenţă în proximitatea sa vestică.

Din punct de vedere strategic, subminarea sistemului de alianţe occidentale, în special a celor sub egida Washingtonului, reflectă o abordare ce combină decuplarea de sistemul economic globalizat şi susţinut de puterea hard sau de mecanismul coercitiv realpolitik cu rolul de a menţine globalizarea.

Această strategie urmăreşte forţarea partenerilor din alianţe, precum NATO, să contribuie mai mult, pentru ca SUA să poată redirecţiona resursele spre gestionarea ameninţării sistemice reprezentate de China.

Recurenţa mesajelor şi actelor de dispreţ faţă de Uniunea Europeană sau faţă de acordurile USMCA (United States–Mexico–Canada Agreement), dar şi în relaţiile bilaterale, cum ar fi cele cu Canada sau Germania, poate fi interpretată greşit şi totodată contraproductivă în contextul eforturilor comune necesare pentru o eventuală confruntare economică şi tehnologică mai intensă cu Republica Populară Chineză.

Reverberaţiile subminării alianţelor şi aliaţilor tradiţionali afectează profund şi climatul de securitate în regiunea Asia-Pacific, alianţe precum QUAD sau cooperarea cu ASEAN – în 2024, comerţul SUA-ASEAN a reprezentat 476,8 de miliarde dolari, exporturile americane către ASEAN fiind estimate la 124,6 miliarde de dolari (Office of the United States Trade Representative, 2024) - vor fi puse în faţa unor dileme dificile din punct de vedere strategic.

Promovarea conceptului „America First", sub egida sacrificării intereselor naţionale ale aliaţilor nu va putea oferi avantajul competitiv pe care Statele Unite l-au deţinut de-a lungul deceniilor. Vidurile de securitate rezultate pot conduce la formarea unor colaborări contraproductive pentru Washington iar înarmarea previzibilă şi logică a aliaţilor şi a rivalilor de pe plan mondial va spori probabilităţile izbucnirii unor conflicte armate (Benjamin Jensen, 2025).

Obiectivele cercetării

Obiectivele cercetării țin de necesitatea calculării traiectoriei strategice a SUA, dincolo de volatilitatea politicilor administrației actuale, unde abordarea tranzacțională primează, cu riscuri imense în ecuația războiului economic îndreptat împotriva procesului de globalizare ce a transformat China sau Uniunea Europeană în competitori și parteneri bine integrați în lanțurile de aprovizionare globală, critice totodată pentru stabilitatea economică mondială.

În „The 2025 Annual Threat Assessment (ATA)", realizat de către Comunitatea de Intelligence a SUA (ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY, DNI.GOV), China și regiunea Asia-Pacific reprezintă cea mai mare provocare pentru americani.

Vitalizarea și tehnologizarea armatei chineze reprezintă un risc major pentru climatul de securitate regional și global, mai mult decât atât, China dorește ca până în anul 2030 să depășească SUA în materie de AI iar coordonarea adversarilor din axa China, Iran și Coreea de Nord reprezintă un risc major ca Washingtonul să se confrunte cu adversari multipli, concomitent în mai multe teatre.

Cuantificarea impactului deciziei de a oferi atenție exclusivă regiunii Asia-Pacific, ca factor pozitiv sau negativ din punct de vedere strategic va putea oferi noi perspective asupra dinamicii internaționale, pivotarea spre Pacific având în vedere mai multe puncte de luat în calcul, puncte precum vizarea coridorului economic din Arctic pentru a balansa poziția extrem de favorabilă a Chinei și a Federației Ruse de-a lungul regiunii bogate cu resurse importante de minereuri și minerale rare, respingerea acțiunilor coercitive ale Armatei Populare de Eliberare, în proximitatea maritimă estică din Marea Chinei de Sud și de Est asupra disputelor teritoriale cu partenerii Washingtonului sau contracararea proiecției Beijingului de a monopoliza a lanțurile tehnologice complexe.

Dinamica actuală și impactul reorientării americane în Asia-Pacific

Vice-Președintele SUA, JD. Vance, a oferit semnale concludente în cadrul Conferinței de la Munchen despre direcția politicii externe americane, respectiv preocupările principale ale Washingtonului:

- menținerea și dezvoltarea primatului economic american la nivel global;
- competitivitatea cu China;

- retragerea SUA ca hegemon stabilizator global (problemele globale nu mai sunt şi ale Washingtonului).

Povara securităţii europene, transferată direct europenilor semnifică o terapie de şoc pentru aliaţii de pe bătrânul continent, semnalele din trecut, oferite de prima administraţie Trump nefiind luate în serios de către membrii blocului european.

Negocierile purtate peste capul europenilor şi al ucrainenilor întruchipează noua paradigmă realistă, iar partenerii trebuie să se adapteze rapid. Un exemplu elocvent este redat de dificultăţile post-război din Ucraina, care vor fi preluate, în cea mai mare măsură de către europeni.

Autonomia strategică este singura proiecţie concludentă emisă de blocul european în spaţiul public şi politic. Divergenţele de viziune dintre marile puteri europene, ce ţin de disfuncţionalitatea NATO şi, respectiv, proiectul unei armate europene (ReArm Europe), oferă timp preţios Federaţiei Ruse pentru a pregăti şi stimula atacuri hibride pe continent, întrucât presiunea internă este atât de mare, încât alegerile naţionale din interiorul UE capătă un imperativ geostrategic direct proporţional cu dinamica negativă a războiului din Ucraina.

Membrii NATO din Europa investesc doar 1,9% din PIB în hard-power, iar în următorul summit NATO, la Haga, în 24-26 iunie, se va propune, cel mai probabil, ridicarea cifrelor de investiţii la 3% sau chiar la mai mult, nevoia de investiţii militare gigantice fiind absolut necesare pentru formularea unei strategii smart-power europene, în care stimularea producţiei industriei de apărare să devină un punct cheie în strategiile de securitate ale actorilor din Europa, stimularea fiind posibilă doar prin interoperabilitatea factorilor socio-economici, un model de urmat fiind cel polonez sau finlandez, unde populaţiile acestora deţin o reziliență strategică extraordinară în raport cu contracararea ingerinţelor străine, conştientizând necesitatea înarmării pentru deţinerea unui mecanism viabil de descurajare a Kremlinului pe termen lung (Alexandra de Hoop Scheffer, 2025).

Impactul reorientării ar putea oferi pârghii semnificative Beijingului de a se apropria de Europa, Uniune Europeană fiind prinsă între ostilitatea administraţiei Trump (tarife economice, declaraţii oficiale, incoerenţă aliată asupra războiului din Ucraina) şi pe de altă parte, de interesele Chinei.

Din perspectivă europeană, sprijinul politic acordat partidelor pro-ruse şi populiste, oferit direct de moguli MAGA, precum Elon

Musk, ridică probleme şi accentuează fisuri transatlantice care erau de neconceput în urmă cu câțiva ani.

Motivul principal al actualului impediment strategic este percepția diferită asupra amenințării sistemice, europenii considerând Federația Rusă drept cea mai mare amenințare la adresa securității continentale europene, în timp ce SUA percep Republica Populară Chineză drept principala amenințare sistemică, perspectiva americană având ca fundament geostrategic puterea coercitivă economică şi militară pe care Beijingul o poate instrumentaliza în prezent.

Războiul comercial cu aliații subminează reziliența pe termen mediu şi lung a Washingtonului, deficitul comercial de aproximativ 267 de miliarde de dolari înregistrat de SUA în schimburile de bunuri cu UE în 2024 fiind folosit ca principal argument pentru tarifele americane asupra produselor europene importate (Plamen Tonchev, 2025).

Pragmatismul administrației Xi în raport cu aparenta divergență transatlantică este redat de Wang Yi, ministrul de extern chinez, în cadrul Conferinței de securitate de la München, oficial care a evocat un punct extrem de sensibil pentru sinergia transatlantică, anume acela al asocierii BRI cu Global Gateway: „*Cu o creștere de 5% a PIB-ului anul trecut, China a contribuit la aproape 30% din creșterea economică mondială. A servit ca un motor important pentru creșterea economică globală și a împărtășit cu lumea beneficiile pieței sale supradimensionate. China este dispusă să asocieze cooperarea de înaltă calitate Belt and Road cu strategia Global Gateway a Uniunii Europene, astfel încât să se împuternicească reciproc și să împuternicească întreaga lume*" (Ministry of Foreign Affairs The People's Republic of China, 2025).

Autonomia strategică europeană era de foarte mulți ani dorită de Beijing, dependența de Washington a europenilor şi cooperarea strânsă din punct de vedere economic cu aceştia, nu permitea Chinei să fructifice oportunitățile unui eventual acces extins în piețele europene.

Perspectivele noi ale rolului blocului european pe plan global țin de necesitatea Uniunii Europene de adopta politici realiste în strategiile sale de politică externă, strategii care ar putea umbri liberalismul instituțional promovat de-a lungul timpului.

Sinergia dintre factorii geopolitici duri şi cei ai securității economice europene este imperativă în contextul actual, iar echilibristica între alinierea strategică cu Statele Unite şi cooperarea economică cu Beijingul este din ce în ce mai dificil de gestionat (Marry Gallagher, 2025).

Mai mult decât atât, relația încordată dintre cei doi actori sino-europeni este redată de un deficit comercial uriaş al blocului european

cu pieţele chineze, de 291 de miliarde de euro în anul 2023, respectiv la expunerea în faţa unor riscuri ce ameninţă arhitectura de securitate europeană, riscuri redate de spionajul industrial întreprins de-a lungul anilor şi de ajutorul tehnologic oferit Kremlinului în războiul din Ucraina.

În aceeaşi ecuaţie, monopolizarea sectorului de tehnologie verde, instrumentat de către firmele chineze, supraproducţia industrială a Chinei, element ce oferă pârghii de acces neloial în pieţele statelor europene, incapacitatea entităţilor europene de a concura în China, contribuie şi ele la menţinerea unui climat geopolitic combativ dar asimetric din foarte multe puncte de vedere.

Prin acordul Comisiei Europene cu Mercosur sau acordul bilateral cu India, în vederea unui acord liber schimb, blocul european caută pieţe şi parteneri care pot aplana efectele schimbărilor bruşte economice pe care Washingtonul le-a dezlănţuit asupra pieţelor integrate la nivel global.

Vulnerabilizarea Occidentului a deschis drumul Chinei către obţinerea statutului de superputere mondială, proiecţiile sale regionale/ globale fiind în concordanţă cu ritmul impus de doctrina MAGA privind rezilierea şi regândirea parteneriatelor şi alianţelor în care este implicat Washingtonul (Plamen Tonchev, 2025).

Terapiile de şoc, în materie de politică externă aduc în prim planul strategic american şi chinez două posibile căi de relaţionare distincte, cu toate că navigarea tuturor posibilităţilor este indispensabilă în acest climat volatil iar schimbarea status-quo-ului de la graniţa hegemonilor fiind variabile tot mai concludente de luat în calcul iar astfel putem contura câteva scenarii:

Primul ar fi continuarea unei politici hiper-competitive, cu tarife şi reciprocităţi tarifare economice, tensiuni în proximitatea estică a Chinei pe seama statutul insulei Taiwan, incursiunile în zonele aflate în zona exclusivă a Filipinelor, exerciţii în apropierea Australiei (insulele Darwin), posibilitatea ridicată a izbucnirii unui război economic dezlănţuit (disruptiv pentru lanţurilor globale de aprovizionare), scenariul acesta asigurând o continuitate a primei administraţiei Trump în raport cu rivalul asiatic. (probabilitate mai mare)

Un al doilea ar fi accepţiunea unei noi realităţi geopolitice, anume revenirea sferelor de influenţă, reconcilierea şi găsirea unui consens care ar oferi un echilibru economic şi militar sino-american, problemele interne ale Chinei şi ale Washingtonului fiind reciproc avantajate, fundamentarea multipolarităţii echilibrate, subordonarea Taipeiului sub pretextul asimetriei balanţei economice în raport cu Washingtonul

(element cu o probabilitate mai mica de fructificare, dar posibil), respectiv slăbirea angajamentelor de securitate acordate Japoniei, Coreei de Sud și Filipinelor.

Cel de-al doilea scenariu s-ar sprijini pe tendința iliberală pe care SUA o îmbrățișează, sau mai bine zis pe simpatia pe care administrația americană o dedică liderilor ce inspiră putere și influență brută, totodată, semnalele tot mai frecvente de respingere a conceptului de multilateralism instituțional ar pune sub semnul întrebării viabilitatea alianțelor regionale, capabile să influențeze balanța de putere, alianțe precum QUAD sau AUKUS în Pacific, Beijingul devenind actorul ce va deține prim-planul, respectiv puterea de influență regională (Scott Kennedy, 2025).

Vizualizarea strategiilor competitive chineze

Premierul Li Qiang a propunea în 2024 implementarea strategiei „AI Plus", inițiativă care urmărește integrarea inteligenței artificiale în toate sectoarele economice. Strategia vizează stimularea inovației private în domeniul AI, precum și o coordonare națională coerentă pentru implementarea inovației în întreaga economie.

Raportul guvernamental de lucru al Chinei pentru anul 2025 conturează principalele direcții strategice în materie de politică externă, obiective economice și politici de securitate iar în acest context, Li a evidențiat în mod repetat paradigma protecționismului și a abordărilor unilaterale care creează dificultăți mari pentru fluxurile de import-export și pentru stabilitatea lanțurilor economice consolidate de-a lungul anilor.

Sporirea și eficientizarea capacităților hard-power ale Chinei până în anul 2027, repetate în raport, este în deplină concordanță cu liniile promovate de Xi Jinping deoarece, din punct de vedere militar, China urmărește dezvoltarea unei doctrine de apărare autonomă din perspectivă tehnologică, prin catalizarea platformelor spațiale și cibernetice cu tehnologiile informației în arsenalul Armatei Populare de Eliberare (PLA) (Armata de Eliberare a Poporului).

Anunțul creșterii bugetului de apărare cu 7,2 din PIB este un unul dintre punctele clare ale ambițiilor regional-globale, anunțul fiind foarte îngrijorător pentru statele aflate în proximitatea sa sud-estică, indiferent dacă acestea abordează politici competitive sau flexibile cu actorul chinez (Neil Thomas, 2025).

Cifrele economice ale Chinei în 2025 sunt surprinzătoare, în primul sfert al acestui an cu o creștere de 5,4% față de începutului anului

2024, schimburile economice cu ASEAN fiind şi ele pe un trend ascendent, de 7,1%, vizarea pieţelor din regiunea Asiei Centrale prin creşterea comerţului în această zonă cu 6.9% indică traiectoria strategică a Chinei, sub egida partenerilor proiectului BRI cu scopul de a scădea dependenţa de pieţele americane.

Poziţia fermă a administraţiei Trump asupra tarifelor, a impus Beijingului o grăbire a exporturilor, înaintea escaladării cu peste cifre de 100% asupra importurilor din China, proiecţia economică asupra exporturilor Chinei fiind pe un trend negativ asupra următorului trimestru de an din prisma afectării pieţelor interne şi externe, excepţia de la regula a tarifelor reprezentând electronicele, industria de semiconductori şi de telefoane deoarece ambele tabere sunt conştiente asupra faptului că blocarea pieţei tehnologice ar duce garantat la o situaţie de lose-lose într-un timp relativ scurt (Qian Zhou, Arendse Huld, 2025).

Variabila tehnologică a competitivităţii geostrategice sino-americane trebuie luată în calculul oricărei analize bine fundamentate deoarece industria cipurilor, vitală pentru deţinerea şi instrumentalizarea avantajului strategic de ordin militar şi economic, are la bază măsurile protecţioniste abordate de ambele tabere în ecuaţia evoluţiei tehnologiei AI, China calculându-şi extrem de pragmatic proiecţia tehnologică pe termen lung, ţinta fiind în primul rând, monopolizarea pieţelor ASEAN şi destabilizarea celei mai importante fabrici în materie de proiectare a semiconductorilor la nivel mondial, aflată în Taiwan, anume TSMC (Taiwan Semiconductor Manufacturing Company Limited).

Ramificaţiile impactului tehnologic din Asia Pacific va coordona în aceeaşi ecuaţie viitoarea arhitectură de securitate globală, de aceea nevoia de prioritate exclusivă asupra regiunii, în viziunea factorilor de decizie americani trebuie realizată rapid deoarece China nu va mai putea fi oprită în cursa acesteia de a detrona poziţia de hegemon global a SUA până în anul 2049, an simbolic pentru doctrina comunistă chineză a Beijingului.

Christopher Miller, autorul „Chip Wars" subliniază punctul cheie al strategiei chineze în materie de tehnologie de vârf*: „Dacă tentativa Chinei de a obţine autosuficienţă economică în materie de semiconductori reuşeşte, vecinii săi, care au de regulă economii dependente de export, ar avea şi mai mult de suferit. Circuitele integrate însemnau, în 2018, 15% din exporturile Coreei de Sud, 17% din cele ale statului Singapore, 19% din ale Malaysiei, 21% din ale Filipinelor şi 36% din ale Taiwanului. „Fabricat în China 2025" este o ameninţare pentru toate aceste ţări. Miza este cea mai*

densă rețea de lanțuri de aprovizionare și fluxuri comerciale din lume, industriile electronice stând la baza creșterii economice și stabilității politice Asiei în ultima jumătate de secol." (Chris Miller, 2023, p.277).

Tendința globală de creștere a investițiilor militare va necesita o atenție deosebită regiunii din sud-estul Asiei, în 2024 Asia Pacific reprezenta aproape 22% din totalul cheltuielilor globale în sectorul militar, China reprezentând 46% din cuantumul investițiilor regionale, iar relevanța marii strategii chineze raportată la avântul tehnologic în privința inteligenței artificiale integrate și dedicate sectorului militar va transforma climatul de securitate din Pacific în cea mai mare provocare pentru Washington și aliații săi regionali (DefenseOne, 2025).

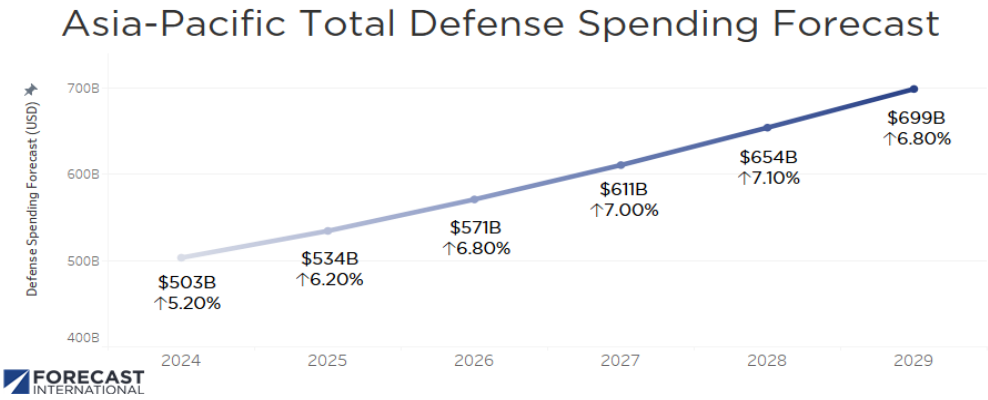

Figura 1: Prognoza a investițiilor militare regionale din Asia-Pacific, Sursă:DefenseOne

Interconectarea complexelor de securitate din estul Europei, din Orientul Mijlociu și Asia de sud-est pot fi înțelese sub egida axei China-Federația Rusă-Iran, Coreea de Nord, toate constituind o formulă strategică ce vizează distrugerea primatului de securitate american în favoarea revenirii unui concept realist în arhitectura globală de securitate, acela al sferelor de influență bazate pe răsturnarea echilibrului de putere.

Doctrina Trump și nevoia regândirii excepționalismului american

Încrâncenarea triumfalistă nu poate aduce plusvaloare sustenabilă pentru Washington, deoarece China dispune de pârghii superioare de producție și de un sector naval aflat într-o asimetrie frapantă față de cel american, iar viteza modernizării sale militare poate reduce

semnificativ capacitatea SUA de a înfrunta, de una singură, colosul geopolitic din Pacific.

Noua paradigmă evidenţiază nevoia unui efort aliat pentru a genera o putere de descurajare bine coordonată printr-o promovare a unei politici de interoperabilitate şi viteză de reacţie cu actori precum: Japonia, Coreea de Sud, Taiwanul, Filipine, India, Vietnam şi Singapore, astfel ele pot contribui la construirea unui sistem capabil să contrabalanseze avantajul chinez, reprezentat de o capacitate industrială şi de producţie profund integrată în economiile naţionale ale acestora.

Catalogarea fenomenelor interne negative ale Republicii Populare Chineze, precum: populaţie îmbătrânită, şomaj, crize imobiliare, controlul şi despotismul faţă de sectorul privat, în dezavantaje strategice sunt cel puţin superficiale, subestimarea rezilienţei strategice chineze fiind un factor recurent al politicilor şi discursurilor politice ale Washingtonului, elementele principale de luat în vedere fiind redate de investiţiile în infrastructura civilă şi militară, cercetarea tehnologică constantă, capacitatea de a influenţa fluxurile de comerţ, puncte pe care China le înregistrează consecvent în ultimii ani.

De la aderarea sa la Organizaţia Mondială a Comerţului (OMC) în 2001, ponderea Chinei în producţia globală a crescut la 30% din totalul comerţului mondial, în timp ce cea a Statelor Unite a scăzut la 15% în acelaşi interval. Prejudecăţile legate de copierea tehnologică nu mai sunt viabile în prezent, Beijingul devenind lider în domenii precum producţia de roboţi şi tehnologii verzi , China producând aproximativ 90% din panourile solare la nivel global şi 2/3 din totalul maşinilor electrice (Kurt M. Campbell and Rush Doshi, 2025).

Sectorul militar chinez se află, de asemenea, într-o ascensiune accelerată, prin inovarea în domeniul rachetelor balistice şi hipersonice, precum şi prin prognoza conform căreia capacitatea de foc navală a Chinei ar putea depăşi-o pe cea a Statelor Unite până în 2027.

Unilateralismul doctrinar al administraţiei Trump ridică noi dileme strategice, direct proporţionale cu subestimarea propriilor vulnerabilităţi în favoarea unei viziuni distorsionate asupra punctelor (aparent) slabe ale rivalului sistemic de peste Ocean.

Imperativul contracarării emergenţei constante a capabilităţilor Chinei necesită coordonare din partea Washingtonului, alianţele tradiţionale precum NATO, QUAD sau AUKUS necesitând o aprofundare, mai precis o integrare economică şi tehnologică la scară industrială.

Exemplul Ucrainei a fost o lecţie atent analizată de către rivali, care au evaluat capacităţile Statelor Unite de a susţine un război de

amploare împotriva Chinei, fie într-un singur teatru de conflict, fie concomitent în mai multe regiuni de contact unde aliații Chinei din cadrul BRICS vizează vulnerabilitățile partenerilor occidentali.

Aparenta fractură în relațiile SUA cu aliații săi din Europa sau din zona Asia-Pacific pot deveni, la rândul lor, pârghii strategice pentru Beijing, mai ales în ceea ce privește angajamentele economice cu partenerii tradiționali ai Washingtonului, fie din blocul european, fie cu rivali istorici precum Japonia sau Coreea de Sud sau cu partenerii din ASEAN.

În timp ce direcția strategică a SUA este în proces de revizuire, aliniamentul dintre Coreea de Nord, Iran, China și Rusia profită de regresul occidental, implicându-se activ în conflicte sau ocolind sancțiunile internaționale, cu exemple precum: trimiterea de soldați nord-coreeni în teatrele operative din Ucraina, prin transferuri tehnologice chineze către Federația Rusă sau prin sprijinul economic oferit Iranului în evitarea sancțiunilor.

Creșterea sau scăderea influenței RPC va fi direct proporțională cu reziliența alianțelor și angajamentelor strategice ale Washingtonului deoarece o politică externă exclusiv concentrată în jurul sloganului și excepționalismului american permite actorului chinez o manevrabilitatea strategică considerabilă în proximitatea sa, în relația economică cu UE sau prin creșterea angajamentelor în Orient pentru monopolizarea lanțurilor comerciale globale, precum IMEC sau prin angajamentul sino-rus în perspectiva de a domina regiunea Arctică din punct de vedere economic și militar (Kurt M. Campbell and Rush Doshi, 2025).

Pe baza tendințelor și variabilelor regăsite în analiză se pot formula două direcții geopolitice distincte a politicii externe americane în raport cu aliații europeni și asiatici:

- Continuarea unei fracturi transatlantice, apropiere economică Beijing-UE, subestimarea capacității Chinei de a inova din punct de vedere tehnologic, incapacitatea SUA de a purta un război economic prelungit cu actorul chinez, abandonarea intereselor naționale ale actorilor din Europa sau continuarea politicii de menținere a tarifelor economice asupra aliaților tradiționali, vulnerabilizându-i, ar putea conduce spre o izolare geopolitică, accelerând declinul strategic american, cel din prezent fiind unul parțial.
- Promovarea unui angajament selectiv cu aliații care pot contribui la construirea unor avantaje strategice, în contextul maratonului geopolitic sino-american, precum și catalizarea treptată a responsabilităților de securitate către aceștia, ar trebui să fie însoțite de menținerea unei relații

echilibrate, cu angajamente economice şi militare unitare, în raport cu pluralitatea intereselor naţionale ale fiecărui actor aliat.

O proiecţie interesantă, pe termen lung, a dinamicii turbulente pe care competiţia marilor puteri, respectiv a viitoarelor axe aferente ale acestora pe care o vor creiona pentru următorii zece ani este cuprinsă în „Global Foresight 2025", (Atlantic Council, 2025), unde accepţiunea generală este aceea că în anul 2035, arena internaţională va fi împărţită în axe distincte, anume axa condusă de USA, respectiv de China.

Probabilităţile unui conflict mondial fiind în creştere în viziunile celor 350 de experţi, de asemenea, revenirea în scenă a erei înarmărilor nucleare este şi ea preconizată ca fiind foarte probabilă, cele mai mari procente în a folosi arma nucleară fiind reprezentate de Federaţia Rusă şi Coreea de Nord, 37% dintre respondenţi estimând faptul că în următorul deceniu arma nucleară va fi folosită.

Scăderea puterii soft-power americane este estimată la 35% de către repondenţi, în timp ce 71% estimează faptul că hard-power-ul Washingtonului va fi dominant şi în următorii zece ani. Comparativ cu „Global Foresight 2024", (Atlantic Council, 2024) toate cifrele de sondare din anul 2025 sunt în scădere în raport cu rolul SUA în lume, primatul economic american fiind şi el în scădere cu câteva procente, de la 52%, la 49%.

Multipolaritatea emergentă este strâns legată de proiecţiile acestea, cifrele fiind şi ele fluctuante în funcţie de instabilitatea întregului sistem internaţional de state.

Acelaşi sondaj indică o scădere profundă a rolurilor instituţiilor internaţionale globale democratice, 75% susţinând faptul că ONU va fi mai puţin capabilă în a rezolva diversele probleme globale, precum problemele climatice. Scăderea ponderilor importanţei precum G7, 49% apreciind o scădere a importanţei grupului în următorii ani, G20 având un procentaj de 38% în raport cu pierderea capabilităţilor de influenţă pe plan mondial.

ASEAN este apreciată ca fiind mai capabilă în următorii zece ani, cu o pondere de aproximativ 40%, UE cu o pondere pozitivă aproximativ egalitară cu cea a ASEAN, tot de 40%, BRICS-ul fiind apreciat de 43% ca fiind mai capabil pe viitor (Mary Kate Aylward, Peter Engelke, Uri Friedman, Paul Kielstra, 2025).

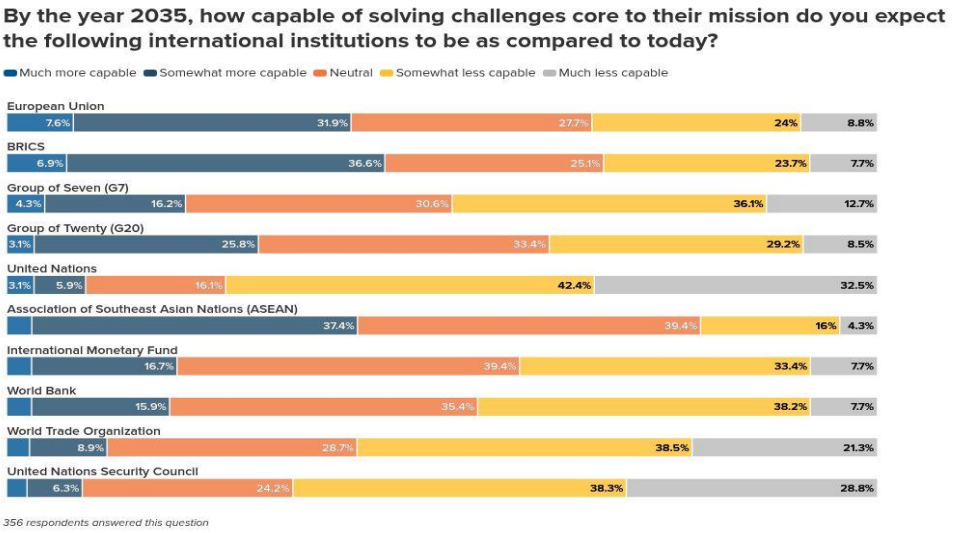

Figura 2: Sondaj, procentaj de aproximare a viitoarelor capabilități ale organizațiilor internaționale, Sursa: Atlantic Council, Scowcroft Center for Strategy and Security

Concluzii

Recalibrarea polilor de putere se suprapune cu tendința de reașezare a centrului de greutate american în Pacific, noua direcție strategică de origine realistă din punct de vedere teoretic, fiind redată de calculul lipsit de sustenabilitate, menținut de-a lungul mandatelor administrațiilor precedente asupra menținerii unei omniprezențe globale.

Așa cum în spațiul public factorii de decizie americani au repetat faptul că problemele lumii nu mai sunt și cele ale SUA, Washingtonul nu mai poate purta povara unei omniprezențe militare, axa emergentă a rivalilor de tipul China, Rusia, Iran, Coreea de Nord profitând de regresul hegemonic american, în regiunile fiecărui rival existând tensiuni sau chiar conflicte cinetice.

Bluful strategic american, deghizat ca o intenție de politică realistă și aparent ancorată în interesele naționale, fără să aibă în vedere și cele ale aliaților tradiționali, aliați care pot influența decisiv balanța de putere la nivel regional și global, ar putea fi reprezentat de continuarea unei politici externe conflictuale față de propriii parteneri, conturată în jurul excepționalismului singular al Washingtonului în competiția geopolitică de tip maraton cu Republica Populară Chineză.

De asemenea, concentrarea asupra raportului cost-beneficiu pe o axă scurtă de timp în viziunea doctrinară a administrației Trump,

raportată la sistemele de alianţe construite de Statele Unite de-a lungul deceniilor anterioare, creează imaginea unui pariu riscant şi greu de anticipat, anume găsirea unui echilibru rapid între stimularea partenerilor de a-şi securiza propriile interese în faţa adversarilor sistemici şi pivotarea imperativă către zona Pacificului.

Configuraţia multipolară a viitorului va reflecta implicaţiile reaşezării strategice americane din prezent, recalibrarea balanţei de putere fiind direct proporţională cu intensificarea tensiunilor în zonele de contact ale faliilor geopolitice. Deznodământul acestei reaşezări din Pacific va fi determinat de avansul tehnologic militar de vârf şi de mobilizarea economică protecţionistă asupra tehnologiilor critice în cadrul binomului sino-american, în zona lor de contact.

Marea strategie a Chinei se va concentra pe izolarea Statelor Unite prin oferirea de avantaje şi stimulente economice atât europenilor, cât şi vecinilor săi asiatici, în contextul condamnării şi redresării politicii tarifare americane. Această dualitate strategică urmăreşte, pe de o parte, consolidarea influenţei Chinei în proximitatea sa, în detrimentul Coreei de Sud, Japoniei, Australiei şi Filipinelor, şi, pe de altă parte, extinderea influenţei BRICS la nivel global, totodată, în acelaşi calcul strategic, guvernul condus de Li Qiang şi Xi Jinping urmăreşte să depăşească Statele Unite din punct de vedere tehnologic până în anul 2030.

Bibliografie

1. Asia Society Policy Institute. 2025. „Key Takeaways from China's Two Sessions in 2025." Asia Society, 2025. https://asiasociety.org/policy-institute/key-takeaways-chinas-two-sessions-2025 (accesat 3 aprilie 2025).

2. Aylward, Mary Kate, Peter Engelke, Uri Friedman, şi Paul Kielstra. 2025. „Welcome to 2035: What the World Could Look Like in Ten Years, According to More Than 350 Experts." Atlantic Council Strategy Paper Series. Atlantic Council, 12 februarie 2025. https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/welcome-to-2035/, (accesat 2 aprilie 2025).

3. Campbell, Kurt M., şi Rush Doshi. 2025. „*Underestimating China: Why America Needs a New Strategy of Allied Scale to Offset Beijing's Enduring Advantages*." Foreign Affairs, 10 aprilie 2025. https://www.foreignaffairs.com/china/underestimating-china, (accesat 11 aprilie 2025).

4. Davidson, Janine. 2014. „*The U.S. 'Pivot to Asia*.'" American Journal of Chinese Studies 21: 77–82. http://www.jstor.org/stable/44289339.

5. de Hoop Scheffer, Alexandra. 2025. „*JD Vance's Speech at the Munich Security Conference Should Be Seen as a Clarification of Donald Trump's Vision*." German Marshall Fund of the United States, 19 februarie 2025. https://www.gmfus.org/news/jd-vances-speech-munich-security-conference-should-be-seen-clarification-donald-trumps-vision.

6. Defense One. 2025. „*Global Snapshot: The Asia-Pacific Defense Environment*" Defense One, 24 februarie 2025. https://www.defenseone.com/sponsors/2025/02/global-snapshot-asia-pacific-defense-environment/403229/, (accesat 29 martie 2025).

7. Gallagher, Mary. 2025. „*Europe Is Caught Between Trump's Disruption and China's Status Quo*" World Politics Review, 2 martie 2025. https://www.worldpoliticsreview.com/europe-us-trump-china/, (accesat 11 aprilie 2025).

8. Jensen, Benjamin. 2025. „*Grand Bargains in History: Trump's Ukraine Gambit*." Center for Strategic and International Studies (CSIS), 20 februarie 2025. https://www.csis.org/analysis/grand-bargains-history-trumps-ukraine-gambit (accesat 22 aprilie 2025).

9. Kennedy, Scott. 2025. „*The United States' Illiberal Turn Recasts a Potential Deal with China*." Center for Strategic and International Studies (CSIS), 13 martie 2025. https://www.csis.org/analysis/united-states-illiberal-turn-recasts-potential-deal-china (accesat 3 aprilie 2025).

10. Miller, Chris. 2023. „*Războiul cipurilor: Lupta pentru cea mai importantă tehnologie din lume*", București: Humanitas.

11. Ministry of Foreign Affairs of the People's Republic of China. 2025. „*A Steadfast Constructive Force in a Changing World*." 15 februarie 2025. https://www.fmprc.gov.cn/eng/wjbzhd/202502/t20250215_11555665.html (accesat 10 aprilie 2025).

12. Office of the Director of National Intelligence. 2025. „*Annual Threat Assessment of the U.S. Intelligence Community".,* 25 martie 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf, (accesat 24 aprilie 2025).

13. Office of the United States Trade Representative. 2024. „*Association of Southeast Asian Nations (ASEAN).*" Accesat la 29 martie 2025. https://ustr.gov/countries-regions/southeast-asia-pacific/association-southeast-asian-nations-asean.

14. Tonchev, Plamen. 2025. „*The EU Squeezed Between the US and China.*" The Diplomat, 3 martie 2025. https://thediplomat.com/2025/03/the-eu-squeezed-between-the-us-and-china/, (accesat 23 aprilie 2025).

15. Zhou, Qian, şi Arendse Huld. 2025. „*China's Economy Beats Expectations in Q1 2025 – Can Momentum Last?*" China Briefing, 2025. https://www.china-briefing.com/news/chinas-economy-q1-2025-5-4-percent-gdp-growth/, (accesat 29 martie 2025).

AUTONOMIA STRATEGICĂ – ELEMENT DISCURSIV ŞI REALITATE EUROPEANĂ

Mălina-Maria RÎNDAŞU*

Abstract:

Predictability in the international system is an increasingly rare characteristic of state actors' intentions. The belligerent tendencies of states and terrorist organizations have a direct impact on societies. Organizations such as NATO, the UN, and the European Union aim to maximize negotiation and mediation as means of resolving differences. The capacities and capabilities of these organizations are among the most diverse. While the European Union is recognized for providing expertise and assistance in conflict zones, NATO brings to the forefront an operational area, focused on using military capabilities. The paper aims to provide a critical analysis of the Strategic Compass, the security practices carried out to maximize security at the European level. Starting from a theoretical framework focused on security developments, the preparation of the literature review will revolve around an integrative approach. The study will apply deductive coding according to the main themes extracted from the literature to synthesize research directions. The research question to be answered is titled "How do the speeches of European leaders from 2022 to 2024 address resilience and strategic autonomy?". The discursive perspective is rendered by a qualitative methodology, cantered on documents and rhetorical elements. The conclusions validate a split among European leaders on the EU-NATO dynamic, in line with the findings of researcher Frédéric Mauro. While some states with security risks in their proximity opt for the security offered by the military organization, others are betting on a quasi-economic approach at the leadership level. They propose a decision-making autonomy at EU level in relevant military matters to increase the relevance of this entity at international level.

Keywords: *autonomie strategică, reziliență, mediu de securitate, context internațional*

Introducere

Uniunea Europeană nu se rezumă doar la drepturi, reglementări şi managementul elementelor de natură internă. Un aspect deosebit de important pe agenda sa îl constituie şi securitatea. În acest conglomerat legislativ care marchează funcţionarea UE şi reprezentativitatea statelor

* Babeș Bolyai University, Doctoral School of International Relations and Security Studies, Cluj-Napoca, malina.rindasu@ubbcluj.ro

membre, conceptul de „transfer de suveranitate" a generat mari dezbateri de viziune. Pe de o parte, unii autori au evidențiat faptul că sensul suveranității se redefinește dintr-o perspectivă a extinderii. La polul opus, euroscepticii au susținut diminuarea competențelor suverane ale statelor, în detrimentul acestora (Wæver, 1996, p. 116). Discursurile de polarizare interpretativă privind atribuțiile Uniunii Europene, alimentate de contexte economice sau politice nefavorabile, au conturat două categorii majore de raportare: susținători și opozanți ai UE. Ambele viziuni continuă să caracterizeze scrierile despre construcția europeană. Cedarea de suveranitate și prioritizarea intereselor modelează comportamentele statelor în raport cu securitatea europeană.

La nivel discursiv, politicienii europeni își doresc o Europă mai sigură („(...) capabilă să își asume responsabilitățile pentru propria securitate și pentru pacea și stabilitatea internațională în general" (Mauro, 2021, p. 4)). Cu toate acestea, structurile de leadership din țările de graniță continuă să se bazeze preponderent pe garanțiile de securitate sub egida NATO și parteneriatelor strategice cu SUA, în contextul lipsei unui consens privind implicațiile dezvoltării autonomiei strategice europene la nivel politic. Așa cum vom observa pe parcursul lucrării, chiar dacă Uniunea Europeană oferă direcții precise de dezvoltare în domeniul securității și apărării, consensul liderilor europeni în materie decizională întârzie să apară.

În vederea configurării unei perspective discursive asupra securității, această lucrare își propune să realizeze o analiză critică a Busolei Strategice și practicilor de securitate cu scop în maximizarea securității la nivel european. Pornind de la un cadru teoretic axat pe evoluțiile în materie de securitate, revizuirea literaturii de specialitate va gravita în jurul unei abordări integrative. Astfel, prin analiza Busolei Strategice, vom aplica o codare deductivă, în conformitate cu principalele tematici extrase din literatură. Acest tip de analiză metodologică vizează identificarea, în baza scrierilor existente, a unor structuri tematice recurente, datele fiind ulterior clasificate în funcție de acestea. În acest mod, cercetătorul verifică, analizează și interpretează corelațiile dintre cadrele teoretice deja existente și datele colectate, în conformitate cu subiectul de cercetare enunțat.

Numeroase studii abordează critic documentele strategice elaborate la nivelul Uniunii Europene în domeniul securitate și apărare. Cu toate acestea, asocierea unor dimensiuni concrete cu perspectiva discursivă a liderilor europeni a fost aplicată izolat, cu eforturi reduse de

a lega cele două variabile. Considerăm importante analizele privind atitudinile unor astfel de lideri, pentru a putea înţelege, ulterior, poziţionarea statelor membre în raport cu diverse probleme de pe agendă. În vederea abordării acestei lacune existente în literatura de specialitate, lucrarea îşi propune să realizeze o analiză critică a Busolei Strategice pe două dimensiuni de referinţă: autonomie strategică şi reziliență. Acestea vor fi analizate atât prin raportare directă la cuprinsul documentului, cât şi, mai ales, prin intermediul unor secvenţe discursive asociate liderilor europeni. Studiul îşi propune să răspundă la întrebarea de cercetare *„Cum abordează discursurile liderilor europeni din perioada 2022–2024 reziliența și autonomia strategică?”*, utilizând un cadru teoretic axat pe cele două problematici şi o analiză deductivă a datelor colectate.

Scopul lucrării rezidă în raportarea problemei la corpusul de date constituit, pentru a vizualiza cum sunt interpretate cele două dimensiuni la nivel discursiv şi, implicit, pentru a evidenţia relaţiile de putere dintre actori. Aşa cum vom observa, deşi Uniunea Europeană acţionează uneori ca un monolit în anumite domenii de competenţă, liderii statelor sau instituţiilor europene încearcă să îşi impună propriile viziuni asupra securităţii. Impredictibilitatea mediului de securitate favorizează conturarea unor perspective sectoriale, influenţate de amplificarea unor riscuri în proximitatea statelor, de priorităţile propriilor interese naţionale şi de poziţia percepută a acestora în cadrul organizaţiei.

Revizuirea literaturii de specialitate

În vederea realizării unei analize critice asupra Busolei Strategice şi a contextului în care aceasta a fost lansată, lucrarea urmează firul logic al unei cercetări academice, fiind structurată în trei secţiuni. Prima secţiune este dedicată cadrului conceptual, în care vor fi definiţi principalii termeni. De asemenea, se va elabora revizuirea literaturii şi direcţiile de cercetare statuate în cadrul analitic. Cea de-a doua secţiune este reprezentată de elemente metodologice, iar ultima cuprinde partea de analiză.

Această abordare permite cititorului să urmeze îndeaproape evoluţiile tematice ale subiectului existente în literatură. Ulterior, este introdusă o dimensiune critică, generată pentru a reflecta asupra importanţei şi potenţialului de implementare a deziderateloor asumate la nivelul politicii europene prin Busola Strategică.

Ce este autonomia strategică?

Preocuparea Uniunii Europene pentru securitate și relații externe este vizualizată atât prin existența unei palete largi de proiecte instituționale și documente strategice, cât și prin intervenții și inițiative în plan securitar. Realizarea constantă a unor radiografii ale mediului de securitate orientează atât răspunsurile operative ale Uniunii, cât și configurarea unor noi trasee de acțiune. Tendința de a acționa autonom – fie singular, fie în parteneriat cu alți actori – este o prioritate pentru membri, în contexte vaste de gestionare a situațiilor tensionate. În acest sens, dezbaterea privind potențialul autonomiei strategice la nivelul Uniunii Europene s-a conturat începând cu anii 1990 (Järvenpää, Major și Sakkov, 2019, p. IV), iar dinamicile ulterioare ale mediului de securitate au menținut acest interes, însă într-un mod fragmentat. Conceptul de „autonomie strategică" este legat de politica de apărare comună a UE și de definirea pilonului european al NATO (Abeele, 2021, p. 14). Termenul edifică, pe de o parte, necesitățile multiple ale membrilor Uniunii în drumul către consolidarea capabilităților de securitate și apărare. Pe de altă parte, autonomia strategică vizează, în acest context particular, procesul trenant de armonizare a deciziilor politice, caracterizat de fluctuații determinate de apariția iminentă a unor riscuri. Printre principalii lideri europeni care au susținut transpunerea operațională a conceptului la nivelul Uniunii se numără Emmanuel Macron, Angela Merkel și Sauli Niinistö. Fiecare dintre aceștia a promovat o perspectivă de consens asupra proceselor decizionale, dar nu s-a identificat un consens cu privire la formă și aplicații practice (Brustlein, 2018, p. 2). Autonomia strategică comportă o serie de înțelesuri în studiile de specialitate. Enunțarea sa în cadrul Strategiei Globale de Politică Externă și de Securitate a Uniunii Europene (2016) o asociază cu o abilitate a organizației de a „(...) promova pacea și securitatea în interiorul și în afara granițelor sale" (Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy, 2016, p. 9). Una dintre definițiile des întâlnite asociază conceptul cu următoarea explicație:

> (...) capacitatea de a stabili priorități și de a lua decizii în materie de politică externă și securitate, împreună cu mijloacele instituționale, politice și materiale pentru a le duce la bun sfârșit – în cooperare cu terți sau, dacă este necesar, singur. (Lippert *et al.*, 2019, p. 3)

Autonomia strategică este un concept predilect în politicile de securitate ale statelor. Un exemplu relevant în acest sens este modelul francez, care, în 2013, asocia termenul cu trei niveluri de definire: „politic, operaţional şi industrial şi tehnologic" (Arteaga *et al.*, 2016, p. 8). Prin intermediul acestor niveluri de acţiune, Franţa îşi propune să dezvolte capabilităţi, să acţioneze în comun cu partenerii săi şi, implicit, să genereze stabilitate în proximitate (Arteaga *et al.*, 2016, p. 8–9). Autonomia strategică a statelor se pliază pe implicaţiile suveranităţii şi pe modul în care leadershipul politic utilizează legitimitatea pentru a acţiona atât pe plan intern, cât şi extern.

Interpretările oferite autonomiei strategice polarizează mediul academic. În timp ce unii autori utilizează o perspectivă discursivă a liderilor europeni în raport cu acest subiect (Mauro, 2021, p. 2), alţii relevă interdependenţa crescută dintre state şi suprapunerea de responsabilităţi în rândul organizaţiilor internaţionale. Concretizarea autonomiei strategice depinde, de asemenea, de „evoluţiile constituţionale viitoare în integrarea UE între aprofundare, diferenţiere şi inversare" (Lippert *et al.*, 2019, p. 9). În rapoartele de evaluare ale mediului strategic, realizate de către instituţiile europene, autonomia strategică este frecvent menţionată ca fiind prioritară pentru evoluţia organizaţiei şi, implicit, a membrilor. Se recunoaşte astfel importanţa conducerii de misiuni în afara teritoriului statelor membre, în promovarea păcii (Abeele, 2021, p. 13), precum şi realizarea unor progrese privind propriile capabilităţi deţinute. În acest ultim subiect menţionat, adaptarea constantă a dimensiunii capabilităţilor polarizează liderii europeni, îngreunând transpunerea în practică a autonomiei strategice prin direcţii clar definite.

Fragmentarea înţelegerii autonomiei strategice rămâne o constantă în rândul liderilor statelor membre ale Uniunii Europene. Astfel, în timp ce ţări precum Belgia, Franţa, Germania, Luxemburg, Polonia, Portugalia, Slovacia şi, înainte de Brexit, Marea Britanie echivalează autonomia strategică cu agregarea voinţei politice, membrii din Europa Centrală şi de Est au o viziune mai aplicată, axată pe maximizarea capacităţilor civile şi militare în vederea asigurării securităţii (Lucia Retter *et al.*, 2021, p. 18).

Fiind un concept versatil şi greu de încadrat ca sens în interiorul unor graniţe definiţionale, autonomia strategică este criticată adesea de către cercetători şi practicieni. Pe măsură ce îngrijorările privind comportamentul Rusiei şi Chinei cresc, iar instabilitatea din Orientul Mijlociu se accentuează, diviziunea muncii cu NATO rămâne încă o

soluție operațională pentru Uniunea Europeană (Mauro, 2021, p. 5). Transpunerea în practică a autonomiei strategice se remarcă drept un deziderat, în lipsa unor membri hotărâți să traseze concret delimitările securității europene din punct de vedere politic. În timp ce unele state rămân fidele angajamentelor de apărare asumate în cadrul NATO, altele preferă o dezvoltare a autonomiei strategice cu un caracter complementar. Contradicțiile discursive devin persistente în acele contexte în care liderii europeni creionează o separare totală a Uniunii de capabilitățile euroatlantice, generând tensiuni între capacitate de decizie absolută și interoperabilitate.

Ce este reziliența?

Utilizat într-o paletă largă de domenii, conceptul interdisciplinar de „reziliență" este configurat la scară largă în științele sociale pentru a defini adaptabilitatea unor actori la concretizarea unor riscuri, mai precis, capacitatea acestora de a rezista. Termenul a fost introdus programatic și în domeniul relațiilor internaționale, odată cu teza lui Michel Foucault privind comportamentele statelor în situații de criză (Bourbeau, 2015, p. 374).

Răspunsul și timpii de reacție, determinarea unor schimbări sau reforme, precum și adaptabilitatea sunt toate elemente corelate cu un caracter rezilient, indiferent de natura actorului de referință. Ca în cazul multor alte concepte fără o definiție universal admisă, reziliența este asociată cu o serie de interpretări. Totuși, unii cercetători din domeniul relațiilor internaționale au definit-o drept un proces de ajustare a răspunsurilor formulate de către diverse entități (indivizi, societăți, state), „în fața șocurilor endogene sau exogene" (Bourbeau, 2015, p. 375). Dezvoltarea rapidă a practicilor reziliente a devenit o soluție prioritară pentru actorii statali și non-statali. Indicând un set de alternative pentru numeroase amenințări de securitate („inundații, criminalitate cibernetică, terorism, crize financiare, infrastructură critică, colaps și dezordine socială" (Brassett, Croft și Vaughan-Williams, 2013, p. 222)), reziliența presupune anticiparea evenimentelor traumatice și schițarea unor direcții de acțiune pentru a menține controlul.

Există diverse domenii în care reziliența se poate permanentiza atât ca practică discursivă, cât și la nivel operațional. Instituțiile publice, actorii privați, statele, dar și indivizii pot interfera cu termenul „reziliență" atunci când doresc să proiecteze un plan de contingență pentru situații ipotetice. Reziliența este asociată cu un proiect de edificiu

anticipativ şi a cunoscut o creştere a proeminenţei sale la nivel internaţional după atacurile teroriste din septembrie 2001. În acest context, conceptul a fost definit drept „abilitatea de a detecta, de a preveni şi, dacă este necesar, de a gestiona provocările perturbatoare" (Coaffee şi Wood, 2006, p. 504), în vederea limitării constante a unor ameninţări. Întrucât Uniunea Europeană este o organizaţie internaţională care a metamorfozat relaţionarea dintre state şi avantajele care decurg dintr-o cooperare structurată, reziliența ocupă un rol primordial pe agenda strategică. Dezastrele naturale, acţiunile subversive ale actorilor ostili din proximitate, dar şi pandemia COVID-19 au evidenţiat utilitatea practică a rezilienţei pentru construirea unei Uniuni mai puternice.

Chiar dacă a fost invocată deseori înainte de elaborarea Strategiei globale a UE, reziliența devine, din anul 2016, „unul dintre cele cinci principii directoare pentru rolul UE în lume" şi, implicit, un mod de a evalua securitatea pentru statele membre (Tocci, 2020, p. 176). Recunoscând realitatea unui climat de securitate în continuă schimbare şi a unor ameninţări tot mai virulente în apropiata vecinătate, Comunicarea Comună „O abordare strategică privind reziliența în cadrul acţiunii externe a UE" a accentuat condiţiile de schimbare şi necesitatea adaptării statelor după perioade de şoc (Tocci, 2020, p. 50).

Multitudinea domeniilor în care este definită reziliența întăreşte argumentul imposibilităţii comprimării tuturor explicaţiilor oferite într-un cadru unitar. Din acest motiv, este utilă identificarea unor definiţii de bază care interferează cu domeniul relaţiilor internaţionale sau prezintă o congruenţă specifică cu acesta.

Zona organizaţională prezintă prioritate pentru ceea ce numim „guvernanţă europeană" şi asigurarea funcţionării reţelelor instituţionale. Din acest motiv, reziliența este definită ca „abilitatea unei organizaţii de a absorbi tensiunea şi de a îmbunătăţi funcţionarea în ciuda prezenţei adversităţi" (Hosseini, Barker şi Ramirez-Marquez, 2016, p. 50), de a maximiza logica transformării riscurilor în oportunităţi. În spectrul social reziliența este multifaţetată. Conceptul vizează sectorial capacităţile indivizilor, a grupurilor compacte, comunităţilor de a favoriza organizarea şi de a rezista ameninţărilor de natură internă sau externă. Urmând logica definiţională propusă de Hosseini, Barker şi Ramirez-Marquez, definim reziliența în zona socială astfel:

> (...) capacitatea grupurilor sau comunităţilor de a face faţă stresului şi perturbărilor externe ca urmare a schimbărilor sociale, politice şi de mediu. (Hosseini, Barker and Ramirez-Marquez, 2016)

Aplicând conceptului filtrul sectoarelor de securitate propuse de către Școala de la Copenhaga (Buzan, Wæver și Wilde, 1998, p. 1), planul social se poate extinde progresiv, atât la nivel micro (indivizi, comunități), cât și macro (societăți, state, alianțe). Latura economică propune o definiție mai aplicată rezilienței, în termeni de minimizare a pierderilor: „abilitatea inerentă și răspunsul adaptativ care permite firmelor și regiunilor să evite pierderile potențiale maxime" (Hosseini, Barker și Ramirez-Marquez, 2016, p. 50). Plecând de la multidimensionalitatea teoretică a conceptului „reziliență", dar și elementele de natură practică ce sunt asociate cu acesta (mecanisme, planificări, anticipare, prevenție și răspuns, minimizare a pierderilor), această lucrare își propune să evidențieze retorica liderilor europeni (și non-europeni) în raport dinamica climatului de securitate și, implicit, instrumentele specifice de acțiune la nivelul UE privind operaționalizarea acestui concept.

Autonomia strategică a Uniunii Europene: deziderat politic?

Percepută de către unii autori drept o necesitate, iar de către alții un simplu deziderat politic, autonomia strategică a Uniunii Europene își începe evoluția odată cu Summit-ul franco-britanic de la Saint-Malo din 1998 (Daniel Fiott, 2018, p. 1). Indicațiile președintelui Clinton privind calibrarea implementării unei autonomii militare europene au fost direcționate înspre o statuare a echilibrului între capabilitățile asociate partenerilor. Totodată, nu se dorea să se „dubleze eforturile existente sau să discrimineze față de membrii non-UE" (Daniel Fiott, 2018, p. 1). Practic, o colaborare strânsă dintre NATO și Uniunea Europeană ar fi permis tuturor membrilor celor două organizații să își maximizeze interesele și, implicit, să desfășoare acțiuni autonome pentru stabilitate și pace.

Creșterea interdependențelor între state, colaborările comerciale extinse, dar și reticența unor cercetători privind iminența unui conflict tradițional, au eclipsat discuțiile de la nivel european despre importanța capacităților și capabilităților armate. Cu toate acestea, acțiunile Federației Ruse, amploarea fenomenului terorist, dar și războaiele înghețate din vecinătate au introdus constant tematica autonomiei strategice pe agenda discuțiilor. În 2016, Strategia globală pentru politica externă și de securitate a Uniunii Europene reiterează importanța autonomiei strategice pentru „a promova pacea și securitatea în interiorul și în afara granițelor sale" (European Union Global Strategy, 2016, p. 9). Brexitul și, ulterior, leadershipul american în mandatul lui Donald Trump au favorizat continuarea dezbaterilor privind împărțirea

muncii între NATO şi UE şi au adus în prim-plan problema capabilităţilor reale ale organizaţiilor pentru garantarea de securitate (Howorth, 2017, p. 454). În acest context versatil, „nesiguranţa cu privire la angajamentele viitoare ale Statelor Unite faţă de securitatea europeană" a fost dublată de atitudinea liderului american în raport cu mediul turbulent din Orientul Mijlociu (Zieliński, 2020, p. 5).

În limbajul Uniunii Europene, autonomia strategică este reprezentată de capacitatea de a dispune de resurse eficiente pentru îndeplinirea obiectivelor externe, atât singular, cât şi în acţiune cu partenerii (Morillas, 2021, p. 2). Acest deziderat a fost tergiversat de-a lungul timpului din cauza unei palete largi de factori: de la reticenţa statelor naţionale, lipsă de consens, dar şi lipsa de conştientizare din partea publicului pentru o „Europa asertivă" (Howorth, 2017, p. 457). De asemenea, schimbările de leadership din Statele Unite ale Americii şi câteva decizii proeminente (formarea alianţei militare AUKUS, lipsa consultărilor prealabile cu europenii privind retragerea SUA din Afganistan (Morillas, 2021, p. 3) au indicat problema autonomiei strategice a UE în raport cu unilateralismul decizional al SUA. Unii cercetători denumesc această relaţionare drept „dilema de securitate euro-atlantică" şi realizează un scenariu de dezvoltare în care capacităţile Europei ar putea conduce la o echilibrare în raport cu SUA (Howorth, 2019, p. 85). Elementele de natură decizională în aplicarea autonomiei strategice sunt şi ele multiple şi scindează membrii UE în două categorii: „suveranitatea deplină şi autonomia flexibilă în domeniul securităţii şi apărării" (Zieliński, 2020, p. 5). În timp ce îngrijorările cu privire la comportamentul Rusiei cresc (Mauro, 2021, p. 5), mai ales pentru statele de graniţă care resimt cel mai puternic efectele de undă ale crizelor din proximitate, autonomia strategică poate deveni o realitate doar prin intermediul unui consens politic.

Există o multitudine de cercetători care abordează problematica autonomiei strategice şi decuplarea decizională a Uniunii Europene de NATO în materie de politică externă. Printre aceştia, Frédéric Mauro operaţionalizează conceptul de autonomie strategică prin apelul la trei componente principale interdependente: voinţă politică, capacitate de a decide şi, respectiv, capacitatea de acţiune (Mauro, 2021, p. 11). Această ramificare procedurală face trimitere atât la prioritizarea consensului între liderii europeni, cât şi la capabilităţile reale de care Uniunea Europeană dispune pentru a fi un exportator relevant de securitate. De la Strategia Globală a Uniunii Europene şi până la lansarea Busolei Strategice, mediul de securitate a suferit o serie de metamorfozări.

A rămas autonomia strategică o constantă la nivelul Uniunii și, implicit, la nivelul discursurilor liderilor europeni? Secțiunea de analiză a lucrării va reflecta un răspuns în acest sens.

Cadrul analitic

În cadrul revizuirii literaturii de specialitate, am identificat o paletă largă de abordări privind analizarea Busolei Strategice și a evoluțiilor anterioare realizării ei. Studiile au subliniat importanța planificării strategice ca proces fundamental pentru elaborarea documentelor organizaționale. În același timp, cercetările au examinat dilema de securitate euro-atlantică și au identificat constantele prezente în strategiile emise de Uniunea Europeană. Toate aceste elemente au permis trecerea printr-un filtru critic a evoluțiilor care au precedat Busola Strategică din 2022. Dacă până în acest punct lucrarea a vizat o dimensiune teoretică a subiectului de cercetare, principalul obiectiv care va fi operaționalizat în partea de analiză este reprezentat de asocierea unor elemente discursive cu direcțiile de acțiune asumate în document.

În parcursul lucrării, mă voi axa pe doi factori majori care caracterizează Busola Strategică: elementele de reziliență și autonomie strategică. Acestea se regăsesc cu preponderență în corpul documentului și modelează și discursurile liderilor europeni (și non-europeni) despre o Europă rezilientă și autonomă decizional.

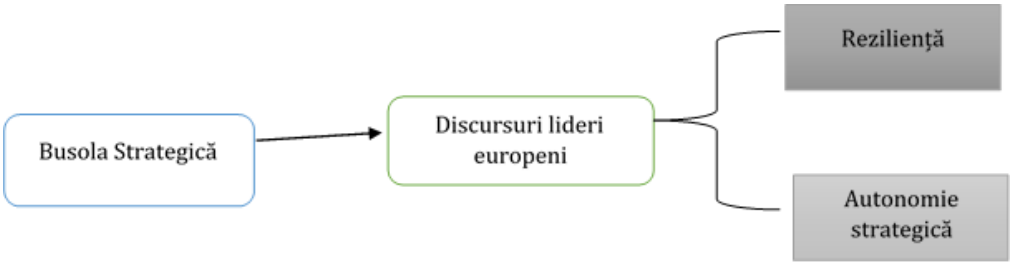

Figura nr. 1: Cadrul analitic[1]

Concluzionând, în cadrul primului capitol am abordat tema de cercetare prin definirea conceptelor securitate europeană, autonomie strategică și reziliență. Prin prisma revizuirii literaturii de specialitate, am conectat subiectul de cercetare cu studiile anterioare într-o manieră critică. Utilizând o abordare deductivă, am extras din literatura de

[1] Figura este realizată de autor, pe baza datelor extrase din literatura de specialitate.

specialitate principalele direcţii de cercetare portretizate în cadrul cadrului analitic. Acestea vor fi operaţionalizate în acord cu discursurile liderilor europeni şi vor stabili potenţialul de implementare al planului de acţiune intitulat „Busola strategică".

Metodologia cercetării

Dinamica activităţilor academice din ştiinţele sociale în ultimele decenii s-a axat pe „volumul crescut de cercetare empirică" (Gherghina şi Katsanidou, 2013, p. 333), aspect ce reflectă consistenţa problemelor identificate la nivel social, dar şi tendinţa specialiştilor de a le ancheta. Sistematizarea principalelor metode de cercetare utilizate într-o lucrare, indiferent de natura ei calitativă sau cantitativă, este un procedeu complex care necesită etapizare. Astfel, secţiunea dedicată metodologiei acestei lucrări îşi propune să sublinieze, pe rând, metoda de selecţie a cazului, instrumentul de colectare a datelor şi analiza utilizată.

Selecţia cazurilor

Generarea constantă de strategii de securitate, odată cu schimbările de leadership, sunt acţiuni asociate preponderent cu activitatea statelor. Plecând iniţial de la o formă de cooperare economică, Uniunea Europeană şi-a extins treptat sectoarele de activitate, devenind, prin intermediul procesului de integrare, un monolit în anumite domenii de competenţă. Datorită faptului că Politica Externă şi de Securitate Comună a Uniunii Europene face parte din categoria competenţelor speciale ce sunt gestionate de către organizaţie, principalele instituţii care se ocupă de definire şi aplicabilitate sunt Consiliul Uniunii Europene şi Consiliul European (*Repartizarea competenţelor în cadrul Uniunii Europene | EUR-Lex*, fără dată). Aspiraţiile Uniunii către rolul de actor global au fost evidenţiate în Strategia Globală de Politică Externă şi de Securitate din 2016. Concretizarea ulterioară a unor ameninţări în vecinătatea sa au temperat ambiţiile Uniunii Europene. Tensiunile din estul Ucrainei care validau o tendinţă beligerantă din partea Rusiei nu au fost diminuate cu ajutorul extinderii progresive a sancţiunilor economice (Bogzeanu, 2017, p. 166). Rolul de exportator de securitate fără deţinerea unor capabilităţi proprii, la fel şi activitatea complementară pe care trebuie să o desfăşoare în raport cu NATO, conduc la edificarea unei organizaţii multidimensionale, cu responsabilităţi multiple.

Cercetările dedicate aspectelor metodologice evidenţiază existenţa mai multor tipologii de studii de caz. În această lucrare, utilizăm un caz

prototip. Uniunea Europeană se încadrează cu desăvârşire în această categorie datorită particularităţilor unice care o diferenţiază de alte tipuri de organizații internaționale. Analiza critică a Busolei Strategice prin intermediul elementelor de natură discursivă vine să ofere moduri specifice de agregare a intereselor în rândul liderilor europeni. Dinamica legislativă, structura instituțională care dorește să minimizeze deficitul democratic, dar şi modul în care statele membre îşi prioritizează suveranitatea în domenii cheie, transformă Uniunea Europeană într-o platformă de armonizare sau concurenţă a intereselor naționale. Încercarea de a le armoniza pe acestea din urmă se pliază pe o politică de tip win-win, care relativizează consistența câştigurilor.

Metoda de colectare a datelor

Datele colectate pentru această lucrare acoperă dimensiunile enunțate în cadrul analitic, concentrându-se pe identificarea unor elemente discursive ale liderilor europeni (şi non-europeni) pe tematica autonomiei strategice, respectiv a rezilienței. Remarcând modul în care sunt relatate faptele şi fiind axate pe conținut, colectarea datelor aduce în prim-plan texte şi documente cu relevanță pe tematica propusă.

Declarațiile de presă, discursurile publice sau interviurile realizate de alți cercetători pe tematici afiliate reprezintă date operaționale pentru această lucrare. Prin urmare, având în vedere datele utilizate şi natura calitativă a acestora (documentele scrise, rapoarte oficiale, cărți de specialitate, articole științifice, statistici), analiza va surprinde doar schematic modul în care liderii europeni se raportează la implementarea direcțiilor de acțiune din Busola Strategică prin cele două filtre aplicate. În cadrul acestui studiu, criteriul utilizat în vederea selecției documentelor utilizate este cel al diversității, având scopul de a evidenția poziții politice cât mai variate despre subiectul propus. Documentele conțin cuvinte şi imagini înregistrate fără intervenția cercetătorului şi, prin urmare, oferă o resursă validă de interpretare pentru direcțiile stabilite.

Metoda de analiză a datelor

Metoda de interpretare utilizată în acest studiu este analiza tematică deductivă. În literatura de specialitate, termenul „analiză tematică" este integrat în categoria abordărilor calitative prin care se prezintă teme şi clasificări referitoare la date (Ibrahim, 2012, p. 40). O caracteristică importantă a acesteia, anume flexibilitatea, face referire la posibilitatea analizării unei game largi de tipuri de date, de la cele intitulate ca fiind „tradiționale" (metode de colectare (interviu sau focus

grup)),până la datele textuale, jurnale, forumuri de discuţii online sau alte surse media (Willig şi Stainton Rogers, 2017, p. 22). Cu ajutorul analizei tematice deductive, literatura de specialitate este codată pe baza principalelor tematici abordate. Acest procedeu are rolul de a extrage esenţa din datele colectate şi de a vizualiza principalele interpretări desfăşurate în zona de analiză.

În vederea exemplificării analizei tematice deductive pentru subiectul de cercetare aferent acestei lucrări, analizez succint datele primare obţinute în urma identificării discursurilor relevante. În prealabil, am identificat temele şi codurile regăsite predominant în literatură. Exemple ilustrative în acest sens se regăsesc în tabelul 1, unde se poate vizualiza principala temă, însoţită de subteme şi, implicit, de propoziţiile extrase din discursuri care se potrivesc codurilor.

Tabelul nr. 1: Exemplu de codare a temelor[2]

Tema	Coduri/Subteme	Propoziţii care se potrivesc codurilor
Busola Strategică	**Autonomie strategică**	„autonomia strategică europeană trebuie dezvoltată „în completare cu NATO"", *Emmanuel Macron,* (*European Strategic Autonomy after Macron's Trip to China | Wilson Center*, 2023) „capacitatea Europei de acţiune autonomă, ca o completare a NATO", *Emmanuel Macron,* (*European Strategic Autonomy after Macron's Trip to China | Wilson Center*, 2023) „Autonomia strategică trebuie să fie bătălia Europei", *Emmanuel Macron,* (*France's Macron Says Europe Must Develop Its Own Autonomy Separate From US - Bloomberg*, fără dată)
	Rezilienţă	„Europa ia în serios reziliența.", *Elisabeth Braw,* (*Judy Asks: Is Europe Taking Resilience Seriously? | Carnegie Endowment for International Peace*, fără dată) „am văzut o schimbare semnificativă în gândirea guvernelor despre rezilienţă şi am făcut parte din mai multe inițiative guvernamentale pentru a construi rezilienţa în anumite domenii", *Elisabeth Braw, (Judy Asks: Is Europe Taking*

[2] Tabelul este realizat de autor, pe baza datelor colectate.

		Resilience Seriously? | Carnegie Endowment for International Peace, no date) „UE s-a angajat să consolideze reziliența, ceea ce pandemia a arătat că îi lipsește Europei.", *Andrea Christou, (Judy Asks: Is Europe Taking Resilience Seriously? | Carnegie Endowment for International Peace*, no date) „Reziliența nu este ceea ce face Europa; este ceea ce este Europa.", *Caroline de Gruyter, (Judy Asks: Is Europe Taking Resilience Seriously? | Carnegie Endowment for International Peace*, no date)

În cadrul acestei secțiuni, am prezentat trei aspecte importante ale procesului metodologic: selecția cazului reprezentativ, metoda de colectare a datelor primare și codarea deductivă ca metodă de analiză a datelor brute. Analiza critică a Busolei Strategice va evalua transpunerea la nivel empiric, prin instrumente specifice, a dezideratelor autonomie strategică, respectiv reziliență.

Analiza

Privire de ansamblu

Busola Strategică este un document prioritar în materie de securitate și relații externe. Nevoia de elaborare a unui astfel de document strategic a fost conturată de necesitatea unor clarificări pentru „imaginea generală a cooperării UE în domeniul apărării" și, mai ales, de reducerea decalajului dintre dezideratele propuse și acțiunile care pot avea aplicabilitate (Pepios, 2021, p. 234).

Mediul de securitate volatil și amenințările complexe conturate în jurul anului 2020 au transpus în practică numeroase probleme de poziționare asociate Uniunii. Pandemia COVID-19 și sistemele de sănătate depășite, restrângerea unor drepturi ale cetățenilor, criza economică și persistența terorismului ca amenințare constantă, armele de distrugere în masă, dar și proximitatea Federației Ruse și a amenințărilor propagate, toate acestea au fost doar câteva dintre elementele radiografiate în Busola Strategică. De lungă durată și cu un impact copleșitor asupra drepturilor, economiei, sănătății, pandemia COVID-19 a creat necesitatea consolidării rezilienței sistemelor medicale și a definit o zonă de acțiune pentru care Uniunea a fost desemnată

„să-şi extindă competenţele şi puterile" (Renda şi Castro, 2020, p. 7). Chiar dacă managementul ameninţărilor transfrontaliere la adresa sănătăţii sunt fundamentate pe decizii ale UE (alături de agenţia coordonatoare Centrul European de Prevenire şi Control al Bolilor), insuficienţa bugetului şi strategiile de avertizare timpurie necesită metamorfozări complexe pentru o funcţionare optimă (Renda şi Castro, 2020, p. 5). Cu toate că pandemia COVID-19 rămâne un punct de inflexiune pentru evaluarea mediului de securitate înainte de redactarea Busolei Strategice, aceasta a adus în prim-plan nevoia empirică de o puternică reziliență. Mai mult, evaluarea riguroasă a ameninţărilor asimetrice a statuat în cadrul Uniunii nevoia de adaptare instituţională şi extindere de competenţe la cererea statelor. În discursurile publice susţinute de specialişti şi lideri europeni se evidenţiază deseori divergenţele de viziune ale statelor membre.

Din punct de vedere structural, Busola Strategică prezintă patru mari direcţii, în afara radiografiei iniţiale dedicate analizării mediului de securitate. Intitulate „acţiune", „securitate", „investiţii", „parteneriatele", secţiunile Busolei sunt însoţite de exemple concrete de acţiune, de o calibrare punctuală a capabilităţilor instituţionale deţinute. La toate acestea se adaugă partea de concluzii. Analizele critice statuate în literatura de specialitate pe subiectul Busolei Strategice sunt deseori contrastante. În timp ce unii autori atestă realismul operaţional al busolei şi modul pragmatic prin care se raportează la mediul de securitate, echilibrând potenţialul cu ambiţiile (Nováky, 2021, p. 112), alţii sugerează că documentul se concentrează în jurul unui tip de „securitate protectoare" care reduce şi dispersează capacităţile (Tallis, 2022, p. 3).

Busola Strategică oferă un plan de acţiune şi implementare până în anul 2030, evaluând inclusiv starea critică a conflictului dintre Federaţia Rusă şi Ucraina (Hartley, 2023, p. 4). În raport cu astfel de situaţii care afectează suveranitatea unui stat, cercetătorii remarcă o poziţionare fermă a Uniunii: „clauza de asistenţă reciprocă a Uniunii Europene, (...) obligă membrii să-i ajute „prin toate mijloacele în puterea lor" pe acei membri care se confruntă cu o agresiune armată". Cu toate că pot fi identificate lacune majore în ceea ce priveşte capacităţile, documentul reprezintă o „contribuţie originală de identificare a tehnologiilor critice unde UE este dependentă de naţiuni străine pentru aprovizionare" (Hartley, 2023, p. 4). Vizând conversia vulnerabilităţilor în puncte forte, acest document strategic oferă statelor membre ale Uniunii Europene sectoare multiple de dezvoltare în vederea maximizării securităţii.

În secțiunile următoare, voi trata succint implicațiile autonomiei strategice și ale rezilienței în cadrul documentului, totul în raport cu secvențele discursive identificate în rândul liderilor europeni înainte dar și după lansarea busolei.

Autonomia strategică

Utilizarea la nivel discursiv a conceptului „autonomie strategică" în raport cu Uniunea Europeană a stârnit valuri de controverse în rândul statelor membre, dar și al cercetătorilor. Într-unul dintre articolele sale, Frédéric Mauro categorizează statele în funcție de percepția asupra amenințării, susținerea securității europene respectiv, garanțiile de securitate oferite de NATO. Din perspectiva analizelor realizate de acesta, Italia, Spania, Grecia, țările Benelux, țările nordice, dar și Republica Cehă sunt printre statele care încurajează o apărare europeană mai integrată (Mauro, 2021, p. 13). Se mai adaugă și Franța, care dorește să își asume statutul de lider informal pe zona de proiectare a apărării. Capacitățile industriale ale Germaniei sunt și ele elemente care trebuie să primească o atenție deosebită, chiar dacă trecutul beligerant al statului a avut un ecou puternic în timp. Deși Polonia cunoaște o dezvoltare economică proeminentă în ultimii ani, mediată de apartenența la Uniunea Europeană, autonomia strategică europeană o plasează pe aceasta pe lista statelor care investesc o încredere absolută în NATO și angajamentele aferente de securitate. Mateusz Morawiecki, prim-ministru al Poloniei, afirma într-o declarație de presă susceptibilitatea sa cu privire la poziționarea Uniunii Europene în raport cu marile puteri economice actuale: „Autonomia europeană sună elegant, nu-i așa? Dar înseamnă mutarea centrului de greutate european către China și ruperea legăturilor cu SUA.". Având în vedere această sumară categorizare a statelor în funcție de balanța intereselor, putem opera la nivel teoretic cu una dintre concluziile induse în articolul lui Mauro: statele care percep amenințări reale și în proximitate nu vor renunța la NATO până la o alternativă europeană credibilă (Mauro, 2021, p. 9). Parteneriatul NATO-UE continuă să ofere statelor o pârghie de stabilitate în ceea ce privește complementaritatea dintre capabilități și capacități.

Liderii europeni portretizează la nivel discursiv interesele propriilor state în raport cu dinamica relațiilor internaționale. Atunci când discutăm despre autonomia strategică europeană, nu putem omite poziționarea fermă și de durată a președintelui francez Emmanuel Macron în raport cu NATO și Statele Unite ale Americii. Deși acesta susține coeziunea de tip parteneriat între UE și NATO, el subliniază în

anumite contexte modelarea deciziilor europene în raport cu statutul american faţă de o problemă: „Paradoxul ar fi că, depăşiţi de panică, credem că suntem doar adepţii Americii". Suplimentar, liderul francez mai menţionează şi dependenţa europeană de capabilităţile americane şi modul în care ea creionează direcţiile de politică externă „Nu vrem să depindem de alţii pentru subiecte critice". Criticat de mulţi de fermitatea poziţiilor sale în raport cu autonomia strategică europeană, Emmanuel Macron şi discursurile sale produc însă o conştientizare a lipsei de resurse tehnologice cu care Uniunea Europeană se confruntă. Chiar dacă aspiră să fie un exportator de securitate şi un model de rezilienţă la nivel organizaţional, Uniunea Europeană rămâne în confuzie atunci când autonomia strategică trebuie valorificată practic. Cu toate că Charles Michel, fost preşedinte al Consiliului European, a declarat că „A existat un salt înainte în ceea ce priveşte autonomia strategică în comparaţie cu acum câţiva ani", în realitate avizul favorabil din partea NATO continuă să funcţioneze ca o certificare a acţiunilor Uniunii Europene în materie de securitate . Una dintre cele mai consistente probleme de la nivelul UE rămân capabilităţile. Aşa cum indică literatura de specialitate, există numeroase probleme în sectorul industriei de apărare care necesită revizuire: „fragmentare, dublare, colaborare industrială insuficientă, o necesitate de consolidare a pieţei UE a echipamentelor de apărare (...) şi îmbunătăţirea competitivităţii industriei de apărare din UE" (Hartley, 2023, p. 10).

O dinamică surprinzătoare la nivelul discursurilor liderilor şi specialiştilor europeni (şi non-europeni) este reprezentată de relaţia dintre Uniunea Europeană şi Statele Unite ale Americii. Deşi este favorizată armonizarea şi dezvoltarea autonomiei prin parteneriatul cu NATO, modelarea deciziilor de politică externă prin influenţele americane solidifică păreri divergente. În acest context se creează o dilemă des invocată la nivel discursiv: deşi europenii îşi doresc o colaborare strânsă în NATO (majoritatea statelor membre sunt simultan membre UE), unele poziţii din spaţiul politicii se doresc a fi refractare, autonome. Situaţia este exemplificată la nivel discursiv atât de preşedintele Franţei, cât şi de fostul preşedinte al Consiliului European: „dacă această alianţă cu Statele Unite ar presupune că urmărim orbeşte şi sistematic poziţia Statelor Unite cu privire la toate problemele, nu". Fagmentul nu urmăreşte o eliminare a dezideratului principal de acţiune NATO-UE (evitarea suprapunerii eforturilor), ci necesitatea echilibrării raporturilor de putere care ghidează

Dacă, dintr-o perspectivă discursivă, autonomia strategică creează discrepanțe majore de opinie în rândul liderilor europeni, Busola Strategică vine să ofere lămuriri suplimentare despre poziționarea Uniunii față de parteneri. Astfel, încă din introducere este menționată importanța colaborării cu NATO în interdependență cu „respectarea deplină (...) a principiilor incluziunii, reciprocității și autonomiei decizionale a UE, (...) esențiale pentru securitatea noastră în ansamblu." Deși interpretarea președintelui francez asupra autonomiei strategice implică această componentă de independență decizională, autonomia strategică operațională rămâne pentru Uniunea Europeană un deziderat.

Reziliența

Asociată deseori cu aplicațiile „contemporane ale tratatului „Spre pacea eternă" al lui Immanuel Kant" (Anholt și Wagner, 2020, p. 17), Uniunea Europeană și-a propus, îndeosebi după criza sanitară COVID-19, să transforme reziliența într-o caracteristică cheie a stabilității europene. Conceptul exista în documentele strategice încă din 2016, de la lansarea Strategiei Globale, dar niciodată nu a părut mai necesară decât în timpul pandemiei. În timp ce unele studii vizualizează zona empirică a rezilienței ca un proces de jos în sus, plecând de la structurile locale (Anholt și Wagner, 2020, p. 18), alții invocă premisa societății globale mult prea disipate pentru a angrena acest deziderat. Indiferent de abordare, persistența în timp a nevoii de reziliență este proeminentă și în Busola Strategică, acolo unde este explicitată o dimensiune a reciprocității între membri, dar și în plan extern.

Elementele de natură discursivă pot evidenția înțelesurile asociate pe care zona de leadership le aplică pentru diverse politici și practici. La fel ca multe alte concepte utilizate în spectrul studiilor de securitate, reziliența a cunoscut diverse accepțiuni până în zilele noastre. Așa cum este prezentat și în literatura de specialitate, inițial aceasta a fost asociată mai mult cu prevenirea crizelor și șocurilor (Anholt și Wagner, 2020, p. 19), iar ulterior, accentul s-a deplasat pe capacitatea entităților de a gestiona aceste situații cu pierderi minime. Practic, acum reziliența se asociază cu menținerea „capacității unei comunități de a-și susține funcțiile de bază în cazul unui șoc și de a-și recupera în timp util după șocuri" (Anholt și Wagner, 2020, p. 19). Pentru a promova direcții orientative statelor membre cu privire la cultivarea rezilienței și a unei culturi strategice comune, Uniunea Europeană a elaborat, pe lângă strategiile tradiționale menționate până acum, și comunicarea „O abordare strategică a rezilienței în acțiunea externă a UE", în anul 2017. Acest

document de viziune comună are rolul de a sublinia importanţa resurselor financiare pentru stabilitate în timpul crizelor, dar şi post-criză, şi mai ales, modul în care structurile de guvernare locală sunt prioritare pentru consolidarea rezilienţei externe.

Secvenţele de natură discursivă care vin să sprijine importanţa rezilienţei în tandem cu viziunile din literatură sunt, în special, provenite din rândul specialiştilor care analizează subiectul. Astfel, subliniind faptul că „UE s-a angajat să consolideze reziliența, ceea ce pandemia a arătat că îi lipsește Europei.", unii analişti susţin numeroasele evoluţii pe care Uniunea Europeană le-a statuat în raport cu noile ameninţări ale mediului de securitate:

> Raportul strategic prospectiv pentru 2020 și Busola strategică au făcut multiple referiri la construirea unei Europe mai reziliente, în special în ceea ce privește clima, apărarea și energia. *Andrea Christou, (Judy Asks: Is Europe Taking Resilience Seriously? | Carnegie Endowment for International Peace, no date)*

Fiind o prioritate pentru Uniunea Europeană, reziliența este promovată și la nivel extern prin transferul de democrație și stabilitate pe care dorește să-l permanentizeze. Pentru „a construi societăţi incluzive, prospere şi sigure" (Anholt şi Wagner, 2020, p. 21), UE ajută, prin Politica europeană de vecinătate, statele din est şi sud în domenii cheie precum economie, securitate şi politică. Ameninţările care provin din aceste teritorii sunt multiple şi diverse, de la tendinţe beligerante ale unor actori statali până la instabilitate politică, economică şi societală. Această perspectivă de acţiune vine să crească reziliența membrilor UE prin atenuarea efectelor produse de undele crizelor în sectoare care necesită un nivel ridicat de reziliență (de exemplu, infrastructuri critice). Prin această „abordare cu mai multe faţete a rezilienţei în regiunile înconjurătoare" (Anholt şi Wagner, 2020, p. 21), Uniunea Europeană urmărește să gestioneze fluxul ameninţărilor externe şi, implicit, să reducă impactul acestora asupra statelor membre. Astfel, se realizează concomitent dezideratul prim asumat de construirea rezilienţei (prevenirea), cât şi adaptarea răspunsurilor într-o manieră calibrată, pentru a limita efectele negative (indiferent de natura acestora).

În cadrul Busolei Strategice, reziliența ocupă un loc central și se regăsește constant în toate cele patru secțiuni principale. Aceasta nu este privită ca un dat, ca o reglementare fixă, ci denotă un „concept dinamic care are nevoie de adaptare constantă" (Mölling şi Schütz, 2020). Asociată cu Politica de securitate și apărare comună în plan extern, dar și cu statuarea capacităţilor sociale și societale de a rezista în fața crizelor,

reziliența europeană poate fi evaluată într-o modalitate precisă atunci când măsurile adoptate sunt monitorizate într-o manieră activă. Exemple precum criza energetică, războiul din Ucraina sau gestionarea fluxurilor de refugiați pot fi studii de caz relevante pentru cercetarea rezilienței Uniunii Europene.

Concluzii

Această lucrare a avut drept scop analiza modului în care reziliența și autonomia strategică sunt implementate la nivelul documentelor strategice primordiale pentru activitatea Uniunii Europene. Având ca studiu de caz analiza critică a Busolei Strategice, studiul a oferit un răspuns pentru întrebarea de cercetare *„Cum abordează discursurile liderilor europeni din perioada 2022–2024 reziliența și autonomia strategică?*". Utilizând secvențe discursive regăsite în presa internațională în perioada 2022-2023, lucrarea a edificat nuanțele de înțeles ale conceptelor definite și a prezentat un cadru larg, cronologic al securității europene pentru ultimul deceniu. Constatările, dublate de o perspectivă critică a documentelor strategice (Strategia de securitate a UE din 2003, Strategia globală- 2016 și Busola Strategică – 2022), relevă faptul că Uniunea Europeană și-a temperat în ultimii ani viziunile de actor global, nu abandonându-le, ci punând un accent deosebit pe stabilitatea zonei regionale și a construirii în spațiul extern de actori reziliențI.

Constatările indică problemele cu care se confruntă Uniunea Europeană la nivel operațional, lipsa de capacități și capabilități fiind deseori criticată și subliniată drept un punct vulnerabil. Acesta conduce și la incapacitatea UE de a se remarca la nivel mondial ca un exportator relevant de securitate, iar perspectiva internă este și ea destul de fragilă. Scindarea statelor în mai multe categorii de interese, modul în care acestea prioritizează relația cu NATO datorită garanțiilor de securitate, dar și orientarea politicii externe în corelare cu SUA au fost constructe teoretice fundamentate în acest studiu.

Rezultatele confirmă, dintr-o perspectivă discursivă, rolul important pe care Uniunea Europeană dorește să și-l asume autonom pe scena relațiilor internaționale. Secvențele discursive ale liderilor europeni Charles Michel, Emmanuel Macron sau Josep Borrell doresc să evidențieze importanța parteneriatului UE-NATO, dar, în același timp, și autonomia politică față de SUA. Limitele cercetării constau în numărul redus de secvențe discursive identificate în presa internațională, precum și în faptul că, dată fiind natura sa calitativă, rezultatele nu sunt

generalizabile. Astfel, principala problemă care poate fi identificată este reprezentată de imposibilitatea aplicării acestor rezultate într-un mod exhaustiv. În cadrul cercetărilor viitoare destinate aprofundării acestei analize, utilizarea unor analize semantice ale documentelor strategice poate reprezenta o soluția mai aplicată privind validitatea rezultatelor. Acest tip de analiză ar putea viza atât documentele de referință, cât și rapoartele de implementare ale acestora elaborate la nivelul Uniunii.

Bibliografie

1. Abeele, Éric Van den. 2021. 'Towards a New Paradigm in Open Strategic Autonomy?' Working Paper 2021.03. Brussels: European Trade Union Institute (ETUI). https://hdl.handle.net/10419/299691.

2. Anholt, Rosanne, and Wolfgang Wagner. 2020. 'Resilience in the European Union External Action'. In Projecting Resilience Across the Mediterranean, edited by Eugenio Cusumano and Stefan Hofmaier, 17–36. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-23641-0_2.

3. Arteaga, Félix, Tomás Jermalavicius, Alessandro Marrone, Jean-Pierre Maulny, and Marcin Terlikowski. 2016. 'Appropriate Level of European Strategic Autonomy'. Ares Group Reports 8.

4. Atanasiu, Mirela, Cristina Bogzeanu, Cristian Băhnăreanu, Alexandra Sarcinschi, Cătălina Todor, Mihai Zodian. 2017. Evaluare strategică 2016: Crize și provocări la adresa securității internaționale. București: Editura Universității Naționale de Apărare „Carol I".

5. Becher, Klaus. 2004. 'Has-Been, Wannabe, or Leader: Europe's Role in the World After the 2003 European Security Strategy'. European Security 13 (4): 345–59. https://doi.org/10.1080/09662830490500008.

6. Blockmans, Steven, Dylan Macchiarini Crosson, and Zachary Paikin. 2022. 'The EU's Strategic Compass: A Guide to Reverse Strategic Shrinkage?' CEPS Policy Insight. https://ssrn.com/abstract=4136255.

7. Bourbeau, Philippe. 2015. 'Resilience and International Politics: Premises, Debates, Agenda'. International Studies Review, May, n/a-n/a. https://doi.org/10.1111/misr.12226.

8. Brassett, James, Stuart Croft, and Nick Vaughan-Williams. 2013. 'Introduction: An Agenda for Resilience Research in Politics and International Relations'. Politics 33 (4): 221–28. https://doi.org/10.1111/1467-9256.12032.

9. Brustlein, Corentin. 2018. 'European Strategic Autonomy: Balancing Ambition and Responsibility'. Éditoriaux de l'Ifri 16.

10. Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. Security: A New Framework for Analysis. Boulder, Colo: Lynne Rienner Pub.

11. Calderon, J. 2021. 'The European Union Strategic Compass'. Madrid: Instituto Espanol de Estudios Estrategicos.

12. Coaffee, Jon, and David Murakami Wood. 2006. 'Security Is Coming Home: Rethinking Scale and Constructing Resilience in the Global Urban Response to Terrorist Risk'. International Relations 20 (4): 503–17. https://doi.org/10.1177/0047117806069416.

13. Council of the European Union. General Secretariat of the Council. 2009. Strategia europeană de securitate : o Europă sigură într-o lume mai bună. LU: Publications Office. https://data.europa.eu/doi/10.2860/18429.

14. Daniel Fiott. 2018. Strategic Autonomy: Towards 'European Sovereignty' in Defence? LU: Publications Office. https://data.europa.eu/doi/10.2815/247228.

15. 'European Strategic Autonomy after Macron's Trip to China | Wilson Center'. 2023. 9 May 2023. https://www.wilsoncenter.org/article/european-strategic-autonomy-after-macrons-trip-china.

16. Fiott, Daniel, and Gustav Lindstrom. 2022. Strategic compass: new bearings for EU security and defence? Luxembourg: Publications Office of the European Union.

17. 'France's Macron Says Europe Must Develop Its Own Autonomy Separate From US - Bloomberg'. n.d. Accessed 3 May 2025. https://www.bloomberg.com/news/articles/2023-04-09/macron-says-europe-must-develop-its-own-autonomy-separate-from-us.

18. Gherghina, Sergiu, and Alexia Katsanidou. 2013. 'Data Availability in Political Science Journals'. European Political Science 12 (3): 333–49. https://doi.org/10.1057/eps.2013.8.

19. Hartley, Keith. 2023. 'European Defence Policy: Prospects and Challenges'. Defence and Peace Economics, March, 1–12. https://doi.org/10.1080/10242694.2023.2185425.

20. Hosseini, Seyedmohsen, Kash Barker, and Jose E. Ramirez-Marquez. 2016. 'A Review of Definitions and Measures of System Resilience'. Reliability Engineering & System Safety 145 (January):47–61. https://doi.org/10.1016/j.ress.2015.08.006.

21. Howorth, Jolyon. 2017. 'EU–NATO Cooperation: The Key to Europe's Security Future'. European Security 26 (3): 454–59. https://doi.org/10.1080/09662839.2017.1352584.

22. ———. 2019. 'Strategic Autonomy and EU-NATO Cooperation: A Win-Win Approach'. L'Europe en Formation n° 389 (2): 85. https://doi.org/10.3917/eufor.389.0085.

23. Ibrahim, M. 2012. 'Thematic Analysis: A Critical Review of Its Process and Evaluation'. In. https://www.semanticscholar.org/paper/THEMATIC-ANALYSIS%3A-A-CRITICAL-REVIEW-OF-ITS-PROCESS-Ibrahim/0c66700a0f4b4a0626f87a3692d4f34e599c4d0e.

24. Järvenpää, Pauli, Claudia Major, and Sven Sakkov. 2019. European Strategic Autonomy: Operationalising a Buzzword. Report / RKK - ICDS. Tallinn, Estonia: International Centre for Defence and Security.

25. 'Judy Asks: Is Europe Taking Resilience Seriously? | Carnegie Endowment for International Peace'. n.d. Accessed 3 May 2025. https://carnegieendowment.org/europe/strategic-europe/2022/10/judy-asks-is-europe-taking-resilience-seriously?lang=en&center=europe.

26. Lippert, Barbara, Nicolai Von Ondarza, Volker Perthes, and Stiftung Wissenschaft Und Politik. 2019. 'European Strategic Autonomy: Actors, Issues, Conflicts of Interests'. SWP Research Paper, 4/2019. https://doi.org/10.18449/2019RP04.

27. Lucia Retter, Stephanie Pezard, Stephen Flanagan, Gene Germanovich, Sarah Grand Clement, and Pauline Paille. 2021. European Strategic Autonomy in Defence: Transatlantic Visions and Implications for NATO, US and EU Relations. RAND Corporation. https://doi.org/10.7249/RRA1319-1.

28. Mauro, Frédéric. 2021. 'Europe's Strategic Autonomy: That Obscure Object of Desire'. L'Institut de Relations Internationales et Stratégiques.

29. Mölling, Christian, and Torben Schütz. 2020. 'The EU's Strategic Compass and Its Four Baskets: Recommendations to Make the Most of It'. Berlin: Forschungsinstitut Der Deutschen Gesellschaft Für Auswärtige Politik. https://www.ssoar.info/ssoar/handle/document/71305.

30. Morillas, Pol. 2021. 'Afghanistan, AUKUS and European Strategic Autonomy'. JOINT Briefs, no. 4.

31. Nováky, Niklas. 2021. 'The Strategic Compass: Charting a New Course for the EU's Security and Defence Policy'. European View 20 (1): 112–112. https://doi.org/10.1177/17816858211009978.

32. Pepios, George. 2021. 'Another Article on the Strategic Compass (Kind Of)'. European View 20 (2): 234–36. https://doi.org/10.1177/17816858211062490.

33. Renda, Andrea, and Rosa Castro. 2020. 'Towards Stronger EU Governance of Health Threats after the COVID-19 Pandemic'. European Journal of Risk Regulation, April, 1–10. https://doi.org/10.1017/err.2020.34.

34. 'Repartizarea Competențelor În Cadrul Uniunii Europene | EUR-Lex'. n.d. Accessed 3 May 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:ai0020.

35. Strategy, EU Global. 2016. 'Shared Vision, Common Action: A Stronger Europe'. A Global Strategy for the European Union's Foreign and Security Policy.

36. Tallis, Benjamin. 2022. 'Why Europe's Strategic Compass Points to Trouble'. Internationale Politik Quarterly, no. 2.

37. Tocci, Nathalie. 2017. 'From the European Security Strategy to the EU Global Strategy: Explaining the Journey'. International Politics 54 (4): 487–502. https://doi.org/10.1057/s41311-017-0045-9.

38. ———. 2020. 'Resilience and the Role of the European Union in the World'. Contemporary Security Policy 41 (2): 176–94. https://doi.org/10.1080/13523260.2019.1640342.

39. Wæver, Ole. 1996. 'European Security Identities'. JCMS: Journal of Common Market Studies 34 (1): 103–32. https://doi.org/10.1111/j.1468-5965.1996.tb00562.x.

40. Willig, Carla, and Wendy Stainton Rogers, eds. 2017. The SAGE Handbook of Qualitative Research in Psychology. Second edition. Thousand Oaks, California: SAGE Publications Inc.

41. Zieliński, Tadeusz. 2020. 'Strategic Autonomy of the European Union in Security and Defence'. Lithuanian Annual Strategic Review 18 (1): 5-22. https://doi.org/10.47459/lasr.2020.18.1.

THE GRAY ZONE PROBLEM, SECURITY ISSUES ARISING FROM THE INTERSECTION OF MILITARY AND CIVILIAN AFFAIRS

George-Mihai NICULA*

Abstract:

Military aggression has been a part of a nation's political arsenal since the very beginning of statecraft, being always available as a means to achieve a state's aims and objectives. This process primarily involved direct confrontations of armed forces on the field of battle, for the purpose of physically destroying the enemy side. Aggression done through indirect means held an equal, or even greater, importance in state competition, a state of affairs remarked by the earliest theoreticians of warfare. Operating in the liminal gray-zone between outright combat and non-aggression became a fundamental piece of successful foreign policy. This two-pronged approach to competition is necessary precisely because a nation's ability to wage warfare in the first place is dependent upon a series of domestic factors, which lay outside the realm of combat, such as demography, economy and the general will of the society in question. If successful, targeting these areas will have a significant impact on a state's ability to exert direct aggression towards others, operations of such a nature posing at the same time a lesser degree of danger for the aggressor. In today's international environment, the prospect of open war poses incredible danger for the participants, especially between developed countries, creating an incentive to resort to hybrid methods. In parallel, deep changes in the economic and social fabric of contemporary nations, especially those brought forth by technological development, have created new gray areas which are now being exploited in full by state actors, emboldened by an increasingly uncertain state of international affairs. This issue creates new security challenges both on a state and human level, leading to situations where large portions of civil society are the target of strategic operations, done through hybrid means.

Keywords: *gray-zone conflict, hybrid war, state aggression, international security, human security*

Introduction

The contemporary system of international relations is characterized by an increasing degree of instability, tension and uncertainty, caused by intense state competition and the efforts to change the order of global affairs pursued by dissatisfied actors. This broad paradigm is composed of multiple interconnected problems that should be studied both as

* Graduate of Lucian Blaga University of Sibiu, georgemihai.nicula@gmail.com

individual phenomena and as components of a broader trend. The problems that arise from the intersection of the civil and the military spaces is one such contemporary issue that should receive the attention of analysts, policy makers and the public at large, because of its deep and serious implications for national and human security. The phenomenon of "the gray zones" represents both a systemic feature of the modern security environment, where the integration of various sectors of a society contribute to its overall operational capability and position in the international hierarchy, but it also constitutes an opportunity for state actors to leverage influence over others in novel ways.

Research into the topic has attempted to establish a solid theoretical framework to characterize the phenomenon and apply it to a national policy context. This represents a good foundation on which the full impact of the issue can be understood more generally, especially its impact on human survival and living conditions.

Methodology and limitations

This paper uses the comparative method, in a qualitative manner, in order to showcase the nuances of the phenomenon of conflict in the gray zone, the participants engaged in this praxis, the operational framework they utilize, and the various documented instances of the problem in practice. Case studies are provided in order to better showcase the workings on in the issue and provide a more concrete level of analysis. The information has been selected from peer reviewed studies, speciality publications, think-tanks and credible journalistic sources.

The research is structured in four sections: the first tries to tackle the issue of terminology and definitions, aiming to create a framework of analysis for the subject matter, as well as attempt to trace the historical origins of the problem; the second part analyses the actors involved, with the theoretical assumptions they work under for fulfilling their objectives, the third part tackles the ways in which the phenomenon affects public life and compiles a series of recommendations on how to address that, while the fourth part encompasses the conclusions of the research.

Research in this area is limited by the purposefully obscure nature of the practice, with the doctrines and operations often being inferred after they even have already taken place, without any insights from the sources of gray aggression. There is a powerful incentive on the side of the attacker to keep these actions secret and deny any accusations that operations ever took place, while the target has a similarly powerful

incentive to deny that it has been victimized by a foreign agent, which makes the documentation of these events from open sources difficult. The attention of given to authoritarian states by the literature takes away from analysis of how democratic states engage in this sort of behaviour, either in a retaliatory or premeditate manner, which could provide important insights into the phenomenon and how it can best be addressed. Research can also be expanded to see how gray aggression can be used by non-state actors, notably terrorist and criminal organizations, to pursue their objectives. Analysts and academic should continue to tackle the problem and the security implications that emerge from it.

Terminology definition and historical context

The establishment of universally agreed upon terminology and definitions for a given phenomenon is a traditional challenge in the field of political and international studies. This dilemma is applicable in full for the problem posed by the intersection of military and civil affairs, because of the inherent ambiguity, fluidity and covertness of the actions employed by participants. A variety of terms have been proposed to designate the issue, including: irregular warfare, hybrid warfare, political warfare, asymmetric conflict, unconventional warfare or low-intensity conflict (Jones 2025). This paper will utilize the term gray zone conflict to refer to the subject matter. The notion of a "gray zone" was introduced by the US defence community, military publications and think-tanks (Jordan 2020, 1). It designates a space, be it physical, virtual or cognitive, where the traditional distinction between war and peace becomes impossible to assess with certainty, because of the tactics utilized in the context of state competition (Azad, Haider, and Sadiq 2023, 85). The use of "conflict" rather than "warfare" further emphasizes the broad level of application for the concept and the strategic ambiguity that defines the practice.

There is a debate about the level of overlap between GZC and other terms, notably hybrid warfare, and the level to which they can be used interchangeably. GZC and hybrid aggression combine the military power of a state with the involvement of non-combatants, in order to achieve strategic objectives. Both are characterized by a multidimensional approach towards competition, engaging the political, economic, social, informational, diplomatic and military sectors of a given country (Jordan 2020, 3-4). The difference between the two is that hybrid warfare explicitly has a primarily kinetic dimension, that operates simultaneously and is enabled by the non-military aspects, while GZC is specifically

focuses on the later, avoiding the overt application of hard power (Azad, Haider, and Sadiq 2023, 93). The scope of hybrid warfare similarly engages the whole of a society, in terms of participation in the conflict and the potential targets of aggression during it. GZC is enabled by the same logic and uses comparable means of aggression, but stopping at formalized military intervention (Carmet and Belo 2020, 21-22). Hybrid war can thus be viewed as a variation of GZC that takes places specifically in a wartime context, while GZC takes places in a permanent and continuous manner, outside of the scope of declared violence. The cause of this paradigm is that wartime success is increasingly dependent on peace time preparations, making the distinction between conflict and its absence increasingly nebulous. This rationale is what underpins all manifestations of GZC, with every domain of activity being a potential field of confrontation where actions must be taken without restrictions, in order to secure national advantage (Behrendt 2022). Keeping all this in mind, GZC can be defined as a practice done in the context of state competition, done by exerting influence outside of the military realm and implicating non-military domains of activity, for the purpose of weakening an adversary's strategic capabilities, all while keeping the aggression covert, ambiguous and at a low level (Azad, Haider, and Sadiq 2023, 88). GZC can occur in a context where all diplomatic and international standards of conduct are followed by both participants, making it harder to identify ongoing operations (Jordan 2020, 3).

Actions meant to lower a rival combatant's battlefield success, which targeted non-combatants, have been a staple of great power competition and conflict throughout the millennia (Atlantic Council 2022). The contemporary form of GZC is a result of war practices of the late modern period. Technological developments achieved in the late 19th and early 20th centuries have fundamentally altered the dynamic of the battlefield, making military success dependent on the prowess of the economic and industrial sectors of the participant nations, professional coordination of supply chains, domestic support and international backing. Conflicts of this era involved the mobilization of a high number of soldiers, equipped with state of the art weaponry, which resulted in a heavier degree of material and human casualties that did not necessarily translate into a definitive strategic advantage (Steinberg 2008, 4-5). The cost of direct conflict has further been raised by the invention of atomic weaponry, which fundamentally altered the risk calculus of conflict, to a degree that became unacceptable for the potential combatants and the rest of the international community (Kissinger 2014, 299). This severe problem lowered the overall level of

overt aggression between states, but did not eliminate their need for competition and the desire to subvert a rival's capabilities. GZC emerges in this context, especially in situations where a military confrontation would be symmetrical (Carmet and Belo 2020, 22-23). The globalization of the economic realm and the proliferation of digital technologies have increased the avenues for GZC operations to take place (Atlantic Council 2022).

Operational doctrines for CZG

The discussion about gray zone tactics largely conceives the phenomenon as actions employed by revisionist actors, who seek to challenge the US lead world order (Azad, Haider, and Sadiq 2023, 95-96), notably the Russian Federation (RF) and the People's Republic of China (PRC). This plays into a deeper collective anxiety about the position of the Western world in global affairs, which has lost a lot of its traditional influence and is in the position of becoming subject to the influence of other national actors (Mussetti 2023, 88-84). Authoritarian regimes have a predisposition for these behaviours because they have fewer restraints on the decision-making process and can intervene in more invasive ways in internal affairs, than their democratic counterparts (Carmet and Belo 2020, 22). International actors of this type have an advantage in GZC operations, because they don't have to be accountable to their own public (Jordan 2020, 10). Autocracies have GZC built into their strategic doctrines, while democracies are struggling to form a consensus around the issue and implement countermeasures at a society wide scale (Atlantic Council 2022). The interconnected global economy creates incentives for willful blindness to the antagonism of strategic rivals; authoritarian states provide resources and cheap labor that is used by liberal societies for short term gain (Carmet and Belo 2020, 37). The success of authoritarian states in the GZC realm normalizes and spreads the practice throughout the globe, eroding the framework and legitimacy of international law (Carmet and Belo 2020, 22). The degree to which Russia and China cooperate in GZC operations is unclear, taking into account the so-called "partnership without limits" between the two countries (Jones 2025).

Russia's gray zone strategy is opportunistic and adaptable, focusing on a multitude of operations that could succeed or not, rather than a concrete action plan. The lack of a written doctrine makes it harder to gather evidence for analyzing such a strategy, increasing the strategic posturing of the Russian state, but also makes it harder to

identify hybrid operations, leading to potential false positives (Jordan 2020, 9-10). The misnomer of "Gerasimov doctrine" is often used as shorthand for the GZC strategy of Russia but this is a misconception. This so-called doctrine is an attempt at creating an operational framework for pursuing the strategic outline proposed by former minister Yevgeny Primakov, which postulated that the RF should encourage the emergence on a multipolar international order that ends the global primacy of the USA, Russian dominance in its traditional sphere of influence and opposition to the expansion Nord Atlantic security structures. Primakov's term as foreign minister, beginning in 1996, marked a radical shift from Moscow's strategy of accommodating the West, to a path of independence and the later antagonism that we see today (Rumer 2019).

This attitude has become the new normal since the annexation of the Crimean Peninsula in 2014, wrapping up significantly after the invasion attempt started in 2022. GZC actions are deliberate and aim to undermine the credibility of Western collaboration and security structures in order to intimidate member states into giving political concessions or meeting the demands of the Kremlin and enabling its own war effort (Ng and Rumer 2019). Russia's efforts in this regard include: intelligence operations in the Western world meant to sway public opinion in the favor of its state interests, coercing states, companies of individuals from providing aid to Ukraine, preventing its own citizens from defecting, creating frictions between NATO members and interfering in democratic political processes. These aims are achieved through aggressive actions done below the threshold of war, often through third parties, in order to avoid getting responsibility pinned on Russian authorities and avoiding a singular military response from a target state, or even collective action from NATO. These actions have the added benefit of being significantly cheaper than a military intervention. Countries that did not provide support to Ukraine, like Hungary and Serbia, have seemingly not been attacked in this manner (Jones 2025).

Russian hybrid aggression was always underpinned by its significant hard power and its most successful operations in its near abroad have been reliant on this advantage. Military intimidation is employed as a form of psychological deterrence, in order to discourage a response from the target state. This includes actions like the violation of airspace, military exercises close to the border, the deployment of missile systems in Kaliningrad and the occupied Crimean Peninsula, or aggressive posturing around the nuclear arsenal. Moscow's GZC operations are initiated after a careful risk assessment and should not be viewed as reckless aggression on the part of Russian forces (Rumer

2019). Operations are commissioned by the political elements in Moscow, which are executed by the military state apparatus, with the Main Directorate of the General Staff of the Armed Forces of the RF being the likely coordinator of most operations (Jones 2025). Recruitment for Russian proxies is done online, employing gangs, youth or migrants to carry out criminal acts in the target state (Körömi, Roussi 2025).

Chinese GZC should be viewed as a confrontational form of cognitive control, intended to block or hinder opposition to the Chinese Communist Party (CCP) in the space of information, being more accurately classified as a political strategy, rather than a military project (Behrendt 2022). Two concepts are usually assigned to China in the space of GZC doctrines, those being "unrestricted warfare" and the three warfares"(3W) framework.

The former notion comes from the eponymous book, published in 1999 by military officials Qiao Liang and Wang Xiangsui. In the vision formulated by the two, contemporary conflict has blurred the line between combatant and noncombatant, with hackers, terrorists and financial speculators playing as much of a role in the achievement of military success as soldiers do. Armed force is no longer enough to compel the enemy to submit to one's will, the process requiring the full spectrum of means of influence that a state has at its disposal, be it formal or informal, lethal, nonlethal, thus making the practice of warfare unrestricted (Wojtowicz and Krol 2021, 167). The publication of the book has been met with a mixed response in China, with the potential policies proposed being too disruptive to the political, military and industrial establishments. As a result, unrestricted warfare has never been formally adopted as part of China's state policy. The publication of "Unrestricted Warfare" into English was interpreted as a potential influence operation in of itself, meant to create a distorted perception of China's actual strategic outlook (Behrendt 2022).

In the case of the latter, as the name suggests, the 3W framework consists of a triad of non-military aggression types: opinion warfare, psychological warfare and legal warfare, which are ultimately employed in order to weaken the adversary's ability to wage a conventional war against the PRC. The framework of this concept was first outlined in 2003 by the Chinese Communist Party Central Committee and the Central Military Commission (Behrendt 2022). Opinion warfare consists of disseminating information in a way that will create a useful or advantageous perspective on reality for Beijing, psychological warfare consists of using hard and soft power to intimidate other state actors into behaving in an advantageous manner and legal warfare consists of

influencing the international law system to constrain China's adversaries and enable the country's own strategic objectives (Wojtowicz and Krol 2021, 171).

Chinese GZC thinking emphasizes the ability to demoralize the enemy, while at the same time keeping the morale and coherence of one's own forces as high as possible. Operations carried out for this purpose must follow hierarchically the guidance of central commands and guidelines, gain the initial advantage by publicly releasing the information before other sources in order to shape the narrative, adapt to any changes or retorts within the story and using all available means to successfully complete the operation. 3W operations are implemented by political officers, military officials which hold a rank equal to commanding officers and have the responsibility to maintain party control over the military, as well as ensuring adequate conditions for the troops and cultivating good public relations. The 3W doctrine was developed as compensation for the failure to modernize the PLA within the desired time frame, with the initial goal to match the American military prowess by the year 2020, an objective now pushed towards the middle of the century (Behrendt 2022). Both of these GZC concepts are rooted in the CCP's threat assessment that concluded, after the turmoil of the Tiananmen Square events in 1989, the risk of military land invasion of the Chinese mainland by a military power is low and the main threat to the CCP will come from the realms of ideology and information, justifying the development of non-kinetic strategic capabilities (Behrendt 2022).

Although GZC is specific to the foreign policy of the most prominent autocratic regimes, it is by no means exclusive to it, with democratic governments also engaging in this type of tactic. This is partially the case because all regime types face the dilemma that direct conflict is both costly and dangerous, while competition remains necessary, creating incentives for indirect aggression. The other factor motivating this behaviour is the strategic success that autocracies had so far because of their use of GZC, encouraging the use of similar tactics to avoid ceasing advantage to them. Democratic regimes have a more limited scope in their GZC operations, such actions carrying a higher political cost. The US has been a constant target of GZC operations, owing to its position of global dominance, while its own attention had to constantly shift from one adversary to another (Atlantic Council 2022). America views the concept of GZC as a form of subversion exerted by hostile powers towards the USA, while its own practice aims to use military force in symmetrical conflicts, while avoiding the full

mobilization of the society, resources and administrative attention (Wojtowicz and Krol 2021, 167). In other words, it seeks to leverage the US' considerable military advantage over other countries to coerce them into certain behaviour, without actually committing to the use of force against them. A parallel can be drawn to the Russian concept GZC, similarly rests its ability to wage this form of aggression on a firm foundation provided by military backing. Because of its position of primacy in the international hierarchy of power and global rules-based system it upholds, America does not need to rely on covert pressure to pursue its strategic objectives, making its use of GZC minimal and the attention of its analysts have been on countering the use of the practice by its rivals. A notable use of hybrid war tactics by the US has been during the Gulf War, where military operations have been combined with diplomatic offensives and economic sanctions against Iraq (Wojtowicz and Krol 2021, 168). Chinese thinkers would identify this type of intervention as a successful GZC influence operation, that would later contribute to the development of PRC strategic models (Behrendt 2022).

GZC practices and their impact

The blurred lines between military and civilian has created situational ambiguity, which states leverage for strategic advantage, comes at the immediate cost of individual wellbeing and carries over broader social, economic and political implications for the targeted society. Human security represents the practice of identifying and addressing all-encompassing challenges to human survival, livelihood and dignity, endorsed as a framework by the United Nations, following the resolution 66/290 of the General Assembly (United Nations Trust Fund for Human Security n.d.). Based on manner in which gray aggression has an effect on the population of the targeted society, a typology of GZC operations can be established. The proposed classification includes: influence operations, sabotage operations, civilian endangerment, and military-civilian integration.

Influence operations represent offensive GZC actions that are meant to influence a target-state's behaviour or response capability by exerting political, psychological or economic pressures upon its population. Influence operations are used as a compensation for situations in which the use of conventional force is impossible (Hansen 2018). These efforts alter the way a state or society is viewed domestically and abroad by its partners, reducing the prestige and trust the state in question receives. The targets include both the general public

and the authority structures of a certain society, with the purpose of disrupting the latter's function (Behrendt 2022). An example of this practice is the Russian Federation's media operations against the Western nations, who has leveraged its informational advantage over Western countries to encourage division, social unrest, distrust into national authorities and political extremism. Russia supports both far left and far right movements as well as secessionist groups, such as those in Catalonia and Texas (Jordan 2020, 11). The cultivation of unrest being the main point, rather than any ideological promotion. Information operations were utilized to secure the annexation of Crimea, by further undermining local resistance. The rapid nature of the event put in the face of the West an already accomplished fact, which resulted in a weak international response that was largely countered by Russia at the United Nations (Azad, Haider, and Sadiq 2023, 96-97).

Economic pressuring involves the manipulation of resources in a manner that denies the rival's ability to fulfill their material needs. Economic sanctions, widely used by Western democracies and their allies, fall into this category of GZC. Mirko Mussetti identifies the economic dimension as a key factor in non-kinetic state competition, being just as important as information disruption. This is achieved through creating advantageous economic relations with other countries and disrupting this process for rival states in order to preserve the advantage (Mussetti 2023, 102-103). For the purpose of national interest, there is no clear hierarchy between military and economic affairs (Carmet and Belo, 37). This type of GZC measures is intended to coerce changes in behaviour, but their practical goal is to restrain the operational capacities of the target by imposing higher costs on their actions. For sanctions to have a real chance at success, trade links between the sender and the target must be significant before the sanctioning process, being a significant part of the GDP or sector for the target (Biersteker and Bergeijk 2015, 18-20). Democratic systems are the most vulnerable to sanctions, monarchies and personality dictatorships are somewhat vulnerable and military dictatorships and one party states are the least vulnerable, because they can impose the cost on political rivals or the general population (Biersteker and Bergeijk 2015, 24).

Sabotage operations represent offensive GZC actions that are meant to reduce a target's response capabilities by damaging its critical infrastructure, productive capabilities, coordination and communication structures. A prominent example of this type of activity is the destruction of submarine internet cables, perpetrated both by the RF and the PRC,

notably in the Baltic Sea and the maritime vicinity of mainland China. The purpose of these operations is to test the resilience and response capacity of the target state, disrupt its functioning and exert strategic pressure, all while avoiding responsibility for the act and a retaliatory response (Chiang 2025). Cable cutting also inflicts a substantial financial loss, draining state resources on repairs so they cannot be mobilized for another purpose (Rensbergen 2025). The ships used to carry out these operations are registered under foreign navies but stuffed with crews from the perpetrating nation (Chiang 2025; Jones 2025). The use of commercial vessels staffed by civilian crews to carry out the task of destroying critical communication infrastructure demonstrates a clear intersection with strategic interests. On the 26th of December 2024, the Russian oil tanker Eagle S was detained by Finnish authorities on suspicion of destroying underwater internet cables in the Baltic Sea by dragging its anchor along the seafloor, as well as potential espionage operations, based on equipment found on board (Rensbergen 2025). During the same year, the ship Yipeng 3 was linked to the destruction of 2 cables connecting Finland to Germany and Finland to Lithuania (Chiang 2025).

Russia has engaged in various cases of sabotage on the European mainland as well. The distribution of targets for these operations is as follows: 27% of the targets have been transportation vehicles, 27% were government and military locations and personnel, 21% against critical infrastructure and another 21% against industrial facilities. One common through-line for these operations is that the affected objectives could be linked to support given to the Ukrainian armed forces. Attacks have been carried out via explosives, incendiary devices, blunt or edge instruments, electronic means, with one instance of firearms use and even weaponized migration flows. The collateral damage and denial of services that results from these operations is a direct threat to the security of the general public (Jones 2025). Cyber-attacks are very hard to catalogue and attribute to a specific actor because they don't necessarily have physical effects. They could be used for gathering intelligence, rather than disrupting activities and the target state has the incentive to deny that the attacks took place (Jones 2025). When these actions have tangible effects, they are part of the sabotage operation typology.

Civilian endangerment represents imposing physical dangers upon non-combatants, in order to divert the authorities of that state away from a strategic objective, or for the purpose of imposing political pressure. A common form of endangerment is the use of migrants and an

instrument of GZC, by mobilizing them in a manner that puts their management, accounting and physical safety in the hands of the target state, as well as the logistical and moral burdens associated with their presence. Coerced engineered migration represents the creation and management of migration flows by a state actor. Similarly to other forms of pressuring listed earlier, the aim of the operation is to compel changes in a state's behaviour or manufacture a crisis situation that diverts attention and resources away from other operations. The flow of people is used as leverage, the intention being to coerce the target state into complying with the aggressor's demands, rather than face the issues caused by the movement and settling of migrants. This can be done by directing flows to a country that are larger than its ability to accommodate them, or by degrading the willingness of the target society to do so. The possibility or reality of a migration crisis creates two very strong and polarized responses: a pro-migration camp and an anti-migration camp. Agitation comes from the fact that these groups are both defending their position very ardently and have incompatible goals, which creates additional vulnerabilities that can be later exploited for GZC operations (Greenhill 2016, 24-26).

Countries in the vicinity of the European Union are aware that large flows of migration impose a high economic cost and anti-migration policies put into question the moral foundations of the European political project. This creates incentives for certain state actors to manufacture migration events, in order to extract economic benefits and political support, or as a retaliatory measure against unfavourable European rulings or remarks. The EU, in turn, has been reluctant to accept migrants since the Syrian crisis in 2015, leading to increased tension. This has been exploited by Belarus in 2021, as a response to sanctions imposed by Brussels over internal repression. Minsk has manufactured a migration crisis at the border with Poland, Lithuania and Latvia, by erasing entry policies for Middle Eastern migrants and enabling their travel towards the Western neighbors, thus creating a flow too big to handle by border authorities (Miholjcic n.d. 2-7). The migrants were later pushed back into Belarus by the border authorities of targeted countries (Greenhill 2022).

A more extreme form of endangerment comes in the form of direct attempts at an individual's life, deemed problematic to a state's agenda or undesirable. In 2024, US intelligence services warned their German counterparts about an attempt to end the life of Armin Papperger, CEO of Rheinmetall, a company manufacturing munitions and tanks for Ukraine (Lillis, Bertrand and Pleitgen 2024). James Appathurai,

NATO Deputy Assistant Secretary-General for Innovation, Hybrid, and Cyber, has officially confirmed that the assassination attempt was connected to Russia (Körömi, Roussi 2025).

Military-civilian integration is a political practice that aims to raise a country's strategic advantage by enabling cooperation between the military realm, the production sector and elements of the civil society. One of the most intensely studied variations of this practice is the military-civil fusion (MCF) developed by the PRC. The core of MCF is the participation of civilians in military affairs and the conversion of military efforts for civilian purposes. The concept also includes the development of logistics, the gathering of human capital and its mobilization (Kania 2019). This effort is intended to create and leverage synergies between economic development and military modernization, allowing the defense and commercial enterprises to collaborate and synchronize their efforts through the sharing of talent, resources, and innovations (Kania and Laskai 2021). MCF is frequently associated with the leadership of Xi Jinping, but the practice dates back further, to the era of Deng Xiaoping, who was the first to introduce the notion of synchronization between economic development and military modernization, as part of his economic reforms (Kania and Laskai 2021).

In this matter, China views America as an example to be emulated. The innovation environment of the US, involves the federal government, corporations and top universities, representing the platonic ideal of MCF, a fact often overlooked or ignored by American policy makers (Kania and Laskai 2021). Consequently, Beijing's MCF policies attempt to recreate an American style environment, under its direct supervision (Kania 2019). The freedom of association in the US innovation system is a comparative advantage. Companies and universities in China can impose a lower level of resistance to military co-opting, than their American counterparts, however these are less willing to collaborate by their own volition. (Kania 2019). The defense industry of China is dominated by state owned monopolies, which discourage the involvement of private enterprises in the domain, the latter are in turn unwilling to be subjected to unfair market competition. As a result, a great number of companies and universities are not openly involved in the MCF process (Kania and Laskai 2021). This constitutes a fundamental systemic issue for the Chinese MCF initiative, with the end goal of a state managed apparatus being at odds with the desire to emulate the market driven dynamism of the American approach.

The practice does complicate economic relations collaboration between the US and the PRC to a great deal. America already views

Chinese individuals and enterprises with a level of suspicion. The practice of MCF complicates this further, because of the fear of unwitting information transfers or accidental exchanges of dual use technologies (Kania and Laskai 2021). Products that result from MCF can be used in influence and sabotage operations. In 2020, a group of engineers from Lishui University in the PRC created an anchor-like device, meant to be used for cutting submarine cables by dragging it along the bottom of the sea, with the specification that a successful cut would be indicated by copper residue being specifically formulated on the patent. The explanation given for the development of this technology is to destroy illegally placed cables alongside the Chinese shores, but this has raised suspicion about its use in GZC efforts. The process of cable sabotage involves locating them, excavating the area and then performing the operation itself, which represents a complex and costly task. Having a specialized device that can perform the act in a short time frame, would greatly enhance sabotage operations by reducing the time frame and detection (Tatlow 2025).

Recommandations

Because of the amplitude and complexity of the issue, as well as the very large space in which it can manifest, there cannot be a single issue policy that addresses the problem in its totality. A response to GZC must be multidimensional, integrated, synergistic and constantly adaptable (Jordan 2020, 18).

Despite their systemic vulnerability to GZC, democracies have the advantages of transparency, a free press that can shine a light on irregularities and coherent and reliable alliance structures, all of which can be used to counter foreign operations (Atlantic Council 2022). Democratic governments should be proactive, instead of reactive, when it comes to narrative control. This should not be a call to distort the facts of a situation, rather to release them immediately, without giving GZC actors the opportunity to frame the story early on. The window for attack and the success of GZC operations is contingent on the conditions present in the target society. Domestic irregularities within a state provide openings for such situations to take place, increasing vulnerability to foreign interference. The disruptions brought worldwide by the COVID-19 pandemic have exacerbated these conditions to significantly higher levels than the pre-pandemic context (Jordan 2020, 10). Government and public institutions should build trust for their public and their international partners, through consistent displays of competence. Prioritizing special interests over

public interests gives external actors opportunities to discredit public trust in state institutions, or to exert influence through the individuals that benefit from those policies, who are susceptible to corruption or blackmail. Policy makers should focus on ensuring the smooth functioning of state mechanisms, in order to diminish potential attack vectors and opportunities for influence operations, as well as continuously be on guard for the ever-changing realities of gray zone competition. Educating the public about the dangers of GZC should be a core aspect of building resilience. The aim of this effort should be building a higher level of collective discernment about the ways in which GZC tactics affect them, and psychologically preparing the general population for such situations. Attempting to decouple the military and civilian domains would not necessarily reduce the risks associated with GZC, and has the very high chance of actually accentuating them, by forfeiting the strategic advantages brought by the cooperation between civil and military spaces.

Surveillance operations should be able to identify hybrid attacks as early as possible. Deconstructing the ambiguity of the attacker is very important for any counter measures for GZC operations (Azad, Haider, and Sadiq 2023, 100). The use of proxies to carry out operations reduces their professionalism and increases the chances of detection and interference from state authorities (Jones 2025). GZC actions can backfire, causing a rally around the flag effect (Jones, 2025). If it can be established early on that a foreign influence operation is underway, this can be leveraged to obtain public support and undermine the desired disruptive effect.

Because of their covert and unregulated nature, GZC situations are resistant to resolution. The international community is ill equipped to tackle the issue because it cannot influence participants actors and its historical focus has been preventing conventional wars, thus international institutions need to find novel ways to address this type of aggression (Carmet and Belo 2020, 24). Regional security organizations have a higher potential for gray conflict management, but a great deal of the resolution will depend on bilateral dealings between participants (Carmet and Belo, 36-37).

Conclusions

The use of GZC tactics presents a paradoxical interplay between the exertion of conventional force and the avoidance of escalation. Hard power must be left on the table in order to bring credibility to the coercive effect of the operation, but its actual use is counterproductive to

the motivation that underpins the use of GZC tactics in the first place. This inherent contradistinction underpins the entire praxis and must be kept in mind when evaluating an actor's predisposition and capability to engage in this type of competition.

GZC should be viewed as a faced of state competition, conflict and warfare. National state actors are the primary drivers and beneficiaries of this type of competition, but they are also the primary targets of GZC operations. The harm done to civilian elements is not a goal in of itself, rather an underhanded attempt to inflict strategic pressure on the institutions and response capabilities of the respective society.

The ability of a state to respond to gray zone aggression is condition by the degree of competence with which its internal structures are operated. In the case of democratic system, a well ran state apparatus, which is invested in the wellbeing of its citizenry is generally a harder to affect target, than a state with incompetent structures and an ambivalent attitude towards the matter. In turn, the general public should also cultivate an attitude of awareness and willingness to cooperate with the authorities, in order to ensure public safety from this type of threat.

Continued research into the phenomenon should be pursued, both in order to fill the gaps in the current vision regarding it, but also in order to the fluid, dynamic and ever shifting character that it displays. Measures that will eventually be imposed to counter gray zone aggression will eventually be overcome or subverted by potential attackers, a continuously evolving understanding is required to maintain competitive response capabilities. This effort requires multidimensional and multidisciplinary involvement, as well as good cooperation between the participants and proper public dissemination of the findings.

Bibliography

1. Atlantic Council. 2022. "Today's wars are fought in the 'gray zone.' Here's everything you need to know about it". Accessed May 10, 2025. https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/.

2. Azad, Tahir, Haider, Muhammad W. and Sadiq, Muhammad. 2023. "Understanding Gray Zone Warfare from Multiple Perspectives" *World Affairs* 186 (1): https://doi.org/10.1177/00438200221141101.

3. Behrendt, Paweł. 2022. "San Zhong Zhanfa or Three Warfares. Chinese Hybrid Warfare". Boym Institute. Accessed May 7, 2025.

https://instytutboyma.org/en/san-zhong-zhanfa-or-three-warfares-chinese-hybrid-warfare/.

4. Biersteker, Thomas, Bergeijk, Peter van. 2015. "How and When Sanctions Work? The Evidence" In *On target? EU sanctions as security policy tools*, edited by Iana Dreyer and José Luengo-Cabrera. EU Institute for Security Studies.

5. Carment, David and Belo, Dani. 2020. "Gray-zone Conflict Management Theory, Evidence, and Challenges" *The Air Force Journal of European, Middle Eastern, & African Affairs* 2 (2)

6. Ching, Gahon Chia-Hung. 2025. "Countering China's Subsea Cable Sabotage". Global Taiwan Institute. Accessed May 10, 2025. https://globaltaiwan.org/2025/03/countering-chinas-subsea-cable-sabotage/.

7. Greenhill, Kelly. 2016. "Migration as a Weapon in Theory and Practice". *Military Review*. November-December

8. Greenhill, Kelly. 2022. "When Migrants Become Weapons". *Foreign Affairs*. February. https://www.foreignaffairs.com/articles/europe/2022-02-22/when-migrants-become-weapons.

9. Hansen, Flemming Splidsboel. 2018. "Russian influence operations". Danish Institute for International Studies. Accessed May 7, 2025. https://www.diis.dk/en/research/russian-influence-operations.

10. Jones, Geth G. 2025. "Russia's Shadow War Against the West". Center for Strategic & International Studies. Accessed May 7, 2025. https://www.csis.org/analysis/russias-shadow-war-against-west.

11. Jordan, Javier. 2020. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict." *Journal of Strategic Security* 14 (1): https://doi.org/10.5038/1944-0472.14.1.1836.

12. Kania, Elsa B. 2019. "In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate". The Strategy Bridge. Accessed May 6, 2025. https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

13. Kania, Elsa B. and Laskai, Lorand. 2021. "Myths and Realities of China's Military-Civil Fusion Strategy". Center for New American Security. Accessed May 7, 2025. https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

14. Katie Bo Lillis, Natasha Bertrand and Frederik Pleitgen. "Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine". CNN. Accessed May 10, 2025. https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot.

15. Kissinger, Henry. 2014. *World Order*. Penguin Press.

16. Körömi, Csongor and Roussi, Antoneta. "NATO: There was officially a Russian plot to kill European weapons chief". Politico. Accessed May 10, 2025. https://www.politico.eu/article/nato-official-confirms-russian-plot-kill-european-weapons-chief-armin-papperger/.

17. Miholjcic, Nina. n.d. "Migration as an Instrument of Modern Political Warfare: Cases of Turkey, Morocco and Belarus" Jean Monnet Network on EU Law Enforcement Working Paper Series 12/22

18. Mussetti, Mirko. 2023. *Roza Geopolitică: Economie, strategie și cultură în relațiile internaționale*. Editura Militară.

19. Ng, Nicole and Rumer, Eugene. 2019. "The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture". Carnegie Endowment for International Peace. Accessed May 6, 2025. https://carnegieendowment.org/posts/2019/07/the-west-fears-russias-hybrid-warfare-theyre-missing-the-bigger-picture?lang=en.

20. Rensbergen, Arno Van. 2025. "Hybrid threats: Russia's shadow war escalates across Europe". The Parliament Magazine. Accessed May 10, 2025. https://www.theparliamentmagazine.eu/news/article/hybrid-threats-russias-shadow-war-escalates-across-europe.

21. Rumer, Eugene. 2019. "The Primakov (Not Gerasimov) Doctrine in Action". Carnegie Endowment for International Peace. Accessed May 9, 2025. https://carnegieendowment.org/research/2019/06/the-primakov-not-gerasimov-doctrine-in-action?lang=en.

22. Steinberg, John. 2008. "Was the Russo-Japanese War World War Zero?" In *The Russian Review* 67 (1): https://doi.org/10.1111/j.1467-9434.2007.00470.x.

23. Tatlow, Didi Kirsten. 2025. "Exclusive—Chinese Patents Reveal Aim to Cut Undersea Cables". Newsweek. Accessed May 10, 2025. https://www.newsweek.com/china-conflict-undersea-cables-cutting-internet-data-subsea-marine-baltic-taiwan-2012396.

24. United Nations Trust Fund for Human Security. n.d. "What is Human Security". Accessed May 10, 2025. https://www.un.org/humansecurity/what-is-human-security/.

25. Wojtowicz, Tomsz and Krol, Darius. 2021. "Chinese Concept of Unrestricted Warfare - Characteristics and Contemporary Use" *Humanities and Social Sciences* 28 (4): https://doi.org/10.7862/rz.2021.hss.39.

TRACE: A STRUCTURED AI-SUPPORTED MODEL FOR CULTIC RISK AND NATIONAL SECURITY THREAT ASSESSMENT

Iancu-Marius BUFNEA[*]

Abstract:

Understanding the structure, behavior, and risk level of organizations exhibiting cult characteristics is crucial for ***defense, public order, and national security system structures, policymakers, and researchers****. The range of organizations that exhibit these characteristics ranges from non-violent ideological movements to extremely dangerous extremist groups. This paper aims to develop an initial, first stage* ***framework for assessing cult and national security risks****, by creating an innovative multidimensional model that integrates* ***psychological, organizational, and security*** *indicators to assess organizations that exhibit cult-like characteristics. This framework, at later stages, after solid and comprehensive trial and testing by both AI and human subjects, can be refined and perfected as well as adapted in order to suit the specific needs of various branches and departments concerned with public order and national security.*

The difference between this academic effort and previous ones on the subject, which have taken into account in fragmentary and disparate evaluation elements such as psychological manipulation or leadership dynamics, is that this tool incorporates and integrates all these levels into a ***quantitative and qualitative scoring system*** *to assess the level of potential threat of an organization* ***to national*** *security. This framework provides a first-stage to-be-tested structured method of distinguishing between* ***high-risk groups, such as ISIS and Hizb ut-Tahrir, and low-risk ideological movements, such as the LaRouche Movement and NXIVM,*** *by assessing factors such as* ***charismatic leadership, ideological rigidity, social control, financial dependency, and security*** *threats. Moreover, by establishing a concrete framework for qualitative and quantitative analysis, the process of collecting and analyzing information is thus facilitated, in particular by clearly identifying the* ***direction of collection****, as we will see.*

The framework is applied to four distinct case studies: ***ISIS,*** *a global terrorist network that supports violent jihad and seeks territorial control;* ***Hizb ut-Tahrir****, an Islamist organization that promotes a global caliphate without engaging in direct violence but encourages ideological radicalization;* ***The LaRouche Movement,*** *a nonviolent political organization known for its conspiracy theories and hierarchical structure; and* ***NXIVM,***

[*] PhD student at the Babeș-Bolyai University of Cluj Napoca, Faculty of History and Philosophy, Doctoral School of International Relations and Security Studies, International Relations and European Studies domain. Police Inspector, specialist officer of the Schengen and International Relations Department within the Cabinet Service of the Cluj County Police Inspectorate. Cluj-Napoca. E-mail address: iancu.bufnea@ubbcluj.ro; b.iancumarius@gmail.com.

a self-improvement group that developed into a system of exploitation. The results illustrate how ***religious structures exist in different areas, but they have very different levels of risk. ISIS is approaching the maximum threshold, confirming its status as an existential security threat, while Hizb ut-Tahrir represents a latent risk through ideological radicalization. On the other hand, the LaRouche Movement and NXIVM, despite their internal coercive mechanisms, remain non-violent entities with minimal security implications for*** *national security.*

A significant advance in this study is the integration ***of artificial intelligence (AI).*** *AI can systematically process large amounts of data and assign preliminary scores based on* ***patterns, organizational behavior, and geopolitical impact****. However, the final evaluation and ranking of an organization* ***must remain a human-driven process****, in which* ***intelligence analysts critically evaluate the AI-generated ratings, validate the arguments behind the assigned scores, and ensure that ethical considerations are adhered to****. This approach aims to ensure both* ***efficiency and accuracy****,* ***while preventing the misclassification of non-violent groups****.*

This study demonstrates the applicability of the framework ***to various organizations,*** *providing* ***national*** *security structures with a refined tool to* ***assess, classify, and monitor risks and threats, while ensuring attention to ethical concerns****.*

Keywords: *national security, cults, analytical framework, OSINT, intelligence analysis.*

Introduction

In order to facilitate the operative and conceptual reference to the model developed in this work, it will be hereinafter referred to by the acronym **T.R.A.C.E.** (***Threat and Risk Assessment of Cultic Entities***). The T.R.A.C.E. framework proposes a structured, multidimensional methodology that quantifies the degree of danger associated with an organization by analyzing both psychological and ideological traits of a cultic type, as well as coercive organizational mechanisms and risk indicators with relevance to national security. This designation reflects the dual objective of the model:

(1) identifying and ranking the level of internal risk, respectively

(2) the estimation of the external threat that such an entity may pose to the constitutional order, institutional stability or security of the population.

Information analysis is a complex, time-consuming and demanding process for both the analyst and the operational team responsible for collecting, initial processing and transmitting data. Raw, unprocessed, and uncorrelated information needs to be transformed into actionable intelligence, but this analytical process poses many challenges.

From the very first stage of the analysis cycle, the right targeting of information collection is essential. If an organization shows

indications that it could pose a risk to national security or the constitutional order, it is crucial that the entire process – from collection to dissemination – takes place within a clear, well-defined and relevant framework.

Starting from this need, the present paper proposes a comprehensive analytical framework, applicable to organizations that present traits similar to cults and that may represent a threat to national security. Currently, there is no clear tool to differentiate between the level of risk associated with entities such as ISIS, which systematically resort to violence, and organizations that have not yet exhibited such overtly aggressive behaviors, such as the Antifa movement. This paper aims to contribute to filling this analytical gap. It is important to note from the outset that the proposed analysis focuses on factors that influence or have the potential to directly and significantly influence public safety component of national security, clearly distinguishing them from those that affect public order and safety only punctually or in the short term. To clarify this aspect, we mention the fact that within the specialized works, the concepts of national security, national defense and public order are included and incorporated into the field of national security (Mâță 2016). We shall thus use the definition according to which national security, according to the national legislation of Romania, represents the state of legality, balance and social, economic and political stability necessary for the existence and development of the Romanian national state as a sovereign, unitary, independent and indivisible state, for the maintenance of the rule of law, as well as for the climate of unrestricted exercise of the fundamental rights, freedoms and duties of citizens, according to the democratic principles and norms established by the Constitution. (...) National security is achieved by knowing, preventing and removing internal or external threats that can harm the values provided (...) (Parlamentul României 2014). On the other hand, Public order, as a component part of national security, represents the state of legality, balance and peace, corresponding to a socially acceptable level of compliance with legal norms and civic behavior, including in the digital environment. It is maintained, ensured and restored in case of disturbance, by specific police measures (Guvernul României 2023). In other words, we refer to public safety as a strategic element or level of national security and to public order representing, in essence, its strategic-operational level, at least from the point of view of this paper which focuses on the first element, as mentioned. This approach allows for a more nuanced and focused assessment of potentially significant risks to essential state structures.

Methodology

The TRACE framework is grounded in three complementary and well-established research traditions. The first concerns the study of cultic dynamics and coercive social control, which has documented mechanisms of thought reform, psychological manipulation, bounded choice, and dependency within closed groups (Lifton 1961) (Galanter 1999) (Lalich 2004) (Hassan 2015). The second draws on sociological and political analyses of charismatic leadership and hierarchical authority in insulated organizations, explaining how legitimacy, obedience, and internal discipline are constructed and maintained (Post 2014). The third integrates contemporary models of radicalization and violent extremism developed in security studies and intelligence analysis, which identify pathways through which ideological commitment, organizational structure, and grievance narratives translate into security threats (Horgan 2008) (Borum 2011).

The three analytical layers proposed in TRACE, namely basic cultic traits, coercive organizational practices, and national security risk indicators, represent a structured synthesis of these theoretical directions. The selected indicators reflect recurrent empirical patterns identified in historical studies of destructive cults and extremist movements, allowing TRACE to function as a coherent analytical architecture for examining organizations that combine ideological closure, internal coercion, and potential external destabilization.

First of all, in simple terms, it is important to mention that the intention of this paper is to provide specialists in the field of information analysis with a conceptual model that they can apply, after testing, refinement and adaption, to a wide range of organizations that are the subject of an analytical approach. Thus, the analysis framework will be structured on three levels: ***cult-type characteristics***, ***organizational practices***, ***national security risk indicators***, each level having its specific evaluation criteria and a well-defined scoring range. Following the study of the characteristics and particularities of organizations such as *Peoples Temple*, led by Jim Jones; Manson Family, led by Charlie Manson; Aum Shinrikyo, led by Shoko Asahara; Fundamentalist Church of Jesus Christ of Latter-Day Saints, led by Warren Jeffs; House of Dom Inácio de Loyola; Buddhafield, led by Jaime Gomez; Heaven's Gate, led by Marshall Applewhite; The Rajneesh (Osho) movement, led by Bhagwan Rajneesh and the Unification Church (Moonies), led by Sun Myung Moon, respectively, showed a number of such traits, each of which was assigned a possible score from 0 to the maximum specific to each category (6, 8 or 10 points), the maximum score total being 166 points, as follows:

BASIC CULTIC TRAITS (PSYCHOLOGICAL AND IDEOLOGICAL) – MAXIMUM 45 POINTS:

- **Absolute Charismatic Leader**: The central figure of the organization is considered infallible or the only legitimate source of truth.
- **Ideological exclusivism**: The organization claims to have the only correct interpretation of reality, and any different point of view is considered erroneous, dangerous or heretical.
- **Demonization of outsiders**: Anyone who criticizes or opposes the organization is considered an "enemy," "traitor," "heretic," or part of a conspiracy. In extreme cases, reference is made to the cosmogonic struggle subsumed by the Manichaean dichotomy.
- **Sacrifice on behalf of the group**: Members are encouraged to put their organization above their own personal good, sometimes even to the point of extreme sacrifice (excessive work, self-destruction, violent acts).
- **Psychological manipulation**: The use of complex and advanced strategies and techniques of psychological manipulation through fear, guilt and social pressure to maintain loyalty to the group and its interests.
- **Isolation from external influences**: Discouraging or effectively prohibiting contact with family, friends, or sources of information that contradict the group's ideology.
- **Promoting an apocalyptic or messianic mission**: The organization claims to be fighting to save the world or prevent an impending disaster.
- **Rigid hierarchy structure**: Decisions are made exclusively by the leader or by a small circle of initiates, without democratic mechanisms.
- **Absolute dogmatism**: Group beliefs cannot be challenged; any doubt is severely sanctioned.

ORGANIZATIONAL PRACTICES (CONTROL AND COMPLIANCE) – MAXIMUM 42 POINTS:

- **Information control**: Members are exposed only to information approved by leaders, and access to other sources is discouraged or prohibited, sometimes even using the principle *of need-to-know* adapted to the group's operating framework.

- **"Us vs. them" dynamics**: The organization creates an artificial separation between members and "others" (state, society, family, etc.), which reinforces dependence on the group.
- **Financial exploitation**: Mandatory donations or taxes are requested, and financial resources are concentrated in the hands of leaders.
- **Behavioral uniformity**: Strict rules regarding clothing, language, lifestyle or accepted thinking in the group.
- **Inducing a sense of duty or guilt**: Members are forced to feel that they have to "pay" for belonging to the group.
- **Punishments for dissidents**: Excommunication, intimidation, public defamation or even violence against those who leave the organization.
- **Creating a system of internal oversight**: Members are encouraged to supervise and report to their colleagues.

NATIONAL SECURITY RISK INDICATORS (VIOLENCE AND DESTABILIZATION) – MAXIMUM 79 POINTS:

- **Active and manipulative recruitment**: The organization seeks to attract members who are vulnerable (or in a period of psychological or social vulnerability), often using insidious or manipulative persuasion techniques.
- **Rejection of state authority**: The group argues that the government is totally or partially illegitimate, and members are urged to ignore or undermine the authorities.
- **Creation of parallel governance structures**: The organization seeks to replace or suppress state institutions through its own rules and systems of justice or administrative-political nature.
- **Glorification of violence**: Whether through propaganda or direct actions, violence is presented as a legitimate and justified solution to achieve the group's goals.
- **Militarization and paramilitary training**: Organizing training camps or preparing members for armed confrontations and/or affiliated militarized entities or structures.
- **Attacks on opponents or critics**: Using threats, intimidation, or even physical aggression to silence critics or detractors.
- **Illegal or non-transparent funding**: The Group obtains its funds through opaque methods, including fraud, trafficking, or sponsorships that may be illegal.

- **Indoctrination for extreme actions**: Members are convinced that they must commit attacks or sacrifice themselves for the group's cause.
- **Clandestine and subversive activities**: Organizing illegal actions to destabilize the social order.

The scoring architecture of TRACE employs differentiated maximum values for individual indicators in order to reflect their unequal analytical relevance to security risk. Certain traits, such as glorification of violence, indoctrination for extreme actions, rejection of state authority, or paramilitary organization, are consistently identified in the security literature as direct predictors of destabilizing capacity and violent escalation (Borum 2011). These indicators therefore receive higher maximal weights. Other traits, such as behavioral uniformity or ritual rigidity, primarily describe internal group dynamics and receive lower maximal values, as their direct impact on national security is indirect or can be of significance only in conjunction with others.

This weighted approach prevents mechanical aggregation that would artificially inflate the influence of marginal variables and aligns the model with established multi-criteria risk assessment practices in criminology and intelligence analysis (Heuer Jr. 2007) (Monahan and Skeem 2015). TRACE thus balances descriptive completeness with analytical proportionality.

Thus, to recap, each organization analyzed receives a score based on three dimensions:

1. **Basic cultic traits** (*Leadership and psychology*): Maximum **45 points;**
2. **Organizational practices** (*Control & Compliance*): Maximum **42 points;**
3. **National security risk indicators** (*Violence and destabilization*): Maximum **79 points;**

Each trait is **ranked on a score scale from 0 to a maximum of 10**, where:

- **0 = Not present at all** (There is no clear evidence of this trait in the organization)
- **1-2 = Present in a weak form** (Isolated or undeveloped elements)
- **3-5 = Moderately present** (Occurs frequently, but is not required for all members)

- **6-8 = Strong presence** (It is one of the defining traits of the organization)
- **9-10 = Dominant** (The trait is a central element, essential for the functioning of the group)

In order to further detail and explain this methodology, we exemplify through the following tables, for each dimension analyzed:

1. BASIC CULTIC TRAITS (MAX: 45 POINTS)

TRAIT	EXPLANATION	POSSIBLE SCORE (1-6)
Absolute charismatic leader	The group revolves around an infallible figure, who controls decisions.	**0** (no leader) – **6** (absolute leader, awe)
Ideological exclusivism	The group claims to have the only "true" interpretation of reality.	**0** (accepts plurality) – **5** (only group ideology is valid)
Demonization of outsiders	The group considers critics to be enemies or part of a plot.	**0** (accepts criticism) – **5** (labels all opponents as malicious)
Sacrifice on behalf of the group	Members are encouraged to put their organization above their own good.	**0** (no sacrifice requests) – **5** (members are obliged to give up everything for the group)
Psychological manipulation	Using fear, guilt, and social pressure for loyalty.	**0** (no handling) – **6** (continuous handling)
Isolation from external influences	Members are discouraged from having contact with family, society or the independent press.	**0** (no restrictions) – **4** (complete isolation)
Apocalyptic/Messianic Mission	The group claims to be fighting to save the world or prevent a disaster.	**0** (no such ideas) – **6** (the group's mission is perceived as crucial for survival)

Rigid hierarchical structure	The group has a strict hierarchy where decisions are made by a small circle.	**0** (democratic structure) – **4** (absolute hierarchy, unopposed)
Absolute dogmatism	Any doubt is considered a betrayal.	**0** (Ideological flexibility) – **4** (Rigid doctrine, any deviation is punished)

2. ORGANIZATIONAL PRACTICES (MAX: 42 POINTS)

TRAIT	EXPLANATION	POSSIBLE SCORE (1-8)
Information control	Restricted (or hierarchical) access to information.	**0** (Open access) – **6** (Absolute control, prohibition of any external source)
The "us vs. them" dynamic	Artificial separation between group and society.	**0** (Open collaboration) – **7** (Total separation, the group sees society as an enemy)
Financial exploitation	Members are forced to contribute financially.	**0** (No mandatory contributions) – **6** (Seizure of personal property)
Behavioral uniformity	The group imposes strict rules of life.	**0** (No Code Enforced) – **7** (Full Uniformity)
Inducing a sense of duty or guilt	Constant emotional manipulation.	**0** (No pressure) – **8** (Heavily induced debt/guilt)
Punishments for dissidents	Members who intend to leave the group are threatened with punishment or retaliation.	**0** (Leaving is free) – **5** (Severe punishment, violence or intimidation)
Creation of an internal surveillance system	Members are required to spy on each other.	**0** (No such practices) – **3** (Severe supervision)

3. NATIONAL SECURITY RISK INDICATORS (VIOLENCE AND DESTABILIZATION) - MAX: 79 POINTS

TRAIT	EXPLANATION	POSSIBLE SCORE (1-10)
Active and manipulative recruitment	The group uses aggressive methods to attract members.	**0** (Open Recruitment) – **7** (Manipulative Methods/ Forced Recruitment)
Rejection of state authority	The group claims that the state is illegitimate.	**0** (Accepts the authority of the state) – **9** (Actively militates against the state)
Creating parallel governance structures	The group replaces the state with its own structures.	**0** (No alternative structures) – **8** (Total parallel governance)
Glorification of violence	Violence is considered a legitimate means.	**0** (Non-violent) – **10** (Active encouragement of violence)
Militarization	The group has paramilitary training.	**0** (No Military Aspect) – **8** (Armament and Active Training)
Attacks on opponents	The group uses violence against critics.	**0** (No such attacks) – **10** (Organized attacks)
Illegal financing	The group has opaque sources of income.	**0** (Full transparency) – **8** (Illegal financing, crime)
Indoctrination for extreme actions	Members are persuaded to commit attacks.	**0** (No such tactics) – **9** (Active indoctrination)
Clandestine and subversive activities	Organizing illegal actions against the state.	**0** (Legal activities) – **10** (Organized subversive operations)

Final distribution of the score in the analysis framework

Analyzed size	Number of traits	Maximum score per trait	Maximum total score
1 . Basic cultic traits	9	6	45
2 . Organizational practices	7	8	42
3. National security risk indicators	9	10	79
MAXIMUM TOTAL	25	6/ 8/ 10	166

The methodology of evaluation and interpretation of the score is based on the prior quantification of the score obtained on each level and on each feature. After applying the scores, the organizations are classified in a risk category, as follows:

FINAL SCORE	RISK LEVEL
0 - 40	Minimal/non-existent risk
41 - 90	Cultic, but low risk
91 - 120	Moderate risk
121 - 149	High risk
150 - 166	Imminent risk / existential danger

The organizations analyzed through this methodological framework are then classified into one of five risk levels, each reflecting the degree of threat that the entity may pose to national security, in particular to the security component. Depending on the score obtained, recommendations can be made on the necessary measures from the institutions with responsibilities in the field of national security and public order.

At the first level of risk, corresponding to a score between 0 and 40 points, the organization is classified as representing a minimal or non-existent risk. It may have some marginal or latent cultic features, but it does not present elements of coercive control over members, does not promote extremist ideological views and does not adopt practices that could have a destabilizing impact on society, the state or the constitutional and legal order. In such cases, it is not necessary for the

security institutions to intervene directly, but it is necessary to maintain a discreet and adequate level of passive monitoring in order to detect possible developments that could indicate a change in the dynamics of the group or its associated practices. Moreover, if it is found that an organization falls into one of these risk levels, whatever it may be, it is mandatory that the entity be constantly monitored in order to identify indicators that point toward a potential transition to a higher level of risk.

The second level of risk, in the range of 41-90 points, includes organizations that have a moderate degree of cultic influence, but do not directly pose an imminent danger to national security. These entities may exhibit forms of control over members and adopt exclusivist rhetoric, but without resorting to violence or illegal activities. In this context, the strategy of discreet surveillance of security institutions must focus on monitoring public discourse, recruitment channels and possible developments that could lead to radicalization.

In the case of a score between 91 and 120 points, the organization is considered to have a moderate risk to national security. It can manifest tendencies of isolation from society, can use advanced techniques of psychological manipulation on members and can begin to openly reject the authority of the state, whether it is jurisdiction from a legal point of view or manifested against public officials or dignitaries. This category can also include groups that, although they do not directly resort to violence, encourage and/or issue discourses that justify hostile or destabilizing actions against state institutions, certain segments of the population or civil society. In such situations, the authorities must take proactive measures, including active surveillance, investigating sources of funding and assessing the risk of radicalization of members, so as to be able to prevent an escalation of the group's activities. At this stage, it is very likely that the entity itself or certain members of it have committed or have a manifest intention to commit acts that constitute a criminal offence. Thus, the measure of applying special methods of supervision or investigation, as specified and defined by the Code of Criminal Procedure of 2010 (LAW no. 135/2010), Chapter IV, art. 138, may be ordered immediately, namely:

(1) The following are special methods of surveillance or research:

a) interception of communications or any type of distance communication;

b) access to a computer system;

c) video, audio or photographic surveillance;

d) locating or tracking by technical means;
e) obtaining data on the financial transactions of a person;
f) detaining, handing over or searching postal items;
g) the use of undercover investigators and collaborators;
h) authorized participation in certain activities;
i) supervised delivery;
j) obtaining traffic and location data processed by providers of public electronic communications networks or providers of electronic communications services intended for the public

Here, we mention that such surveillance measures can obviously also be ordered at lower levels of risk, in compliance with all the legal norms in force, when there is reasonable suspicion about the commission of serious crimes. Also, these methods are provided by way of example, extracted from the national legislation in Romania, being considered appropriate and relevant since most European states or part of the North Atlantic alliance have adopted legislative elements similar to them. These methods are salutary starting with this level of risk, as organizations classified on one of the higher levels have the potential to implement actions that can lead to serious disturbances of peace and public order or even of the constitutional order, representing particularly serious crimes, resulting in extended custodial sentences. We mention, in this regard, the provisions of Article 397 of the Criminal Code, namely:

(1) Armed action undertaken for the purpose of changing the constitutional order or hindering or hindering the exercise of state power shall be punished with imprisonment from 15 to 25 years and the prohibition of exercising certain rights.

(2) Undertaking violent actions against persons or property committed by several persons together, in order to change the constitutional order or to hinder or hinder the exercise of state power, if national security is endangered, shall be punished with imprisonment from 10 to 20 years and the prohibition of exercising certain rights.

When the score obtained falls between 121 and 149 points, the organization is defined as having a high risk to national security. It adopts internal coercive structures, actively opposes state institutions, and may have the capacity to mobilize significant human and material resources for subversive actions. Groups in this category also generally exhibit an advanced degree of control over members, imposing drastic penalties on dissidents and resorting to practices that may include aggressive recruitment and the accumulation of resources for illegal purposes.

Security institutions must implement firm measures, including constant monitoring of group leaders, discovering and dismantling support networks and, where legislation allows, initiating concrete legal actions to prevent imminent risks.

The last level of risk, corresponding to a score between 150 and 166 points, signals an extreme and immediate threat to national security. Organizations in this category usually function as clandestine entities, consisting of paramilitary structures, illicit sources of funding and radical rhetoric that can lead to terrorist actions or violent acts against the state and the population. In such cases, the responsible institutions must take urgent measures, including counterintelligence operations, group infiltration, dismantling support networks and, where necessary, direct intervention through law enforcement.

International cooperation can also be key to tackling these groups, especially if they have cross-border links and external sources of funding.

Numerical scoring alone cannot, by any means, capture the complexity of organizational dynamics or their security implications. TRACE therefore incorporates an interpretative layer in which score distributions across analyzed entities are examined comparatively. This enables identification of structural patterns differentiating violent extremist organizations, latent ideological networks, and coercive but non-political cultic entities. The interpretation focuses on how combinations of cultic intensity, organizational coercion, and security-oriented behaviors interact to produce distinct risk profiles.

This approach corresponds to contemporary multi-level threat assessment frameworks used for analyzing hybrid non-state actors, where qualitative interpretation remains essential for extracting analytical meaning from quantitative indicators (Schmid 2013) (Schmid 2013). TRACE thus operates not only as a classificatory mechanism, but as a proposed structured lens for understanding how specific organizational architectures translate into differentiated security risks.

APPLICATION OF THE T.R.A.C.E FRAMEWORK TO SPECIFIC CASES

As mentioned in the introduction, one of the novelty and innovation elements proposed by TRACE is the integration of Artificial Intelligence within the information analysis process, in order to assess the degree of danger and threat to the national security of some organizations. To exemplify, we will use the ChatGPT tool from Open AI,

the paid version, version 4o. Thus, it will be requested to effectively apply the TRACE model for four organizational structures, about which it will collect information only from OSINT open sources. Thus, in the case of real-life analyses, the intelligence analyst will be able to either ask the model for the same actions, or personally enter the raw data and information collected as part of specific missions, asking the model to perform the preliminary analysis, and then critically evaluate the AI's assumptions and conclusions, in order to deliver an analysis that is as accurate and viable as possible.

The advantage of using this model is evident even when information cannot be obtained from open sources, the analyst having to rely exclusively on classified information collected by the operative teams. In this scenario, the analyst's work is facilitated by the fact that, from the direction phase of information collection, he is provided with a template with clear lines of action.

To exemplify the scenario mentioned above, let's assume that an institutional client – receiver and beneficiary of the intelligence product requests a certain intelligence service as the Primary Intelligence Requirement to find out whether or not the ISIS group represents a threat to national security. In this case, in the absence of a directive model, the analyst must make an additional effort, often time-consuming – which can in itself represent an additional danger, to establish Secondary and Tertiary Intelligence requirements (IRs), without having a structured guiding path. On the other hand, by using the TRACE model, the analyst already has the premises of the general direction for collecting information about ISIS, which can be used directly as Secondary IRs, the analyst only having to add Tertiary IRs, if necessary. Also, by using this model, the elaboration of the Intelligence Collection Plan (ICP) is significantly facilitated, and even the sources and methods of collection (OSINT, HUMINT, SIGINT, IMINT, etc.) can be more easily established.

Moreover, given the cognitive biases inherent in human psychology, through the existence of a clear qualitative and quantitative analysis framework, the subjective approach on the part of both the analyst and the operative teams is avoided as much as possible. In-depth studies in the field categorically support this approach, the author of the interpretation according to which major intelligence failures are usually caused by failures of analysis, not failures of collection (Heuer Jr. 1999, 65), supports the creation of standard models of information analysis that provide as few possibilities for error on the part of the analyst as

possible, by avoiding and raising awareness of cognitive biases. Heuer conceives and proposes the Analysis of Competing Hypotheses (ACH) as a structured analytical method created by him within the CIA, designed to help analysts avoid cognitive biases and make more rational decisions under conditions of uncertainty. The TRACE model complements and enhances the Analysis of Competing Hypotheses (ACH) method by providing a coherent framework for structuring assumptions, categorizing information and quantifying risks. Through its three levels (cultic traits, organizational practices and risk indicators), TRACE facilitates the formulation of comparable hypotheses in the ACH, reduces the ambiguity of the qualitative assessment and introduces a quantitative dimension that allows the prioritization of hypotheses on an objective basis. Thus, TRACE functions as an analytical filter that supports the selection and testing of hypotheses in a systematic way, reducing the influence of cognitive biases and ensuring the logical consistency of analytical reasoning.

Thus, we can apply the TRACE model in order to establish the degree of risk represented by ISIS, the analysis carried out by AI, exclusively based on OSINT, being as follows:

"Basic Cultic Traits (Leadership and Psychology) – ISIS Total Score: 45/45 (maximum)

1. **Absolute Charismatic Leader – Score: 6/6.** ISIS organized around a leader with the status of an infallible "Caliph". Abu Bakr al-Baghdadi was revered as the sole legitimate authority, with his cult of personality dominating the group (rand.org). Oaths of allegiance were made first to Baghdadi, then to ISIS (rand.org), indicating his central and undeniable role.
2. **Ideological exclusivism – Score: 5/5.** ISIS ideology proclaims that it holds **the only** "correct" interpretation of Islam, qualifying all other views as erroneous or heretical. As part of jihadist Salafism, ISIS has an *exclusivist* view that one's own version of Islam is the only authentic one, justifying violence against other Muslims through takfir (accusation of apostasy) (brookings.edu). In other words, anyone who does not adhere to the ISIS doctrine is considered an infidel.
3. **Demonizing outsiders – Score: 5/5.** ISIS systematically labels critics and external categories as *diabolical enemies*. Shiites, for example, are declared apostates guilty of religious

"innovation", a crime that in ISIS's view deserves death (theatlantic.com). The organization has an explicit Manichaean view of the world, dividing it into two camps – *us vs. them*, believers vs. non-believers – in which anyone who does not join them is an enemy worthy of destruction (philosophersmag.com). This perspective rhetorically justifies a "cosmic war" against all outsiders.

4. **Sacrifice on behalf of the group – Score: 5/5.** ISIS glorifies **martyrdom** and encourages its members to give their lives for the group's "cause." The group's propaganda *industrialized martyrdom*, widely using suicide bombers and suicide bombers as military tactics (theguardian.com). Between 2015–2016, ISIS carried out more than 900 suicide attacks in a single year, treating the deaths of its members as a heroic sacrifice and rewarded religious sacrifice (theguardian.com). This culture of supreme sacrifice shows that the followers of ISIS were ready to give up their own lives for the group (considering that they were either achieving earthly victory or the "paradise" of the martyrs).
5. **Psychological manipulation – Score: 6/6.** ISIS has used fear, guilt, and social pressure as deliberate tools to control members. For example, after suffering territorial losses, ISIS threatened its *defectors* through video messages, accusing them of treason and warning them with divine and land punishments if they left the fight (jns.orgjns.org). Such tactics – the threat of damnation in the afterlife or immediate execution – maintained obedience through terror. At the same time, ISIS inculcates guilt in potential Muslim recruits by suggesting that if they do not join the Caliphate, they are committing a grave sin against the faith.
6. **Isolation from external influences – Score: 4/4.** In the controlled territories, ISIS has imposed an almost total isolation of the population and members from the outside world, *cutting off access to independent information*. In Mosul, for example, he banned satellite television and destroyed satellite dishes, claiming that images of "infidels" *"brainwash"* Muslims (washingtonpost.com, washingtonpost.com). Also in Raqqa, ISIS banned **internet at home** and closed most internet cafes (theguardian.com). The goal was to block foreign news and prevent contact with outside family or friends, keeping members in a propaganda-controlled "information bubble."

7. **Apocalyptic/Messianic Mission – Score: 6/6.** ISIS's rhetoric is profoundly apocalyptic. The group claims that it fights according to end-time prophecies, considering itself a key agent of the coming apocalypse (theatlantic.com). ISIS ideologues frequently referred to the prophecy of the final battle of Dabiq against the "Romans" (Westerners) and the imminent coming of the global caliphate. This messianic vision gave the members a sense of **sacred mission**, presenting their war as necessary for the salvation of Islam and the establishment of divine order on earth.
8. **Rigid hierarchical structure – Score: 4/4.** ISIS had a strict internal hierarchy with no democratic mechanisms or internal contestation. All major decisions were made by Baghdadi and his select council (Shura/Delegate Committee), which ensured unified command over the entire territory. After the declaration of the Caliphate, ISIS created central institutions (e.g. *Administration of the Distant Provinces*) precisely to maintain **command of the leadership from the center** over the new occupied territories (ctc.westpoint.edu). Thus, global expansion was also governed by a hard core, directly loyal to the leader. There was no consultation of the rank-and-file members; on the contrary, military discipline and obedience were absolute.
9. **Absolute dogmatism – Score: 4/4.** ISIS's beliefs and rules were dogmatically imposed, any deviation being met with **Extreme retaliation**. The group instituted a regime of terror in which *any criticism or doubt* to doctrine was equivalent to treason. Through *City Documents* (2014), ISIS codified the obligations of life in the Caliphate and listed severe punishments – from amputation and stoning to execution – for deviations from the imposed religious line (institute.global). Basically, it governed through fear: the population quickly understood that the strict non-compliance with ISIS dogmas (such as the prohibition of smoking, music, the imposition of prayers on time, etc.) entails brutal punishments, sometimes filmed and publicly exposed, for example (theguardian.comtheguardian.com). This **Total intolerance** Compared to any other perspectives, it cemented a climate in which no one dared to challenge the dogmas of the organization.

Organizational Practices (Control and Compliance) – ISIS Total Score: 42/42

1. **Information Control – Score: 6/6.** ISIS exercised almost total control over the information to which members and the population had access. The organization **censored** any external sources: it banned unapproved TV shows and newspapers, blocked the internet uncontrollably, and used only its own media channels for propaganda. In Raqqa, for example, *all* private internet connections were banned, and most internet cafés were closed (theguardian.com). In Mosul, ISIS seized and destroyed locals' TV antennas to prevent them from watching foreign news or entertainment (washingtonpost.com). The goal was to isolate the community under an "information barrage" and ensure that members only receive **messages approved by ISIS**, safe from the "lies of infidels."
2. **"Us vs. Them" Dynamic – Score: 7/7.** From the beginning, ISIS has cultivated a total artificial separation between *ISIS community* and the rest of the world. The organization's discourse clearly demarcated the camp of the righteous believers (the mujahideen of the Caliphate) from the mass of "infidels" – be they local governments, Westerners or even Muslims who did not join them. This binary view of society – the world divided between good and evil – has been used to reinforce the addiction of followers to the group. ISIS has instilled in its members the idea that the Iraqi and Syrian state, and indeed the entire international order, are illegitimate and hostile to Islam. Through this rhetoric, *Exclusive loyalty* towards the group was encouraged, any links with "the others" being suspect. Analyses indicate that ISIS was imposing its authority and internal cohesion through **Terror and a dualistic vision** – society is either with ISIS (good) or against ISIS (bad) (institute.global). In this climate, members come to regard even former friends or family (outside the Caliphate) as potential enemies, reinforcing the break with the external society.
3. **Financial exploitation – Score: 6/6.** ISIS financed its "state" largely on the backs of the captive population, through **forced taxes, looting and confiscations** for the benefit of the leaders. Estimates show that about *half* of ISIS's revenue came from *taxing and extorting* local businesses and confiscating the

property of the subjugated (theguardian.com). The group imposed various forms of payment: from zakat (mandatory Islamic giving) and commercial transaction taxes, to absurd fines (for example, those who could not answer questions in the Qur'an were fined) (theguardian.com). In addition, ISIS robbed banks (in Mosul, it stole millions of dollars) and forcibly took over natural resources (oil fields, agricultural crops). All these funds were centralized non-transparently in the organization's treasury, financing the war machine and enriching the upper hierarchy. Basically, under ISIS domination, the population was systematically plundered, **without any public accountability of the leaders** regarding the use of money.

4. **Behavioral uniformity – Score: 7/7.** Daily life under ISIS was regulated down to the smallest detail, imposing a *single code of conduct* for all. Attire, speech, religious rituals, and even daily activities were strictly controlled. Women, for example, were required to wear *black full-face garments (niqab)* and could not go out unaccompanied. Men had to have beards according to Salafist norms and were forbidden to wear "Western" clothes. ISIS *banned cigarette* and hookah smoking, declared music illegal, and abolished all "non-religious" entertainment (theguardian.com). It also *imposed participation in daily prayers*: in Raqqa, taxi drivers were forbidden to work during prayer, and those caught not going to the mosque were punished (theguardian.com). Any offense – no matter how small, such as listening to music at home – was punished by public beatings, imprisonment or even exemplary executions. This forced leveling of behaviors created an almost totalitarian environment, in which individuals *suppressed their personalities* for fear of reprisals, automatically conforming to the group's rules.
5. **Inducing a sense of duty/guilt – Score: 8/8.** ISIS propaganda has intensively cultivated the idea that *every Muslim has a religious duty* to support the Caliphate – either by emigrating to ISIS territory, or by financial support or at least by declared loyalty. The group's ideologues preached that *Hijra* (migration to the Islamic State) is an **individual obligation** for believers. "[ISIS] doctrine requires believers to live in the Caliphate if possible" (theatlantic.com), notes Graeme Wood. Thus, those

who hesitated to join were made to feel guilty – as if they were betraying their religion by refusing *the "true Islamic State".* ISIS also offered potential recruits options to contribute: if they did not want to or could not fight, they were asked **for material support** – donations of money, equipment, help for the families of the "martyrs", etc. (gmfus.org). This manipulative approach lowered the barrier to entry into the organization: people felt that at least they had to "do something" for the cause of ISIS, otherwise they carry the burden of the sin of abandoning their Muslim brothers (gmfus.org). Essentially, ISIS has succeeded in turning participation in jihad (active or passive) into a *moral norm* so that members feel permanently beholden to the group and guilty if they do not contribute enough.

6. **Punishments for dissidents – Score: 5/5.** Leaving or betraying ISIS was considered capital crimes. The organization instituted cruel punishments – from *public executions* to **media lynching** – against any member who showed signs of dissent. Hundreds of real or supposed deserters were killed as an example. In 2014, for example, ISIS *executed ~150 members of the Sunni Albu Nimr tribe* who had resisted it, dumping their bodies in a ditch in Ramadi (theguardian.com). Those caught trying to flee the group's cities were also summarily "judged" as traitors – *"whoever flees is considered an apostate,"* warned ISIS, which had instituted *a ban on leaving* the Caliphate without permission (theguardian.com). Even high-ranking members suspected of plotting were eliminated (sometimes filmed to discourage others). In addition to physical violence, ISIS resorted to intimidation and defamation: it publicly called the disloyal "hypocrites" (munafiq) and threatened them with torment in the afterlife (jns.orgjns.org). In conclusion, the fear of extreme punishment has made *it almost impossible to leave ISIS*, thus keeping members captive in the organization.
7. **Creation of an internal surveillance system – Score: 3/3.** ISIS has developed an effective internal network of *Espionage and control*, designed to prevent betrayal or plots. There was a special security unit (Amniyat) that infiltrated informants among the fighters and the population, reporting any deviations or criticisms. Members were tacitly encouraged to keep an eye on their comrades and even their families, knowing that **everyone** could inform management of their loyalty.

According to research, after 2014 ISIS formalized counterintelligence structures to protect its *monitor its own activists and leaders*, applying strict discipline to them (institute.global). For example, if a commander was suspected of corruption or ideological deviation, he was immediately investigated by the caliphate's emissaries. This climate of permanent suspicion ensures compliance: *Anyone knew he could be tracked*. In addition, ISIS implemented "religious police" (Hisba) patrols that checked everyone in cities for compliance with the rules and recruited locals as informants. Through this ubiquitous surveillance system, **any thought of opposition was quickly discouraged**, the members becoming themselves guardians of the regime for fear of being denounced by others.

National Security Risk Indicators (Violence and Destabilization) – ISIS Total Score: 79/79

1. **Active and manipulative recruitment – Score: 7/7.** ISIS has carried out one of the most aggressive and sophisticated recruitment campaigns in the history of terrorist groups. Unlike the old al-Qaeda (which recruited slowly and selectively), ISIS *revolutionized recruitment tactics*, combining **modern online propaganda** with traditional methods of persuasion (gmfus.org). The organization leveraged social media, video platforms, and forums to reach a global audience of potential supporters in record time. ISIS's messages were carefully calibrated psychologically: first, the recruit was instilled with mental support for the Caliphate (legitimacy and obligation to support it) – without being directly asked for immediate violent action (gmfus.org). Through propaganda videos and online magazines (Dabiq, Rumiyah), ISIS *romanticized* life in the Caliphate and the jihadist cause, presenting it as a heroic and meaningful adventure. At the same time, it hid the cruel aspects, initially avoiding calling for attacks or suicide missions, precisely to **lower the moral barrier** of hesitant recruits (gmfus.org). Once sympathy was earned, ISIS moved on to stage *two*: it conveyed to new followers that it was time to prove loyalty – either by migrating to Syria/Iraq or by acting in their countries. This two-step strategy, along with the intense use of emotions (the humiliations

suffered by Muslims, the call for revenge, the promise of glory and "brotherhood"), allowed ISIS to recruit tens of thousands of followers from all over the world in a very short time (gmfus.or, ggmfus.org). Many of them were vulnerable young people, seduced by the clever propaganda of ISIS that promised them identity and purpose.

2. **Rejection of state authority – Score: 9/9.** ISIS has openly and violently challenged the legitimacy of any existing state, proclaiming that *the only legitimate authority* is their theocratic Caliphate. The group urged its members and supporters **not to recognize the laws or governments** of their home countries. At its peak, ISIS erased the official border between Syria and Iraq – in 2014 it blew up border crossings and declared the "end of the Sykes-Picot era" (aljazeera.com), i.e. the arbitrary cancellation of borders established by colonial powers. This symbolic gesture was accompanied by intense rhetoric: ISIS called modern states in the Middle East *"illegitimate constructs"* and their governments – apostate, corrupt or puppets of the West. For example, it proclaimed *the "Caliphate"* in the conquered territories, claiming its exclusive sovereignty and asking the Muslim community to obey it at the expense of all other loyalties. In the controlled territories, ISIS completely eliminated the institutions of the previous states: the administration, courts and law enforcement of the Syrian and Iraqi governments were either destroyed or seized. Through such actions, ISIS sought to undermine the existing state order – both locally (through rebellion and the establishment of its own government) and globally (by inviting followers abroad to civil disobedience). The statements of its ideologues make it clear that *"worldly governments"* have no authority – *"Allah is sovereign, not the laws of men"* was a motto – so members had to ignore or destroy the laws of "taghut" (worldly tyrants). This refusal of any secular authority has turned ISIS into a direct threat to the sovereignty of states in the region and beyond.
3. **Creating parallel governance structures – Score: 8/8.** In the conquered areas, ISIS replaced or suppressed state institutions with **its own administrative and legal apparatus**, establishing a totalitarian type of government. The group divided the territory into *wilaya* (province) according to the Islamic historical model and appointed governors (wali) and

kadis sharia in each. He established *Sharia Courts* which eliminated the pre-existing civil courts, judging everything according to their radical interpretation of Islamic law. It also organized *Police force* (Hisba – morality police, and military internal security force) who took the place of the regular police, constantly patrolling and enforcing the group's rules. ISIS created **diwans (government departments)** specialized – from Diwan al-Ta'lim (Education), which dictated the Islamist school curriculum and took out "non-Islamic" subjects, to Diwan al-Sihha (Health), which managed hospitals, or Diwan al-Zakat, which collected taxes and distributed part of it as pseudo-social aid. These structures were meant to make the Caliphate function as a full-fledged state. The organization has also issued identity documents and certificates (e.g., marriage certificates under the ISIS seal), set up its own markets, and even tried minting a currency (the ISIS gold and silver dinar). *"City Documents"* 2014, distributed to residents, practically served as a **constitution** of the Caliphate, setting out the obligations of citizens and the corresponding punishments (institute.global). All these mechanisms demonstrated that ISIS was not only a terrorist group, but aspired to the quality of *quasi-state entity*: it suppressed the legitimate state administration and put in its place its own theocratic system of government, subordinate to the jihadist command.

4. **Glorification of violence – Score: 10/10.** Extreme violence was not only practiced, but also *Celebrated openly* by ISIS as a legitimate and even desired tool for achieving its goals. The group's official propaganda abounds in images of cruelty elevated to the rank of virtue: executions filmed in detail, public beheadings, burning alive, throwing from buildings – all presented as *Vigilante shows* meant to frighten enemies and inspire followers. ISIS inherited from its predecessor in Iraq (Zarqawi's group) *proclivity for violence and its glorification* (bearworks.missouristate.edu). For example, after the impact of beheading videos began to wane, ISIS innovated even more shocking methods: it broadcast a video in which a prisoner Jordanian pilot was burned alive in a cage, justifying barbarism as "legal" punishment and a triumph of faith (reutersinstitute.politics.ox.ac.uk). At the same time, propaganda

combines cruel images with *Complimentary messages*: fighters who commit acts of extreme violence are presented as heroes, "lions of Islam" who bring divine justice. Even social media channels that recruited young people displayed, along with bloody pictures, posts describing *Romanticized Adventures and Rewards* for those in ISIS (jnslp.com) – associating violence with enthusiasm and glory. Thus, ISIS's organizational culture normalized and encouraged gratuitous violence: mass executions were proudly announced, suicide bombings were called *"Martyrdom operations"* and celebrated in songs (nashid). In essence, ISIS has turned violence into a *brand of terror* – a central means of communicating its power – and in a value in itself, suggesting to followers that ruthless cruelty is not only allowed, but even **virtuous** in the service of the cause (institute.global). This glorification of violence fueled the rapid radicalization and atrocious behavior of the members, constituting a clear indicator of the danger that the group represented.

5. **Militarization and paramilitary training – Score: 8/8.** ISIS organized as an irregular army-type military force, investing heavily in *the combat training* of its members, including children. The group set up dozens of **training camps** where recruits were trained in weapons handling, guerrilla tactics and religious indoctrination. Images released by ISIS show cohorts of youths in uniform, running on shooting ranges or firing Kalashnikov under the supervision of instructors. Child soldiers ("Caliphate Dogs") were also trained in these camps – a well-documented phenomenon, from *public executions committed by minors* to Qur'anic memorization competitions followed by military exercises (ctc.westpoint.edu). Between 2014 and 2016, ISIS increasingly routinely integrated *children and adolescents onto the battlefield*, using them as engineers, spies or suicide bombers, according to CTC West Point (ctc.westpoint.edu ctc.westpoint.edu) reports. In addition, ISIS has seized huge amounts of weaponry (tanks, artillery, armored vehicles) from the Syrian and Iraqi armies and has formed structured paramilitary units (full of experienced fighters, including former Baathist officers). At its peak, ISIS had *tens of thousands of* armed fighters, organized into

brigades and battalions, coordinated by a central command. This intense militarization allowed them to carry out classic offensives (such as the siege of Kobane) and maintain *territorial control* over a vast area for several years. Basically, ISIS has behaved like a professional jihad army: it has systematically trained fighters (local and foreign), equipped them with heavy weaponry and used them in both conventional and unconventional terrorist operations. The ability to operate as a disciplined military force has made ISIS particularly dangerous, far exceeding the usual level of an insurgent group.

6. **Attacks on opponents or critics – Score: 10/10.** ISIS has resorted to *assassinations and massacres* to silence any opponents, whether individuals or entire groups. Targets have included local journalists, anti-ISIS activists, tribal leaders who refused to obey them, rival Muslim clerics and, of course, members of the security forces or politicians of states in the region. The modus operandi was extremely brutal, meant not only to eliminate a critical voice, but also to send a message to the terror of the surrounding community. A notorious example: in the summer of 2014, the Sunni tribe Al-Shaitat in eastern Syria revolted against the occupation of ISIS; In retaliation, the jihadists executed **nearly 700 members** of the tribe (including civilians) in a series of filmed massacres, leaving their bodies exposed for days (en.wikipedia.org). Similarly, in Iraq, ISIS killed hundreds of members of the Albu Nimr tribe, known for opposing extremists – in a single mass grave in Ramadi 150 bodies of the tribe were found, all *shot for daring to confront ISIS (*theguardian.com). Citizen journalists from the group "Raqqa is Being Slaughtered Silently" who documented ISIS abuses were hunted down and murdered, some even in refuge in Turkey. ISIS has also issued *death sentence fatwas* for public figures who have criticized them: for example, it has claimed responsibility for the killing of moderate Muslim clerics labeled "apostates" for condemning the group's violence. Through such actions, ISIS demonstrated that it **does not tolerate even the slightest opposition**: any critical voice was met with threats and, very often, physical elimination. The terror established made many locals or even potential internal

dissidents not dare to express themselves. In conclusion, ISIS's strategy of *exterminating its opponents* – often publicly – confirms the extreme level of risk it represents: an actor who consolidates his power through localized genocide and the *export of assassinations* (including attacks in Paris, Istanbul, etc. against those perceived as "enemies of ISIS").

7. **Illegal or non-transparent funding – Score: 8/8.** ISIS's sources of funding have been largely **illicit and opaque**, violating national and international laws. Half of the revenue, as mentioned, came from *taxes and forced confiscations* – basically institutionalized extortion (theguardian.com). In addition, ~43% came from smuggling stolen oil (theguardian.com): ISIS seized oil fields in eastern Syria and northern Iraq, artisanally refined the crude oil and sold it on the black market (sometimes with the complicity of cross-border criminal networks). This oil trafficking violated embargoes and directly financed terrorism. Other clandestine funding activities included: **trafficking in antiquities** (archaeological pieces looted from ancient sites – e.g. Palmyra – illegally sold on international markets), **kidnappings for ransom** (kidnapped Western journalists and aid workers, some released for millions), human **trafficking** (including the sale of Yazidi women as slaves) and hidden donations from radical private sponsors in the Gulf region. All these financial flows were unreported, managed exclusively by the ISIS leadership through secret cashiers. Basically, the group operated as a criminal underground economy: it obtained money through organized crime, evaded the international financial system (using cash, gold or cryptocurrencies) and did not account to anyone for spending these funds. The opacity was so great that, even after the collapse of the territorial Caliphate, the authorities have difficulty in tracking where the accumulated money reserves disappeared (it is suspected that they were hidden to finance the post-caliphate clandestine networks). In conclusion, the **deeply illegal nature** of ISIS's finances – based on looting, smuggling and trafficking – highlights its character as a global criminal actor and the associated risk of the proliferation of black economies and cross-border corruption.

8. **Indoctrination for extreme actions – Score: 9/9.** ISIS has not been content to passively recruit followers, but has *actively indoctrinated them* to commit acts of extreme violence and terrorist attacks, including at the cost of their own lives. The group's propaganda contains numerous *explicit calls to action*: Abu Mohammad al-Adnani, the spokesman, urged Western sympathizers in 2014 to carry out attacks at home if they cannot reach Syria – *"kill the infidels however you can, with a car, with a knife, poison them."* ISIS has managed to convince thousands of young people to become **"lone wolves"** and strike in their countries. Basically, he turned extremist violence into a *civic duty* for his nonsensical supporters: "the call of ISIS – especially to Muslims in the West – promotes violence as an individual decision and a civic obligation" (brookings.edu). At the same time, in the controlled territories, the younger generation was systematically educated to hate and attack the "enemies of Islam". In ISIS-run schools, textbooks were replaced with versions that glorified violent jihad; Children were accustomed to guns from an early age and sent to attend public executions to *desensitize* them. Many teenagers have been persuaded to enlist as suicide bombers – they have been promised paradise and told that *there is no more honorable deed* than to detonate yourself in the midst of "enemies of Allah". The result of this brainwashing: horrible attacks committed with fanaticism. Examples: the minor who blew himself up at a pop concert in Manchester (2017) or the radicalized families in Sri Lanka who blew themselves up in churches (2019) – all inspired by ISIS propaganda. Moreover, adult members of ISIS were also under continuous pressure to prove devotion through extreme acts. Defectors reported that during training, they were asked to *kill unarmed prisoners* to test their loyalty and eliminate their empathy. In short, ISIS created an environment in which *indoctrination to the ultimate violence* was the norm: it managed to turn ordinary people into suicide bombers and executioners, convinced that this way they were fulfilling their religious destiny. This indicator directly reflects the terrorist danger that ISIS has posed globally.

9. **Clandestine and subversive activities – Score: 10/10.** Even after the loss of territories, ISIS proved a high capacity to operate **clandestinely** and destabilize states through underground networks. The group created a specialized *"external operations"* unit, designed to plan and execute terrorist attacks outside the areas it controlled (abcnews.go.com). This secret department (known as *Emni*) was responsible for coordinating major attacks such as those in Paris (Nov. 2015) and Brussels (2016). Western officials confirmed that ISIS had a dedicated structure for attacks in the West, separate from the Syria-Iraq front (abcnews.go.com, abcnews.go.com). These conspiracy cells used Syrian-trained members sent to Europe, along with local recruits radicalized online, to organize *"complex, commanded and controlled"* operations remotely (abcnews.go.com). At the same time, in the Middle East, after 2017, ISIS infiltrated underground: it formed *"sleeper cells"* that switched to classic insurgency tactics – guerrilla attacks, bombings, assassinations of local leaders – with the aim of destabilizing the new authorities and maintaining chaos. For example, in Iraq and Syria, these hidden cells continue to attack military convoys, sabotage infrastructure (power lines, pipelines) and intimidate the population with night attacks, even years after the official loss of the Caliphate (crisisgroup.org). ISIS has also *branched out into other countries* through (provincial) franchises such as ISIS-K in Afghanistan, which acts subversively against local governments. ISIS's ability to plot in the shadows also emerges from the fact that it has inspired terrorist cells as far away as Southeast Asia (the attacks in Sri Lanka, 2019, were claimed by ISIS as part of the "global war"). Essentially, even without a visible "state," ISIS remained a global terrorist network, with *transnational conspiracies*, covert funding, and the ability to strike unexpectedly in various corners of the world. This clandestine persistence underscores the character of **an ongoing threat**: ISIS has demonstrated that it can move from a quasi-state to a subversive terrorist mafia, destabilizing entire societies through terror and sabotage.

ISIS Final Score: 166 points (**out of 166**) – which places the organization at the level ● **of Imminent Risk / Existential Danger** to

National Security. This maximum cumulative score confirms that, during the peak period of 2014–2019, ISIS met practically all the indicators of a violent extremist cult and a terrorist entity with a major destabilizing capacity. **The overall level of risk** is therefore extremely high: ISIS has posed a direct threat to the constitutional order, the territorial integrity of states and the safety of citizens, both in the Middle East and internationally – a fact demonstrated by its attacks and by the group's own statements. The international community has treated ISIS as such, launching a global military campaign against it. In conclusion, by applying the TRACE framework, ISIS ticks all cultic and terrorist risk factors to the highest degree, justifying its classification as an **existential threat** to national and global security in the analyzed interval.

Methodological note: The analysis applied to the ISIS case study was generated with the assistance of an artificial intelligence (AI) system, using exclusively open-source intelligence (OSINT). The scoring and interpretation were produced automatically based on the TRACE framework, without access to classified or sensitive data. As such, the content does not reflect any official institutional position and is intended solely as an exploratory and illustrative example of the model's functionality.

Artificial intelligence is integrated into TRACE as a pre-processing and consistency-testing instrument designed to systematize large volumes of open-source information and generate preliminary indicator values. AI-assisted scoring enables rapid identification of relevant patterns, supports internal coherence testing of the framework, and facilitates exploratory cross-case comparison. Final evaluation, interpretative judgment, and ethical responsibility remain inherently human functions.

In order not to exceed even more the space limits allocated to this article, we will only mention the interpretation and the final score attributed **to Hizb ut-Tahrir and the LaRouche and NXIVM movements, respectively,** thus showing that the application of the TRACE model can be done even by using AI, strictly from OSINT, resulting in quite precise risk assessments that can then be refined by the intelligence analyst:

"◈ **Hizb ut-Tahrir (HuT) –** ***Latent ideological threat***
Although declaratively non-violent, HuT promotes a radical theocratic ideology, openly advocates the abolition of secular states and the establishment of a global caliphate, rejects democracy, and promotes a binary worldview. Its hierarchical structure, infiltration capacity, and potential for indirect radicalization position it as a **mid-to-high-level latent threat**.
Total TRACE score: 157/166

◈ **The LaRouche Movement –** ***A Marginal Ideological Cult with Low Disruptive Potential***
Although it has multiple cultic traits (worship of the leader, dogmatism, ideological manipulation), the LaRouche Movement does not have a paramilitary structure, does not promote violence, and does not develop parallel governance structures. Its risk lies in the potential for disinformation, polarisation and ideological undermining, especially in times of crisis.
Total TRACE score: 101/166

◈ **NXIVM –** ***Coercive cult with high social and individual risk, but limited security impact***
NXIVM operated as a coercive organization with strong cult traits, using manipulation, psychological abuse, and strict control of members. Although it caused serious personal and social damage, it did not present a paramilitary character or an agenda of a systemic political or subversive nature, falling within a **high internal risk, but with little relevance for national security**.
Total TRACE score: 113/166"

Conclusion

This article has presented the TRACE model (Threat and Risk Assessment of Cultic Entities) as a proposed, to-be-tested, systematic analytical tool intended to evaluate organizations with cult-like characteristics potentially posing threats to national security. Drawing from seminal aspects of cult theory, organizational studies, and risk indicators common in the intelligence community, TRACE allows analysts to examine ideologically motivated and unorthodox actors in a systematic manner. Through ISIS, Hizb ut-Tahrir, NXIVM, and the

LaRouche Movement case studies, the model has shown to distinguish violent extremist organizations, latent ideological threats, and socially injurious but apolitical cults.

The deployment of TRACE, even where drawing solely from OSINT and tool-enabled artificial intelligence, provides comprehensive and actionable judgments which may then be further developed by human experts. This mirrors not only its functional value but its responsiveness to existing and prospective analytical environments. In scoring entities along the three key levels, cultic behaviors, organizational habits, and national security signals, TRACE fills an intelligence methodology gap, one which is particular to environments where conventional threat frameworks struggle to reflect the subtlety of hybrid or surreptitiously subversive actors.

TRACE aggregates partial scores across its three analytical layers in order to obtain a synthetic measure of cumulative cultic intensity, organizational coercion, and security relevance. Proposed risk thresholds serve as reference points derived from comparative case-study distributions, rather than fixed universal cut-offs. This allows flexible calibration as additional empirical testing is conducted.

The primary aim of TRACE is to provide a coherent analytical framework for structuring information, guiding systematic observation, and supporting reasoned judgment in the assessment of organizations exhibiting cult-like and potentially destabilizing characteristics. Full scientific validation and transformation into a mature operational instrument are envisaged as subsequent research stages, to be pursued through cross-evaluations between expert human analysts and AI-assisted scoring systems.

Limitations and Future Directions for Development

As with any analytical tool, TRACE has its limitations. One possible weakness is its susceptibility to reliance on the subjective judgment of the analyst, particularly at the scoring phase, where some traits might seem indeterminate or fall along a continuum. In its current implementation, the model is largely reliant on open-source intelligence (OSINT), which is potentially incomplete, biased, and vulnerable to disinformation. As such limitations are largely minimal and can readily be addressed in practice, TRACE does not supplant human expertise but augments it, presenting a logical and consistent model that is refined or modified by the analyst in light of the context of operations and classified information.

Future directions include offering a firm basis for the construction of specialist or sector-specific adaptations (e.g., to digital ideological subcultures, radicalized religious networks, or extensive conspiratorial milieux). It might also be incorporated into an AI-enabled digital platform with the capability to conduct initial automated scoring and alerting to repeated risk patterns. Scaling up the model through longitudinal research and cross-cultural uses will further reinforce its global validity and its analytical resilience to evolving hybrid threats.

Bibliography

1. Borum, Randy. 2011. "Radicalization into Violent Extremism I: A Review of Social Science Theories." Journal of Strategic Security. 4. Vol. 4. Accessed 01 17, 2026. https://www.jstor.org/stable/26463910?seq=1.

2. Galanter, Marc. 1999. Cults: Faith, Healing and Coercion. Oxford University Press.

3. Guvernul României. 2023. Strategia Naţională din 9 noiembrie 2023 de ordine şi siguranţă publică 2023-2027.

4. Hassan, Steven. 2015. Combating Cult Mind Control: The #1 Best-selling Guide to Protection, Rescue, and Recovery from Destructive Cults. Kindle Edition. doi:978-0967068824.

5. Heuer Jr., Richards J. 2007. Psychology of Intelligence Analysis. Pherson Associates, LLC. doi:978-0979888007.

6. —. 1999. Psychology of Intelligence Analysys. C.I.A. doi:1 929667-00-0.

7. Horgan, John. 2008. "From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism." The Annals of the American Academy of Political and Social Science. Vol. 618. Sage Publications, Inc., July. Accessed 01 17, 2026. https://www.jstor.org/stable/40375777.

8. Lalich, Janja A. 2004. Bounded Choice: True Believers and Charismatic Cults. University of California Press. doi:978-0520240186.

9. Lifton, Robert Jay. 1961. Thought reform and the psychology of totalism: A study of "brainwashing" in China. W. W. Norton & Company.

10. Mâţă, D.C. 2016. Securitatea naţională – Concept. Reglementare. Mijloace de ocrotire. Bucureşti: Ed. Hamangiu.

11. Monahan, John, and Jennifer L Skeem. 2015. Risk Assessment in Criminal Sentencing. 12 11. Accessed 01 17, 2026. doi:10.1146/annurev-clinpsy-021815-092945 .

12. Parlamentul României. 2014. Legea nr. 51/1991 privind securitatea națională a României, republicată.

13. Post, Jerrold M. 2014. Narcissism and Politics: Dreams of Glory. Cambridge University Press. doi:978-1107401297.

14. Schmid, A.P. 2013. Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review.

15. Schmid, A.P. 2013. "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review." The Hague. doi:https://doi.org/10.19165/2013.1.02 .

DRAGNETING THE DRAGON: THE PEOPLE'S REPUBLIC OF CHINA, EUROPEAN UNION AND FIVE EYES, CAUGHT IN THE WEB OF MUTUAL ESPIONAGE

Alida Monica Doriana BARBU[*]

Abstract:

The Intelligence world can be depicted as a global Panoptikon, with multiple layers of surveilling eyes, except that the distinction between guards and prisoners is erased. The transfer from one side to the other is more than likely to occur due to the unclear sepia colours of the espionage environment and deep tides that drag people from one "shore" to the other.

The EU's nuanced strategy towards China since 2019 Strategic Outlook Joint Communication is continued today by the De-risking or De-coupling Strategy. The People's Republic of China is considered a partner for negotiation and cooperation, an economic competitor and a systemic rival, whereas the US National Defense Strategy treats China as an enemy of the United States. These strategies are translated in the approach of Intelligence agencies. Even if espionage incidents and cyber attacks occur on a daily basis, the war between USA and China is openly declared, whereas EU has a more moderate public approach.

Keywords: *European Union Intelligence Agency, People's Republic of China, Russian Federation, Five Eyes, Club of Berne, CGT, Hafnium, Equifax, Echelon-Prism-XKeyscore Triad, VPNs.*

Introducere

Five Eyes reprezintă o organizaţie strategică în timpul Noului Război Rece (Abrams 2022). Regatul Unit, membru al *Five Eyes*, face parte și din *Clubul de la Berna*, al cărui partener nelipsit este SUA. Colaborarea între SUA şi Uniunea Europeană este strânsă din punct de vedere al comunicării informaţiilor de Intelligence, având în vedere Strategia de Securitate Naţională (NSS) a SUA din 2022 care a identificat Federaţia Rusă şi Republica Populară Chineză drept ameninţări la adresa

[*] Alida Monica Doriana Barbu, PhD and PhD candidate, Babes Bolyai University, History and Philosophy Faculty, Doctoral School of International Relations and Security Studies, Cluj-Napoca, email: alida.barbu7@gmail.com. alida.barbu@ubbcluj.ro.

intereselor SUA, în timp ce Uniunea Europeană recunoaşte China drept un rival sistemic. Scopul articolului este de a reliefa lupta Est-Vest care se poartă atât la nivel ideologic, cât şi în domeniul şi prin instrumentarul acţiunilor de Intelligence între aliatele *Five Eyes*+Uniunea Europeană şi rivala China, evidenţiind elementele de noutate din peisajul geopolitic. Obiectivele urmărite sunt familiarizarea publicului cu mijloacele folosite de Republica Populară Chineză în vederea obţinerii supremaţiei mondiale. Prezenta cercetare utilizează metoda calitativă a analizei de discurs. Rezultatele obţinute constau în găsirea punctelor slabe atât ale agenţiilor de Intelligence europene, cât şi ale alianţei *Five Eyes*, în timp ce contribuţia personală vine sub forma unor soluţii menite a creşte reziliența societăţii civile la ingerinţele autocraţiilor şi a unor recomandări de corijare a vulnerabilităţilor serviciilor de informaţii.

Five Eyes

Alianţa *Five Eyes* (FVEY) este alcătuită din SUA, Regatul Unit al Marii Britanii, Canada, Australia şi Noua Zeelandă, cele cinci părţi semnatare ale Acordului UKUSA. Iniţial, preexistent a fost Acordul BRUSA care a fost semnat la data de 17 mai 1943 de către Departamentul de Război al SUA şi GC&CS (United Kingdon), urmărindu-se schimbul de informaţii între cele două ţări în vederea sprijinirii forţelor americane din Europa în timpul celui de-al Doilea Război Mondial. BRUSA a stat la baza Acordului UKUSA, semnat la 5 martie 1946 de către colonelul Patrick Marr-Johnson în numele Consiliului de Informaţii al Semnalelor din Londra şi de către locotenent-generalul Hoyt Vandenberg, preşedinte al Consiliului de Informaţii pentru Comunicaţii dintre Statul, Armata şi Marina SUA (STANCIB). În 1949 s-a alăturat UKUSA şi Canada, iar din 1956, împreună cu Australia şi Noua Zeelandă, formează Alianţa FVEY în componenţa sa actuală. Acordul nu a fost recunoscut oficial până în 2010, deşi se cunoştea existenţa sa încă din anii 1980 la nivelul marelui public. Ca parte a tendinţelor de transparentizare din lumea Intelligence-ului, cea de-a 75-a aniversare a parteneriatului formal dintre GCHQ (General Communication Head Quarters) din Marea Britanie şi Agenţia Naţională de Securitate a SUA (NSA) a fost celebrată la 5 martie 2021 (GCHQ 2021).

Scopul acordului menţionat este partajarea între semnatarii săi a informaţiilor bazate pe *Signal Intelligence* (SIGINT) – interceptarea semnalelor electromagnetice de transmisie. SIGINT se împarte în trei ramuri : *Communication Intelligence* (COMINT) – interceptarea apelurilor telefonice ale persoanelor şi a comunicaţiilor prin text, precum e-mailurile şi mesajele text ; *Electronic Intelligence* (ELINT) – utilizarea senzorilor

electronici pentru interceptarea semnalelor de la sisteme de rachete sol-aer sau radare ; *Foreign Instrumentation Signature Intelligence* (FISINT) – interceptarea şi analizarea semnalelor utilizate pentru operarea aeronavelor sau sateliţilor. Agenţiile de informaţii ale ţărilor din cadrul *Five Eyes* : NSA (Agenţia Naţională de Securitate din SUA), GCHQ (Sediul Central al Comunicaţiilor Guvernamentale din Marea Britanie), Institutul de Securitate a Comunicaţiilor din Canada (CSE), Direcţia Australiană de Semnale (ASD) şi Biroul de Securitate a Comunicaţiilor al Guvernului din Noua Zeelandă (GCSB) împărtăşesc informaţii între ele în special despre inamicii geopolitici. Acordul UKUSA, născut în urma Cartei Atlanticului din 1941, avea scopul originar de a monitoriza Uniunea Sovietică şi aliaţii acesteia, însă obiectivele alianţei au cunoscut extinderi şi în sfera colectării comunicaţiilor private din timpul Războiului contra Terorismului de după 11 Septembrie 2001 (Karbauskas 2025).

Fiecare membru este responsabil pentru culegerea şi interpretarea datelor din zona de pe glob atribuită lui. Statele membre colaborează prin intermediul sistemelor de informaţii integrate, care, alături de accesul la baze de date, presupun şi sisteme de procesare şi decodarea în domeniile cibernetic şi maritim. SIGINT a jucat un rol decisiv între 1939 şi1945 şi ulterior în limitarea comunismului. Recent, SUA şi Marea Britanie au oferit publicului informaţii declasificate în ianuarie 2022, înainte de începerea conflictului Rusia-Ucraina, pentru contracarea propagandei ruseşti. Abordarea tridimensională a informaţiilor integrează informaţii umane, semnale şi operaţii militare, SUA şi aliaţii NATO oferind Ucrainei informaţii esenţiale despre locaţia generalilor ruşi, dar şi tehnologie avansată, drone Switchblade, alături de date despre atacul rusesc asupra aeroportului Hostomel din 2022. Ucraina a valorificat informaţiile şi tehnologia primită, scufundând nava de asalt rusească Moskva în Marea Neagră (Sherazi 2025).

În cele ce urmează vom vedea mai în profunzime detaliile confruntării dintre Occident şi Republica Populară Chineză, alături de cazurile cele mai importante şi de rolul jucat de infrastructura *Five Eyes*.

Confruntarea Five Eyes cu China

Five Eyes deţine un rol strategic în eforturile depuse de ţările occidentale şi de SUA de a controla China. Five Eyes, NATO şi Uniunea Europeană (UE) au condamnat public Republica Populară Chineză în 2021 pentru implicarea în atacul cibernetic asupra Microsoft Exchange (MSE). Centrul Microsoft de Informaţii privind Ameninţările (MSTIC) are ca atribuţii investigarea şi răspunsul la atacuri, descoperind astfel

hackerii din guvernul chinez denumiți *Hafnium* care intraseră în serverele Exchange. Microsoft a urmărit doar din iunie 2020 acest grup, care avea ca mod de operare țintirea sistemelor neactualizate ale companiilor medicale, agențiilor guvernamentale și universităților. Intrușii au reușit accesul în serverele Exchange și preluarea controlului din cauza unor erori de codare. Condițiile necesar a fi îndeplinite erau doar două: departamentul IT al companiei să controleze local sistemele, „on premises", iar sistemele să fie conectate la internet. Din fericire, *Office 365* de la Microsoft nu a fost afectat de breșa de securitate, datorită rulării sale în cloud, ceea ce conferă o protecție mai mare. Atacatorii au plasat cod, de îndată ce au pătruns în serverele Exchange, solicitând documente, e-mail-uri, PDF-uri, păcălind serverele de la celălalt capăt că solicitarea era legitimă. Atacul cibernetic a căpătat amploare, provocând răspunsuri guvernamentale din partea consilierului pentru securitate națională din timpul administrației Biden, Jake Sullivan. Agenția pentru Securitate Cibernetică și Infrastructură, Grupul de lucru convocat de Casa Albă și FBI s-au implicat, obținând o hotărâre judecătorească pentru scanarea legală a internetului în încercarea de a găsi serverele sparte de chinezi și apoi a elimina proactiv virușii (Temple-Raston 2021).

Atacul cibernetic de la *Office of Personnel Management* a permis hackerilor chinezi să acceseze și să-și însușească 21,5 milioane de înregistrări din baza de date a guvernului federal. Breșa de securitate *Equifax*, un veritabil succes al Serviciului de Contrainformații ale Partidului Comunist Chinez, a oferit pe tavă Republicii Populare Chineze datele financiare a 147,9 milioane de americani. Infractorii cibernetici au furat 78 de milioane de numere de securitate socială, nume și date de naștere de la asigurătorul de sănătate *Anthem Inc*. În 2018, hackerii chinezi au spart bazele de date ale hotelurilor *Marriott* și au preluat toate informațiile despre carduri de credit, rezervări, pașapoarte a 500 de milioane de persoane. Reprezentanții serviciilor de informații americane opinează că China deține în prezent informațiile personale de identificare a 80% dintre cetățeni și colectează informații despre restul de 20%. Prin datele obținute de la Anthem, OPM, Marriott, Equifax, despre cardurile de credit, împrumuturi, ipoteci, scor de credit, americanii sunt susceptibili la a fi abordați de către ofițeri de informații chinezi și de a răspunde afirmativ, fie în urma șantajului, fie a oferirii de avantaje materiale în cazul în care contul în bancă nu e substanțial sau deținătorul întâmpină probleme financiare (Temple-Raston 2021).

Chinezii au adunat cantități uriașe de date care fac parte dintr-un plan mai amplu de dezvoltare a inteligenței artificiale. În 2017, Partidul Comunist Chinez a anunțat că inteligența artificială de anvergură

mondială a devenit o prioritate naţională, concentrându-se pe formarea informaticienilor în scrierea algoritmilor şi hrănirea algoritmilor cu un număr imens de informaţii pentru a putea învăţa. Interesul Chinei în inteligenţa artificială este demonstrat de cele peste 1.000 de firme de inteligenţă artificială, iar faptul că are o populaţie de peste 1 miliard de oameni despre care colectează informaţii, la care se adaugă furturile imense de date, ajută la dezvoltarea inteligenţei artificiale la scară globală. Pericolul constă în rolul tot mai important pe care îl dobândeşte inteligenţa artificială în viaţa noastră, prin acordarea creditelor, aprobarea ipotecilor şi accesul la datele noastre medicale (Temple-Raston 2021).

Directorul GCHQ Anne Keast-Butler a declarat la Centrul Naţional de Securitate Cibernetică (NCSC), CYBERUK din Birmingham, că statul chinez reprezintă un risc cibernetic în creştere pentru Regatul Unit şi că acesta intenţionează să folosească capacităţile sale cibernetice pentru atingerea deziderateloor naţionale. Provocarea chineză devine prioritatea principală a GCHQ, cu cele mai multe resurse alocate în comparaţie cu oricare altă misiune, conlucrând alături de aliaţi şi colegii din mediul academic şi privat pentru a combate şi descuraja ameninţările cibernetice din partea statelor naţionale şi a actorilor ostili (GCHQ 2024).

Drept contrareacţie occidentală, Meng Wanzhou, directorul financiar al companiei chineze Huawei, a fost arestată în 2020 graţie *Five Eyes* de către autorităţile americane în Canada pentru acuzaţia de încălcare a securităţii naţionale. Mai mult decât atât, patru dintre naţiunile *Five Eyes* au interzis Huawei şi tehnologia sa 5G. Canada a interzis nu doar Huawei, ci şi firma ZTE şi tehnologia 5G. Liderii *Five Eyes* au criticat public China pentru furtul drepturilor de proprietate intelectuală şi spionaj după o întâlnire din 2023 cu companii din Silicon Valley, Beijing-ul respingând acuzaţiile. *Five Eyes*, SUA şi Australia au oferit informaţii guvernului canadian despre uciderea liderului separatist sikh Hardeep Singh pe teritoriul canadian de către Research and Analysis Wing (RAW), agenţia de informaţii externe indiană (Rajput 2023). În octombrie 2024, Canada a expulzat diplomaţi indieni, în timp ce SUA a îndemnat India să coopereze cu Canada. În timpul operaţiunilor NATO din Afganistan după 11 septembrie, operaţiuni conduse de SUA, membrii *Five Eyes* au cooperat cu Pakistanul împotriva acţiunilor insurgente şi a terorismului transfrontalier. Cu toate acestea, *Five Eyes*, îndeosebi SUA, favorizează în prezent India în parteneriatele lor strategice, ceea ce reprezintă o provocare pentru Pakistan (Sherazi 2025). Agenţia de informaţii a Noii Zeelande a denunţat ingerinţele străine din partea

Chinei și Federației Ruse, care ar putea aduce atingere securității naționale. Serviciul de Informații de Securitate al Noii Zeelande (NZSIS) a anunțat public acțiunile de spionaj și ingerință "în și împotriva" țării din partea serviciilor de informații chineze, dar și faptul că aliații vor fi alături de Noua Zeelandă (Financial Intelligence 2023).

Triada Echelon-Prism- XKeyscore versus VPNs

După cum s-a precizat în primul capitol, FVEY s-a specializat în domeniul SIGINT. Misiunea capitolului prezent devine aceea de a-l imersa pe cititor în detaliile tehnice ale practicilor de Intelligence. *Five Eyes* utilizează programul global *ECHELON*, prin care interceptează comunicațiile private cu ajutorul sateliților de comunicații, comunicații stocate și apoi analizate. *ECHELON*, primul sistem de supraveghere *Five Eyes*, datează din 1971, cu scopul de a monitoriza comunicațiile diplomatice și militare ale Uniunii Sovietice și ale partenerilor săi din blocul estic în timpul Războiului Rece. *PRISM*, înființat în 2007, este un sistem de supraveghere al *Five Eyes*, ce adună date despre comunicații ale cetățenilor americani cu sprijinul giganților de tehnologie Microsoft, Yahoo!, Google, Facebook etc. *XKeyscore* este un alt sistem de urmărire recent al *Five Eyes*, care oferă NSA posibilitatea de a ști locația oricărui dispozitiv *smart* și de a citi orice comunicare online (Karbauskas 2025).

Țările din Alianța *Five Eyes* partajează datele private privind comunicațiile transfrontaliere. *Patriot Act* din SUA a dat undă verde din 2001 supravegherii în masă a cetățenilor americani. În 2016, Regatul Unit al Marii Britanii a adoptat *Carta Snoopers*, agențiile de informații putând colecta date despre comunicațiile cetățenilor, în timp ce companiile de telecomunicații și furnizorii de servicii de internet sunt obligați să stocheze date despre utilizatori. Australia a adoptat o lege asemănătoare, modificând legea privind telecomunicațiile, solicitând furnizorilor de servicii de internet să stocheze datele utilizatorilor timp de 2 ani. Țările semnatare ale Acordului UKUSA au pledat pentru eliminarea criptării și pentru alte încălcări ale confidențialității, invocând securitatea statelor și a cetățenilor. Cetățenii au apelat la servicii VPN, e-mail-uri securizate și aplicații de mesagerie criptată, însă dacă acestea au sediul într-o țară din Grupul *Five Eyes*, confidențialitatea totală nu e asigurată. *Five Eyes* au declarat în 2018 că vor depune toate diligențele pentru ca backdoor-uri de criptare să fie asigurate de către companiile de tehnologie. Australia a votat deja un proiect de lege care obligă companiile să predea agențiilor guvernamentale datele utilizatorilor și să creeze backdoor-uri pentru

datele criptate. William Barr, Procurorul general al SUA, a cerut la rândul său un proiect de lege similar, fiind secondat de către Canada, Regatul Unit şi Noua Zeelandă. Companiei Apple i s-a solicitat de către Marea Britanie în 2025 să ofere acces la datele utilizatorilor. Guvernele Regatului Unit şi al SUA obligă VPN-urile să partajeze datele utilizatorilor cu organele de aplicare a legii în câteva ocazii, fără a li se aduce la cunoştinţă cetăţenilor imvestigaţi (Karbauskas 2025).

Lavabit, un furnizor de e-mail din SUA, a fost închis după ce a refuzat să ofere agenţiilor chei de criptare în 2013, cînd era vizat Edward Snowden. Riseup, un furnizor de VPN/email din SUA, a asigurat accesul la datele utilizatorilor urmare a 2 mandate şi a păstrat tăcerea asupra acestui fapt. O reţea VPN importantă din SUA, IPVanish, a colectat şi a oferit datele utilizatorilor la cererea FBI-ului în 2016, deşi susţinea că respectă politica de neînregistrare. HideMyAss, un furnizor VPN din Marea Britanie, furnizează autorităţilor date despre utilizatori şi recunoaşte asta în mod public. Graţie Acordului UKUSA, datele internauţilor pot ajunge la agenţiile de informaţii din SUA, Australia, Canada sau ale partenerilor, dacă se impune. Private Internet Access a fost hotărâtă în a nu păstra datele utilizatorilor, reprezentând cea mai bună strategie de marketing. IPVanish a fost descoperit când se conecta la conturi, deşi avea atunci un alt proprietar, iar HideMyAss e obligat prin lege să colecteze date despre utilizatori. Hushmail, un serviciu canadian de email privat, a predat în 2007 la solicitarea FBI-ului 12 CD-uri cu e-mailuri. Tutanota (Germania) a fost obligată de instanţă să ofere backdoor-uri de criptare. CounterMail (Suedia) nu mai primeşte înregistrări noi (Karbauskas 2025).

Clubul de la Berna

Dacă până acum am luat cunoştinţă de cartografia cooperării naţiunilor de limbă engleză, acum ne vom îndrepta atenţia spre Europa continentală unde echivalentul FVEY este Clubul de la Berna. Acesta din urmă a coordonat activităţile de informaţii ale statelor europene şi ale altor state timp de decade. Organizaţia odată informală, care reuneşte şefii serviciilor de securitate ale UE, a ajuns să opereze la nivel transnaţional. Ziarul austriac „Oesterreich" a publicat în luna noiembrie a anului 2019 un document intern al Clubului de la Berna (CdB), reprezentând cea mai mare scurgere de informaţii din istoria lui. Cel puţin în 2011, CIA, FBI şi Mossad, alături de alte servicii, au făcut schimburi de informaţii în cadrul CdB, contrazicând schimbul intra-

european între serviciile de informaţii prezentat până atunci publicului. Istoricul elveţian Aviva Guttmann a descoperit în urma cercetărilor sale în cadrul Arhivelor Federale Elveţiene că Clubul a făcut schimb de informaţii în afara Europei imediat după înfiinţarea sa în 1969, când nouă servicii secrete din Europa de Vest au început să partajeze informaţii despre teroriştii palestinieni cu serviciile secrete israeliene Shin Beth şi Mossad, dar şi cu FBI prin sistemul de telegrame criptat *Kilowatt*. Din 1974, sistemul de telegrame *Megaton* se referea la terorismul non-palestinian. Munca de cercetare a lui Guttmann nu trece mai departe de anii 1980, deoarece nu pot fi desecretizate documentele mai recente de 50 ani (Jirat 2020).

Documentul secret al CdB, făcut public de *Oesterreich* se referă la un control de securitate efectuat în februarie 2019 de *Soteria*, un grup intern al CdB incluzând serviciile secrete din Elveţia, Marea Britanie, Germania şi Lituania, la serviciul secret austriac BVT (Oficiul Federal pentru Protecţia Constituţiei şi Combaterea Terorismului). Raportul despre BVT a relevat deficienţe în domeniul securităţii clădirilor şi în verificările de securitate asupra personalului, iar securitatea cibernetică evaluată drept neglijentă. Până şi hackerii de talie mijlocie ar fi putut utiliza reţeaua internă BAT pentru a penetra reţeaua IT a CdB - *Poseidon*. Încă din anii 1970, CdB a devenit o reţea globală. Reţeaua de comunicare a Clubului numită *Capriccio* organizează schimbul de informaţii despre extremismul islamic, în timp ce *Toccata* organizează schimbul de informaţii despre terorismul non-islamic. Spre deosebire de Capriccio, *Toccata* nu include CIA, Mossad sau ISA (Agenţia Israeliană de Securitate), în timp ce extremismul de stânga şi de dreapta sunt tratate de *RILE*. În 2011, alături de cele 27 de servicii ale UE şi serviciile din Norvegia şi Elveţia, au apărut şi serviciile secrete non-europene cu următoarele coduri: 12 CSIS (Ottawa), 06 Mossad (Tel Aviv), 19 FBI (Washington), 25 NZSIS (Wellington), 22 ASIO (Canberra), 94 ISA (Tel Aviv), 28 CIA (Bruxelles) (Jirat 2020).

Grupul Antiterorist (CTG) a fost fondat în 2001 ca un subgrup CdB, interfaţă cu UE în domeniul combaterii terorismului, oferind analize ale ameninţărilor politicienilor de rang înalt din UE. Astfel, CTG influenţează discursul politic privind securitatea din statele membre UE, fără să aibă mecanisme de supraveghere şi prevederi statutare. Agenţia de Poliţie Europol a efectuat două exerciţii de simulare cu CTG în 2018, la care au participat şi Centrul pentru Introducerea Clandestină de Migranţi (EMSC), Centrul pentru Combaterea Terorismului (ECTC) şi Oficiul Europol pentru Divulgarea Conţinutului de pe Internet. Deşi UE

nu are mandat, va continua să coopereze cu CTG şi cu CdB. Istoricul şi expertul în informaţii austriac Thomas Riegler remarcă faptul că cele două nu sunt oficial integrate în arhitectura UE şi nu există niciun acord contractual. Clubul de la Berna şi Grupul Antiterorist sunt ţinute să respecte doar legile naţionale ale statelor respective şi nicio regulă imperativă, controlul fiind imposibil (Jirat 2020).

Andrej Hunko, membru al Bundestagului german, este de părere că serviciul secret intern german – *Oficiul Federal pentru Apărarea Constituţiei (BfV)* – a devenit un serviciu secret extern din 2016 odată cu folosirea platformei operaţionale CTG, acest lucru reclamând informarea publicului. Serviciul de informaţii elveţian a răspuns că FIS colaborează cu peste 100 de servicii partenere străine, listă aprobată de Consiliul Federal şi clasificată, iar FIS nu comentează despre cooperarea cu serviciile sale partenere. În noiembrie 2016, netzpolitik.org a relatat despre o platformă operaţională a CTG la sediul serviciului secret olandez AIVD, lângă Haga. AIVD a refuzat să comenteze despre Clubul de la Berna, la fel şi autoritatea independentă de supraveghere a activităţilor de informaţii din Elveţia - AB-ND, organismului parlamentar de supraveghere GPDel şi Comisarului federal elveţian pentru protecţia datelor. Baza de date *Phoenix* a CTG colectează date cu caracter personal despre jihadişti, conform Autorităţii de supraveghere olandeze CTIVD. Serviciile de informaţii americane deţin statut de observator în cadrul CTG. Istoricul elveţian Adrian Hänni menţionează că CdB este vârful aisbergului platformelor care operează în secret: grupul SIGINT Seniors cu sediul la Paris, Grupul de combatere a terorismului (CTG) al Clubului de la Berna, G 13+ şi Grupul de lucru al poliţiei privind terorismul (PWGOT). Legile naţionale, precum noua Lege privind Serviciul Elveţian de Informaţii, permit cooperarea cu serviciile străine, dar nu există nicio bază legală pentru cooperarea multilaterală în domeniul informaţiilor în cadrul CdB şi nicio prevedere pentru supraveghere (Jirat 2020).

Dată fiind această arhitectură organizaţională, modul cum aceasta răspunde provocărilor întrunite ale Moscovei şi Beijingului devine subiectul următorului capitol.

Încercarea de destabilizare a Occidentului din partea alianţei sino-ruse

Chiar dacă poate ideologia nu mai joacă un rol atât de important astăzi ca în timpul Primului Război Rece, acţiunile de spionaj şi contraspionaj, recrutările şi interceptările nu şi-au pierdut valabilitatea.

Aşadar, Republica Populară Chineză recrutează politicieni ai Uniunii Europene care au manifestat simpatie faţă de Moscova, operaţiunile de spionaj, recrutare şi influenţă ale Moscovei şi Beijingului ajungând să se suprapună tot mai mult în UE. Şeful agenţiei de informaţii interne a Republicii Cehe, Michal Koudelka, a subliniat că cele două puteri au aceleaşi intenţii de subminare a sprijinului pentru Ucraina, de destabilizare a Occidentului şi de antagonizare a societăţii civile din democraţiile liberale. Politicienii anti-occidentali marginali din Europa sunt ţintele predilecte de recrutare de către China şi Federaţia Rusă, însă colaborarea agenţiilor chineze şi ruseşti de informaţii este doar tangenţială, demonstrând precauţie. Nu se urmăreşte coordonarea serviciilor lor de informaţii, ci doar lupta împotriva unui inamic comun, Occidentul colectiv. POLITICO a oferit dreptul la replică ambasadelor Republicii Populare Chineze sau Federaţiei Ruse din Belgia, însă acestea nu au răspuns invitaţiei. Koudelka este primul oficial european de informaţii de rang înalt care a vorbit public despre operaţiunile de spionaj chineze şi ruseşti din Europa de când agenţia de informaţii a Republicii Cehe a descoperit o campanie majoră de influenţare rusească în martie 2024. Membri ai Parlamentului European au fost invitaţi la emisiunea TV *Vocea Europei*, despre care s-a aflat ulterior că era finanţată de agenţi pro-Kremlin, în timp ce mai mulţi participanţi la programele *Vocea Europei* erau plătiţi de China (Vinocur 2024).

Liderii europeni nu au acuzat făţiş Beijing-ul, spre deosebire de omologii americani. Un exemplu este Josep Borrell care a negat cunoaşterea vreunei dovezi de furnizare de arme Rusiei de către China în războiul din Ucraina, lucru care a dat apă la moară şefilor spionajului chinez, care au căutat profiluri de politicieni simpatizanţi ai Rusiei. Un exemplu al unei astfel de recrutări încrucişate este Frank Creyelman, un politician naţionalist flamand, exclus din partidul său Vlaams Belaang în 2023 pentru acceptarea de plăţi de la un spion chinez în schimbul traficului de influenţă în favoarea Beijingului. Creyelman demonstrase anterior o poziţie pro-rusă, prin opunerea publică la ideea ajutorului Vestului pentru Ucraina şi prin călătoriile în capitala rusă. Alte cazuri reprezentative sunt asistentul parlamentarului european de extremă dreapta german Maximilian Krah, acuzat şi arestat pentru spionaj în favoarea Chinei sau Filip Dewinter, un membru al aceluiaşi partid, ce a efectuat misiuni de observare a alegerilor din Rusia înainte de a fi căutat de un şef al spionajului chinez. Raportul belgian susţinea că Dewinter a acceptat plăţi de la companii-fantomă şi de la *Asociaţia Chineză pentru*

Contact Prietenos Internațional (CAIFC), o faţadă pentru serviciile secrete chineze, conform anchetei belgiene. Dewinter a negat contactul cu CAIFC în Belgia sau faptul de a fi lucrat cu bună ştiinţă pentru serviciul secret chinez, singurele sale contacte fiind cu *Fundaţia Europeană pentru Cultură şi Educaţie*. POLITICO nu a putut verifica existenţa acestei fundaţii, în schimb a descoperit că Dewinter a fost asociat cu *China Europe Foundation of Culture and Education*, cu sediul în Olanda, a cărei misiune era de a consolida legăturile educaţionale şi culturale dintre China şi Europa. Dewinter nu a fost demis din partidul Vlaams Belang, spre deosebire de Creyelman (Vinocur 2024).

Wiegand, cercetător invitat la German Marshall Fund, coautor al unui raport despre alinierea China-Rusia, cât şi Filip Jirous, un analist independent specializat în China, afirmă că în vederea antagonizării ţărilor UE şi a răcirii relaţiei acestora cu Washingtonul, agenţii ruşi şi mai nou chinezi recrutează oficiali europeni, vulnerabili fie la promisiuni, fie ideologic. Politicieni de extremă dreapta şi de extremă stânga (membri ai Alternativei pentru Germania, Adunării Naţionale din Franţa şi Vlaams Belaang, etc.) din mai multe ţări ale Uniunii Europene participă la misiuni care servesc intereselor Moscovei, precum cele de observare a alegerilor într-un teritoriu contestat (ex. zonele ocupate de Rusia din Ucraina), creând o bază solidă de posibili recruţi. Conform relatărilor din Spiegel, Le Monde şi Financial Times, Creyelman a acceptat plăţi ani de zile de la spionul Daniel Woo, al cărui interes era slăbirea parteneriatului dintre Europa şi Statele Unite prin propaganda chineză şi influenţarea Bundestag-ului german. Deşi reţeaua europeană a lui Woo a fost destructurată, nu e singurul chinez care urmăreşte ademenirea parlamentarilor sau angajaţilor parlamentari (Vinocur 2024).

Fostul preşedinte finlandez Sauli Niinistö a declarat că UE are nevoie de propria agenţie de informaţii în lupta cu sabotorii şi agenţi străini care operează în ţările de pe întreg continentul, ca răspuns la solicitarea din partea preşedintei Comisiei Europene, Ursula von der Leyen, de a redacta un raport referitor la pregătirea UE pentru război şi apărarea civilă. Un serviciu de cooperare în domeniul informaţiilor la nivelul UE ar acoperi atât nevoile strategice, cât şi cele operaţionale, în opinia sa. Mulţi diplomaţi au fost expulzaţi din capitalele europene fiind acuzaţi de spionaj, iar Bruxelles-ul a devenit centrul de activitate al agenţilor, prin prisma multitudinii de instituţii şi ambasade din oraş. Din moment ce totuşi adunarea informaţiilor cade în sarcina statelor membre, îmbunătăţirea fluxului de informaţii constituie primul pas. Apoi

pregătirea unui număr cât mai mare de experți în securitate cibernetică și includerea civililor în apărarea națională (Posaner 2024).

În luna noiembrie a anului 2025 s-a accentuat ideea înființării unei agenții de informații europene, de data aceasta sub conducerea președintei Comisiei Europene, Ursula von der Leyen, ceea ce a ridicat probleme sub aspectul distribuirii suveranității între statele europene și Bruxelles în deciziile legate de securitatea națională. Scopul declarat al agenției de informații europene este coordonarea informațiilor colectate de serviciile statelor europene și de Uniunea Europeană. Un purtător de cuvânt al UE a declarat către DPA, agenția de presă germană, că agenția se află într-un stadiu incipient de formare, cu posibilitatea de a recruta personal din serviciile secrete naționale (Höller 2025).

Financial Times menționează că cele 27 de țări membre ale UE ar putea ridica obiecții legate de suveranitate. Conducerea actualului serviciu secret al Uniunii Europene – Serviciul European de Acțiune Externă (SEAE) – nu e de acord cu o agenție coordonată de von der Leyen. Un prim motiv invocat este duplicarea activității SEAE, dar punctul cel mai sensibil este încălcarea suveranității naționale. Securitatea națională cade în sarcina exclusivă a statelor naționale, conform tratatelor UE. În ciuda faptului că războiul din Ucraina a condus la integrarea europeană în domeniul apărării, suveranitatea statelor nu este negociabilă, cu atât mai mult cu cât țările membre au loialități diferite, unele înclinând puternic în favoarea Federației Ruse (Höller 2025).

Conform ziarului FT, diplomații UE văd în această agenție sub conducerea Ursulei von der Leyen, o creștere substanțială a influenței președintelui Comisiei Europene, dar și posibila periclitare a propriilor cariere și reducerea puterii Kajei Kallas, Înaltul Reprezentant al Uniunii Europene pentru Afaceri Externe și Politica de Securitate. Paula Pinho, purtătoarea de cuvânt a Comisiei Europene, a menționat că noua agenție va veni în sprijinul Serviciului European de Acțiune Externă și va anticipa Colegiul de Securitate, alcătuit din von der Leyen și cei 26 de comisari. Colegiul de Securitate a avut prima întrunire în luna martie a anului 2025, când Comisia și-a extins prerogativele în materie de securitate (Euronews 2025).

Cele 27 de state membre nu au fost consultate încă în privința agenției europene și se așteaptă să opună o rezistență delegării competenței de informații către Bruxelles, deși această agenție se dorește a fi funcțională și pentru a contracara amenințarea hibridă reprezentată de

Federaţia Rusă pe fondul reducerii schimbului de informaţii şi a garanţiilor de securitate din partea S.U.A. (Euronews 2025).

Uniunea Europeană are o politică restrictivă şi în privinţa Republicii Populare Chineze, faţă de care îşi ia precauţii în domeniile de cercetare vizând securitatea civilă şi digitală, bioeconomie, climă, cultură şi sănătate. Începând din 2026, China nu va mai putea fi parte în proiectele de cercetare finanţate de Horizon Europe pentru dezvoltarea noilor tehnologii (Naujokaitytė 2026).

Ameninţările chineze sub forma spionajului sunt întâmpinate cu iniţiativa formării agenţiei de informaţii UE şi reducerea riscului reprezentat de dependenţa de furnizorii de tehnologii chineze (reţele 5G, infrastructură critică), care au ajuns să fie ori restricţionaţi, ori interzişi (Reuters 2026).

Kaja Kallas, Înaltul Reprezentant al UE pentru afaceri externe şi politica de securitate a UE, consideră interesul Chinei pentru zona arctică un risc major de securitate. Zona arctica se află in prim-planul competiţiei mondiale pentru energie, resurse, rute comerciale, lanţuri de aprovizionare, materii prime critice ca importanţă strategică. (Pala 2026).

Comisia Europeană urmăreşte nu doar protejarea proprietăţii intelectuale europene de transferuri către China, ci şi creşterea securităţii cibernetice împotriva manipulării informaţiilor străine (FIMI) din China. Drept răspuns, *European Democracy Shield* (Scutul Democraţiei Europene), format de Comisia Europeană şi Serviciul European de Acţiune Externă (SEAE), are ca ţel menţinerea integrităţii spaţiului informaţional legat de alegeri şi procese democratice, combaterea infiltrărilor din mediul privat (FIMI) şi a dezinformării (EUvsDisinfo 2026). O democraţie solidă se întemeiază pe jurnalismul liber, pe educaţia civică şi informarea corectă.

Concluzii

Din moment ce operaţiunile de contrainformaţii intră în sfera competenţelor naţionale, măsuri împotriva acestui lucru pot fi luate la nivel naţional, însă e de dorit şi conştientizarea la nivel european din partea serviciilor naţionale de informaţii care colaborează pentru contracararea operaţiunilor de manipulare a agenţiilor străine non-europene.

Five Eyes şi Clubul de la Berna ar fi bune exemple pentru o reţea europeană de agenţii de Intelligence, care să partajeze informaţii

sensibile și să conlucreze. Un serviciu de informații european unificat ar putea proteja democrația de imixtiuni străine. Agențiile naționale de informații europene pot solicita și oferi informații una alteia. Necesitatea unei metode unificate de analiză a informațiilor din Uniunea Europeană prin dezvoltarea propriilor capacități de colectare a informațiilor este justificată pentru crearea unui front european rapid și mai asertiv în evaluarea amenințărilor, inclusiv a celor la adresa securității cibernetice. Amenințările interferențelor străine pretind un răspuns coordonat și unificat, care ar crește exponențial rezultatul eforturilor de la nivel național. Infiltrarea propagandei rusești sau chinezești în Uniunea Europeană reclamă un demers ferm din partea statelor europene pentru apărarea democrației și securității colective, cu accent pe unitatea și colaborarea în domeniul informațiilor. Un argument pentru înființarea unei agenții europene comune de informații îl poate constitui asigurarea securității și apărării colective, dar și a imaginii de solidaritate și coeziune pe care o oferă în exterior. Acest aspect este esențial într-o epocă a incertitudinii geopolitice și a schimbării alianțelor. Criticii vin cu contraargumentul atingerii aduse suveranității naționale și a dublării structurilor naționale de intelligence. Din acest motiv societatea civilă are o contribuție importantă în vederea combaterii dezinformării și a influențelor străine prin campaniile de informare, cooperarea cu organizațiile de verificare a faptelor, în coroborare cu Legea europeană privind serviciile digitale.

Reziliența democrației liberale depinde în mare măsură de capacitatea cetățenilor de a lua decizii informați și de alegerea parlamentarilor ce respectă valorile europene. În timp ce se prefigurează pericolul unei alianțe globale a autocrațiilor ce urmărește destabilizarea Occidentului, iar partidele extremiste câștigă teren, propaganda populistă și ingerințele străine trebuie combătute prin păstrarea echilibrului politic, reziliență, strategii eficiente, transparență și menținerea democrației și a statului de drept.

Bibliografie

1. Abrams, Elliott, ”The New Cold War”, Council on Foreign Relations, 04 march 2022, https://www.cfr.org/articles/new-cold-war-0

2. Euronews, ”Is the EU spy unit about to become reality? Von der Leyen wants her own secret service”, 11/11/2025 - 18:50 GMT+1, https://www.euronews.com/2025/11/11/is-the-eu-spy-unit-about-to-become-reality-von-der-leyen-wants-her-own-secret-service

3. EUvsDisinfo, ”FIMI and disinformation as global threats”, Disinformation Review, January 30, 2026, https://euvsdisinfo.eu/fimi-and-disinformation-as-global-threats/

4. Financial Intelligence, ”Noua Zeelandă denunţă riscuri pentru securitatea sa provocate de ingerinţe străine (raport)”, 11 august 2023, 12:23, https://financialintelligence.ro/noua-zeelanda-denunta-riscuri-pentru-securitatea-sa-provocate-de-ingerinte-straine-raport/

5. GCHQ, “A Brief History of the UKUSA agreement”, 5 March 2021. https://www.gchq.gov.uk/information/brief-history-of-ukusa

6. GCHQ, ”GCHQ and NCSC heads warn of increasing cyber risk from China”, 14 May 2024, https://www.gchq.gov.uk/news/cyberuk-2024

7. Höller, Linus, ”The European Union wants its own intelligence branch”, Defence News, Nov 12 2025, https://www.defensenews.com/global/europe/2025/11/12/the-european-union-wants-its-own-intelligence-branch/

8. Jirat, Jan, ”The Club de Berne: a black box of growing intelligence cooperation”, About Intel, 1. April 2020, https://aboutintel.eu/the-club-de-berne/

9. Karbauskas, Šarūnas, ”Five, Nine, and Fourteen Eyes alliances explained”, Cyber News, 22 April 2025, https://cybernews.com/resources/5-eyes-9-eyes-14-eyes-countries/

10. Naujokaitytė, Goda, ”Explained: China has been kicked out of most of Horizon Europe”, Science Business, 27 Jan 2026 | https://sciencebusiness.net/news/r-d-funding/horizon-europe/explained-china-has-been-kicked-out-most-horizon-europe

11. Pala, Melike, ”EU foreign policy chief warns about security risks from China's growing interest in Arctic”, AA, 03.02.2026, https://www.aa.com.tr/en/world/eu-foreign-policy-chief-warns-about-security-risks-from-chinas-growing-interest-in-arctic/3819220

12. Posaner, Joshua, ”Create a CIA-style European spy service, von der Leyen is told”, Politico, October 30, 2024 1:39 pm CET, https://www.politico.eu/article/europe-spy-service-cia-ursula-von-der-leyen/

13. Rajput, Neeraj, ”RAW ‘Hunts’ Mossad Style! Ex-Raw Officer Makes Sensational Claims On Hardeep Singh Nijjar’s Assassination”, The Eurasiantimes, 19 September 2023. https://www.eurasiantimes.com/raw-hunts-mossad-style-trudeau-accuses-india-of-assassinating-khalistani-leader-on-canadian-soil/

14. Reuters, ”EU moves to force the phase-out of Chinese suppliers from key infrastructure, FT reports”, January 17, 2026, 9:52 AM GMT+2, https://www.reuters.com/world/china/eu-bar-chinese-suppliers-critical-infrastructure-ft-reports-2026-01-17/

15. Sherazi, Anees Fatima, ”Critical Analysis of Five Eyes Alliance”, ISSRA, January 13, 2025, https://www.issra.pk/insight/2025/critical-analysis-of-five-eyes-alliance/insight.html

16. Temple-Raston, Dina, ”China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying”, NPR, August 26, 2021, 5:00 AM ET, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

17. Vinocur, Nicholas, ”‘Dragon-Bear’: How China and Russia’s spy operations overlap in Europe”, Politico, September 13, 2024 4:20 am CET, https://www.politico.eu/article/dragon-bear-how-china-and-russias-spy-operations-overlap-in-europe/

ADVANCING A C2I FRAMEWORK FOR ENHANCED INTELLIGENCE SECURITY IN THE SHIPPING INDUSTRY

Anastasios-Nikolaos KANELLOPOULOS*

Abstract:

The Shipping industry, known for its strong revenues and political weight, functions within a complex and evolving global landscape. To navigate this complex landscape, companies must adopt competitive operational and tactical processes that encompass both offensive and defensive capabilities. Offensive capabilities, such as Competitive Intelligence, are essential for gathering information on competitors and gaining a strategic advantage. Defensive capabilities, including Counterintelligence, are equally important for protecting businesses from malicious actions by competitors.

This paper explores the potential coexistence of Competitive Intelligence and Counterintelligence within a unified operational framework within the Shipping industry, highlighting their complementary roles in addressing the challenges of the internationalized business world. The study follows a qualitative conceptual approach based on a review and synthesis of academic and professional literature on Competitive Intelligence, Counterintelligence, and the Shipping business environment, in order to develop an integrated operational framework. Subsequently, it proposes a unified C2I Business Framework for shipping companies, supporting the establishment of a centralized C2I Office that combines intelligence collection, analysis, and protective countermeasures to improve decision-making, reduce operational vulnerabilities, and strengthen strategic resilience.

Keywords: Competitive Intelligence, Counterintelligence, Shipping Industry, C2I Business Framework.

Introduction

The global shipping industry has evolved into a highly competitive and influential sector, playing a pivotal role in the world economy. As global trade agreements proliferate and supply chain systems become increasingly dynamic, shipping companies are compelled to navigate complex challenges to maintain competitiveness.

* PhD Candidate in Intelligence, Department of Business Administration, Athens University of Economics and Business, Greece. Email: ankanell@aueb.gr

Despite operating theoretically under perfect competition, the reality of the shipping sector presents unique barriers to entry, distinct regional dynamics, and a continuous flux of social and geopolitical influences that shape market opportunities.

The objective of this paper is to examine how Competitive Intelligence (CI) and Counterintelligence can coexist within a unified operational framework in the Shipping industry, and to propose an integrated corporate model that strengthens both competitive positioning and organizational protection. In this volatile environment, the importance of Competitive Intelligence and Counterintelligence has grown significantly. CI involves systematically gathering and analyzing data about competitors, customers, and the broader market to inform strategic decision-making. Meanwhile, Counterintelligence focuses on protecting sensitive business information from external threats, including espionage and cybersecurity risks. Both intelligence frameworks are crucial for shipping companies striving to secure their assets, anticipate market shifts, and enhance operational efficiency.

Methodologically, this paper follows a qualitative conceptual approach based on a structured review and synthesis of academic and professional literature on CI, counterintelligence, and maritime business dynamics. Through comparative analysis of the two intelligence functions, it develops a unified C2I framework adapted to the operational realities and threat environment of the Shipping industry. A comprehensive C2I framework addresses not only competitive dynamics but also internal vulnerabilities, integrating proactive intelligence gathering with protective measures. The establishment of a C2I Office within a shipping organization serves as a strategic hub for intelligence activities, bridging the gap between data collection and actionable insights. Led by a Chief Intelligence Officer (CINO), this office fosters a unified intelligence culture, leveraging human intelligence networks, open-source data, and technological tools to detect emerging threats and capitalize on new opportunities.

By institutionalizing intelligence practices, shipping companies can enhance their strategic foresight and adaptability, positioning themselves advantageously in a highly unpredictable business landscape. The adoption of a C2I framework is not just an operational necessity but a strategic imperative, helping organizations navigate the complexities of globalization, technological advancements, and evolving competitive forces.

Theoretical Background: Intelligence in the Shipping Business Environment

Shipping Environment and Intelligence

The Shipping Industry has become globalized and highly influential in the world economy due to the increasing use of ships, the dynamic development of global supply chain systems, and the emergence of international trade agreements between states and corporations. To illustrate the sector's economic significance, maritime transport remains the dominant mode for global trade: over 80 % of the volume of international trade in goods is carried by sea, according to the United Nations Conference on Trade and Development, and in many contexts this figure is reported at around 90 % of world merchandise trade by volume. Ships serve as the backbone of global supply chains, linking producers, markets, and consumers across continents and sustaining economic growth and development worldwide (UN Trade & Development, 2025). Adam Smith highlighted Shipping as a fundamental cornerstone of global economic development in his book "The Wealth of Nations." Shipping contributed to the international trade system, fostering competition, specialization, and efficiency in the global economy. Stopford (2008) further explores the impact of globalization on the Shipping sector in his book "Maritime Economics," emphasizing how technological advancements and changing economic and business environments affect companies' competitiveness.

Shipping is a unique sector with characteristics that distinguish it from other industries. Theoretically, it operates under conditions of perfect competition and exhibits a highly globalized nature. Numerous shipping businesses compete with each other in an elastic and globally regulated market, striving to gain a competitive advantage (D'agostini et al., 2019). No shipowner has ever acquired a double-digit market share (Emmanuelides and Tsavliris, 2019). Lorange (2009) argues that shipping is a perfectly competitive part of the world economy, and even innovative segments of the sector gradually become perfectly competitive due to the potential for imitation by new entrants. While perfect competition implies no entry or exit barriers and equal access to information for all shipping corporations, in reality, this is rarely the case, as different parts of the Shipping market have distinct barriers to entry and exit (e.g., capital requirements for vessel acquisition, access to finance, regulatory and compliance costs, port access and slot

availability, long-term charter contracts, shipyard capacity and delivery times, and technological/cybersecurity requirements), and companies' information is not always identical.

Furthermore, few industries worldwide are subject to as many social and geopolitical influences as Shipping due to its operational nature and direct correlation with overall world trade. Local changes and trade discontinuities constantly reshape the global trade map, altering the supply-demand balance at local and regional levels and creating a continuous stream of shipping opportunities (Emmanuelides and Tsavliris, 2019). Therefore, the dynamics of the Shipping business environment are unique for each company, often influenced by internal corporate intelligence culture (David, 2013; Chen et al., 2015).

CI The frequent changes in the macro business environment pose limitations and concerns for business decision-making (Miller, 2001). Effective decision-making requires obtaining a comprehensive understanding of qualitative data in a business sector and its competitive landscape (Bose, 2008; Nasri and Zarai, 2013; Kula and Naktiyok, 2021). Companies form their perception of competition through a systematic scanning process that leads to competitive advantages (Nasri, 2012). CI is the process used to gather, process, and analyze data and information related to competitors, customers, and products, thereby supporting business decision-making (Franco et al., 2011; Dabrowski, 2018). It involves the transfer of knowledge from the business environment to corporations, following established analytical rules (Phathutshedzo and Tiko, 2011; Tahmasebifard, 2018), which enhances the understanding of the competitive landscape (Ferrier, 2001; Nasri, 2011; Carvalho, 2021).

In addition, CI differs from Business Intelligence in terms of its information sources. Business Intelligence primarily relies on companies' internal systems, while CI incorporates both internal and extensive external data sources (Gieskes, 2000; Bose, 2008; Saxena and Lamest, 2018; Barnea, 2021). CI traces its roots back to the middle of the 20th century when it was primarily used for military intelligence gathering (Greene, 1966). It is worth noting that there is no universally established international definition for CI (Global Intelligence Alliance, 2005; Franco et al., 2011). An intriguing definition proposed by Tena and Comai (2004) describes CI as a systematic process recognized and embraced throughout an organization for searching, selecting, analyzing, and distributing information about the business environment to gain a

significant competitive advantage. This definition portrays CI as a holistic process that involves the entire company, rather than limiting its capacity and capabilities to specific individuals, groups, or departments.

Moreover, CI combines defensive and offensive intelligence to inform about competitors' plans, strategies, weaknesses, and opportunities. It is not merely a framework for scanning and collecting data, information, and intelligence from the corporate environment; it also entails adding value to companies through intelligence processes and analysis that empower managers to be proactive and make informed decisions (Auster and Choo, 1994; Prescott, 2001; Johns and Van Doren, 2010; David, 2013). CI operates within a completely legal framework for collecting, managing, analyzing, and disseminating information and intelligence, facilitating decision-making processes and the formulation of business strategies (Hedin, 2004; Amiri et al., 2017).Eventually, CI procedures yield two main results: an alert intelligence product that highlights immediate and significant changes in the macro and micro business environment, and an operational or strategic intelligence product that aids in formulating business strategies and making future decisions (Porter, 1991; García-Madurga and Esteban-Navarro, 2020).

Competitive Intelligence Business Framework

The CI framework consists of the development of intelligence analysis products within a specific time period, following existing procedures and based on an intelligence cycle (Prescott, 1999; Bartes, 2013; Kula and Naktiyok, 2021). The Intelligence Cycle, as described by the American Productivity and Quality Center (1996), is a dynamic and interactive process that allows organizations to gather data and information from various sources, analyze it, and take action based on the insights gained. It is an ongoing process that serves as a daily framework for keeping businesses informed about the competitive landscape and supporting informed decision-making.

According to Dishman and Calof's research (2008), the Intelligence Cycle framework is built upon CI awareness and structure. "Competitive Intelligence awareness" refers to the need for an appropriate analytical and operational culture that supports the effective management of information within the company (Miller, 2005; Gaspareniene et al., 2013; Chen et al., 2015). Through the establishment of a CI business culture, company executives play a crucial role in

collecting, managing, and analyzing information, effectively acting as the recipients of necessary information and data. This enables the company to have the required resources to conduct proper analyses and support decision-making processes by managers (Auster and Choo, 1994; David, 2013). Global Intelligence Alliance (2004) suggests the application of a CI cycle consisting of eight steps, drawing on approaches by Bernhardt (1994), Hussey (1995), and Kahaner (1996). This cycle incorporates the fundamental steps of the Intelligence Cycle while addressing the intelligence needs of modern business environments.

Furthermore, Cloutier et al. (2013) proposed a six-step CI Cycle that includes planning and direction, collection, analysis, communication, decision, and evaluation. This model acknowledges the contextual influences that impact an organization, taking into account various internal and external factors. These influences highlight the necessity of establishing appropriate information systems, intelligence frameworks, and a culture that supports informed decision-making. Fostering a CI culture involves upskilling employees, shaping their mentality, incorporating essential environmental knowledge, and promoting operational stability within the business.

Counterintelligence and its Business Framework

Counterintelligence in business refers to the use of tactics and strategies to protect an organization's sensitive information, human resources, and decision-making processes from malicious competitors. It incorporates operational procedures based on frameworks used in the intelligence sector, such as the Intelligence Cycle, which includes functions like collection, analysis, and dissemination of information. While traditionally employed by state intelligence services, counterintelligence is now being adapted for the private sector due to the rapidly changing business environment.

Counterintelligence in the business context is a topic of interest for both executives and academic researchers in fields like International Relations and Business Studies. The literature on counterintelligence is divided between former national intelligence officials and reputable academics and research authors. It is described as the process of safeguarding internal information systems from CI collection efforts by other corporations (Strauss, 1999). Counterintelligence also plays a role in neutralizing operational threats in the business environment (Bernhardt, 2003). The protection of national security is another aspect emphasized in counterintelligence, as highlighted in works such as

"Counterintelligence and National Strategy" by Michelle K. Van Cleave (2007) and "VAULTS MIRRORS AND MASKS Rediscovering U.S.A. Counterintelligence" by Jennifer E. Sims and Burton Gerber (2009), which delve into counterintelligence within the U.S.A. intelligence services, specifically addressing economic and industrial espionage.

In the current business landscape, safeguarding sensitive data, information, and intelligence is crucial for ensuring continuous and uninterrupted operation. Counterintelligence executives are responsible for creating and enforcing comprehensive data security policies and procedures. They also train corporate staff on handling sensitive information properly. Innovative technological means such as data masking, data loss prevention, and encryption applications and hardware are utilized to protect business data systems from unauthorized access. Counterintelligence frameworks are also employed to protect corporate human resources from profiling targeting and espionage activities, as well as to prevent external interference in business decision-making processes (Smith and Brooks, 2013).

Counterintelligence frameworks draw on various sources to operate effectively in a business environment. These include corporate Human Intelligence (HUMINT) based on insider intelligence networks, Open-Source Intelligence (OSINT), and competitor intelligence. Internal counterintelligence networks function as information collection systems to monitor activities that may indicate insider threats (Cho and Lee, 2016). These networks gather and deliver relevant information to the appropriate executives. OSINT collection is important in two directions: detecting threats from internal and external business executives by utilizing publicly available sources such as social media, search engines, and news outlets through advanced analytics and machine learning software (Smith and Brooks, 2013; Elmellas, 2016).

Considering the significance of counterintelligence, its implementation requires an overall counterintelligence culture among the human resources of a business (Chen et al., 2015; Kanellopoulos, 2022). In practice, this means that employees at all levels understand basic information-protection principles, recognize indicators of social engineering and insider-risk behavior, and follow standardized procedures for handling, sharing, and storing sensitive operational and commercial data. Such a culture reduces information leakage and strengthens organizational resilience by ensuring that counterintelligence is embedded in daily routines rather than treated as a purely technical or isolated security function.

Counterintelligence and Competitive Intelligence position in an organization

Counterintelligence and CI hold distinct positions within an organization. The configuration of CI teams can vary depending on the business environment, with some companies having dedicated departments or outsourcing the process to external partners. Internal CI teams collect, process, and analyze data to provide relevant insights to high-level decision-makers (Barnea, 2019). These teams employ CI specialists with different backgrounds, levels of experience, and knowledge of analysis methodologies. They often establish shared access special applications for executives across various departments to facilitate the flow of necessary information and intelligence (Gibbons and Prescott, 1996; Prescott, 2001; Marin and Poulter, 2004; David, 2013; Gaspareniene et al., 2013).

Executives are responsible for organizing the CI framework to ensure the delivery of the best information to decision-makers. Traditional intelligence collection and analysis methods may need to be updated to account for external micro and macro-economic and political influences (Ghoshal and Westney, 1991; Babbar and Rai, 1993; Salles, 2006; Zheng et al., 2011; Abraham, 2012; Gaidelys and Meidute, 2012). The analysis methodologies should not solely rely on individual executives' knowledge and experience or be overly influenced by tactical level changes in the business environment (Levitas et al., 1997; Sliton, 1998; Gaidelys, 2010; Solberg Søilen, 2016).

Furthermore, counterintelligence, as part of the intelligence sector, needs to focus on the business environment. Although it primarily focuses on protecting internal operations and addressing insider threats, it also relies on information and intelligence collected from the external business environment, with a particular emphasis on competitors and CI frameworks (Smith and Brooks, 2013). The counterintelligence team should consist of highly skilled and trusted executives who operate independently and have a deep understanding of the company's plans, objectives, and strategies. Their background should include prior experience in information protection and security positions in both the public and private sectors. Their training should encompass a combination of knowledge from the intelligence and business sectors. Eventually, the counterintelligence team should report directly to the company's CEO.

Competitive Intelligence and Counterintelligence Framework in Shipping

The Shipping industry, with its international nature and reliance on information and intelligence, faces vulnerabilities in terms of cybersecurity and espionage threats. To navigate these challenges and stay competitive, shipping companies can benefit from implementing frameworks such as CI and Counterintelligence.

CI in the shipping industry involves acquiring and utilizing information and intelligence from other companies to gain insights into technological innovation, business environment developments, and shipping cycles. This knowledge enables companies to enter new sub-sectors, apply competitive strategies at the right time, and make informed decisions.

Counterintelligence is crucial in protecting a shipping company's internal resources and information from threats. It involves safeguarding against cybersecurity risks, detecting insider threats, and implementing appropriate protection measures. Counterintelligence in shipping can also focus on preventing intellectual property theft and industrial espionage.

To effectively implement CI and Counterintelligence in the shipping industry, a common Shipping Intelligence framework can be adopted. This framework integrates both functions and utilizes methodologies and processes from the intelligence sector, such as the Intelligence Cycle (Kanellopoulos and Ioannidis, 2024).

Developing an C2I Framework for Shipping industry

To properly execute a Competitive Intelligence and Counterintelligence (C2I) framework in the shipping industry, we propose the establishment of a dedicated corporate-level C2I Office. This office serves as the central hub for strategic intelligence activities, integrating both external competitive insight and internal protective mechanisms. It is designed not only to gather critical information but also to ensure that intelligence is translated into meaningful action, protecting the organization from emerging threats while enabling strategic foresight and agile decision-making.

The C2I Office is structured around two executive groups with distinct but interdependent roles. The first group is tasked with the

collection and management of information. This involves identifying and acquiring relevant data from a wide range of internal and external sources, including open-source maritime intelligence, competitor monitoring, trade networks, and geopolitical analysis. Beyond passive collection, this group actively develops and maintains intelligence networks – both internal, through human intelligence contributions from trained employees, and external, through strategic partnerships with entities such as port authorities, regulatory bodies, and supply chain collaborators. The team also oversees the classification, secure storage, and accessibility of collected information to support operational and analytical readiness across the organization.

The second group within the office focuses on analysis, protective measures, and organizational training. Their primary function is to interpret the data collected by the first group using structured intelligence analysis methodologies. From this analysis, they produce actionable insights that directly inform corporate strategy, operational decisions, and risk mitigation. This group also has a critical role in deploying protective counterintelligence measures. These include cybersecurity protocols, insider threat detection systems, and crisis management procedures, all designed to safeguard the organization's sensitive information and operational integrity. Additionally, the group is responsible for embedding an intelligence-aware mindset across the company. They design and deliver training programs that build awareness among employees about intelligence procedures, threat indicators, and secure communication practices. These efforts are essential to cultivating a workforce that is both alert and actively engaged in the company's broader intelligence mission.

Oversight of the C2I Office is assigned to a senior executive with specialized expertise in intelligence operations. This Chief Intelligence Officer (CINO) must possess comprehensive knowledge in areas such as information collection, competitive analysis, and corporate security. Serving as the strategic bridge between intelligence operations and executive leadership, the CINO reports directly to the CEO and the Board of Directors. This reporting structure ensures that intelligence findings are aligned with top-level decision-making and that intelligence capabilities are positioned as a strategic asset rather than a support function. The CINO plays a critical role in maintaining the cohesion of the office's two groups, balancing proactive intelligence efforts with reactive

protection, and ensuring that outputs are relevant, timely, and actionable at the highest levels of the organization.

A key component of the proposed framework is the development of a shared intelligence culture within the company. This culture represents a significant departure from traditional siloed approaches to information security and market analysis. It encourages active participation from all levels of staff in identifying relevant information, recognizing unusual activity, and contributing local or operational insights to the broader intelligence function. This cultural shift not only increases the flow of intelligence from within the organization but also strengthens its ability to anticipate and respond to changes in the external environment. The emphasis on culture is further supported by the cultivation of human intelligence networks that span both internal departments and external relationships. These networks serve as early warning systems, allowing the organization to detect weak signals and emerging trends that may otherwise go unnoticed.

Operationally, the C2I framework is built around a six-stage cycle that mirrors and enhances traditional intelligence methodologies. The first three stages – Collection, Management, and Networking – are led by the information gathering group and are focused on acquiring and organizing data while building reliable sources of intelligence. The second three stages – Analysis, Measures, and Training – are managed by the analytical group and revolve around processing information into actionable insights, implementing protective strategies, and strengthening organizational resilience through employee education. These stages are iterative and interconnected, forming a dynamic cycle that allows the office to adapt continuously to new challenges and refine its activities based on evolving needs.

Crucially, the success of this model depends on the efficient communication of intelligence products and risk assessments to senior leadership. Intelligence must be presented in a manner that is clear, concise, and relevant to decision-making, enabling executives to understand not only what is happening, but why it matters and how the company should respond. The outputs of the C2I Office should inform both immediate operational choices and long-term strategic planning, serving as a reliable compass in a complex and often volatile global shipping environment.

By establishing a formal, well-resourced C2I Office, shipping companies can institutionalize intelligence as a foundational pillar of

their business model. This approach offers substantial strategic benefits: earlier identification of competitive opportunities, improved detection and mitigation of threats, and enhanced decision-making agility. The model supports resilience and adaptability in a landscape marked by geopolitical uncertainty, technological disruption, and increasing information asymmetries. It transforms intelligence from a reactive support function into a proactive force multiplier that secures assets, enables innovation, and supports sustained competitive advantage.

Conclusion

The global shipping industry's inherent complexities, driven by globalization, technological advancements, and geopolitical shifts, require companies to develop robust frameworks for maintaining competitiveness and protecting vital information. As shipping companies operate within a volatile environment marked by rapid changes and diverse threats, adopting a structured Competitive Intelligence and Counterintelligence framework becomes essential. Integrating these intelligence practices not only strengthens a company's strategic position but also ensures resilience against internal and external challenges.

A well-organized C2I Office, led by a CINO, plays a critical role in navigating this dynamic landscape. By centralizing intelligence functions, the C2I Office fosters an organizational culture where data-driven decision-making and proactive threat management become the norm. The dual focus on gathering competitive insights and implementing counterintelligence measures enables shipping companies to identify emerging opportunities while simultaneously mitigating risks such as industrial espionage and cybersecurity breaches.

Moreover, embedding intelligence awareness at every organizational level encourages collaboration and responsiveness, transforming intelligence from a reactive function into a proactive strategic asset. This holistic approach not only informs long-term strategic planning but also empowers daily operational decisions, thereby enhancing the company's capacity to adapt to market disruptions and geopolitical uncertainties.

Eventually, in an industry where information asymmetry and evolving global trends can significantly impact profitability, the ability to

anticipate changes and safeguard corporate intelligence becomes a competitive differentiator. Shipping companies that embrace the C2I model can better position themselves to thrive, leveraging intelligence to secure assets, drive innovation, and make informed strategic choices. As the shipping environment continues to evolve, maintaining an agile and intelligence-oriented approach will be key to sustaining competitive advantage and ensuring long-term success.

Bibliography

1. Abraham, S. C. 2012. *Strategic planning: A practical guide for competitive success*. Emerald.

2. American Productivity and Quality Center 1996. *Leveraging Information for Action*. Houston, TX.

3. Amiri, N., Shirkavand, S., Chalak, M., and Rezaeei, N. 2017. "Competitive Intelligence and developing sustainable competitive advantage". *AD-Minister*: 173–194. https://doi.org/10.17230/ad-minister.30.9.

4. Auster, E., and Choo, C. W. 1994. "How senior managers acquire and use information in environmental scanning". *Information Processing & Management*, 30(5): 607–618. https://doi.org/10.1016/0306-4573(94)90073-6.

5. Babbar, S., and Rai, A. 1993. "Competitive Intelligence for International Business". *Long Range Planning*, 26(3): 103–113. https://doi.org/10.1016/0024-6301(93)90012-5.

6. Barnea, A. 2019. "Big Data and Counterintelligence in Western Countries." *International Journal of Intelligence and CounterIntelligence* 32 (3): 433–47. https://doi.org/10.1080/08850607.2019.1605804.

7. Barnea, A. 2021. "Big Data Can Boost the Value of Competitive Intelligence". *Competitive Intelligence Magazine*, 26(1).

8. Barnea, A., and Meshulach, A. 2020. "Forecasting for Intelligence Analysis: Scenarios to abort strategic surprise". *International Journal of Intelligence and CounterIntelligence*, 34(1): 106–133. https://doi.org/10.1080/08850607.2020.1793600.

9. Bartes, F. 2013. "Five-phase model of the intelligence cycle of competitive intelligence". *Acta Universitatis Agriculturae Et Silviculturae Mendelianae Brunensis*, 61(2): 283–288. https://doi.org/10.11118/actaun201361020283.

10. Bernhardt, D. C. 1994. "'I want it fast, factual, actionable'—tailoring competitive intelligence to executives' needs". *Long Range Planning*, 27(1): 12–24. https://doi.org/10.1016/0024-6301(94)90003-5.

11. Bose, R. 2008. "Competitive intelligence process and tools for intelligence analysis". *Industrial Management & Data Systems*, 108(4): 510–528. https://doi.org/10.1108/02635570810868362.

12. Bouthillier, F., and Jin, T. 2005. "Competitive intelligence professionals and their interactions with CI technology: Areseach agenda". *Journal of Competitive Intelligence and Management*, 3(1).

13. Carvalho, P. S. de. 2021. Fundamentals of Competitive Intelligence (CI). IF Insight & Foresight.

14. Chen, Y., Ramamurthy, K. and Wen, K.-W. 2015. "Impacts of comprehensive information security programs on information security culture". *Journal of Computer Information Systems*, 55(3): 11–19. https://doi.org/10.1080/08874417.2015.11645767.

15. Cho, I., and Lee, K. 2016. "Advanced risk measurement approach to insider threats in Cyberspace". *Intelligent Automation and Soft Computing*, 22(3): 405–413. https://doi.org/10.1080/10798587.2015.1121617.

16. Cloutier, A. 2013. "Competitive Intelligence Process Integrative Model based on a scoping review of the literature". *International Journal of Strategic Management*, 13(1): 57–72. https://doi.org/10.18374/ijsm-13-1.7.

17. D'agostini, E., Nam, H.-S., and Kang, S.-H. 2019. "Gaining competitive advantage at sea: An overview of shipping lines' strategic decisions". *International Journal of Transportation Engineering and Technology*, 5(4): 74. https://doi.org/10.11648/j.ijtet.20190504.12.

18. Dabrowski, D. 2018. "Sources of market information, its quality and new product financial performance". *Engineering Economics*, 29(1). https://doi.org/10.5755/j01.ee.29.1.13405.

19. David, F. R. 2013. *Strategic Management Concepts and cases: A competitive advantage approach*. Pearson.

20. Dishman, P. and J. Calof 2008. "Competitive intelligence: a multiphasic precedent to marketing strategy," *European Journal of Marketing*. 42(7/8): 766-785.

21. Du Plessis, T., and Gulwa, M. 2016. "Developing a competitive intelligence strategy framework supporting the competitive intelligence needs of a financial institution's decision makers". *SA Journal of Information Management*, 18(2). https://doi:10.4102/sajim.v18i2.726.

22. Elmellas, J. 2016. "Knowledge is power: The evolution of threat intelligence". *Computer Fraud and Security*, 2016(7): 5–9. https://doi.org/10.1016/s1361-3723(16)30051-3.

23. Emmanuelides, G., and Tsavliris, P. 2019. *Winning shipping strategies. theory and evidence from leading shipowners*. Economia Publishing.

24. Ettorre, B. 1995. "Managing competitive intelligence". *Management Review*, 84(10).

25. Ferrier, W. J. 2001. "Navigating the competitive landscape: The drivers and consequences of competitive aggressiveness". *Academy of Management Journal*, *44*(4): 858–877. https://doi.org/10.5465/3069419.

26. Franco, M., Magrinho, A., and Ramos Silva, J. 2011. "Competitive intelligence: A research model tested on Portuguese firms". *Business Process Management Journal*, 17(2): 332–356. https://doi.org/10.1108/14637151111122374.

27. Gaidelys, V. 2010. "The role of competitive intelligence in the course of business process". *Economics and Management*, 15.

28. Gaidelys, V., and Meidute, I. 2012. "Instruments and methods of competitive intelligence". *Economics and Management*, 17(3). https://doi:10.5755/j01.em.17.3.2122.

29. García-Madurga, M., and Esteban-Navarro, M. 2020. "A project management approach to competitive intelligence". *Journal of Intelligence Studies in Business*, 10(3). https://doi.org/10.37380/jisib. v10i3.636.

30. Gaspareniene, L., Remeikiene, R., and Gaidelys, V. 2013. "The Opportunities of the Use of Competitive Intelligence in Business: Literature Review". *Journal of Small Business and Entrepreneurship Development*, 1(2): 9–16.

31. Gelb, B., and Zinkhan, G. 1985. "Competitive Intelligence Practices of Industrial Marketers". *Industrial Marketing Management*, (14): 269-275.

32. Ghoshal, S., and Westney, D. E. 1991. "Organizing competitor analysis systems". *Strategic Management Journal*, 12(1): 17–31. https://doi.org/10.1002/smj.4250120103.

33. Gibbons, P., and Prescott, J. 1996. "Parallel competitive intelligence processes in organisations". *International Journal of Technology Management*, 11(1). https://doi.org/10.1504/IJTM.1996.025425.

34. Gieskes, H. 2000. "Competitive intelligence at lexis-nexis". *Competitive Intelligence Review*, 11(2): 4-11. https://doi.org/10.1002/(sici)1520-6386(200032)11:23.0.co;2-e.

35. Global Intelligence Alliance. 2004. Introduction to Competitive Intelligence. *GIA White Paper*, 1.

36. Greene, R. 1966. *Business Intelligence and Espionage*. Homewood: Dow Jones- Irwin.

37. Harber, J. R. 2009. "Unconventional spies: The counterintelligence threat from non-state actors". *International Journal of Intelligence and CounterIntelligence*, 22(2): 221–236.
https://doi.org/10.1080/08850600802698200.

38. Hedin, H. 2004. Introduction to Competitive Intelligence (1/2004). GIA White Paper.

39. Hussey, D. E. 1995. *Rethinking strategic management: Ways to improve competitive performance*. Wiley.

40. Johns, P., and Van Doren, D. C. 2010. "Competitive intelligence in service marketing". *Marketing Intelligence & Planning*, 28(5): 551–570. https://doi.org/10.1108/02634501011066492.

41. Kahaner, L. 1996. *Competitive Intelligence*. New York: Kane Associates.

42. Kanellopoulos, A.-N. 2022. "The Importance of Counterintelligence Culture in State Security". *Global Security and Intelligence Note*, 5.

43. Kanellopoulos, A-N and Ioannidis, A. 2024. "*Enhancing Maritime Security: Adopting an integrated Intelligence Strategy in the Shipping Sector". NATO* Maritime Interdiction Operations Journal, 26.

44. Kula, M. E., and Naktiyok, A. 2021. "Strategic thinking and competitive intelligence: Comparative research in the automotive and communication industries". *Journal of Intelligence Studies in Business*, 11(2).

45. Levitas, E., Hitt, M. A., and Dacin, M. T. 1997. "Competitive intelligence and tacit knowledge development in strategic alliances". *Competitive Intelligence Review*, 8(2): 20–27. https://doi.org/10.1002/cir.3880080206.

46. Lorange, P. 2009. *Shipping strategy: Innovating for success*. Cambridge University Press.

47. Magee, A. C. 2010. "Countering Nontraditional Humint Collection Threats". *International Journal of Intelligence and CounterIntelligence*, 23(3): 509–520. https://doi.org/10.1080/08850601003798807.

48. Marin, J., and Poulter, A. 2004. "Dissemination of competitive intelligence". *Journal of Information Science*, 30(2): 165-180. https://doi.org/ 10.1177/0165551504042806.

49. Miller, J. P. 2005. "Information science and competitive intelligence: Possible collaborators?". *Bulletin of the American Society for Information Science and Technology*, 23(1): 11-13. https://doi.org/10.1002/bult.33.

50. Miller, S. 2001. "Competitive intelligence - An overview". *Society of Competitive Intelligence Professionals*.

51. Nasri, W. 2011. "Competitive intelligence in Tunisian companies". *Journal of Enterprise Information Management*, 24(1): 53–67. https://doi.org/ 10.1108/17410391111097429.

52. Nasri, W. 2012. "Conceptual Model of Strategic Benefits of Competitive Intelligence Process". *International Journal of Business and Commerce*, 1(6).

53. Nasri, W., and Zarai, M. 2013. "Key success factors for developing competitive intelligence in organization". *American Journal of Business and Management*, 2(3). https://doi.org/10.11634/216796061302397.

54. Phathutshedzo, N., and Tiko, I. 2011. "A Framework for Enhancing the Information Systems Innovation: Using Competitive Intelligence". *The Electronic Journal of Information Systems Evaluation*, 14(2).

55. Porter, M. 1991. "Towards a dynamic theory of strategy". *Strategic Management Journal*, 12(2): 95–117. https://doi.org/10.1002/smj.4250121008.

56. Prescott, J. 1999. "The Evolution of Competitive Intelligence - Designing a process for action". *Association of Proposal Management Professionals*.

57. Prescott, J. E. 2001. "Competitive intelligence: Lessons from the Trenches". *Competitive Intelligence Review*, 12(2): 5-19. https://doi.org/10.1002/cir.1013.

58. Saayman, A., Pienaar, J., De Pelsmacker, P., Viviers, W., Cuyvers, L., Muller, M., and Jegers, M. 2008. "Competitive intelligence: Construct exploration, validation and equivalence". *Aslib Proceedings*, 60(4): 383-411. https://doi.org/10.1108/00012530810888006.

59. Salles, M. 2006. "Decision making in SMEs and information requirements for competitive intelligence". *Production Planning & Control*, 17(3): 229–237. https://doi.org/10.1080/09537280500285367.

60. Sapkauskiene, A., and Leitoniene, S. 2010. "The Concept of Time-Based Competition in the Context of Management Theory". *Inzinerine Ekonomika-Engineering Economics*, 21(2).

61. Saxena, D., and Lamest, M. 2018. "Information overload and coping strategies in the Big Data Context: Evidence from the hospitality sector". *Journal of Information Science*, 44(3): 287–297. https://doi.org/10.1177/0165551517693712.

62. Sims, J. E., and Gerber, B. L. 2009. *Vaults, mirrors, and masks: Rediscovering U.S. counterintelligence*. Georgetown University Press.

63. Sliton, P. 1998. "Society of Competitive Intelligence Professionals, various proceedings and publications". *Competitive Review*, 9(2).

64. Smith, C. L., and Brooks, D. J. 2013. *Security science: The theory and practice of security*. Butterworth-Heinemann.

65. Solberg Søilen, K. 2016. "A research agenda for Intelligence Studies in business". *Journal of Intelligence Studies in Business*, 6(1). https://doi.org/10.37380/jisib.v6i1.151.

66. Stopford, M. 2008. *Maritime economics: Martin Stopford*. Routledge.

67. Strauss, K. G. 1999. *Marketing Telecommunication Services*. Artech House Telecom Company.

68. Tahmasebifard, H. 2018. "The role of competitive intelligence and its sub-types on achieving market performance". *Cogent Business & Management*, 5(1): 1540073. https://doi.org/10.1080/23311975.2018.1540073.

69. Tena, J. and Comai, A. 2004. *La Inteligencia Competitiva en las Multinacionales Catalanas*. Barcelona: Emecom.

70. UN Trade and Development (UNCTAD) 2025. *Review of Maritime Transport 2025: Staying the course in turbulent waters. Available at:* https://unctad.org/publication/review-maritime-transport-2025 (Accessed in 26/01/2026).

71. Van Cleave, M. 2007. Counterintelligence and national strategy. https://doi.org/10.21236/ada471485.

72. Weiss, A., and Wright, S. 2006. "Dealing with the Unknown - A Holistic Approach to Marketing and Competitive Intelligence". *Competitive Intelligence*. 9(5).

73. Zheng, E., Fader, P., and Padmanabhan, B. 2011. "From business intelligence to competitive intelligence: Inferring competitive measures using augmented site-centric data". *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1323587

BUNE PRACTICI ÎN PREVENIREA RADICALIZĂRII ŞI A EXTREMISMULUI VIOLENT LA NIVEL EUROPEAN: REVIZUIREA SISTEMATICĂ A LITERATURII DE SPECIALITATE

Ioana CHIȚĂ *

Abstract:

The aim of the present literature review is to provide a comprehensive overview of the models and initiatives implemented by European states to prevent radicalization and violent extremism. Two research questions are addressed: (1) How are prevention models and initiatives implemented in European states represented and analyzed in the academic literature? *and (2)* How are the effectiveness and impact of these prevention strategies evaluated in the existing academic literature?

A systematic literature search was conducted, including peer-reviewed empirical studies employing qualitative or quantitative methods. A total of 98 articles were selected for in-depth analysis. The findings clearly indicate that prevention initiatives are broadly categorized into three areas: individual- or group-focused interventions, community-based approaches, and practitioner- or institution-focused strategies. While a wide range of models exists, including mentoring, family support, digital tools, and multi-agency cooperation, their representation in the literature is uneven and fragmented. Furthermore, the review highlights significant gaps in the evaluation of these strategies. Longitudinal studies are scarce, cultural adaptability is insufficiently addressed, and digital interventions remain under-researched. Overall, although many initiatives show short-term promise, the lack of rigorous and sustained evaluation limits the ability to assess their long-term effectiveness. Future research must address these gaps to support evidence-based policy aligned with EU strategic objectives.

Keywords: *radicalization, violent extremism, preventing radicalization.*

Introducere

Radicalizarea şi extremismul violent reprezintă ameninţări semnificative la adresa securităţii europene, coeziunii sociale şi valorilor democratice ale societăţilor europene, inclusiv cea românească. Aceste provocări complexe şi în continuă evoluţie au determinat răspunsuri

* PhD Candidate, "Mihai Viteazul" National Intelligence Academy, Bucharest, email adress chita.ioana@animv.eu

coordonate și inovatoare atât la nivelul Uniunii Europene (UE), cât și în cadrul fiecărui stat membru. În ultimele două decenii, o gamă largă de inițiative – de la programe bazate pe comunități până la campanii de contra-narațiuni derulate online – au fost dezvoltate pentru a aborda factorii cauzali multipli ai radicalizării. Reflectând diverse contexte naționale, sisteme juridice și realități socio-culturale, aceste eforturi sunt integrate în strategia mai amplă a UE pentru prevenirea radicalizării și a extremismului violent.

Unul dintre principiile de bază ale strategiei comunitare este prioritizarea prevenției prin implicarea tuturor părților interesate, colaborare intersectorială și diseminarea celor mai bune practici între statele membre. În timp ce programele individuale au demonstrat rezultate promițătoare, dovezile rămân fragmentate, subzistând nevoia critică de a evalua modul în care inițiativele aplicate la nivelul statelor europene funcționează și în ce condiții.

Astfel, prezentul studiu își propune să reducă acest decalaj printr-o analiză sistematică a literaturii de specialitate menită să sintetizeze cunoașterea academică existentă privind modelele de inițiative și bune practice existente în prevenirea radicalizării și a extremismului violent la nivel european. Mai exact, analiza își propune să cartografieze peisajul intervențiilor actuale și să identifice modele de impact. În plus, studiul analizează modul în care aceste inițiative sunt reprezentate și criticate în discursul academic, oferind perspective valoroase asupra eficacității, provocărilor și potențialului lor de a consolida reziliența europeană la radicalizare și extremism violent. Prin consolidarea perspectivelor din diverse inițiative, analiza aspiră să informeze atât dezbaterea academică, cât și elaborarea de politici bazate pe dovezi, contribuind la un răspuns european mai coerent și rezilient.

Metodologie

Am utilizat analiza sistematică a literaturii de specialitate pentru a identifica, analiza și sintetiza studiile academice relevante privind modelele și inițiativele de prevenire implementate de statele europene. Două întrebări de cercetare au ghidat procesul de căutare, selecție și evaluare, respectiv:

1. Cum sunt reprezentate și analizate în literatura academică modelele și inițiativele de prevenire implementate în statele europene?

2. Cum sunt evaluate eficacitatea și impactul acestor strategii de prevenire în literatura academică existentă?

Criteriile de includere a literaturii sunt: articole peer reviewed, capitole de carte și rapoarte guvernamentale sau instituționale care

examinează modele, inițiative sau politici de prevenire a radicalizării sau extremismului violent aplicate la nivel european. Au fost incluse atât studii calitative, cât și studii cantitative. De asemenea, studiile trebuie să evalueze eficacitatea (impactul) acestor inițiative sau – cel puțin – să ofere informații despre experiențele de implementare a inițiativelor. Analiza include studii publicate în limba engleză în perioada 2010 și 2024. Nefiind aplicat un criteriu de excludere specific referitor la grupul țintă al intervențiilor analizate[1], analiza a urmat o abordare comprehensivă care să reflecte diversitatea circumstanțelor ce pot contribui la vulnerabilitatea față de radicalizare.

Strategia de căutare este rezumată în Figura 1. Am utilizat diagrama de flux PRISMA[2] pentru a documenta procesul de selecție a studiilor, oferind transparență și reproductibilitate. În ceea ce privește selecția, în primul rând am consultat mai multe baze de date academice, respectiv Google Academic, Campbell Collaboration, JSTOR, ProQuest, PsycInfo și SCOPUS, pentru a capta o gamă cuprinzătoare de articole peer reviewed, capitole de carte, cărți, manuale și rapoarte (de cercetare, guvernamentale și de evaluare). Pentru completarea căutărilor referitoare la impact am apelat și la Impact Europe PVE intervention database (Impact Europe 2017).

Am utilizat următoarele cuvinte cheie și operatori booleeni: radical*, extrem*, interven*, program*, train*, treat*, prevent*, diseng*, derad*, eval*, impact*, quant*, effect, „preventing radicalization", „prevention models", „prevention initiatives", „evaluating radicalization prevention programmes", „preventingviolentextremism", „evaluating violent extremism prevention programmes", "preventing radicalization "AND"prevention initiatives"AND"european states", "preventing radicalization"AND"prevention models"AND"european states", "preventing violent extremism"AND"prevention models"AND"european states", "preventing violent extremism"AND"evaluating programs" AND"european states", "preventing radicalization"AND"evaluating programs"AND" european states", "preventing radicalization"OR"preventing violent extremism".

Căutările au fost rafinate folosind filtre pentru datele publicării (2010–2024), limba (engleză) și relevanța pentru contexte europene (acolo unde căutarea avansată a permis un astfel de filtru specific).

[1]Astfel, unele dintre inițiativele analizate vizează spre exemplu membri ai comunității musulmane, migranți, adolescenți, elevi.

[2]Diagrama de flux PRISMA (http://www.prisma-statement.org) asigură claritate în raportarea numărului de înregistrări verificate și excluse în fiecare etapă, împreună cu rațiunea excluderilor, cum ar fi irelevanța tematică sau calitatea metodologică insuficientă.

În ansamblu, categoriile de surse au fost identificate prin intermediul unei abordări de căutare ce a inclus :

- O căutare sistematică în bazele de date, acoperind o serie de jurnale și periodice importante din domeniu.
- O căutare în rețea după autori, respectiv experții de referință în domeniu. Precizăm că acolo unde există studii similare ale aceluiași autor, am ales varianta cea mai recentă.
- O abordare de tip „bulgăre de zăpadă" unde literatura suplimentară este identificată pe baza lecturii lucrărilor existente.

Căutarea inițială în bazele de date menționate a rezultat într-un număr de 19.480 publicații (Figura 1), dintre care 10.100 publicații prin Google Academic, 5.220 prin JSTOR și 4.160 alte baze de date (Campbell Collaboration, ProQuest, PsycInfo și SCOPUS). După eliminarea a 1.460 de duplicate, 18.020 de înregistrări au fost verificate pe baza titlurilor lor. Dintre acestea, 17.655 au fost excluse deoarece nu au îndeplinit criteriile de relevanță pentru obiectivele cercetării. Restul de 365 de abstracte au fost supuse unui screening suplimentar, restrângând selecția la 124 de studii pentru revizuirea integrală. În această etapă a intervenit un proces suplimentar de identificare în care, pe baza studiilor revizuite integral au fost identificate alte 19 înregistrări care au urmat ulterior același proces de selecție bazat pe criteriile deja menționate. În cele din urmă, 98 de studii au fost incluse în revizuirea sistematică, reprezentând o sinteză cuprinzătoare a literaturii de specialitate, aliniată cu scopul și obiectivele cercetării.

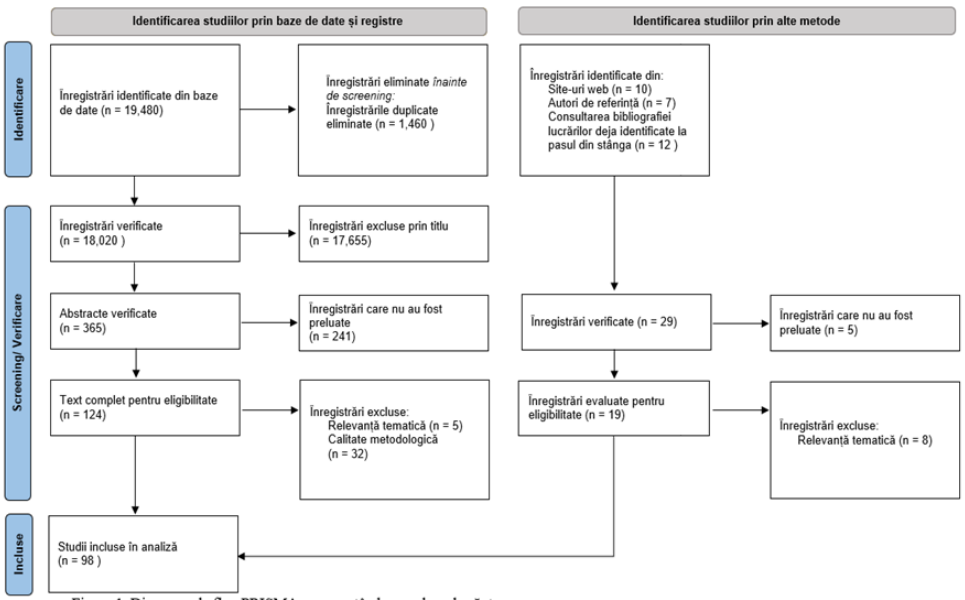

Figura 1. Diagrama de flux PRISMA reprezentând procedura de căutare

Rezultate

Unul din primele aspecte ce a rezultat din analiza sistematică este observaţia că un număr limitat al publicaţiilor analizate investighează impactul iniţiativelor destinate prevenirii extremismului. În schimb, literatura se concentrează pe rezultate care pot întări potenţial eforturile de prevenire sau pe rezultate referitoare la experienţele din implementarea iniţiativelor. Această limitare în cunoaşterea efectelor înseamnă că studiul oferă concluzii limitate asupra efectelor asociate practicilor preventive existente.

În ceea ce priveşte răspunsul la prima întrebare de cercetare analiza literaturii a relevat că există 3 tipuri principale de intervenţii de prevenire la nivel european. respectiv intervenţii destinate individului (indivizilor) care necesită eforturi de prevenire, intervenţiile axate pe mediul social al individului şi cele care vizează mediul profesional. Distribuirea studiilor raportat la categoriile de iniţiative identificate (Figura 2) este următoarea: din totalul de 98 publicaţii, 52 dintre studiile analizate menţionează iniţiative centrate pe individ (indivizi), 31 studii sunt axate pe iniţiative sau abordări ce au ca grup ţintă mediul din jurul individului, respectiv familia, grupul de prieteni sau comunitatea locală, iar 39 studii abordează iniţiative centrate pe profesioniştii din prima linie fie prin dezvoltarea capacităţii lor profesionale, fie prin sporirea cooperării între diferitele categorii profesionale.

Distribuţia studiilor indică faptul că majoritatea iniţiativelor analizate (42 din 98) sunt centrate pe individ, reflectând un interes crescut pentru intervenţiile directe asupra persoanelor vulnerabile la radicalizare. Astfel, priorităţile actuale ale eforturilor preventive vizează indivizii şi grupurile de indivizi. În acelaşi timp, iniţiativele axate pe mediul social al individului (familie, prieteni, comunitate) şi pe formarea profesioniştilor din prima linie (30 studii fiecare) evidenţiază o recunoaştere a importanţei factorilor contextuali şi a cooperării interprofesionale.

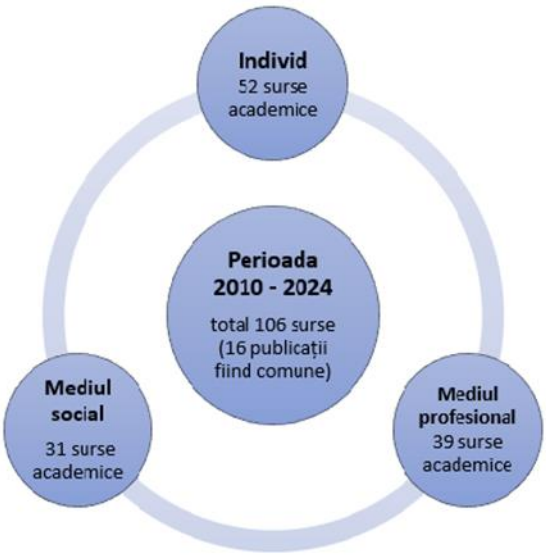

Figura 2. Distribuirea surselor raportat la categoriile de inițiative identificate

În total, analiza a identificat un număr de șase abordări ale eforturilor prevenirii radicalizării și extremismului violent, respectiv:

1. Dezvoltarea cunoștințelor și a capacității individuale (33 surse academice)
2. Sprijin și îndrumare în etapele vulnerabile ale vieții (20 surse academice)
3. Implicarea familiei și a rețelei sociale apropiate (17 surse academice)
4. Implicarea comunității locale (15 surse academice)
5. Dezvoltarea capacității în rândul profesioniștilor (19 surse academice), și
6. Dezvoltarea cooperării în rândul profesioniștilor/ Formatele de cooperare multi-instituțională (20 surse academice).

Inițiative și abordări preventive axate pe individ sau grupuri de indivizi

Inițiativele axate pe individ sunt acele tipuri de intervenții care urmăresc dezvoltarea rezilienței la radicalizare și extremism violent a indivizilor fie prin **dezvoltarea cunoștințelor și a capacității individuale** – prin stimularea conștientizării în privința consecințelor actelor radicale (spre exemplu, prin gândire critică, alfabetizare media),

fie prin **sprijinirea şi îndrumarea acestora în etapele vulnerabile ale vieţii**, cum sunt adolescenţa/reintegrarea în societate post-executare a unei pedepse privative de libertate – oferind suport persoanelor expuse de a se îndepărta de parcursul radical. Acest sprijin poate lua forme variate precum mentoratul, consilierea psihologică, terapia comportamentală, sprijinul educaţional şi asistenţa socială. Mentoratul, în special, apare ca un element de bază în cadrul acestor programe. În termeni specifici, pe baza analizei publicaţiilor incluse, au fost identificate două abordări preventive centrate pe individ, respectiv **(1.) dezvoltarea cunoaşterii şi capacităţii individuale** şi **(2.) sprijin şi îndrumare în etapele vulnerabile ale vieţii.**

1. Dezvoltarea cunoaşterii şi capacităţii individuale

Analiza publicaţiilor incluse subliniază că intervenţiile timpurii care vizează copiii şi tinerii pot avea un efect preventiv semnificativ. Intervenţia timpurie se referă la măsurile proactive implementate în etapele iniţiale ale dezvoltării unui individ sau anterior apariţiei unor potenţiali factori de risc pentru radicalizare. Aceste măsuri sunt concepute pentru a aborda vulnerabilităţile şi pentru a consolida factorii protectivi înainte ca ideologiile sau comportamentele radicale să se înrădăcineze.

Unul din primele aspecte ce a rezultat din analiza sistematică a literaturii a fost că prevenirea timpurie în şcoli are un impact ridicat. Instituţiile educaţionale reprezintă terenul fertil pentru prevenţie iar programele care au demonstrat rezultate solide în creşterea rezilienţei în rândul tinerilor sunt axate pe dezvoltarea gândirii critice, alfabetizare media, dialog intercultural, dezvoltarea valorilor democratice, empatie şi respect. Programele implementate în şcolile europene demonstrează că integrarea acestor teme în curricula şcolară sporesc reziliența, coeziunea socială şi toleranţa.

Astfel, studiile sugerează că **dezvoltarea rezilienţei şi a gândirii critice prin educaţie** este esenţială pentru prevenirea radicalizării şi extremismului violent (Maraj, Mahmut şi Ghosh 2021) (Stephens, Sieckelinck şi Boutellier 2021) (Amit şi Al Kafy 2022), aşa cum este exemplificat de programul „Being Muslim Being British" (Mattsson şi Säljö 2018) (Liht şi Savage 2013) (Davies 2010) (Stephens, Sieckelinck şi Boutellier 2021). În acest sens, programele educaţionale care promovează **cunoştinţe despre democraţie, toleranţă şi respectul pentru diversitate** sunt cruciale (Macnair şi Frank 2017). Prin consolidarea acestor abilităţi, tinerii devin mai rezilienţi în faţa

influențelor radicale (Lahnait 2021) (Davies, Wicked Problems: How Complexity Science Helps Direct Education Responses to Preventing Violent Extremism 2016). Inițiativele educaționale care promovează principiile democratice[3] pot fi instrumente eficiente în prevenirea radicalizării, mai ales atunci când fac parte dintr-un efort mai larg și susținut care implică școli, comunități și factori de decizie (Luter și Glock 2017).

Literatura analizată indică faptul că intervențiile destinate tinerilor nu doar că ajută la prevenirea radicalizării, dar contribuie și la dezvoltarea unei coeziuni sociale mai puternice în comunități. Acestea reduc polarizarea socială (Lindekilde și Parker 2020) (Niemi, și alții 2018), stigmatizarea și promovează dialogul inter-cultural (Grossman, Hadfield, Jefferies, Gerrard, & Ungar, 2020). Deoarece astfel de intervenții destinate tinerilor au loc predominant în instituții educaționale, cum ar fi liceele (Flesner, Larsson și Saljo 2019), un aspect esențial al acestor inițiative este instruirea și sprijinul oferit cadrelor didactice pentru a le permite să identifice și să reacționeze adecvat la semnele de radicalizare în rândul elevilor (Busher, și alții 2017) (Parker, Lindekilde și Gøtzsche-Astrup 2020).

Programele implementate în școli din întreaga Europă (de exemplu, Țările de Jos, Finlanda, Danemarca, Franța și Belgia) au arătat că integrarea acestor teme în programele de învățământ poate stimula reziliența, coeziunea socială și toleranța, permițând tinerilor să reflecteze asupra identității, conflictelor de valori și perspectivelor alternative (Ruyter și Sieckelinck 2023) (Visser și Vermeulen 2021) (van der Vet 2020) (Lahnait 2021). Intervenții precum învățarea bazată pe discuții, formarea în alfabetizarea media și utilizarea intereselor tinerilor (de exemplu, rețelele sociale) ca instrumente de implicare s-au dovedit deosebit de eficiente. Unele programe, precum „Being Muslim Being British" și „Diamond", demonstrează rezultate pozitive în creșterea

[3] O evaluare a lui Lüter și Glock (2017) privind impactul programului *Concepts against Islamist radicalization – Module Prevention of radicalization* a evidențiat rezultate pozitive, inclusiv creșterea gradului de conștientizare și înțelegere a principiilor democratice. Programul Concepts Against Islamist Radicalization, dezvoltat de Kreuzberger Initiative gegen Antisemitismus e.V. (KIgA), abordează problema radicalizării islamiste prin educație. Acesta își propune să prevină radicalizarea prin creșterea gradului de conștientizare a proceselor sale, promovarea valorilor democratice și încurajarea gândirii critice în rândul tinerilor și educatorilor. Programul include ateliere de lucru interactive, materiale educaționale personalizate și instruire pentru facilitatori, pentru a dota participanții (elevi clasa a 8-a și a 9-a) cu instrumente pentru a recunoaște și a contracara ideologiile extremiste.

complexității cognitive, a empatiei şi a stimei de sine, reducând în acelaşi timp susceptibilitatea față de ideologiile extremiste (Liht şi Savage 2013) (Feddes, Mann şi Doosje 2015). În plus, inițiativele care includ mărturii ale foştilor extremişti s-au dovedit promițătoare în discreditarea narațiunilor radicale şi în creşterea gradului de conştientizare cu privire la tacticile de recrutare (Lindekilde şi Parker 2020) (Walsh şi Gansewig 2021).

Pe de altă parte, revizuirea a identificat lacune în cercetare privind intervențiile digitale. În lumina influenței tot mai mari a rețelelor sociale şi a mediului digital în procesele de radicalizare şi recrutare extremistă, este necesară dezvoltarea şi evaluarea de instrumente şi platforme digitale care pot servi ca resurse de prevenire. Astfel, este nevoie să fie acordată o atenție sporită comunicării digitale pentru a angaja eficient tinerii în spațiile virtuale – acolo unde are loc frecvent recrutarea de natură extremistă.

2. Sprijin şi îndrumare în etapele vulnerabile ale vieții.

Revizuirea sistematică a literaturii a indicat faptul că inițiativele de prevenire care oferă sprijin şi îndrumare în fazele vulnerabile ale vieții pot juca un rol substanțial în reducerea susceptibilității la radicalizare şi stimularea dezactivării pe termen lung față de ideologiile extremiste. Aceste tipuri de inițiative se bazează pe ideea că oferirea de suport în stadii vulnerabile ale vieții, cum ar fi adolescența sau revenirea în societate după încarcerare, poate preveni dezvoltarea unor ideologii radicale. Intervențiile bazate pe suport, implementate în diferite țări europene, adoptă adesea o abordare holistică care include mentorat, consiliere psihologică, terapie comportamentală, sprijin educațional, asistență socială, resocializare şi reabilitare. Ele se adresează în special tinerilor, persoanelor expuse riscului, precum şi celor care se reintegrează în societate după încarcerare (D. Koehler 2016) (Aiello, Puigvert şi Schubert 2018) (T. W. Christensen, "I had never reached those Nazi guys without their help" Being a former becoming a mentor - and the value of using formers in exit work 2023).

Mentoratul, în special, apare ca un element de bază în cadrul acestor programe, oferind sprijin emoțional, feedback constructiv şi îndrumări care promovează reziliența, gândirea critică şi formarea de rețele sociale sănătoase (Winterbotham 2020) (van de Donk, Uhlmann şi Keijzer 2020) (Walkenhorst, şi alții 2020). Pe lângă suportul emotional, mentoratul poate oferi şi orientare profesională şi educațională,

facilitând astfel o integrare mai bună în societate (Bertelsen, Mentoring in anti-radicalisation. LGT: A systematic assessment, intervention and supervision tool in mentoring 2018) (Bertelsen 2015).

Utilizarea intervenţiilor de tip mentorat demonstrează un potenţial real în echiparea persoanelor vulnerabile cu abilităţi esenţiale. Studiile subliniază că mentorii pot spori încrederea în sine a persoanei mentorate, abilităţile de comunicare şi participarea comunităţii, acţionând în acelaşi timp ca un buffer împotriva influenţelor negative (Winterbotham 2020). În plus, intervenţiile de mentorat care implică foşti extremişti s-au arătat promiţătoare datorită credibilităţii şi capacităţii lor de a facilita reflecţia prin naraţiuni personale (T. W. Christensen 2023) (Oxford Research 2016) (ICPT 2015) (Bertelsen, Mentoring in anti-radicalisation. LGT: A systematic assessment, intervention and supervision tool in mentoring 2018) (Bertelsen 2015) (T. W. Christensen, "I had never reached those Nazi guys without their help" Being a former becoming a mentor - and the value of using formers in exit work 2023) (Christensen, Lindekilde, şi alţii 2023) (Marsden 2017) (D. Koehler 2016) (Schuurman şi Bakker 2015) (Papp, şi alţii 2022) (van de Donk, Uhlmann şi Keijzer 2020) (Walkenhorst, şi alţii 2020).

Cu toate acestea, evaluările existente privind mentoratul (Winterbotham 2020) sunt adesea lipsite de rigoare metodologică şi nu fac legătura cauzală între persoana mentorată şi reducerea extremismului violent. De asemenea, acele tipuri de intervenţii de sprijin axate exclusiv pe creşterea stimei de sine pot avea efecte nedorite, cum sunt narcisismul şi agresivitatea. Chiar şi în ciuda rezultatelor promiţătoare pe termen scurt menţionate anterior în cazul acestor tipuri de initiative de sprijin, există o lipsă notabilă de studii longitudinale care să evalueze sustenabilitatea efectelor. De exemplu, cercetările realizate de Christensen (2023) şi Koehler (2017) sugerează că mentoratul poate influenţa pozitiv tinerii, însă dovezile concrete care să demonstreze eficacitatea sa durabilă sunt limitate. Ar fi necesare evaluări mai ample, care să urmărească tinerii în timp pentru a evalua stabilitatea rezultatelor acestor intervenţii.

Limitările metodologice, cum ar fi absenţa cadrelor de evaluare standardizate[4] şi a măsurilor de adaptabilitate culturală, limitează, de asemenea, aplicabilitatea mai largă. Dovezile sugerează că astfel de iniţiative sunt cele mai eficiente atunci când sunt sensibile din punct de

[4] aşa cum reiese din cercetările lui Koehler (2017) şi Christensen şi colab. (2023).

vedere cultural[5], sunt integrate în resursele comunităţii şi sunt adaptate nevoilor individuale. Deşi aceste programe nu pot pretinde încă efecte cauzale definitive din cauza datelor limitate, ele par să contribuie semnificativ la stabilizarea persoanelor vulnerabile şi la dezvoltarea factorilor protectivi la radicalizare.

Iniţiativele şi abordările preventive axate pe mediul social al individului

Iniţiativele şi abordările preventive axate pe mediul social[6] al individului utilizează reţele sociale de sprijin proxim din jurul individului respectiv – familia, rudele şi grupul de prieteni, dar şi influenţele societale mai largi, precum comunitatea locală – ca resursă în efortul preventiv. Altfel spus, reţeaua apropiată[7] individului vulnerabil, împrejurimile şi conexiunile sale sociale, dar şi comunitatea locală şi societatea în general, pot acţiona ca factori favorizanţi pentru reconstituirea unui mediu cotidian pozitiv care să conducă individul pe un parcurs de dezangajare faţă de radicalizare şi extremism violent.

Analiza sistematică a literaturii academice a identificat că abordările axate pe mediul social al individului presupun fie **(3) implicarea familiei şi a reţelei sociale apropiate** (iniţiative ce lucrează cu structura de sprijin cea mai apropiată a individului), fie **(4) implicarea comunităţii locale** (abordarea preventivă vizează contextul din jurul individului într-un sens mai larg). Implicarea familiei şi a reţelei sociale apropiate implică iniţiative de suport parental prin terapie, consiliere, coach parentali, crearea de reţele de

[5] Cercetări precum cele realizate de Walkenhorst şi colab. (2020) şi Oxford Research (2016) subliniază necesitatea de a înţelege mai bine modul în care diferenţele socioculturale afectează aplicabilitatea şi succesul programelor de mentorat în comunităţi diverse.

[6] Prin mediul social al unui individ înţelegem contextele sociale în care acesta trăieşte şi interacţionează (online sau offline), în special mediul înconjurător proxim mediat, cum ar fi familia, colegii şi comunitatea, precum şi structurile şi influenţele societale mai largi care îi modelează comportamentul, experienţele şi dezvoltarea în timp. Am inclus în această categorie şi influenţele sociale digitale care pot acţiona asupra unui individ şi schimba comportamentul în timp.

[7] Sintagma reţea socială apropiată se referă la un grup strâns interconectat de persoane cu care individul întreţine interacţiuni (online sau offline) frecvente, semnificative şi adesea de sprijin emoţional şi pe care individul îi percepe ca fiindu-i apropiaţi. Această reţea include de obicei familia (părinţi şi rude apropiate), prieteni apropiaţi şi colegi de încredere, care oferă sprijin social, emoţional şi practic şi joacă un rol semnificativ în modelarea atitudinilor, comportamentelor şi proceselor decizionale ale individului.

părinți, pentru a echipa familiile cu abilități practice care contribuie la recunoașterea semnelor timpurii, gestionarea conflictelor și promovarea rezilienței, în timp ce implicarea comunității locale este centrată pe cooperarea cu părțile interesate locale – cum ar fi actorii societății civile, organizațiile religioase, liderii comunitari și instituțiile – care devin participanți activi la eforturile preventive locale.

3. Implicarea familiei și a rețelei sociale apropiate

Analiza sistematică indică faptul că implicarea familiei și a rețelei sociale apropiate în eforturile de prevenire a radicalizării poate spori semnificativ eficacitatea intervențiilor, în special în stadiile incipiente și vulnerabile ale dezvoltării ideologice. Cercetările recente evidențiază că legăturile emoționale și încrederea inerentă relațiilor de familie și între semeni creează oportunități puternice de a perturba parcursul către radicalizare și sprijini dezangajarea din mediile extremiste (Ellefsen & Sandberg, 2024). De asemenea, aceste cercetări subliniază faptul că intervențiile informale, fundamentate pe conexiuni emoționale și interacțiuni cotidiene, sunt adesea mai eficiente decât răspunsurile instituționale, care pot conduce la alienare.

Implicarea familiei și a rețelei poate conduce la următoarele trei rezultate cheie pozitive, respectiv creșterea motivației individuale de a alege o direcție pozitivă în viață, dezvoltarea de noi conexiuni sociale pozitive sau consolidarea celor existente și stabilizarea vieții cotidiene în afara mediului extremist având susținerea familiei și a prietenilor (Ellefsen & Sandberg, 2024) (Haugstvedt 2021) (Bertelsen și Kruglanski 2020) (Sikkens, și alții 2017) (Hales și Williams 2018) (Bertelsen și Kruglanski 2020) (Cragin, și alții 2015) (Yayla 2020) (Kolbe 2019).

Programele implementate în toată Europa – inclusiv Norvegia, Danemarca, Germania și Țările de Jos – folosesc o serie de abordări, cum ar fi coachingul pentru părinți, consilierea familiei, rețelele de sprijin de la egal la egal și intervenții tip EXIT (Bertelsen și Kruglanski 2020) (Haugstvedt 2021) (Andersson 2018) (Visser și Vermeulen 2021). Aceste inițiative nu oferă doar sprijin emoțional și psihologic, ci dotează familiile și cu abilități practice pentru a recunoaște semnele timpurii de radicalizare, gestiona conflictele și promova reziliența (Cragin, și alții 2015) (Williams, Horgan și Evans 2016). Mentoratul de către profesioniști pregătiți sau chiar foști extremiști a fost, de asemenea, integrat în intervențiile centrate pe familie pentru a oferi îndrumări credibile.

Pe de altă parte, în timp ce familiile pot servi drept factor protectiv în faţa influenţelor extremiste, ele pot fi în anumite cazuri factor de risc în acele contexte de disfuncţie familială, traumă sau comunicare deficitară. Aşadar, răspunsul la radicalizare trebuie particularizat în funcţie de situaţia familială iar implicarea familiei trebuie realizată doar în acele cazuri în care familia actionează ca un factor protectiv, nu unul de risc.

Ţinând cont de importanţa recunoscută a familiilor, cercetările viitoare ar trebui să înţeleagă mai bine dublul rol al familiei – atât ca factor de protectiv, cât şi, uneori, de risc. Deşi sensibilitatea problemelor legate de familie şi stigmatizarea asociată radicalizării împiedică adesea participarea la cercetare şi limitează disponibilitatea datelor solide, multe studii oferind doar perspective calitative sau dovezi anecdotice, totuşi pentru a consolida strategiile de prevenire, cercetările viitoare ar trebui să urmărească dezvoltarea de modele adaptabile cultural, bazate pe dovezi pentru implicarea familiei. Intervenţiile bazate pe familie ar trebui integrate în sistemele comunitare şi de sănătate mintală mai largi, în special pentru tinerii expuşi riscului, pentru a valorifica potenţialul familiei în promovarea rezilienţei şi protejarea împotriva recrutării extremiste.

4. Implicarea comunităţii locale

Implicarea comunităţii locale poate juca un rol semnificativ în prevenirea radicalizării şi a extremismului violent. Abordările bazate pe comunitate sunt centrate pe cooperarea cu părţile interesate locale – cum ar fi actorii societăţii civile, organizaţiile religioase, lideri comunitari – şi pun accent pe consolidarea încrederii, împuternicire şi responsabilitate partajată (Stephens, Sieckelinck şi Boutellier, Preventing Violent Extremism: A Review of the Literature 2021) (T. W. Christensen 2019) (Macnair şi Frank, Voices Against Extremism: A case study of a community-based CVE counter-narrative campaign 2017, Roex şi Vermeulen 2019) (Cherney şi Hartley 2015) (Bonnell, şi alţii 2011) (Ellis şi Abdi 2017) (Pratchett , şi alţii 2010).

Programele care reuşesc pe termen lung sunt cele care investesc timp şi resurse în dezvoltarea unei relaţii de încredere cu comunităţile. Aceasta presupune implicarea actorilor locali, descentralizarea unor sarcini de prevenire, asigurarea competenţei culturale şi evitarea stigmei. Aceste iniţiative poziţionează comunităţile locale nu doar ca destinatari pasivi ai politicilor preventive (Cherney şi Hartley 2015), ci ca participanţi activi la identificarea riscurilor, contestarea naraţiunilor

extremiste și sprijinirea persoanelor vulnerabile (Vermeulen și Bovenkerk, However, community engagement comes with specific policy: local policies in western European cities 2012).

În timp ce dovezile empirice privind impactul direct al implicării comunității asupra reducerii radicalizării rămân limitate, un consens larg al literaturii sugerează că legăturile sociale locale puternice și parteneriatele locale sunt cheie pentru construirea rezilienței comunității și pentru stimularea unui sentiment de incluziune și eficacitate colectivă. Programele implementate în țări precum Țările de Jos, Danemarca, Finlanda și Suedia ilustrează o varietate de modele – de la rețele de prevenire descentralizate și angajamentul figurilor cheie până la colaborarea interconfesională și dialogul cu comunități greu accesibile. De exemplu, strategia descentralizată a Țărilor de Jos (Visser și Vermeulen 2021) și inițiativa „Shoulder to Shoulder" a Finlandei (Tiilikainen și Mankkinen 2020) (Francis, van Eck și van Twist 2015) (Martikainen 2019) demonstrează modul în care cooperarea localizată, bazată pe încredere poate spori atât legitimitatea, cât și durabilitatea eforturilor de prevenire.

Cu toate acestea, implicarea comunității nu este lipsită de provocări. Probleme precum lipsa de încredere, riscul de stigmatizare a comunităților și dificultățile în selectarea partenerilor legitimi pot submina impactul unor astfel de initiative, producând chiar efecte nedorite. Mai mult, rolul societății civile variază în funcție de contexte naționale – fiind parte integrantă a strategiilor de prevenire în Finlanda și Suedia, dar mai puțin clar definit în Norvegia și Danemarca.

Având în vedere că relațiile sociale locale puternice și asumarea comunității asupra acțiunilor preventive sunt cruciale pentru succesul pe termen lung, integrarea actorilor locali în strategiile naționale poate contribui nu numai la o mai mare eficacitate a politicilor, ci și la consolidarea coeziunii comunității, a normelor comune și a rezilienței la influențele extremiste.

Inițiative și abordări preventive adresate profesioniștilor implicați în coordonarea și implementarea eforturilor de prevenire

Analiza publicațiilor incluse a permis identificarea următoarelor două tipuri distincte de abordări preventive destinate practicienilor din prima linie, respectiv (5) **inițiative de dezvoltare a cunoașterii și capacității profesioniștilor** și (6) **formate de cooperare multi-instituțională.** Acest tip de abordări au ca obiectiv principal

consolidarea abilităţilor, cunoştinţelor şi capacităţii de colaborare a profesioniştilor[8] în activitatea de prevenire a radicalizării şi extremismului violent, astfel încât să poată interveni mai eficient în coordonarea şi implementarea eforturilor. Pregătirea profesioniştilor se adresează practicienilor din prima linie (ofiţeri din poliţie, din mediul penitenciar, profesori, asistenţi sociali, terapeuţi, consilieri şcolari, etc.).

Formatele de cooperare multi-instituţională reprezintă acele structuri în care actori din diferite sectoare din domeniul public şi privat asigură luarea de decizii în comun, partajarea informaţiilor în siguranţă şi intervenţii coordonate în speţe concrete de radicalizare şi extremism violent, ceea ce concură la derularea de eforturi preventive eficiente, ţinând cont şi de natura multifaţetată a radicalizării şi de factorii diverşi implicaţi în cadrul proceselor menţionate.

5. Iniţiative de dezvoltare a cunoaşterii şi capacităţii profesioniştilor

Revizuirea sistematică a literaturii evidenţiază rolul esenţial al formării profesioniştilor pentru a detecta şi a răspunde eficient la semnele de radicalizare (Tierney 2017) (R. RAN 2019) (Cowi 2014) (D. Koehler 2016). Astfel de programe de formare pun accentul pe echiparea profesioniştilor, inclusiv asistenţi sociali, profesori şi forţele de ordine, cu cunoştinţele şi instrumentele necesare pentru a aborda vulnerabilităţile şi riscurile.

O temă recurentă în literatura de specialitate este înţelegerea limitată în rândul practicienilor a proceselor de radicalizare, incapacitatea de a recunoaşte semnele timpurii de avertizare şi lipsa strategiilor adecvate de răspuns (Tierney 2017) (R. RAN 2019) (Cowi 2014) (D. Koehler 2016). Astfel, iniţiativele de dezvoltare profesională servesc la creşterea gradului de conştientizare, îmbunătăţirea detecţiei timpurii a semnalelor de radicalizare şi consolidarea capacităţii profesioniştilor de a răspunde în mod adecvat persoanelor sau grupurilor expuse riscului (Brouillette-Alarie, şi alţii 2022) (Bowie şi Revell 2018) (Joyce 2018) (Lakhani 2012) (Younis şi Jadhav 2019) (Kyriacou, şi alţii 2017).

[8] Profesioniştii care acţionează în sfera preventivă sunt definiţi ca totalitatea persoanelor care, în exercitarea atribuţiilor lor profesionale, pot interacţiona cu indivizi vulnerabili sau aflaţi la risc de radicalizare. Această categorie include practicieni din prima linie a prevenirii radicalizării şi extremismului violent, cum ar fi ofiţerii de informaţii, poliţiştii şi personalul penitenciar, precum şi profesionişti din domenii conexe, precum profesorii, asistenţii sociali şi terapeuţii.

Programele de formare se concentrează adesea pe înțelegerea proceselor de radicalizare, evaluarea riscurilor și tehnici de intervenție.

Studiile subliniază că dezvoltarea profesională este cea mai eficientă atunci când include metode de învățare aplicate, cum ar fi studii de caz, jocuri de rol și simulări care reflectă complexitățile lumii reale. Cu toate acestea, există variații semnificative în ceea ce privește instrumentele, cunoștințele și abordările de formare disponibile pentru practicieni, în funcție de contextul instituțional și operațional, evidențiind nevoia unor cadre flexibile, dar coerente, care să se poată adapta la realitățile locale (Koehler, 2016; Tierney, 2017). În timp ce eforturile de consolidare a capacității s-au arătat promițătoare în îmbunătățirea practicilor de prevenire, totuși provocările subzistă. Acestea includ ambiguitatea rolurilor profesionale (în special în sectorul educațional), aplicarea practică limitată a instruirii și riscul unor consecințe nedorite, cum ar fi stigmatizarea, supravegherea sporită și erodarea încrederii în cadrul comunităților afectate.

De asemenea, dovezile empirice care leagă programele de consolidare a capacităților de rezultatele preventive pe termen lung sunt limitate. Cu toate acestea, inițiative precum abordarea pe mai multe niveluri a Țărilor de Jos (Visser și Vermeulen 2021), modelul de cooperare SSP al Danemarcei (A. S. Hemmingsen 2015) și proiectul Dembra din Norvegia (Lenz și Kjeoy 2014) ilustrează eforturile structurate de a integra formarea profesională în strategiile naționale mai largi.

În cele din urmă, în timp ce consolidarea capacității profesionale singură nu poate preveni radicalizarea, ea joacă un rol esențial de susținere, echipând practicienii cu instrumentele și înțelegerea contextuală necesare pentru a se implica din timp și în mod semnificativ cu persoanele expuse riscului. Adaptarea acestor inițiative la nevoile specifice ale grupurilor profesionale și abordarea provocărilor contextuale și operaționale cu care se confruntă sunt esențiale pentru maximizarea potențialului lor preventiv.

6. Formatele de cooperare multi-instituțională

Formatele de cooperare multi-instituțională (‘*Multi-agency working formats’/MAW*) reprezintă acel grup de inițiative ce abordează provocarea complexă și multifațetată a radicalizării și extremismului violent prin crearea de infrastructuri de prevenire care asigură sprijin pentru indivizii vulnerabili din partea diferitelor autorități și organizații pe mai multe niveluri. Acest efort coordonat presupune angajarea

diferitelor sectoare din domeniul public şi privat, atât la nivel naţional, cât şi local. Mai explicit, o abordare multi-instituţională reprezintă un sistem în care informaţiile pot fi partajate în siguranţă între actorii implicaţi, aspect esenţial pentru identificarea şi gestionarea persoanelor expuse riscului de radicalizare/extremism violent. Aceste structuri şi procese de lucru cu mai multe instituţii asigură identificarea mai eficientă a persoanelor vulnerabile, îmbunătăţirea schimbului de informaţii, luarea deciziilor în comun şi intervenţii coordonate, ceea ce ar putea concura la derularea de eforturi preventive eficiente.

Formatele de cooperare multi-instituţională sunt din ce în ce mai mult considerate o abordare promiţătoare ce facilitează identificarea timpurie şi eficientă a persoanelor şi comunităţilor care sunt expuse riscului de radicalizare şi extremism violent (Hardyns, Klima şi Pauwels 2022). Studiile analizate indică o serie de moduri diferite prin care sunt create parteneriate multi-instituţionale, respectiv prin acorduri formale şi informale, precum cadre legislative, memorandumuri de înţelegere sau standarde de politici care stipulează canale pentru schimbul de informaţii între instituţii (El-Said 2015) (D. Koehler 2016).

Cu toate acestea, deşi practica formatelor de cooperare multi-instituţionale este considerată una promitătoare, nu există suficiente dovezi empirice care sugerează că aceste formate conduc la prevenirea radicalizării violente deoarece au fost translatate din principiile de bază ale prevenirii infracţiunilor de drept comun. În practică, aplicarea formatelor de lucru multi-instituţional are la bază presupunerea intuitivă că abordările holistice, coordonate şi de tip colaborativ se adresează mai eficient factorilor plurali care conduc la radicalizare şi extremism violent (L. Mazerolle , şi alţii 2021) (Butt şi Tuck 2014) şi ca urmare a integrării cunoştinţelor trans-sectoriale ale practicienilor implicaţi.

Literatura de specialitate subliniază importanţa strategiilor holistice care combină eforturile de securitate preventivă cu incluziunea socială, dialogul şi construirea încrederii pentru a atenua stigmatizarea şi a spori implicarea comunităţii. Factorii cheie de succes identificaţi includ roluri clar definite, comunicare structurată, obiective comune şi stabilirea încrederii între părţile interesate (L. Mazerolle , şi alţii 2021) (Goodking, şi alţii 2011) (Curnin, şi alţii 2015) (Gill şi Thompson 2017) (B. Ellis, şi alţii 2020) (Sivenbring şi Andersson Malmros 2021) (Clubb, şi alţii 2021) (Solhjell, Sivenbring, şi alţii 2022).

Studiile de impact ale acestor iniţiative sunt specifice, ele constând în evaluări de proces, cum ar fi cele efectuate în cadrul proiectului EMMA (Belgia, Ţările de Jos, Germania) care subliniază că

eficacitatea MAW depinde de coordonare neutră, participare echilibrată și întâlniri comune regulate care promovează înțelegerea reciprocă și responsabilitatea (Vandaele, și alții 2022). Cu toate acestea, mai multe provocări împiedică întregul potențial al acestor inițiative, inclusiv barierele legale și instituționale în calea schimbului de informații, implicarea inconsecventă a părților interesate, resursele limitate și lipsa mecanismelor de evaluare pe termen lung.

Interpretări

Această revizuire sistematică a literaturii academice evidențiază limitări critice în modul în care eficacitatea și impactul pe termen lung al strategiilor de prevenire a radicalizării sunt evaluate în literatura academică existentă. În timp ce numeroase inițiative – de la intervenții la nivel individual și comunitar până la formarea practicienilor și cooperarea între mai multe instituții – s-au dovedit a fi promițătoare de principiu, rămâne un decalaj substanțial în dovezile empirice care confirmă impactul lor în contexte reale. În ciuda numărului mare de inițiative, multe nu dispun de cadre de evaluare riguroase. Multe proiecte raportează succese anecdotice, fără a utiliza metode sistematice de măsurare a impactului. De exemplu, din cele 98 de studii analizate, doar aproximativ 20 oferă informații despre implementarea intervențiilor, iar mai puțin de 20 includ evaluarea impactului acestora. Acest fapt indică o lacună semnificativă în baza de dovezi privind aplicabilitatea practică și eficiența măsurilor de prevenire.

Există un apel tot mai puternic pentru studii longitudinale și evaluări de tip mix-method pentru a înțelege cu adevărat ce funcționează pe termen lung. Majoritatea evaluărilor se concentrează pe rezultate pe termen scurt, mai degrabă decât pe schimbarea comportamentală sau atitudinii pe termen lung. În consecință, nu este clar dacă aceste inițiative generează un impact durabil, în special în rândul tinerilor vulnerabili. Barierele structurale – inclusiv constrângerile de finanțare, presiunea pentru rezultate imediate și provocările metodologice inerente studierii unui fenomen complex precum radicalizarea – împiedică și mai mult implementarea evaluărilor pe termen lung. Abordarea acestui lucru necesită investiții în cercetare cu metode mixte, combinând datele cantitative cu perspective calitative aprofundate.

Un al doilea decalaj critic constă în adaptabilitatea culturală a intervențiilor. Multe programe centrate pe persoană nu reușesc să țină cont de diversitatea mediilor culturale în care sunt implementate. Eforturile de prevenire sunt fragmentate, implicând inițiative adesea

izolate, fără coordonare sau transfer de cunoştinţe transfrontalier. Numărul limitat de studii comparative care evaluează modul în care modelele de prevenire funcţionează în diferite contexte culturale slăbeşte generalizarea şi scalabilitatea strategiilor existente. Acest lucru este deosebit de problematic în comunităţile multiculturale sau non-occidentale, unde modelele standardizate pot să nu rezoneze. Astfel, evaluările viitoare trebuie să adopte metodologii participative, care să implice părţile interesate locale şi experţi culturali atât în proiectare, cât şi în implementare.

Literatura de specialitate relevă, de asemenea, un accent subdezvoltat pe eforturile de prevenire digitală, în ciuda rolului bine documentat al spaţiilor online în recrutarea extremistă. Majoritatea intervenţiilor se bazează în continuare pe formatele tradiţionale face-to-face, neglijând mediile digitale în care radicalizarea se desfăşoară frecvent. Cercetările care evaluează eficacitatea tehnologiilor interactive, a conţinutului digital personalizat şi a instrumentelor bazate pe date pentru implicare şi monitorizare rămân rare. Evaluările din acest domeniu ar trebui să exploreze modul în care intervenţiile digitale pot construi reziliența în rândul nativilor digitali, pot contracara naraţiunile extremiste şi completa strategiile offline. O bază de dovezi mai solidă este esenţială pentru integrarea unor astfel de instrumente digitale.

Un alt domeniu subexplorat, dar esenţial, este rolul familiei în prevenire. Deşi familiile pot servi atât ca factori de risc, cât şi ca factori protectivi, literatura de specialitate nu are abordări interdisciplinare care să integreze perspective din psihologie, sociologie, criminologie şi studii familiale. Fără o astfel de integrare, evaluările trec cu vederea complexitatea influenţei familiale asupra radicalizării. Sunt necesare studii-pilot şi cercetări longitudinale care implică programe centrate pe familie pentru a evalua capacitatea acestora de a consolida reziliența şi de a sprijini persoanele expuse riscului.

Evaluarea intervenţiilor centrate pe practicieni suferă în mod similar de ambiguitate conceptuală şi metodologică. Nu există un consens clar asupra modului în care programele de formare pentru profesioniştii din prima linie ar trebui să fie structurate pentru a produce rezultate eficiente. Cercetarea trebuie să investigheze modul în care instruirea bazată pe nevoi, specifică rolului – care încorporează simulări, scenarii de cazuri reale şi metode de învăţare adaptativă – poate îmbunătăţi capacitatea practicianului. Mai mult, înţelegerea experienţelor practice ale profesioniştilor poate informa dezvoltarea unor programe relevante şi eficiente care reflectă provocările cu care se confruntă în medii reale.

În cele din urmă, practica formatelor de cooperare multi-instituțională nu beneficiază de o evaluare riguroasă. Deși colaborarea între instituții este susținută pe scară largă ca o soluție la eforturile fragmentate de prevenire, dovezile empirice privind eficacitatea acesteia rămân limitate. Studiile sugerează că încrederea, rolurile clar definite și comunicarea regulată sunt factori cheie în cooperarea de succes, dar puține evaluări oferă date despre modul în care evoluează aceste dinamici sau contribuie la rezultatele pe termen lung.

În general, literatura academică existentă oferă doar perspective fragmentate asupra eficacității și impactului pe termen lung al strategiilor de prevenire a radicalizării. Deși există intervenții promițătoare, majoritatea nu beneficiază de evaluări riguroase și sistematice. Aceste lacune împiedică capacitatea de a perfecționa și extinde eforturile de prevenire la nivelul statelor europene. Pentru a reduce acest decalaj, cercetările viitoare trebuie să pună accentul pe:

- Evaluări longitudinale și utilizarea de metode mixte;
- Abordări adaptate cultural și participative;
- Crearea și evaluarea intervențiilor digitale;
- Explorarea interdisciplinară a implicării familiei;
- Formarea practicienilor specifică rolului și bazată pe dovezi;
- Evaluarea mecanismelor de consolidare a încrederii în cooperarea multi-instituțională.

Remedierea acestor lacune prin cercetare empirică solidă va oferi fundamentul necesar pentru cadre de prevenire mai eficiente, durabile și aliniate strategic, contribuind în cele din urmă la construirea rezilienței societale la radicalizare și extremism violent.

Bibliografie

1. Aguiar, C., & Silva, C. S. (2018). Case studies on curriculum, pedagogy, and school interventions tackling inequalities. ISOTIS. doi:https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c0548200&appId=PPGMS

2. Aiello, E., Puigvert, L., & Schubert, T. (2018). Preventing violent radicalization of youth through dialogic evidence-based policies. Int. Sociol., 435-453.

3. Alonso, R., & Bada, J. D. (2016). What Role Have Former Eta Terrorists Played in Counterterrorism and Counterradicalization Initiatives in Spain? Stud. Confl. Terror, 982-1006.

4. Aly, A., Taylor, E., & Karnovsky, S. (2014). "Moral Disengagement and Building Resilience to Violent Extremism: An Education Intervention". Studies in Conflict & Terrorism, 369–385.

5. Aly, A., Taylor, E., & Karnovsky, S. (2014). Moral Disengagement and Building Resilience to Violent Extremism: An Education Intervention. Studies in Conflict & Terrorism, 369-385.

6. Amit, S., & Al Kafy, A. (2022). A systematic literature review on preventing violent extremism. Journal of Adolescence, 1-13.

7. Andersson, E. F. (2018). Evaluation of Forsa and the family support centre. AEF Rapport.

8. Atkinson, M., Jones, M., & Lamont, E. (2007). Multi-agency working and its implications for practice: A review of the literature . Berkshire: The National Foundation for Educational Research in England and Wales.

9. Benjamin, S., Koirikivi, P., Salonen, V., Gearon, L., & Kuusisto, A. (2024). Safeguarding social justice and equality: Exploring Finnish youths''Intergroup Mindsets' as a novel approach in the prevention of radicalization and extremism through education. Education, Citizenship and Social Justice, 292–312.

10. Bertelsen, P. (2015). Danish preventive measures and de-radicalization strategies: The Aarhus model. În W. Hofmeister, P. Rueppel, & M. Sarmah, From the desert to world cities - The new terrorism (pg. 241-253). Konrad-Adenauer-Stiftung.

11. Bertelsen, P. (2018). Mentoring in anti-radicalisation. LGT: A systematic assessment, intervention and supervision tool in mentoring. În G. Overlang, A. Andersen, K. Forde, K. Grudum, & J. Salomonsen, Violent extremism in the 21st century : International perspectives (pg. 312-352). Cambridge: Cambridge Scholars Publishing.

12. Bertelsen, P., & Kruglanski, A. (2020). Life psychology and significance quest: a complementary approach to violent extremism and counter-radicalisation. Journal of Policing, Intelligence and Counter Terrorism, 1-22.

13. Bondokji, N., Wilkinson, K., & Aghabi, L. (2017). UNDERSTANDING RADICALISATION: A Literature Review of Models and Drivers. WANA Institute.

14. Bonnell, J., Kerr, D., Passy, R., Copestake, P., Reed, C., Salter, R., . . . Sheikh, S. (2011). Teaching approaches that help to build resilience to extremism among young people. Department of Education, UK.

15. Bowie, R., & Revell, L. (2018). How Christian universities respond to extremism. Education Sciences, 1-14. Preluat de pe https://doi:10.3390/educsci8030140

16. Boyd-MacMillan,, E. (2016). Increasing cognitive complexity and collaboration across communities: Being Muslim being Scottish. Journal of Strategic Security, 79-110. Preluat de pe https://doi.org/10.5038/1944-

17. Brouillette-Alarie, S., Hassan, G., Varela, W., Ousman, S., Kilinc, D., Savard, É. L., . . . Pickup, D. (2022). Systematic Review on the Outcomes of

Primary and Secondary Prevention Programs in the Field of Violent Radicalization. Journal for Deradicalization, 117-168.

18. Busher, J., Choudhury, T., Thomas, P., & Harris, G. (2017). What the Prevent Duty Means for Schools and Colleges in England: An Analysis of Educationalists' Experiences. London, UK: Aziz Foundation.

19. Butt, R., & Tuck, H. (2014). European counter-radicalisation and deradicalisation:A comparative evaluation of approaches in the Netherlands, Sweden, Denmark and Germany. London: Institute for Strategic Dialogue.

20. By a former mentor in Aarhus, Denmark. (2019). Mentoring and deradicalisation. În S. Jayakumar, Terrorism, Radicalisation & Countering Violent Extremism. Practical Considerations & Concerns (pg. 19-28). Palgrave Pivot.

21. Cherney, A. (2018). The release and community supervision of radicalised offenders: Issues and challenges that can influence reintegration. Terrorism and Political Violence, 1-19.

22. Cherney, A., & Hartley, J. (2015). Community engagement to tackle terrorism and violent extremism: challenges, tensions and pitfalls. 750-763: An International Journal of Research and Policy.

23. Christensen, T. W. (2015). A Question of Participation – Disengagement from the Extremist Right, A case study from Sweden. Roskilde University.

24. Christensen, T. W. (2019). Civil actors' role in deradicalisation and disengagement initiatives: When trust is essential. În S. J. Hansen, & S. Lid, Routledge Handbook of Deradicalisation and Disengagement. Routledge.

25. Christensen, T. W. (2023). "I had never reached those Nazi guys without their help" Being a former becoming a mentor - and the value of using formers in exit work. În G. Clubbs, R. Scrivens, & M. Islam, Former extremists: Roles in preventing and countering violence. Oxford University Press.

26. Christensen, T. W. (2023). Mentorship programmes and approaches in P/CVE. Luxembourg: Publications Office of the European Union.

27. Christensen, T. W., Lindekilde, L., Sivenbring, J., Bjorgo, J., Magnaes Gjelsvik, I., Solhjell, R., . . . Kallio, H. (2023). "Being a Risk" or "Being at Risk": Factors shaping negotiation of concerns of radicalization within multiagency collaboration in the Nordic countries. Democracy and Security.

28. Christiaens, E., Hardyns, W., & Pauwels, L. (2018). Evaluating the BOUNCEUp tool: Research findings and policy implications. Federal Public Service Home Affairs. Preluat de pe http://hdl.handle.net/1854/LU-8579585

29. Chun, R. P., Chui, Y. H., Chan, Y., & Cheng, H. C. (2010). Police work with youth-at-risk: What can social work contribute? The Hong Kong Journal of Social Work, 31-48.

30. Clubb, G., Koehler, D., Schewe, J., & O'Connor, R. (2021). Selling Deradicalisationn: Managing the Media Framing of Countering Violent Extremism. London: Routledge.

31. Cowi. (2014). Evaluering af indsatsen for at forebygge ekstre-misme og radikalisering. Ministry of Social Affairs and Integration (former).

32. Cragin, K., Bradley, M. A., Robinson, E., & Steinberg, P. S. (2015). What factors cause youth to reject violent extremism? Results of an exploratory analysis in the West Bank. Santa Monica: RAND Corporation.

33. Cross, M. J., & Benjamin, G. W. (2022). Preventing and Countering Violent Extremism: Best Practices and Standardizations. În A. J. Masys, Handbook of Security Science. Springer Cham.

34. Curnin, S., Owen, C., Paton, D., Trist, C., & Parsons, D. (2015). Role Clarity, Swift Trust and Multi-Agency Coordination. Journal of Contingencies and Crisis Management, 29-35.

35. Danish Agency for International Recruitment. (2016). Slutevaluering af 'Helhedsorienteret forebyggelse af ekstremisme. Oxford Research.

36. Danish Government. (2016). Preventing and Countering Extremism and Radicalization. National Action Plan. Danish Government.

37. Davies, L. (2010). "Educating against Extremism: Towards a Critical Politicisation of Young People". International Review of Education, 183–203.

38. Davies, L. (2014). Interrupting Extremism by Creating Educative Turbulence. Curriculum Inquiry, 44(4), 450-468. Preluat de pe https://www.jstor.org/stable/43941663

39. Davies, L. (2016). Wicked Problems: How Complexity Science Helps Direct Education Responses to Preventing Violent Extremism. Journal of Strategic Security, 9(4), 32-52.

40. DDIS, D. (2023). Intelligence Outlook 2023. DDIS.

41. Dechesne, M. (2011). Deradicalization: not soft, but strategic. Crime, Law and Social.

42. Disley, E., Weed, K., Reding, A., Clutterbuck, L., & Warnes, R. (2012). Individual disengagement from Al Qa'ida-influenced terrorist groups: A rapid evidence assessment to inform policy and practice in preventing terrorism. RAND Europe.

43. Ellefsen, R., & Sandberg, S. (2024). Everyday Prevention of Radicalization: The Impacts of Family, Peer, and Police Intervention. Studies in Conflict & Terrorism, 1342-1365. doi:10.1080/1057610X.2022.2037185

44. Ellis, B., Miller, A. B., Abdi, S., Schouten, R., & Agalab, N. Y. (2020). The Challenge and Promise of a Multidisciplinary Team Response to the Problem of Violent Radicalization. Terrorism and Political Violence, 1-18.

45. Ellis, H., & Abdi, S. (2017). Building Community Resilience to Violent Extremism Through Genuine Partnerships. American Psychologist.

46. El-Said, H. (2015). New approaches to countering terrorism: Designing and evaluating counter radicalization and de-radicalization programs. New York: Springer.

47. ESS, E.-u. (2018). "Handreiking lokaal netwerk van sleutelfiguren". ESS. Preluat de pe https://www.socialestabiliteit.nl/documenten/publicaties/2018/06/18/handreiking-lokaal-netwerk-van-sleutelfiguren

48. European Commission. (2024). Strategic orientations on a coordinated EU approach to prevention of radicalisation for 2024-2025. Preluat

de pe home-affairs.ec.europa.eu: https://home-affairs.ec.europa.eu/document/download/a4bd65f1-4987-4213-851c-df5b2d071d49_en?filename=Strategic%20Orientations%202024-2025_en.pdf&prefLang=bg

49. Extremism, C. f. (2024). stopekstremisme.dk. Preluat de pe https://stopekstremisme.dk/en/prevention/interventions

50. Extremism, D. N. (2018). Knowledge Synthesis. Mapping of knowledge on extremism and prevention of extremism. National Center for Prevention of Extremism. Preluat de pe https://stopekstremisme.dk/filer/videnssyntese-engelsk-version.pdf

51. Feddes, A. R., Mann, L., & Doosje, B. (2015). Increasing self-esteem and empathy to prevent violent radicalization: A longitudinal quantitative evaluation of a resilience training focused on adolescents with a dual identity. Journal of Applied Social Psychology .

52. Flesner, K. K., Larsson, G., & Saljo, R. (2019). Jihadists and Refugees at the Theatre: Global Conflicts in Classroom Practices in Sweden. Educational Sciences, 80.

53. Francis, M., van Eck, A., & van Twist, D. (2015). Religious literacy, radicalization and extremism. În A. Dinham, & M. Francis, Religious literacy in olicy and practice (pg. 113-134). Bristol: Policy Press.

54. Gill, R., & Thompson, M. M. (2017). Trust and Information Sharing in Multinational-Multiagency Teams. În I. Goldenberg, J. Soeters, & W. H. Dean, Information Sharing in Military Operations. Springer International Publishing.

55. Goodking, J. R., Ross-Toledo, K., John, S., Hall, J. L., Ross, L., Freeland, J., . . . Lee, C. (2011). Rebuilding trust: a community, multiagency, state, and universitypartnership to improve behavioral health care for American Indian Youth, theirfamilies, and communities. Journal of Community Psychology, 452-477.

56. Grossman, M., Hadfield, K., Jefferies, P., Gerrard, V., & Ungar, M. (2020). Youth resilience to Violent Extremism: Development and Validation of the BRAVE Measure. Terror. Politi- Violence, 1-21.

57. Hales, A., & Williams, K. (2018). Marginalized individuals and extremism: the role of ostracism in openness to extreme groups: ostracism and extreme groups. Journal of Social Issues, 75-92.

58. Hardyns, W., Klima, N., & Pauwels, L. (2022). Evaluation and mentoring of the multi-agency approach to violent radicalisation. Antwerpen, Apeldoom, Portland: Maklu Publishers.

59. Hardyns, W., Thys, J., Dorme, L., Klima, N., & Pauwels, L. (2020). MULTI-AGENCY WORKING to prevent violent radicalisation. EU EMMA Project. Preluat de pe https://emmascan.eu/media/E-versie_Evaluation_and_mentoring_of_the_multi-agency_approach_-_IDC_4.pdf

60. Harris, A., & Allen, T. (2011). oung people's views of multi-agency working. British Educational Research Journal, 405-419.

61. Haugstvedt, H. (2021). What can families really do? A scoping review of family directed services aimed at preventing violent extremism. Journal of Family Therapy, 408-421.

62. Hemmingsen, A. S. (2015). An Introduction to THE DANISH APPROACH TO COUNTERING AND PREVENTING EXTREMISM AND RADICALIZATION. Copenhagen: Danish Institute for International Studies (DIIS). Preluat de pe file:///C:/Users/user/Downloads/1617692_240904_144431.pdf

63. ICPT, I. (2015). Preventing Radicalization: A systematic review. International Centre for the Prevention of Crime.

64. Impact Europe. (2017). Impact Europe PVE intervention database. Preluat de pe impact.itti.com: http://www.impact.itti.com.pl/index#/inspire/search

65. Joyce, C. (2018). Exploring teachers' beliefs, values and attitudes towards radicalisation, extremism and the implementation of anti-radicalisation strategies. Preluat de pe University of Sheffield: http://etheses.whiterose.ac.uk/id/eprint/21452

66. Jugl, I., Lösel, F., Bender, D., & King, S. (2021). Psychosocial Prevention Programs against Radicalization and Extremism: A Meta-Analysis of Outcome Evaluations. The European Journal of Psychology Applied to Legal Context , 37-46.

67. Kelman, S., Hong, S., & Turbitt, I. (2013). Are there managerial practices associated with the outcomes of an interagency service delivery collaboration? Evidence from British crime and disorder reduction partnerships. Journal of Public Administration Research and Theory, 609-630.

68. Koehler, D. (2016). Understanding deradicalization: methods, tools and programs for countering violent extremism. London: Routledge.

69. Kolbe, A. R. (2019). Do home-based social work services increase the success of programming to prevent violent extremism: Evidence from a small-scale intervention in an urban East African population. Clinical Research in Psychology.

70. Kyriacou, C., Szczepek Reed, B. B., Said, F., & Davies, I. (2017). British Muslim university students' perceptions of Prevent and its impact on their sense of identity. Education, Citizenship and Social Justice, 97–110. Preluat de pe https://doi.org/10.1177/1746197916688918

71. Lahnait, F. (2021, september). Combatting radicalisation in France: from experimentation to professionalisation. Revista CIDOB d'Afers Internacional(128), 105-125.

72. Lakhani, S. (2012). Preventing violent extremism: Perceptions of policy from grassroots and communitie. The Howard Journal of Criminal Justice, 190–206. Preluat de pe https://doi.org/10.1111/j.1468-2311.2011.00685.x

73. Lenz, C., & Kjeoy, I. (2014). Dembra evalueringsrapport 2013-2015.

74. Lenz, C., & Nustad, P. (2014). Fostering democratic preparedness to prevent group focused anmity in Norwegian schools. ANDRAGOŠKI GLASNIK, 9-23.

75. Liht, J., & Savage, S. (2013). Preventing Violent Extremism through Value Complexity: Being Muslim Being British. Journal of Strategic Security, 44-66.

76. Lindekilde, L., & Parker, D. (2020). Preventing Extremism with Extremists: A Double-Edged Sword? An Analysis of the Impact of Using Former Extremists in Danish Schools. Education Sciences, 1-19.

77. Linkedilke, L. (2012). Neo-liberal Governing of "Radicals. International Journal of Conflict and Vio-lence.

78. uter, A., & Glock, B. (2017). Concepts against Islamist radicalization. Evaluation of a workshop initiative of the Kreuzberger Initiative gegen Antisemitismus. Berlin: Camino. Preluat de pe file:///C:/Users/flori/ Downloads/konzepte_gegen_islamistische_radikalisierung_von_kreuzberger_ initiative_gegen_antisemitismus_e.v%20(2).pdf

79. Macnair, L., & Frank, R. (2017). "Voices Against Extremism: A Case Study of a Community-Based CVE Counter-Narrative Campaign". Journal for Deradicalization, 147–174.

80. Macnair, L., & Frank, R. (2017). Voices Against Extremism: A case study of a community-based CVE counter-narrative campaign. Journal for Deradicalization, 147-174.

81. Maraj, A., Mahmut, D., & Ghosh, R. (2021). What role do French society and its education system play in promoting violent radicalization processes? Journal for Daradicalization, 238-283.

82. Marsden, S. V. (2017). Reintegrating extremists: Deradicalisation and desistance. Palgrave Pivot.

83. Martikainen, T. (2019). The ounding of the Islamic council of Finland. În T. Martikainen, J. Mapril, & A. Hussain Khan, Muslims at the margins of Europe. Finland, Greece, Ireland and Portugal (pg. 27-44). Leiden: Brill.

84. Mattsson, C., & Säljö, R. (2018). Violent Extremism, National Security and Prevention. Institutional Discourses and their Implications for Schooling. British Journal of Educational Studies , 109-125.

85. Mazerolle , L., Cherney, A., Eggins, E., Hine, L., & Higginson, A. (2021). Multiagency programs with police as a partner for reducing radicalisation to violence. Campbell Systematic Reviews, 17.

86. Miller, J. (2013). "REsilience, Violent Extremism and Religious Education". British Journal of Religious Education, 188–200.

87. Murphy, D. (2008). Police-probation partnerships: Managing the risks and maximizing benefits. Justice Policy Journal, 1-26.

88. Niemi, P.-M., Benjamin, S., Kuusisto, A., & Gearon, L. (2018). How and Why Education Counters Ideological Extremism in Finland. Religions, 1-16.

89. Oxford Research. (2016). Slutevaluering af helhedsorientered forebyggelse af ekstremisme. Danish Agency for International Recruitment.

90. Papp, S., Örell, R., Meredith, K., Papatheodorou, K., Tadjbakhsh, S., & Brecht, H. (2022). The role of civil society organisations in exit work.

Publications Office of the European Union. Preluat de pe https://home-affairs.ec.europa.eu/whats-new/publications/role-civil-society-organisations-exit-work-may-2022_en

91. Parker, D., Lindekilde, L., & Gøtzsche-Astrup, O. (2020). Recognising and Responding to Radicalisation at the "Front-line": Assessing the Capability of School Teachers to Recognise and Respond to Radicalisation. British Educational Research Journal, 634-653.

92. Petticrew, M., & Roberts, H. (2006). Systematic Reviews in the Social Sciences: A Practical Guide. Wiley-Blackwell.

93. Ponsot, A.-S., Autixier, C., & Madriaza, P. (2018). Factors facilitating the successful implementation of a prevention of violent radicalization intervention as identified by front-line practitioners. Journal for Deradicalization, 1-33. Preluat de pe https://www.researchgate.net/publication/328146506_FACTORS_FACILITATING_THE_SUCCESSFUL_IMPLEMENTATION_OF_A_PREVENTION_OF_VIOLENT_RADICALIZATION_INTERVENTION_AS_IDENTIFIED_BY_FRONT-LINE_PRACTITIONERS

94. Pratchett , L., Thorp, L., Wingfield, M., Lowndes, V., & Jabbar, R. (2010). Preventing Support for Violent Extremism through Community Interventions: A Review of the Evidence. Communities and Local Publications.

95. RAN, R. (2019). Preventing Radicalisation to Terrorism and Violent Extremism. Approaches and Practices. RAN.

96. Roex, I., & Vermeulen, F. (2019). Preemptive measures against radicalization and local partnerships in Antwerp. În N. Fadil, F. Ragazzi, & M. de Koning, Radicalization in Belgium and The Netherlands: critical perspectives on violence and security (pg. 131-146). London: I.B. TAURIS.

97. Ruyter, D. d., & Sieckelinck, S. (2023). Creating caring and just democratic schools to prevent violent extremism. Educational Theory, 73, 413-433. Preluat pe 2024, de pe file:///C:/Users/Admin/Desktop/IC%20doc/Articole%20analiza%20de%20specialitate/Articole%20educatie/Educational%20Theory%20-%202023%20-%20Ruyter%20-%20Creating%20Caring%20and%20Just%20Democratic%20Schools%20to%20Prevent%20Extremism.pdf

98. Sas, M., Ponnet, K., Reniers, G., & Hardyns, W. (2020). The Role of Education in the Prevention of Radicalization and Violent Extremism in Developing Countries. Sustainability, 1-12.

99. Schuurman, B., & Bakker, E. (2015). Reintegrating jihadist extremists: evaluating a Dutch initiative 2013-2014. Behavioral Sciences of Terrorism and Political Aggression.

100. Sesoft, D., Hansen, S. M., & Christensen, A. B. (2017). The police, social services, and psychiatry (PSP) cooperation as a platform for dealing with concerns of radicalization. International Review of Psychiatry, 350-354.

101. Sieckelinck, S., Sikkens, E., van San, M., Kotnis, S., & Winter, M. (2019). Transitional journeys into and out of extremism. A biographical approach. Studies in Conflict & Terrorism, 662-682.

102. Sikkens, E., van San, M., Sieckelinck, S., & de Winter, M. (2017). Parental influence on radicalization and deradicalization according to the lived experiences of former extremists and their families. Journal for Deradicalization, 12-35.

103. Sivenbring, J., & Andersson Malmros, R. (2021). Collaboration in Hybrid Spaces: The Case of Nordic Efforts to Counter Violent Extremism. Journal for Deradicalization, 54-91.

104. Solhjell, R., Sivenbring, J., Kangasniemi, M., Kallio, H., Christensen, W. T., Haugstved, H., & Gjelsvik, M. I. (2022). Experiencing trust in multiagency collaboration to prevent violent extremism: A Nordic qualitative study. Journal for Deradicalization, 164-191.

105. Stephens, W., Sieckelinck, S., & Boutellier, H. (2021). Preventing Violent Extremism: A Review of the Literature. Studies in Conflict & Terrorism, 346-361.

106. Stephens, W., Sieckelinck, S., & Boutellier, H. (2021). Preventing Violent Extremism: A Review of the Literature. Studies in Conflict and Terrorism, 346-361.

107. Subedi, D. (2017). "Early Warning and Response for Preventing Radicalization and Violent Extremism". Peace Review.

108. Taylor, L., & Soni, A. (2017). "Preventing Radicalisation: A Systematic Review of Literature Considering the Lived Experiences of the UK's Prevent Strategy in Educational Settings". Pastoral Care in Education, 241–252.

109. Thomas, P. (2016). Youth, terrorism and education: Britain's Prevent programme. International Journal of Lifelong Education.

110. Tierney, M. (2017). Using behavioral analysis to prevent violent extremism: Assessing the cases of Michael Zehaf-Bibeau and Aaron Driver. Journal of Threat As-sessment and Man-agement.

111. Tiilikainen, M., & Mankkinen, T. (2020). Prevention of Violent Radicalization and Extremism in Finland: The Role of Religious Literacy. În T. Sakaranaho, T. Aarrevaara, & J. Konttori, The Challenge of Religious Literacy. The Case of Finland (pg. 67-78). Springer.

112. van de Donk, M., Uhlmann, M., & Keijzer, F. (2020). Peer and self review manual for exit work. RAN Centre of Excellence.

113. van der Vet, I. (2020). The role of teachers in prevention of violent extremism and radicalisation in schools: the Belgian experience. Institute for European Studies.

114. Vandaele, B., Dorme, L., Pauwels, N., & Hardyns, W. (2022). Observing Multi-Agency Working: Participatory Observations in Belgian, Dutch and German Cities. În W. Hardyns, N. Klima, & L. Pauwels, Evaluation and mentoring of the multi-agency approach to violent radicalisation (pg. 51-67). Antwerpen | Apeldoorn | Portland: Maklu Publishers.

115. Vermeulen, F. (2014). Suspect Communities – Targeting Violent Extremism at the Local Level: Policies of Engagement in Amsterdam, Berlin, and London. Terrorism and political violence, 286-306.

116. Vermeulen, F., & Bovenkerk, F. (2012). However, community engagement comes with specific policy: local policies in western European cities. The Hague: Eleven International Publishers.

117. Visser, K., & Vermeulen, F. (2021). Preventing violent extremism in the Netherlands: overview of its broad approach. Revista CIDOB d'Afers Internacionals , 131-151.

118. Walkenhorst, D., Baaken, T., Ruf, M., Leaman, M., Handle, J., & Korn, J. (2020). Rehabilitation Manual –Rehabilitation of radicalised and terrorist offenders for first-line practitioners. RAN. Preluat de pe https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/publications/rehabilitation-manual-rehabilitation-radicalised-and-terrorist-offenders-first-line-practitioners_en2

119. Walsh, M., & Gansewig, A. (2019). A former right-wing extremist in school-based prevention work: Research findings from Germany. Journal for Deradicalization, 1-42.

120. Walsh, M., & Gansewig, A. (2021). Long-Term Experience Means Professionalization - Or Does It? An indepth look on the Involvement of Former Extremists in German Prevention and Education. Journal for Deradicalization, 108-145.

121. Williams, M. J., Horgan, J. G., & Evans, W. P. (2016). The critical role of friends in networks for countering violent extremism: toward a theory of vicarious help-seeking. Behavioral Sciences of Terrorism and Political Aggression .

122. Winterbotham, E. (2020). How Effective Are Mentorship Interventions? Assessing the Evidence Base for Preventing and Countering Violent Extremism. London: Royal United Services Institute (RUSI). Preluat de pe file:///C:/Users/flori/Downloads/pcve_mentorship_final_web_version_241202_044753.pdf

123. Yayla, A. S. (2020). Preventing terrorist recruitment through early intervention by involving families. Journal of Deradicalization.

124. Younis, T., & Jadhav, S. (2019). Keeping our mouths shut: The fear and racialized selfcensorship of British healthcare professionals in PREVENT training. Culture, Medicine and Psychiatry, 404-424. Preluat de pe https://doi.org/10.1007/s11013-019-09629-6

Aceasta este al patrulea volum de proceedings al Conferinței Științifice Intelligence și Cultura de Securitate (ICS), care cuprinde lucrările prezentate în cadrul ediției din 2025 - ICS 2025, publicat de Academia Națională de Informații „Mihai Viteazul" (ANIMV). ICS continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Intelligence și Securitate a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.

EDITURA ANIMV

ISSN 2972-1350
ISSN-L 2971-8139