Anul XVI nr. 3/2024

INFOSFERA

Revistă de studii de securitate şi informaţii pentru apărare

Publicaţie indexată în bazele de date internaţionale EBSCO şi CEEOL

Revistă cu prestigiu ştiinţific recunoscut de Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (CNATDCU)

Direcţia Generală de Informaţii a Apărării

CUPRINS

ANIVERSAREA A 165 DE ANI DE LA ÎNFIINȚAREA PRIMEI STRUCTURI DE INFORMAȚII MILITARE DIN ARMATA ROMÂNIEI

PERSPECTIVE ASUPRA ACTIVITĂȚII DE INFORMAȚII MILITARE

MESAJUL MINISTRULUI APĂRĂRII NAŢIONALE, DOMNUL ANGEL TÎLVĂR

Direcția Informații Militare sărbătorește 165 de ani de existență, acest eveniment notabil oferindu-mi prilejul onorant de a adresa mesajul meu de recunoștință și de apreciere uneia dintre structurile de elită ale Ministerului Apărării Naționale.

Istoria Direcției Informații Militare începe cu momentul crucial de la data de 12 noiembrie 1859 - înființarea Corpului de Stat Major General al Armatei Principatelor Unite de către domnitorul Alexandru Ioan Cuza. La acea dată, constituirea primei structuri de informații militare a reprezentat un punct de referință în ceea ce urma să însemne organizarea și dezvoltarea armatei naționale în perioada consolidării statului român.

Ulterior, prin rolul pe care l-a jucat de-a lungul istoriei țării noastre, prin devotamentul, profesionalismul și jertfa cu care a slujit sub Drapelul de luptă, în momentele critice de pe scena regională sau globală, care au construit treptat însăși identitatea statului român, începând cu Războiul de Independență și continuând cu cele două Războaie Mondiale, structura de informații a armatei s-a impus ca un element esențial în apărarea și promovarea intereselor naționale.

Trecerea anilor a pus structurile de informații militare în fața unor nenumărate încercări, dinamica continuă a mediului de securitate fiind principalul factor de transformare și adaptare pentru a face față provocărilor nou-apărute, identificării trendurilor de evoluție, anticipării crizelor și evaluării riscurilor și amenințărilor la adresa securității naționale.

În prezent, România este un stat membru robust și respectat în cadrul NATO și al UE, precum și un partener strategic de încredere al SUA, iar aceasta se datorează și personalului Direcției Informații Militare, care, cu devotament și profesionalism, continuă să participe la misiuni în teatrele de operații din Balcani, Orientul Mijlociu, Asia sau Africa și în comandamente multinaționale sau internaționale. Expertiza Direcției Informații Militare este unanim apreciată la nivelul Alianței, un exemplu în acest sens fiind și decizia de înființare, în România, a Centrului de Excelență NATO în domeniul HUMINT.

De-a lungul timpului, România și-a dovedit statutul de important furnizor de securitate la nivel regional și euroatlantic, precum și de parte componentă activă și fundamentală a mecanismelor de instaurare și menținere a unui climat de securitate global, acordând o importanță deosebită respectării angajamentelor internaționale asumate.

Rolul fundamental pe care îl joacă diplomația militară, în special pentru prevenirea surprinderii strategice, a devenit tot mai relevant în contextul politic și militar internațional actual, extrem de complex și tensionat, marcat de tendința de multiplicare a spectrelor conflictuale, de scăderea coeziunii în formatele multilaterale tradiționale de cooperare și asigurare a securității, precum și de revenirea în prim-plan a instrumentului militar ca modalitate de reglare a relațiilor internaționale.

În prezent, pe lângă rolul vital pe care îl au în consolidarea dialogului strategic în planul apărării cu statele partenere NATO și UE, atașaților apărării le revine dificila sarcină de a identifica, încă din faze incipiente, semnalele reconfigurării și reașezării relațiilor dintre actorii statali sau non-statali, precum și indiciile transformărilor de natură militară, politică și de securitate care pot afecta interesele naționale ale țării noastre.

Cu ocazia acestui moment aniversar, adresez mulțumiri corpului atașaților apărării ai Direcției Informații Militare pentru implicarea în promovarea intereselor naționale de securitate și a imaginii Armatei Române pe scena internațională, pentru faptul că asigură nivelul optim de cooperare pe linie militară și pentru întreaga activitate specifică desfășurată în țările de acreditare.

Direcția Informații Militare și-a confirmat statutul de structură de elită, modernă și rezilientă, adaptându-se rapid la evoluțiile tehnologice care au determinat atât creșterea complexității amenințărilor la adresa securității, în special al celor de tip hibrid, cât și perfecționarea modalităților de răspuns la acestea, prin dezvoltarea capabilităților de culegere, prelucrare și analiză a informațiilor din toate spectrele și domeniile.

La ceas aniversar, doresc să adresez calde urări de sănătate și mulțumiri tuturor celor care au făcut alegerea de a servi Patria în cadrul Direcției Informații Militare și să-mi exprim aprecierea și recunoștința pentru întreaga dumneavoastră activitate.

Vă felicit pentru profesionalismul și devotamentul cu care acționați, pentru implicare, dedicare, loialitate și spirit de sacrificiu și vă urez mult succes în îndeplinirea, pe mai departe, a misiunilor încredințate.

LA MULȚI ANI, DIRECȚIA INFORMAȚII MILITARE!

MESAJUL ȘEFULUI STATULUI MAJOR AL APĂRĂRII, GENERAL GHEORGHIȚĂ VLAD

Direcția Informații Militare, la fel ca Statul Major al Apărării, atinge, în data de 12 noiembrie, o bornă importantă a identității sale structurale: împlinirea a 165 de ani de existență subsumată datoriei apărării naționale. În tot acest timp, Direcția Informații Militare a sprijinit Statul Major al Apărării. În prezent, mai mult decât oricând, suntem înscriși în realizarea dezideratului de întărire a capacității defensive și a statutului țării noastre de pilon de stabilitate în planul securității regionale.

Caracterizată de discreție, activitatea Direcției Informații Militare îmbină numeroase valențe profesionale, cu aport decisiv în planificarea, organizarea și desfășurarea operațiilor Armatei României. Corpul de intelligence militar este deopotrivă expresie a adaptării doctrinare și structurale permanente, furnizor de informații și expertiză, facilitator al cooperării cu statele aliate și partenere, respectiv autoritate națională pe numeroase și sensibile paliere de specialitate. Într-o sinopsă: Direcția Informații Militare constituie, astăzi, un pilon esențial al apărării patriei.

Dragi colegi militari și civili care reprezentați această structură esențială a Armatei României, cei 165 de istorie pe care îi sărbătoriți coincid cu itinerarul unei evoluții structurale de excepție, de perfecționare și dezvoltare neîntreruptă. A fost o perioadă în care predecesorii dumneavoastră, adeseori cu sacrificii în plan personal, au construit o marcă a Armatei. Dumneavoastră înșivă, prin munca de zi cu zi, faceți ca acest destin al performanței profesionale să se împlinească și în prezent. Ați câștigat aprecierea colegilor din întreaga instituție a apărării naționale, precum și considerația reprezentanților militari străini.

Prezentul se încăpățânează să ne ofere provocări din ce în ce mai complexe, completând transformările majore înregistrate de mediul global de securitate din ultimii ani. Realitatea în care acționăm este definită de un spectru tot mai larg de amenințări convenționale și neconvenționale, de diversificarea tipologiei crizelor, de riscul încălzirii conflictelor înghețate și, mai ales, de războaiele de uzură de la granița noastră și din Orientul Apropiat.

Anticiparea evoluțiilor viitoare, respectiv realizarea și integrarea de noi tehnologii au devenit necesități primordiale, care impun reacții multidirecționale și, nu în ultimul rând, personal cu flexibilitate în gândire și concepții, cu deosebire în domeniul dumneavoastră de activitate.

Stimați colegi din Direcția Informații Militare, munca dumneavoastră reprezintă unul dintre factorii cheie ai succesului misiunilor încredințate Armatei României. Vă asigur de aprecierea mea, precum și a întregii echipe de comandă a Statului Major al Apărării. Profit de acest prilej pentru a transmite un gând de recunoștință tuturor celor care au făcut parte și au contribuit, de-a lungul timpului, la formarea structurii mature, robuste și de prestigiu pe care o reprezintă Direcția Informații Militare.

Am convingerea că veți continua să vă onorați misiunile strategice și că veți menține aceleași standarde de exigență în activitatea dumneavoastră. De altfel, consider că sunt în asentimentul colegilor din întreaga structură de forțe care, la marcarea a 165 de ani de existență, doresc să vă transmită sănătate, putere de muncă și împliniri personale. Vă mulțumim pentru sprijinul pe care ni-l acordați și vreau să fiți pe deplin conștienți și mândri de faptul că fiecare acțiune și decizie militară se bazează pe contribuția dumneavoastră.

LA MULȚI ANI, DRAGI CAMARAZI!
LA MULȚI ANI, DIRECȚIA INFORMAȚII MILITARE!

MESAJUL DIRECTORULUI GENERAL AL DIRECȚIEI GENERALE DE INFORMAȚII A APĂRĂRII, GENERAL-LOCOTENENT PETRU BĂICEANU

Cu prilejul sărbătoririi a 165 de ani de la înființarea Direcției Informații Militare, structură născută odată cu România modernă, prin Înaltul Ordin de Zi nr. 83 emis pe 12 noiembrie 1859 de domnitorul Alexandru Ioan Cuza, care înființa Secția a II-a din cadrul Statului Major al Armatei Principatelor Unite, întâia instituție de informații pusă în slujba nevoilor de securitate și apărare națională, vă adresez cele mai calde și sincere felicitări.

Perioada 1859-2024 reprezintă un interval de referință, marcat de realizări excepționale individuale, dar și de contribuții colective și instituționale, care au clădit încet, dar pe baze deosebit de solide, instituția pe care o reprezentați. În tot acest timp, informațiile militare au urmărit cu conștiinciozitate îndeplinirea misiunilor lor esențiale: „cunoașterea armatelor străine, identificarea și analiza pericolelor care pot afecta independența, suveranitatea, unitatea și integritatea României, precum și prevenirea oricăror agresiuni”.

Transformarea Armatei României după momentul 1989 și, mai ales, odată cu aderarea României la Alianța Nord-Atlantică a impus reconfigurarea și adaptarea structurilor de informații militare la evoluția mediului internațional pentru a răspunde cerințelor de securitate și provocărilor pe care le înfruntăm în activitatea curentă. Astfel, au fost dezvoltate capabilități moderne de HUMINT, SIGINT, GEOINT și alte structuri de culegere de informații, care contribuie la îndeplinirea cu succes și eficiență a misiunilor Direcției.

Mai mult, de-a lungul anilor, Direcția Informații Militare s-a evidențiat prin profesionalism și dedicare, personalul instituției stabilind standarde înalte de excelență în ceea ce privește îndeplinirea misiunilor specifice informațiilor militare. Așadar, acesta este un moment de recunoaștere a eforturilor susținute care au condus la rezultate profesionale deosebit, obținute în cadrul unei organizații profund devotate misiunii sale și jurământului militar.

Pe de altă parte, este o datorie de onoare să amintesc faptul că toate aceste realizări profesionale s-au făcut mereu cu sacrificii și constrângeri, rămase adesea în umbră, din cauza specificului activității de Intelligence.

Aniversarea aceasta constituie nu doar o celebrare a unui trecut glorios și plin de realizări, dar și un prilej de reflecție, atât către un prezent marcat de impredictibilitate și provocări complexe, cât și către un viitor care poate aduce noi oportunități de evoluție pentru această structură de elită, indispensabilă în arhitectura de securitate a României.

În același timp, trebuie să rămânem conștienți că trăim într-o lume caracterizată de un grad accentuat de instabilitate și marcată de numeroase amenințări pe care trebuie să le combatem. Pornind de la valorile care ne-au ghidat până în prezent, vom continua să ne pregătim în mod consecvent pentru a menține atât un nivel ridicat de cunoaștere și înțelegere a realităților actuale, cât și o capacitate crescută de adaptabilitate față de provocările care ne vor testa vigilența, puterea individuală și reziliența instituțională.

Din această perspectivă, aș dori să îmi exprim aprecierea pentru înalta expertiză și nivelul ridicat de competență cu care personalul Direcției Informații Militare reprezintă instituția în structuri diplomatice şi militare din străinătate, în teatrele de operaţii, în relaţiile cu omologi din alte instituții din cadrul Comunității Naționale de Informații, dar şi în relaţiile cu partenerii externi.

Închei prin a adresa, cu această ocazie deosebită, în numele meu și al întregii conduceri a Direcţiei Generale de Informaţii a Apărării, cele mai sincere urări de sănătate şi succes întregului personal al Direcției Informații Militare.

LA MULŢI ANI!

MESAJUL ȘEFULUI DIRECȚIEI INFORMAȚII MILITARE, GENERAL-MAIOR ING. CIPRIAN-CONSTANTIN NAN

În cei 165 de ani de existență, pe care sunt onorat să-i aniversăm împreună, Direcția Informații Militare a parcurs, în mod conștient, procese ample de maturizare profesională și instituțională. Acestea s-au impus ca necesare în contextul consolidării statului român, al transformărilor istorice în plan internațional, al evoluțiilor interne și de la nivelul Forțelor Armate.

Sărbătorim, astfel, la 12 Noiembrie, o tradiție solidă a serviciului dedicat țării și a valorilor perene ce-l susțin, dar și instituția modernă și adaptată a informațiilor militare din prezent. Direcția Informații Militare este, astăzi, o structură solidă în arhitectura de intelligence națională, capabilă să răspundă competent și responsabil nevoilor de informare ale decidentului și să asigure plusul informativ care oferă avantaj strategic. Dinamica riscurilor și amenințărilor din plan internațional și creșterea presiunii de securitate în regiune impun, la fel ca de atâtea ori în istoria noastră instituțională, flexibilitate permanentă, o postură asertivă în culegerea informațiilor, luciditate și profesionalism în analiză, promptitudine și viteză de reacție pentru informarea oportună a beneficiarilor noștri, responsabilitate și consistență în îndeplinirea angajamentelor de cooperare internațională asumate. Menținerea acestor standarde de activitate presupune un efort permanent, colectiv, de sistem.

Excelența profesională a personalului Direcției Informații Militare reprezintă, în acest sens, elementul cheie. În plus, dezvoltarea permanentă a capabilităților de culegere prin mijloace tehnice asigură susținerea și instrumentele necesare pentru a ne menține competitivi și actuali într-un mediu informațional și al tehnologiei asociate aflat în transformare permanentă. Acoperirea consistentă a sistemului atașaturii apărării, cu reprezentare asigurată în peste șaptezeci de state, și prezența susținută a ofițerilor de informații militare în teatrele de operații și în numeroase comandamente multinaționale susțin misiunea de cunoaștere aprofundată și de anticipare a evoluțiilor de interes din sfera de securitate și apărare. Relațiile fundamentate de atașații apărării și de către toți reprezentanții Direcției, în formate aliate și multilaterale, aduc valoare adăugată efortului

informativ și promovează interesele de securitate ale României pe plan extern. Toate aceste paliere, funcționând unitar, garantează performanța informațiilor militare românești, informarea corectă și la timp a beneficiarilor, avertizarea timpurie și susținerea actului de decizie.

Marcarea acestui moment aniversar major nu ar fi completă fără celebrarea oamenilor care au construit, de-a lungul timpului, Direcția Informații Militare, din 1859 și până în prezent. Începând cu personalul responsabil de recrutare și pregătire, cel din zonele operative și ale analizei complexe de intelligence, sfera de sprijin, echipele de conducere, cu toții respectăm aceleași principii testate de timp – loialitate față de țară și instituție, onoare, adevăr, competență, profesionalism, disciplină, spirit al datoriei, discreție. Ne bucurăm, ca serviciu de informații, de o vastă istorie, de modele autentice de profesioniști și de repere în îndeplinirea misiunii. Avem trecutul punctat, de asemenea, de sacrificii și de eroi, pe care îi păstrăm în memorie și cărora le suntem recunoscători. Toate acestea ne inspiră și ne obligă la continuitate în performanță, iar personalul Direcției Informații Militare - mentori și generație tânără - este conștient de nevoia de pregătire permanentă, de cunoaștere în profunzime a evenimentelor de securitate, precum și de adaptare la noi și variate cerințe. Conștientizarea faptului că informațiile pot soluționa crize și câștiga războaie ne motivează pe toți, în fiecare zi.

Cu aceste gânduri, salut întreg personalul Direcției Informații Militare, precum și pe predecesorii noștri, cadre militare în rezervă sau în retragere și personal civil. Îmi exprim aprecierea pentru serviciul față de România, pentru profesionalismul de excepție și pentru lucrul neobosit, în umbra secretului, pentru îndeplinirea misiunilor.

Vă urez succes în activitate și împlinire!

LA MULȚI ANI!


DIRECȚIA INFORMAȚII MILITARE
1859 - 2024

INTELLIGENCE ÎN COMUNICAREA STRATEGICĂ

Daniel COCOLICI*

Abstract

The controlled disclosure of intelligence in order to achieve strategic effects of public diplomacy is not a novelty. In recent years, however, Western states have strategically shared rapidly-declassified information with the public, in the run-up to an invasion, while benefiting from the unplanned support of an emerging open-source public intelligence community. Thus, Western officials' claims were validated by non-state entities that published their own public intelligence, allowing the Western world to regain initiative in the informational domain. While in this case the rapidly-developing open-source intelligence community proved beneficial for both the governments and the public, a protracted success in strategic communication might still prove challenging in future crises, given the democratization of intelligence.

Keywords: *intelligence; strategic communication; intelligence community; public diplomacy; open-source intelligence community; democratization of intelligence.*

INTRODUCERE

Înaintea invaziei neprovocate a Federației Ruse în Ucraina, SUA și Marea Britanie au desfășurat o campanie preventivă de comunicare strategică, urmărind simultan două obiective: convingerea statelor aliate cu privire la iminența invaziei ruse (inclusiv pentru crearea condițiilor pentru mobilizarea sprijinului pentru Ucraina) și descurajarea Kremlinului/ respectiv împiedicarea invaziei.

Utilizarea evidentă de informații sensibile, declasificate în timp record, a fost un element central în această campanie. Occidentul a recâștigat inițiativa în războiul informațional, inițiativă care, potrivit unor autori precum Joshua Huminski, fusese cedată anterior, în mare parte, Federației Ruse[1]. Succesul acestui efort determină în mod inerent o creștere a așteptărilor, atât din partea factorilor decizionali, cât și din partea publicului larg. Sunt, de asemenea, readuse în atenție provocări mai vechi care afectează/ influențează utilizarea *intelligence*[2] în diplomația publică. Cursul războiului din Ucraina (dar și alte crize în desfășurare) evidențiază, astăzi, lecții învățate din succese și eșecuri anterioare, oferind și avertizări pentru viitor.

UTILIZAREA INTELLIGENCE ÎN DIPLOMAȚIA PUBLICĂ ...

Utilizarea *intelligence* în sprijinul eforturilor politice și diplomatice ale statelor pentru obținerea de efecte strategice nu este un element de noutate. Astfel, produse de *intelligence* sunt utilizate în mod curent în diplomația publică, *„în activitatea*

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

conducerii politice, în declarații publice, în întâlniri diplomatice și în materiale transmise către mass-media"[3]. În plus, statele folosesc *intelligence* în fiecare fază a conflictelor politice și militare pentru descurajarea adversarilor, convingerea aliaților sau comunicarea cu publicul larg. Chiar și folosirea unor informații sensibile (obținute prin mijloace specifice) în sprijinul politicii nu este un element nou.

Pe timpul crizei rachetelor din Cuba (1962), SUA au declasificat imagini obținute cu aeronave de cercetare U-2, care au fost folosite pe timpul discursului lui Adlai Stevenson, ambasadorul SUA la ONU[4]. De asemenea, în perioada Războiului Rece au existat numeroase situații în care informații clasificate au fost diseminate selectiv de guverne către instituții mass-media prietene, institute de analiză, grupuri activiste, în scopul obținerii unui avantaj în plan informațional[5]. De noutate au fost însă, în ultimii ani, viteza și frecvența cu care informații sensibile și de valoare au fost declasificate și diseminate către publicul larg înaintea unei invazii, cu scop de descurajare a agresorului și de raliere a sprijinului aliaților. Acestea au demonstrat faptul că serviciile de informații occidentale au avut acces la informații vehiculate la nivelul elitelor politice și militare ruse, iar declasificarea informațiilor a fost realizată cu intenția clară de obținere a unor efecte strategice.

... PRESUPUNE ASUMAREA UNOR RISCURI ȘI VA GENERA TENSIUNI ...

Probabil cea mai importantă problemă asociată utilizării de *intelligence* în discursul public constă în tensiunea generată de necesitatea protejării surselor și metodelor, precum și a utilității informațiilor obținute. Necesitatea protejării surselor umane sau metodelor specifice de culegere a informațiilor (ex.: din mediul cibernetic, prin exploatarea unei vulnerabilități unice) și nevoia de informare a decidenților politici (care apoi modelează mediul politic și diplomatic) sunt preocupări continue ale structurilor de informații. O atenție deosebită este acordată atunci când *intelligence* este diseminat în spațiul public, existând riscul ca adversarul să deducă tipul de capabilități folosite și/ sau să își identifice propriile vulnerabilități, ceea ce poate conduce la pierderea oportunității de exploatare.

Astfel de îngrijorări vor exista mereu, iar protecția surselor și capabilităților va rămâne un principiu de bază al activității structurilor de informații. Există însă riscul ca protejarea excesivă a acestora să conducă la restrângerea utilității informațiilor obținute. Astfel, *„prea multă protecție reduce utilitatea, prea multă utilizare riscă expunerea și pierderea sursei"*[6], iar aceste extreme pot fi evitate doar prin utilizarea judicioasă și diseminarea selectivă a informațiilor.

Informațiile declasificate și publicate de administrația americană, pe parcursul ultimelor luni ale anului 2021 și la începutul anului 2022, cu privire la capabilitățile și intențiile Federației Ruse au fost impresionante din punct de vedere al specificității acestora:

- „*Federația Rusă planifică o operație ofensivă împotriva Ucrainei la începutul anului 2022, contingentul de forțe implicat urmând să fie dublu față de ce a fost observat în primăvara anului 2021 pe timpul exercițiului de alertare din proximitatea frontierei cu Ucraina. Planurile includ dislocarea a 100 grupuri tactice de nivel batalion (BTG), cu un total de aprox. 175.000 de militari și tehnică de luptă blindată și de artilerie*"[7].
- „*Comunicații interceptate obținute de SUA arată că unii dintre oficialii ruși sunt îngrijorați cu privire la faptul că o invazie la scară largă în Ucraina va fi mai costisitoare și mai dificilă decât realizează Vladimir Putin și alți lideri de la Kremlin, potrivit declarațiilor a patru persoane familiare cu intelligence pe acest subiect*"[8].
- „*SUA au obținut intelligence privind un plan al Federației Ruse de a fabrica un pretext pentru o invazie în Ucraina folosind un fake video care va fi folosit ca parte a campaniilor de dezinformare*"[9].
- „*Comunitatea americană de intelligence a penetrat mai multe cercuri ale conducerii*

politice ruse, serviciilor de informații și forțelor armate, de la nivel decizional la nivel de execuție, potrivit unor oficiali americani"[10].

Aceste informații ar fi putut fi obținute doar de la persoane din cercuri ale elitei ruse sau prin interceptarea și exploatarea rețelelor de comunicații ale Federației Ruse. Diseminarea lor (chiar și sanitizarea/ aducerea acestora la un nivel minim de clasificare) are potențialul de a deconspira agentul din teren, respectiv de a anula vulnerabilitatea exploatată. Foarte probabil, autoritățile de la Moscova porneau de la presupunerea că există structuri de informații străine care depun eforturi – care au sau nu succes – de supraveghere a Federației Ruse. În urma declarațiilor administrației americane, Moscova a demarat, cel mai probabil, un efort contrainformativ susținut de identificare a sursei informațiilor folosite de SUA.

Este posibil (însă improbabil) ca statele occidentale să fi intenționat doar crearea impresiei că dețineau informații despre procesul de luare a deciziei din Federația Rusă în scopul generării de confuzii la nivelul autorităților de la Moscova, fără să dețină în realitate astfel de informații. În timp ce fabricarea de *intelligence* este posibilă, acest lucru ar fi fost expus probabil de către Federația Rusă sau de către alte state, ceea ce ar fi condus la erodarea credibilității comunității guvernamentale occidentale de *intelligence*, într-o perioadă în care această credibilitate era vitală între aliați. În acest caz, iminența amenințării și nevoia de mobilizare a sprijinului aliat au fost considerate ca fiind mai importante decât îngrijorările privind sursele și metodele.

Cu toate acestea, SUA au declasificat și diseminat către publicul larg *intelligence* privind intențiile Federației Ruse, însă nu au fost publicate și rapoarte primare după interceptări[11]. Această abordare - relativ prudentă - a permis însă menținerea unui anumit grad de scepticism la nivelul conducerii politice a unor state privind calitatea, veridicitatea și posibila politizare a comunității de informații americane. În cazuri precum cel al Franței și Germaniei, acest scepticism inițial poate fi explicat și printr-o percepție mai redusă a amenințării ruse[12]. Utilizarea *intelligence* în comunicarea strategică, de către Administrația Biden, înaintea invaziei ruse în Ucraina a fost un exemplu de acțiune profesionistă și calculată în scopul obținerii efectelor dorite.

Tensiunile dintre comunitatea de informații și oficialii politici sunt însă inerente în diferite etape ale unor crize, iar diferențele de abordare sunt uneori semnificative. Un astfel de exemplu este publicarea de către conducerea politică israeliană, la data de 06 iunie 1967 (în cea de-a doua zi a Războiului de Șase Zile), a unei convorbiri între președintele egiptean de la momentul respectiv, Gamal Abdel Nasser, și regele Hussein al Iordaniei, interceptată de către structurile de informații militare israeliene. În cadrul acestei convorbiri, președintele egiptean se oferea să declare că SUA și Marea Britanie au participat la executarea atacului asupra unor baze aeriene egiptene. În ziua următoare, mass-media arabe au început să publice acest narativ, ceea ce a condus la influențarea opiniei publice în lumea arabă și la presiuni politice asupra SUA. Conducerea politică israeliană a decis să publice convorbirea interceptată, anticipând că Egiptul ar putea încerca să atragă URSS în război pe baza tratatelor bilaterale în domeniul apărării semnate de cele două state (URSS se angajase să sprijine Egiptul în cazul în care SUA sprijinea Israelul). Interceptarea a fost, așadar, publicată potrivit deciziei conducerii politice, în pofida faptului că directorul structurii de informații militare israeliene de la momentul respectiv, Aharon Yariv, s-a opus[13].

Cea mai bună modalitate de a alege între necesitatea politică și riscurile asociate la adresa metodelor utilizate pentru obținerea informațiilor este identificarea unei soluții în urma unor consultări între conducerea politică și comunitatea de informații privind natura metodelor utilizate, conținutul materialelor, efectele obținute prin expunerea acestora și consecințele asupra forțelor proprii. Eșalonul politic are însă dreptul de a utiliza informațiile, chiar dacă reprezentanții comunități de informații se opun. De exemplu, prim-ministrul israelian, Benjamin Netanyahu,

a reiterat această abordare, declarând că Israelul este *„un stat care are intelligence, nu intelligence care are un stat”*[14].

... DAR POATE SCHIMBA CURSUL ISTORIEI ...

Înaintea invaziei ruse în Ucraina, prin declasificarea unor informații, SUA au semnalat Federației Ruse faptul că planurile și intențiile Moscovei sunt cunoscute de autoritățile de la Washington. După prezentarea acestora, Administrația Biden a comunicat și consecințele probabile în situația în care Moscova decide să acționeze potrivit acelor planuri[15]. Declasificarea informațiilor și publicarea acestora de către SUA nu au modificat planurile lui Vladimir Putin de invadare a Ucrainei, însă au schimbat semnificativ contextul în care această invazie a avut loc. Prin comunicarea planurilor și intențiilor Moscovei, Occidentul a subminat potențialele provocări și a expus discrepanța dintre declarațiile Kremlinului și acțiuni, forțând Federația Rusă să schimbe narativele destinate comunității internaționale și opiniei publice interne.

Campania americană a fost eficientă din punct de vedere al anticipării operațiilor ruse de tip *false flag* (concepute astfel încât să poată fi atribuite unui alt actor) și al convingerii factorilor de decizie de la nivel politic din statele occidentale (și chiar din Ucraina) cu privire la iminența amenințării din partea Federației Ruse. Au fost astfel create condițiile pentru mobilizarea sprijinului internațional pentru Ucraina.

... DACĂ ADEVĂRUL ESTE DE PARTEA TA.

Campania de informare a SUA a avut, în mare parte, succes și ca urmare a faptului că Administrația Biden a fost percepută ca fiind o sursă de încredere. Dacă, în viitor, comunitatea guvernamentală de *intelligence* va oferi date eronate sau dacă *intelligence*-ul prezentat va fi perceput ca fiind distorsionat și utilizat în favoarea unor obiective politice (așa cum a fost cazul în 2002 și 2003 - Irak), favorabilitatea opiniei publice se va eroda rapid. *Intelligence*-ul nu este perfect, nu este niciodată pe deplin confirmat, ci doar coroborat, și construiește o imagine parțială, ale cărei elemente lipsă sunt completate cu analiză[16].

Efortul autorităților americane și britanice a beneficiat, de asemenea, de un sprijin nesperat: existența unei validări externe din partea comunității de entități non-statale care a diseminat *intelligence* pe baza informațiilor disponibile în surse deschise. *Public intelligence, intelligence*-ul produs de entități non-statale a fost disponibil la un nivel fără precedent. Aceste entități au oferit, astfel, un mijloc prin care unele informații (nu toate) au putut fi validate de către o terță parte aproape în timp real. Analizele publicate de aceste entități non-statale au confirmat declarațiile autorităților de la Washington, bazate pe informații obținute din surse clasificate.

Conflictul din Ucraina reprezintă un exemplu de cooperare dintre entități statale occidentale (SUA și Marea Britanie) și actori non-statali în scopul colectării de informații care să susțină eforturile forțelor combatante. După invadarea țării de către forțele ruse, autoritățile de la Kiev au solicitat în mod public furnizarea de imagini satelitare comerciale, filmări video de amatori și interceptări audio și traduceri cu ajutorul programelor care incorporează inteligență artificială (IA), în sprijinul culegerii de informații despre inamic.

În acest context, este de subliniat rolul analizei imaginilor satelitare (ramura IMINT a *intelligence*) comerciale de către actori non-statali și experți civili în domeniu, dispuși să confirme IMINT-ul declasificat și diseminat de către SUA și Marea Britanie în cadrul campaniei de comunicare strategică. În esență, este vorba de emergența a ceea ce poate fi numit „democratizarea IMINT”, parte a unui fenomen mai larg al „democratizării *intelligence*” prin proliferarea *social media*, cu un potențial crescut de a combate dezinformarea și a mobiliza mijloace civile atunci când cauza susținută este percepută ca fiind justă[17]. În plus, dezvoltarea și proliferarea comercială a imaginilor satelitare favorizează această „democratizare IMINT”, spre deosebire de alte domenii de *intelligence*, precum HUMINT

sau SIGINT, mult mai sensibile din punctul de vedere al protecției surselor/mijloacelor de culegere a datelor și informațiilor.

În același timp, apelul autorităților de la Kiev către cetățeni de a susține cu informații efortul de război ucrainean a generat un sprijin semnificativ din partea mediului civil. Încorporarea de date audio/ video legate de deplasările forțelor armate inamice diseminate pe rețelele de socializare, coroborate cu informații obținute cu aeronave de cercetare fără pilot (UAV) și sateliți civili, au crescut gradul de flexibilitate și adaptabilitate al acțiunilor de luptă.

Occidentul a avut, în cazul crizei ucrainene, avantajul de a fi de partea adevărului prezentat, iar acest adevăr a fost validat de „jurnalismul cetățenesc" și de analiza surselor deschise realizată de entități non-statale. De asemenea, adevărul și interesele entităților implicate au fost aliniate.

Intelligence-ul din surse deschise este încă o dezvoltare relativ recentă și se bazează pe tehnologii în plină dezvoltare. Comunitatea de *open-source intelligence*/ OSINT poate deveni parte a spațiului de luptă în mediul informațional.

Ce s-ar întâmpla dacă *intelligence-ul* din surse deschise publicat de entități non-statale, percepute drept credibile, ar contrazice sursele de informare oficiale?

Guvernele vor avea, cel mai probabil, în continuare acces la o serie de informații pe care comunitatea *open-source* nu le va putea accesa. Vor exista și situații în care guvernele vor fi interesate să promoveze o anumită politică și să folosească *intelligence* în mod selectiv în sprijinul acesteia, iar mesajele oficiale pot fi în contradicție cu *intelligence-ul* public al comunității *open-source*. Acest lucru va genera o serie de dificultăți pentru guverne în planul războiului cognitiv: o comunitate *open-source* credibilă, dar eterogenă, ar putea să nu fie întotdeauna de acord cu evaluările prezentate oficial de către guverne, iar mass-media ar putea pune sub semnul întrebării narativele prezentate oficial de către instituțiile statului.

În alte situații de criză/ conflict, creșterea rapidă a presiunii și a volumului de informații cu privire la iminența unui conflict armat sau acțiunile de pe timpul desfășurării acestuia s-ar putea dovedi în defavoarea eforturilor unui guvern de a-și promova propriile narative[18]. Postarea online a unor informații privind activitatea forțelor combatante poate fi utilizată și de forțe ostile, pentru a câștiga avantajul informațional. Limitarea sau controlarea fluxului de informații privind acțiunile de pe câmpul de luptă care sunt diseminate de către non-combatanți este dificilă și în viitor va deveni aproape imposibilă. În acest context, circularea informațiilor în timp real pe rețelele de socializare cu privire la succesul/ eșecul unor acțiuni militare punctuale, resursele alocate și pierderile umane necesită eforturi susținute pentru a gestiona riscul erodării rapide a sprijinului intern și internațional pentru o operație militară în derulare.

Entitățile non-statale pot contribui (voluntar sau involuntar, ca urmare a lipsei datelor relevante/ expertizei insuficiente) la difuzarea unor elemente de propagandă și dezinformare ostilă. În plus, indiferent de valoarea de adevăr a informațiilor prezentate și de dovezile deținute, entitățile non-guvernamentale care publică *intelligence* din surse deschise nu vor fi percepute mereu ca nepărtinitoare de către toate părțile implicate într-un conflict[19]. În unele situații, chiar dacă este nepărtinitor și perceput ca atare, *intelligence*-ul public al entităților non-statale poate fi utilizat pentru a amplifica exponențial efectele propagandei ostile, cu precădere în cazul unor societăți deja polarizate (ex.: Israel).

Comunitatea OSINT are o serie de limitări din punct de vedere al capabilităților. Guvernele vor menține anumite mijloace care vor rămâne în afara abilității comunității OSINT de confirmare sau validare. OSINT va putea și în viitor să confirme dislocarea de forțe și mijloace și chiar să desfășoare investigații de intelligence la o scară redusă – precum identificarea ofițerilor serviciului de informații militare al Federației Ruse/GRU responsabili pentru otrăvirea cu Novichok în Salisbury (Marea Britanie)[20]. Informații precum cele cu privire la intențiile elitelor politice și militare ale adversarului vor rămâne însă apanajul serviciilor de informații[21].

LECȚII ÎNVĂȚATE

Din punct de vedere al adaptării instituționale, adițional la încorporarea progresivă și accelerată a OSINT în comunitatea de *intelligence*, ultimii ani au fost martori la folosirea surselor deschise în paralel cu *intelligence* declasificat pentru comunicarea strategică, fapt care a condus la reconfigurări conceptuale și structurale.

Un exemplu de remarcat în acest sens este adaptarea structurii de *intelligence* a Departamentului de Stat al SUA, *Bureau of Intelligence and Research*/ INR, cea mai veche structură civilă de *intelligence* din SUA, înființată în 1947 de către secretarul de stat de la acea vreme, George Marshall, ca succesoare a *Office of Strategic Services/ OSS Research Department* din timpul cel de-al Doilea Război Mondial. Astfel, în contextul marcat de războiul din Ucraina, INR a început instituționalizarea *intelligence-ului* ca instrument al diplomației SUA, prin promovarea și susținerea conceptului de *intelligence diplomacy*[22]. În cadrul acestui demers, utilizarea de OSINT este percepută ca factor multiplicator al capacităților avute, facilitând producția de *intelligence* care poate fi declasificată mai ușor în vederea diseminării către aliați, parteneri și mass-media[23].

Totodată, INR a înființat o unitate de coordonare a folosirii surselor deschise, cu experți pe spațiile F.Rusă, R.P. Chineză și R.P.D. Coreeană, având ca scop redactarea de produse informative cu gradul de clasificare cel mai redus, astfel încât să poată fi diseminate rapid aliaților sau opiniei publice[24]. De asemenea, pe fondul existenței unui *trend* OSINT în cadrul administrației de la Washington, INR a lansat în premieră un plan de dezvoltare a capabilității de OSINT, la scurt timp după lansarea (în martie a.c.) strategiei OSINT la cel mai înalt nivel al comunității de informații a SUA, *Office of the Director of National Intelligence*, strategie menită să asigure cadrul integrării informațiilor disponibile comercial ca surse deschise[25].

În ceea ce privește folosirea de *intelligence* în comunicarea strategică, aceste adaptări instituționale, atât de necesare contextual, vor rămâne însă sub imperiul fricțiunilor inerente dintre domeniul guvernamental/ statal și cel al comunității publice. Diplomația publică are în vedere, în mod natural, susținerea obiectivelor politice și tinde să excludă din discurs informații care nu servesc acestui scop. Desigur, discursul public nu trebuie să conțină elemente false, însă nici nu trebuie să prezinte de fiecare dată, pe larg, o imagine comprehensivă a unei probleme (din toate perspectivele existente).

Comunitatea guvernamentală de *intelligence*, pe de altă parte, are o cunoaștere mai extinsă asupra problemei, precum și obligația, care derivă din etica profesională, de a lua în considerare toate datele deținute, precum și perspective diferite. Astfel, atunci când sunt întocmite materiale de *intelligence* destinate comunicării strategice trebuie menținut un dialog permanent între diplomația publică și structurile de *intelligence* (în care oficialul politic adaptează mesajele astfel încât acestea să fie eficiente și să servească obiectivelor naționale de politică externă, iar reprezentantul structurii de informații îl sprijină în acest demers, astfel încât produsul final să fie ancorat în realitățile raportate)[26]. Tensiunile sunt inerente într-un astfel de proces, însă acestea conduc la cele mai bune rezultate, care servesc intereselor naționale.

O tendință comună a oficialilor comunității de *intelligence* este de a prezenta o gamă largă de detalii pentru a explica un fenomen. Aceasta se bazează pe premisa potrivit căreia adăugarea unor detalii contribuie la validitatea și creșterea credibilității evaluărilor. Abundența detaliilor poate însă afecta semnificativ eficacitatea comunicării strategice, mai ales atunci când produsele de *intelligence* sunt destinate publicului larg. Mesajele ar trebui să fie așadar simple și clare. Menținerea simplității mesajului poate contribui, în unele cazuri, la reducerea riscurilor la adresa surselor și metodelor activității de informații. Valori numerice pot fi aproximate, iar fenomene complexe pot fi prezentate schematic, distanțând comunicarea strategică destinată publicului larg de specificitatea caracteristică produselor de intelligence pe care aceasta se

bazează[27]. Cu toate acestea, experiența arată că „înțelepciunea populară" cu privire la acest subiect nu este neapărat în concordanță cu elementul de impact de care este adesea nevoie pentru a obține efectul dorit, iar menținerea credibilității instituțiilor guvernamentale este un factor decisiv pentru succesul utilizării *intelligence-ului* în comunicarea strategică într-un mediu informațional contestat.

Disponibilitatea *intelligence*-ului public reprezintă, în același timp, un avantaj și o provocare pentru serviciile de informații, cu precădere pe palierul procesării informațiilor și în contextul necesității de verificare a datelor și informațiilor disponibile. Succesul SUA și al Marii Britanii (atât cel real, cât și cel perceput) în eforturile de comunicare strategică înaintea invaziei din Ucraina au creat noi așteptări (probabil unele dintre acestea nerealiste) din partea publicului larg[28].

Reprezentanți ai Ministerului Apărării britanic au precizat deja că nu se așteptau ca *tweet*-urile publicate de către instituție cu privire la conflictul din Ucraina să devină atât de populare și de căutate. *„Ministerul Apărării britanic a devenit rapid victima propriului succes"*[29] atunci când jurnaliști, miniștri și publicul larg au început să aștepte actualizări. Acest lucru a determinat suplimentarea personalului echipei desemnate pentru întocmirea și publicarea informărilor, iar efortul, care a fost gândit inițial drept o activitate temporară, a fost prelungit pentru a răspunde așteptărilor noilor beneficiari; din acest motiv, Ministerul Apărării britanic a continuat să posteze scurte informări actualizate aproape zilnic.

Astfel de decizii pot fi însă riscante – nu toate crizele vor avea impactul invaziei din Ucraina și nu toate crizele vor beneficia de o atenție similară din partea opiniei publice, iar instituțiile implicate trebuie să realizeze o planificare judicioasă a campaniei de informare și a resurselor alocate. Nu în ultimul rând, la problematicile generate de democratizarea *intelligence* și folosirea instituțională în comunicarea strategică se vor adăuga și cele derivate din spectrul ubicuității utilizării, de către actorii statali și non-statali, a inteligenței artificiale, domeniu a cărui democratizare probabil a și început.

BIBLIOGRAFIE

1. ALMROTH Björn Erik, "Democratization of Intelligence? Comparing Vietnam and Ukraine", *Lund University Publications Student Papers* (2023), Lund University, Department of Political Science, http://lup.lub.lu.se/student-papers/record/9112758.
2. BARNES Julian, "U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion", *New York Times*, 3 februarie 2022, https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html.
3. BERTRAND Natasha, Sciutto Jim, Lillis Katie Bo, "US intel indicates Russian officers have had doubts about full scale Ukraine invasion", *CNN*, 7 februarie 2022, https://www.cnn.com/2022/02/07/politics/us-intel-russia-doubts-invasion-ukraine/index.html
4. BORGER Julian, "Biden threatens Putin with personal sanctions if Russia invades Ukraine", *The Guardian,* 26 ianuarie 2022, https://www.theguardian.com/world/2022/jan/26/biden-threatens-putin-with-personal-sanctions-if-russia-invades-ukraine.
5. CARVIN Stephanie, "Deterrence, Disruption and Declassification: Intelligence in the Ukraine Conflict", Centre for International Governance Innovation, 2 mai 2022, https://www.cigionline.org/articles/deterrence-disruption-and-declassification-intelligence-in-the-ukraine-conflict/.
6. HARRIS Shane, "Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion", *The Washington Post*, 16 August 2021,

https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/.

7. HARRIS Shane, SONNE Paul, "Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns", *The Washington Post*, 3 Decembrie 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec8769-2f4ecdf7a2ad_story.html.
8. HOLMGREN Brett M., "Intelligence and Diplomacy: A New Model for a New Era", *The Cipher Brief* Annual Threat Conference, Sea Island, Georgia, 8 octombrie 2023, https://www.state.gov/intelligence-and-diplomacy-a-new-model-for-a-new-era/.
9. HUMINSKI Joshua C., "Russia, Ukraine, and the Future Use of Strategic Intelligence", în MIKLAUCIC Michael (ed.), *PRISM,* vol. 10, Nr. 3, 2023, p. 9-25, National Defense University Press, ISSN 2157- 0663, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3511951/russia-ukraine-and-the-future-use-of-strategic-intelligence/.
10. KUPERWASSER Yossi, SIMAN-TOV David (eds.), "The Cognitive Campaign: Strategic and Intelligence Perspectives", Memorandum No. 197, octombrie 2019, Institute for National Security Studies, Israel, ISBN: 978-965-92750-3-8.
11. MILLER Seumas, "Cognitive warfare: an ethical analysis", *Ethics and Information Technology,* vol. 25, nr. 3, 4 septembrie 2023, https://doi.org/10.1007/s10676-023-09717-7.
12. PEREIRA Daniel, "Cognitive Infrastructure Worldwide is Under Attack", în *The Worst Cognitive Warfare Conditions since WWII*, OODA Loop*,* 8 noiembrie 2023, https://www.oodaloop.com/archive/2023/11/08/cognitive-infrastructure-worldwide-is-under-attack-inthe-worst-cognitive-warfare-conditions-since-wwii/.
13. SEBE Marius, "Why Intelligence? Why do We Need to Include the Word Intelligence in the Romanian Language Dictionary?", *Annals of the University of Bucharest/ Political science series*, vol. 13, nr. 2, 2011, p. 65-80, https://nbn-resolving.org/urn:nbn:de:0168-ssoar-378401.
14. STAFFORD Alexander, "The Role of the Media During the Cold War", *E-International Relations*, 26 octombrie 2013, https://www.e-ir.info/2013/10/26/the-role-of-the-media-during-the-cold-war/.
15. *** *Intelligence Online*, "United States Department of State's intelligence bureau increases OSINT use to support US diplomacy", 26 septembrie 2022, https://www.intelligenceonline.com/government-intelligence/2022/09/26/departement-of-state-s-intelligence-bureau-increases-osint-use-to-support-us-diplomacy,109825674-art.
16. *** *Intelligence Online*, "Intelligence becomes diplomatic weapon at US State Department", 11 martie 2024, https://www.intelligenceonline.com/government-intelligence/2024/03/11/intelligence-becomes-diplomatic-weapon-at-us-state-department,110189664-eve.
17. *** *Intelligence Online*, "Diplomatic intelligence service INR jumps on OSINT bandwagon", 11 iunie 2024, https://www.intelligenceonline.com/government-intelligence/2024/06/11/diplomatic-intelligence-service-inr-jumps-on-osint-bandwagon,110246602-art.

[1] Joshua C. Huminski, "Russia, Ukraine, and the Future Use of Strategic Intelligence", în Michael Miklaucic (ed.), *PRISM,* vol. 10, nr. 3, 2023, p. 18, National Defense University Press, ISSN 2157-0663, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3511951/russia-ukraine-and-the-future-use-of-strategic-intelligence/.

[2] Cuvântul cheie Intelligence va fi folosit în articol ca substantiv neutru, defectiv de plural, împrumutat din limba engleză, în mod similar cu folosirea conceptelor de marketing și management. Totodată, conceptul de intelligence va fi echivalat cu noțiunea de cunoaștere specifică și specializată, dobândită prin procese operativ-informative de culegere, procesare și analiză a datelor și informațiilor. Vezi Marius Sebe, "Why Intelligence? Why do We Need to Include the Word Intelligence in the Romanian Language Dictionary?", Annals of the University of Bucharest/ Political science series, vol. 13, nr. 2, 2011, p. 65 și 80, https://nbn-resolving.org/urn:nbn:de:0168-ssoar-378401.

[3] Colonel Yarden Vatikay O., "When the Intelligence Officer and the Public Diplomat Meet", în Yossi Kuperwasser, David Siman-Tov (eds.), *"The Cognitive Campaign: Strategic and Intelligence Perspectives",* Memorandum Nr. 197, 2019, p. 173, Institute for National Security Studies, Israel, ISBN: 978-965-92750-3-8, https://www.inss.org.il/publication/when-the-intelligence-officer-and-the-public-diplomat-meet/.

[4] *** Adlai Stevenson describes location of missile sites in Cuba using aerial photographs during a United Nations Security Council meeting in New York, Library of Congress, https://www.loc.gov/item/2001696172/.

[5] Alexander Stafford, "The Role of the Media During the Cold War", *E-International Relations,* 26 octombrie 2013, https://www.e-ir.info/2013/10/26/the-role-of-the-media-during-the-cold-war/.

[6] Huminski, "Strategic Intelligence", p. 21-22.

[7] Shane Harris, Paul Sonne, "Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns", *The Washington Post,* 3 decembrie 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec8769-2f4ecdf7a2ad_story.html.

[8] Natasha Bertrand, Jim Sciutto, Katie Bo Lillis, "US intel indicates Russian officers have had doubts about full scale Ukraine invasion", *CNN,* 7 februarie 2022, https://www.latimes.com/archives/la-xpm1986-04-15-mn-4815-story.html.

[9] Julian Barnes, "U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion", *The New York Times,* 3 februarie 2022, https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html.

[10] Shane Harris, "Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion", *The Washington Post,* 16 august 2021, https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/.

[11] Stephanie Carvin, "Deterrence, Disruption and Declassification: Intelligence in the Ukraine Conflict", Centre for International Governance Innovation, 2 Mai 2022, https://www.cigionline.org/articles/deterrence-disruption-and-declassification-intelligence-in-the-ukraine-conflict/.

[12] Huminski, *Op.cit.,* pp. 21-22.

[13] Colonel Yarden Vatikay, *Op. cit.,* p. 172.

[14] Ibidem.

[15] Julian Borger, "Biden threatens Putin with personal sanctions if Russia invades Ukraine", *The Guardian,* 26 ianuarie 2022, https://www.theguardian.com/world/2022/jan/26/biden-threatens-putin-with-personal-sanctions-if-russia-invades-ukraine.

[16] Huminski, *Op. cit.,* p. 16.

[17] Pentru o descrierea conceptuală a „democratizării intelligence", implicații și controverse, vezi Björn Almroth, "Democratization of Intelligence? Comparing Vietnam and Ukraine", Lund University Publications Student Papers, 2023, Lund University, Department of Political Science, http://lup.lub.lu.se/student-papers/record/9112758.

[18] Seumas Miller, "Cognitive warfare: an ethical analysis", *Ethics and Information Technology,* vol. 25, nr. 3, septembrie 2023, https://doi.org/10.1007/s10676-023-09717-7.

[19] Daniel Pereira, "Cognitive Infrastructure Worldwide is Under Attack", în *The Worst Cognitive Warfare Conditions since WWII,* OODA Loop, 8 Noiembrie, 2023, https://www.oodaloop.com/archive/2023/11/08/cognitive-infrastructure-worldwide-is-under-attack-inthe-worst-cognitive-warfare-conditions-since-wwii/.

[20] Bellingcat Investigation Team, 2018, "Skripal Suspect Boshirov Identified as GRU Colonel Anatoliy Chepiga", Bellingcat, 26 septembrie 2018, apud HUMINSKI, "Strategic Intelligence", p. 15.

[21] Huminski, *Op.cit.,* p.15.

[22] Pentru aplicarea conceptului de "intelligence diplomacy" la nivelul Departamentului de Stat al SUA – a se vedea Brett M. Holmgren (secretar de stat adjunct pentru intelligence și cercetare și șef al INS până în iulie 2024), "Intelligence

and Diplomacy: A New Model for a New Era", The Cipher Brief Annual Threat Conference, Sea Island, Georgia, 8 octombrie 2023, https://www.state.gov/intelligence-and-diplomacy-a-new-model-for-a-new-era/.

[23] "Intelligence becomes diplomatic weapon at US State Department", *Intelligence Online,* 11 martie 2024, https://www.intelligenceonline.com/government-intelligence/2024/03/11/intelligence-becomes-diplomatic-weapon-at-us-state-department,110189664-eve

[24] "United States Department of State's intelligence bureau increases OSINT use to support US diplomacy", *Intelligence Online,* 26 septembrie 2022, https://www.intelligenceonline.com/government-intelligence/2022/09/26/departement-of-state-s-intelligence-bureau-increases-osint-use-to-support-us-diplomacy,109825674-art.

[25] "Diplomatic intelligence service INR jumps on OSINT bandwagon", *Intelligence Online,* 11 iunie 2024, https://www.intelligenceonline.com/government-intelligence/2024/06/11/diplomatic-intelligence-service-inr-jumps-on-osint-bandwagon,110246602-art.

[26] Colonel Yarden Vatikay, *Op. cit.,* p. 173-174.

[27] Ibidem, p. 169-171.

[28] Huminski, *Op.cit.,* p. 16.

[29] Ibidem, p. 16.

LOCUL ȘI ROLUL CENTRULUI DE EXCELENȚĂ NATO ÎN DOMENIUL HUMINT ÎN EDUCAȚIA ȘI INSTRUIREA DE SPECIALITATE ÎN NATO*

Iulian BARBU**
Alexandru KIS

Abstract

The NATO HUMINT Centre of Excellence (HCOE) in Oradea, Romania, plays a pivotal role in developing and implementing advanced training programs, ensuring the continuous improvement and alignment of HUMINT formation with NATO standards. Through innovative methods and rigorous quality assurance, the Centre enhances the Alliance's HUMINT capabilities, addressing both current operational needs and future challenges.

This paper presents the major landmarks of the NATO HUMINT Centre of Excellence's activity in education and training, marking its achievements as HUMINT Department Head and NATO-accredited education and training facility.

Keywords: *NATO; HUMINT; education; training; NATO HUMINT Centre of Excellence.*

INTRODUCERE

Managementul educației și pregătirii militare joacă un rol crucial în asigurarea eficienței și eficacității forțelor armate și se bazează pe un proces complex de planificare în vederea alinierii obiectivelor educaționale și de perfecționare cu cerințele operaționale și strategice ale armatei. Pe lângă instruirea forțelor active, formarea viitoarelor cadre militare în cadrul facilităților de educație și instruire, precum și a personalului militar în rezervă reprezintă deopotrivă piloni fundamentali ai acestui sistem, asigurând creșterea/ pregătirea, continuitatea și adaptabilitatea forțelor armate. Instruirea presupune și o gestionare atentă a bazei materiale de instrucție, precum și o planificare riguroasă a exercițiilor naționale și multinaționale, asigurându-se astfel o pregătire practică și teoretică adecvată, care să răspundă standardelor de interoperabilitate și cerințelor de la nivel aliat.

Dezvoltarea doctrinelor și a conceptelor din domeniul instruirii, precum și elaborarea regulamentelor militare generale contribuie la uniformizarea procedurilor și la consolidarea unei culturi comune, esențiale pentru cooperarea eficientă între diferitele structuri militare și pentru asigurarea interoperabilității în cadrul multinațional. În acest scop, activitățile de

** Opiniile și ideile exprimate în aceast articol aparțin autorilor și nu reflectă neapărat politica NATO.*

*** Col. ing. dr. Iulian BARBU este directorul Centrului de Excelență NATO în domeniul HUMINT, iar col. dr. Alexandru KIS este expert în cadrul aceleiași instituții.*

cooperare și coordonare, alături de monitorizarea activităților specifice domeniului „lecții învățate", permit identificarea și implementarea celor mai bune practici din activitatea operațională, asigurând astfel o îmbunătățire continuă a proceselor de instruire. La acest demers contribuie și abordările ce urmăresc proiectarea competențelor necesare în viitor, generate de evoluția tehnologiilor militare și de schimbările generale în societate (incluzând aspecte legate de cadrul legal), care antrenează modificări și adaptări la nivel procedural.

Proiectate la nivelul informațiilor pentru apărare toate aceste cerințe îmbracă forme particulare de management, pornind de la un proces riguros de selecție a personalului ce urmează să își desfășoare activitatea pe diferite paliere ale disciplinei Intelligence (culegerea de date și informații, procesarea informațiilor, sprijinul activităților specifice, cercetare-dezvoltare, comanda și controlul, etc.), urmat de un program consecvent de formare profesională și dezvoltare a competențelor specifice. Având în vedere obiectivele funcției de luptă informaţii/ intelligence în sprijinul operațiilor militare, plasate în contextul războiului hibrid – *sprijinirea generării forţei, sprijin pentru evaluarea situaţiei, realizarea de operaţii ISR (intelligence, surveillance, reconnaisance) în spectrul multi-domeniu, identificarea ţintelor şi obţinerea superiorităţii informaţionale*[1], putem să ne imaginăm un spectru larg de cerințe și specializări pe care aceste obiective le comportă. Dincolo de nivelul instrumental al acestora, dezvoltarea ideologiei, a principiilor și valorilor ce definesc la nivel simbolic o cultură de intelligence[2] reclamă viziune strategică, potențarea formulelor de cooperare internațională, o amplă dezbatere la nivel profesional și academic și instituționalizarea principalelor repere de natură să influențeze dezvoltarea unor capabilități credibile.

În acest sens, odată cu dezvoltarea de aranjamente bilaterale cu partenerii strategici și deschiderea României către cooperarea cu NATO în cadrul Parteneriatului pentru Pace, urmată de aderarea la Alianță în 2004, Direcția Generală de Informații a Apărării, prin Direcția Informații Militare (DIM), a urmărit perfecționarea capitalului uman de care dispune, în baza principiilor și standardelor NATO. Gestionarea participării structurilor de informaţii în diferite teatre de operaţii[3] și aprecierea de care acestea s-au bucurat din partea partenerilor au crescut prestigiul DIM în cadrul comunității de interes în NATO, stimulând implicarea în multiple proiecte de dezvoltare atât a capacităților naționale, cât și a relevanței sprijinului oferit Alianței în diferite formule de acțiune.

Centrul de Excelență NATO în domeniul HUMINT (HCOE) este un exemplu concret pentru rolul crucial al DIM în înființarea sa și pentru contribuția semnificativă a acestuia la dezvoltarea capacităților de culegere de informații din surse umane în cadrul NATO, asigurând interoperabilitatea necesară prin servicii de standardizare, dezvoltare conceptuală, managementul lecțiilor învățate și formare profesională. Activitățile de educație și instruire derulate la nivelul Centrului reprezintă o axă centrală a contribuției pe care instituția o aduce în sprijinul cererilor de suport ale NATO, aliniindu-se cerințelor și standardelor specifice în acest domeniu de activitate, după cum vom sublinia, de altfel, în continuarea acestui articol.

ACTIVITĂȚILE DE INSTRUIRE ÎN NATO

Noul Concept Strategic NATO (2022) descrie noua realitate de securitate și definește provocările cu care se confruntă Alianța, definind sarcinile politice și militare pe care NATO le are de îndeplinit. Războiul din Ucraina (rezultat al agresiunii nejustificate a Federației Ruse în țara vecină), asociat cu acțiunile competitive și/ sau de contestare ale actorilor autoritari (statali și nestatali), erodarea controlului armamentelor și amenințările reprezentate de terorism și instabilitatea pervazivă au determinat Alianța Nord-Atlantică să își revizuiască paletarul instrumentelor de putere de care dispune și să adopte o postură militară de descurajare și apărare în toate mediile operaționale.

În îndeplinirea ambițiilor de proiecție a forței și pentru alinierea acestora la exigențele operațiilor multi-domeniu, unul dintre pilonii principali este instruirea, alături de o politică solidă de dezvoltare a aptitudinilor liderilor militari și de îmbunătățire, în general, a capitalului uman de la toate nivelurile, ca parte a componentei „*Right People, Right Skills*" din agenda NATO de dezvoltare a capacităților de luptă.

Activitățile și evenimentele din spectrul educației și instruirii, atât la nivel individual, cât și colectiv, sunt considerate, la nivel aliat, ca fiind esențiale pentru pregătirea Structurii de Comandă și Structurii de Forțe NATO pentru misiunile actuale și viitoare. Totodată, exercițiile militare au și o componentă puternică de descurajare, demonstrându-și eficiența ca măsuri de asigurare de luptă și indicator al capacităților instrumentului militar de putere de care Alianța dispune. În acest sens, NATO își asumă stabilirea standardelor, principiilor și responsabilităților la care trebuie să adere programele de educație, instruire, exercițiile militare și activitățile de evaluare dintr-un ciclu de instrucție, la nivelul fiecărei discipline.

HCOE ȘI CADRUL NATO PENTRU MANAGEMENT EDUCAȚIONAL

Pentru a asigura o abordare coordonată și eficientă, activitățile de instruire în cadrul NATO sunt gestionate ca parte a unor sisteme de management specifice - *programarea globală (Global Programming/ GP)* pentru educație și instruire individuală și *procesul de gestionare a exercițiilor* pentru instruirea colectivă și exerciții (cu o extensie pentru activitățile de evaluare), ambele urmărind optimizarea calitativă și cantitativă a soluțiilor de instruire și alocarea eficientă a resurselor. Programarea globală dispune de o structură de guvernanță, în cadrul căreia Responsabilul Departamental (Department Head – DH) reprezintă partea care se ocupă cu dezvoltarea/implementarea soluțiilor educaționale, în baza unei metodologii specifice și respectând termenii și parametrii de cantitate și calitate predeterminați.

În domeniul HUMINT (parte a disciplinei *Intelligence*), unde HCOE este desemnat DH din 2015, educația și instruirea individuală se bazează pe prioritățile stabilite de *Planul Strategic de Instruire pentru Intelligence* și pe cerințele posturilor reflectate în Analiza cerințelor de instruire (Training Requirements Analysis/ TRA). În plus, comunitatea de interes HUMINT în NATO are o responsabilitate justificată în exprimarea unei viziuni incluzive privind educația și instruirea, cu efecte asupra dezvoltării curriculare.

DH este, în fapt, o instituție voluntară numită formal de conducerea Comandamentului Aliat pentru Transformare (HQ SACT) pentru a gestiona un program de educație și instruire pentru o disciplină recunoscută (sau subset al unei discipline). Acest rol implică translatarea cerințelor de instruire în soluții și coordonarea portofoliului de soluții pentru a asigura livrarea eficientă și accesul beneficiarilor – structurile de comandă și de forță ale NATO, aliați, parteneri și entități non-NATO, în baza unui sistem de prioritizare. Pentru a realiza acest lucru, DH colaborează cu furnizorii de soluții educaționale, cum ar fi facilitățile acreditate de către NATO sau centre de instruire naționale, asigurând standardizarea și coerența soluțiilor în conformitate cu cerințele specifice NATO. În acest context, GP traduce orientările politico-militare și aspectele funcționale ale operațiilor actuale și viitoare în cerințe specifice pentru instruire, identificate la nivel de abilități, competențe sau capacități tehnice necesare pentru a îndeplini o sarcină/ misiune. Sfera unei cerințe pentru instruire NATO depășește responsabilitățile naționale, abordând necesitatea asigurării interoperabilității între națiuni.

Centrul de Excelență NATO din Oradea este implicat activ în dezvoltarea și managementul unui program de instruire aliat în domeniul HUMINT, care să asigure pregătirea necesară pentru pozițiile HUMINT din structura NATO și pentru pregătirea profesioniștilor în domeniu la nivelul națiunilor aliate. Ca DH, cele mai importante activități în ciclurile de planificare

***Foto 1**: Aspect de la ceremonia de semnare a memorandumului privind acordarea către HCOE a statutului de responsabil departamental pentru educația și instruirea HUMINT în NATO (stânga – adjunctul pentru instruirea forțelor întrunite al șefului de stat major al Comandamentului Aliat pentru Transformare, viceamiral Javier Gonzalez-Huix, dreapta - col. Eduard Simion, directorul HCOE/ 2 septembrie 2015)*[4]

și instruire sunt Conferința anuală a disciplinei și Grupurile de lucru pentru analiza nevoilor de instruire, care sprijină dezvoltarea continuă a disciplinei și menținerea relevanței acesteia la nivelul NATO, contribuind cu soluții de instruire adaptate nevoilor identificate.

Pe lângă acestea, specialiștii Centrului participă regulat sau ad-hoc în diverse grupuri și paneluri de management și coordonare: Grupul de instruire NATO - secțiunea executivă pentru educație și instruire individuală, Consiliile de planificare a programării instruirii individuale și educației în NATO, Forumul DH, Conferința pentru instruire individuală și educație în NATO, conferințe și evenimente de dezvoltare axate pe educație și instruire (ex. Conferința pentru educație și instruire a Agenției NATO pentru Comunicare și Informații, Conferința tehnologiilor de instruire NATO, etc.).

Totodată, HCOE demonstrează un angajament holistic în adaptarea programului NATO de îmbunătățire a capitalului uman/ dimensiunea „*Right People, Right Skills*" a Agendei aliate de dezvoltare a capacităților de luptă și definirea diferiților parametri de lucru cu relevanță în acest domeniu:

- asigurarea unui sistem de îndeplinire a calității în conformitate cu standardele NATO și cerințele ce decurg din statutul Centrului (facilitate de educație și instruire acreditată NATO), incluzând politici și procese de perfecționare continuă;
- definirea profilul profesionistului HUMINT (abilități și trăsături) și corelarea acestora cu viziunea pentru educația și instruirea HUMINT în NATO;
- îmbunătățirea capitalului uman în HUMINT - alinierea cu prioritățile stabilite în Agenda NATO de dezvoltare a capacităților de luptă, corelată cu cerințele și caracteristicile Operațiilor Multi-Domeniu;
- modelarea procesului de selecție și dezvoltare profesională în HUMINT;
- analiza caracteristicilor și a cerințelor de învățare ale cursanților/ studenților din noile generații;
- analiza soluțiilor de modelare și simulare în instruirea în domeniul HUMINT și implementarea tehnologiilor educaționale moderne;
- consolidarea rețelelor de sprijin în domeniul educațional;

- certificarea instructorilor HUMINT;
- dezvoltarea cunoștințelor și abilităților profesionale prin activități academice;
- dezvoltarea competențelor de leadership în HUMINT;
- analiza cerințelor de digitalizare în activitatea HUMINT;
- dezvoltarea unor pachete de competențe prin armonizarea opțiunilor de autodezvoltare cu programele formale de pregătire;
- integrarea de perspective originale, inovative, în dezvoltarea suportului educațional;
- integrarea rezultatelor proiectelor de cercetare în activitatea educațională.

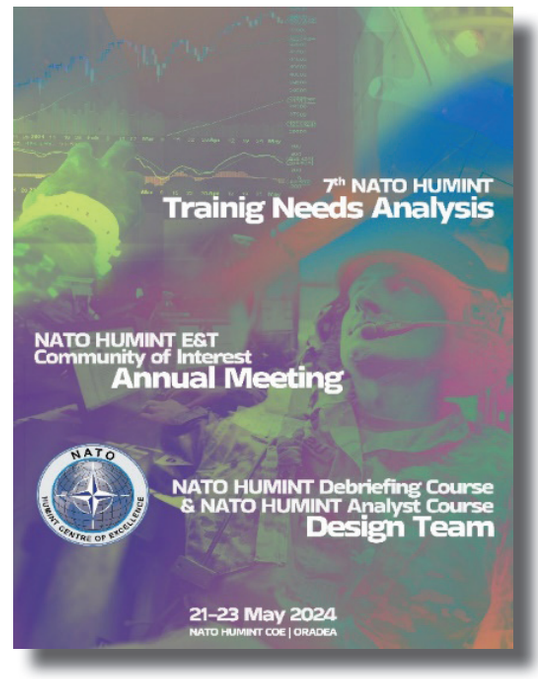
Contribuția generală a NATO HUMINT COE ca DH joacă un rol crucial în alinierea educației și instruirii în domeniul HUMINT cu cerințele specifice NATO. Această poziție strategică permite Centrului să influențeze dezvoltarea și standardizarea capacităților HUMINT în întreaga Alianță, asigurând faptul că programele de instruire sunt coerente, eficiente și răspund nevoilor operaționale actuale și viitoare.

HCOE – FACILITATE DE EDUCAȚIE ȘI INSTRUIRE ACREDITATĂ NATO

Pe lângă adecvarea programelor de pregătire cu cerințele recunoscute în mod formal, asigurarea calității în educație și formare la nivel instituțional este esențială din mai multe motive, fiecare contribuind la eficiența, credibilitatea și sustenabilitatea programelor educaționale.

În primul rând, asigurarea calității garantează că programele educaționale și de formare îndeplinesc standardele stabilite, adesea impuse de organisme de acreditare, organizații profesionale sau agenții de reglementare. În cazul educației și instruirii, acreditarea este asigurată prin structura specializată din cadrul Comandamerntului Aliat pentru Transformare, Direcția pentru dezvoltarea forțelor multi-domeniu (Multi-Domain Force Development/ MDFD), în baza standardelor cuprinse în directiva NATO pentru educație și instruire individuală, BiSC 75-007.

Acestea sunt adaptate după standardele European Association for Quality Assurance in Higher Education (ENQA), la care NATO a aplicat în 2012. ENQA furnizează ghiduri și standarde de asigurare a calității pentru Spațiul European al Învățământului Superior, urmărind să respecte principiul alinierii scopului cu procesul, în timp ce observă diversitatea proceselor de asigurare a calității în sistemele naționale și organizaționale de management al calității[5]. Adoptarea normelor și metodologiei ENQA, alături de monitorizarea permanentă și certificarea externă a calității, asigură referințe de înaltă calitate și consolidează responsabilitatea față de beneficiari și încrederea reciprocă între instituțiile de învățământ superior din diferite țări, cerință fundamentală pentru cadrul instituțional educațional al Alianței. Respectând aceste standarde, instituțiile pot oferi educație și formare de înaltă calitate, în mod consecvent, în cadrul diferitelor programe, grupuri și locații. Mai mult, monitorizarea regulată a programelor și practicilor permite instituțiilor să identifice zonele care necesită îmbunătățiri în proiectarea curriculum-ului, în metodele de predare sau în alocarea resurselor. În centrul asigurării calității se află obiectivul de a îmbunătăți rezultatele



cursanților. Prin implementarea unor procese solide de asigurare a calității, instituțiile se pot asigura că programele lor sunt concepute și livrate în moduri care maximizează învățarea, implicarea și succesul. Aceasta presupune nu doar evaluarea conținutului academic, ci și analiza eficienței metodelor de predare, a practicilor de evaluare și a serviciilor de suport.

Nevoile în educație și formare sunt în continuă evoluție din cauza schimbărilor în materie de proceduri, a progreselor tehnologice, a ridicării standardelor industriei și cerințelor sociale în schimbare. Procesele de asigurare a calității ajută instituțiile să rămână agile și receptive la aceste schimbări, promovând parametri de sustenabilitate și reziliență ca parte a culturii instituționale.

Acreditarea de către NATO asigură alinierea la standardele necesare și oferă garanția de asigurare a calității în baza evaluării: sistemelor și procedurilor interne de asigurare a calității standardelor; procedurilor aplicate la fiecare nivel de cunoaștere pentru a asigura calitatea curriculum-ului individual; proceselor de revizuire a calității programelor și a standardelor curriculum-ului și de implementare a schimbărilor, dezvoltărilor și îmbunătățirilor necesare; informațiilor corecte, complete și fiabile despre calitatea programelor instituției și standardelor curriculum-ului[6]. În acest sens, entitățile de formare și instruire trebuie să demonstreze că sunt apte să implementeze un sistem eficient de management al calității și că-și asumă angajamentul de a îmbunătăți continuu, în condițiile unui program de lucru orientat către cererile de sprijin ale NATO.

În baza evaluării efectuate de echipa de experți a Comandamentului Aliat pentru Transformare, Centrul de Excelență NATO în domeniul HUMINT a obținut acreditarea NATO pentru asigurarea calității în educație și instruire la 15 octombrie 2013, aceasta fiind reconfirmată în 2019. În 2025 este planificat un nou ciclu de evaluare care să reconfirme acreditarea necondiționată a Centrului de către NATO.

ASPECTE PRIVIND ACTIVITATEA DE FORMARE LA HCOE

Complexitatea și realitățile emergente ale mediului operațional au dus la diversificarea cerințelor de dezvoltare profesională în HUMINT, cuprinzând noi competențe și abilități care să răspundă unor provocări emergente. Centrul de Excelență NATO în domeniul HUMINT abordează aceste tendințe evolutive prin:

- acoperirea cu soluții educaționale dedicate a tuturor pozițiilor din cadrul organizației HUMINT, de la operator până la nivelul de management în cadrul celulei de operații HUMINT, susținând competența individuală și interoperabilitatea în baza prevederilor doctrinare și procedurilor specifice cuprinse în fișele de post (cursuri de nivel HUMINT, în format rezident/ hibrid);
- explorarea întregii arii de cunoștințe, abilități specializate și competențe aferente diferitelor tipuri de activități din spectrul HUMINT, în conformitate cu standardele NATO (cursuri de specialitate HUMINT, în format rezident/ hibrid);
- furnizarea de cursuri de „augmentare” a cunoștințelor și abilităților, care vin în completarea soluțiilor rezidente/ hibride (în format online);
- dezvoltarea capacității de a furniza soluții educaționale rezidente (la locația beneficiarului) prin intermediul unor echipe mobile de experți, sprijinite cu resurse locale, soluții customizate care să vină în întâmpinarea cerințelor specifice ale solicitantului/ în ultimii doi ani, astfel de echipe mobile au fost detașate pentru module de instruire în sprijinul unităților de forțe speciale din Armata României și a South-Eastern Europe Brigade (SEEBRIG);
- facilitarea înțelegerii și integrării aspectelor transdisciplinare prin vignete educaționale/ soluții de instruire care evidențiază particularități funcționale ale

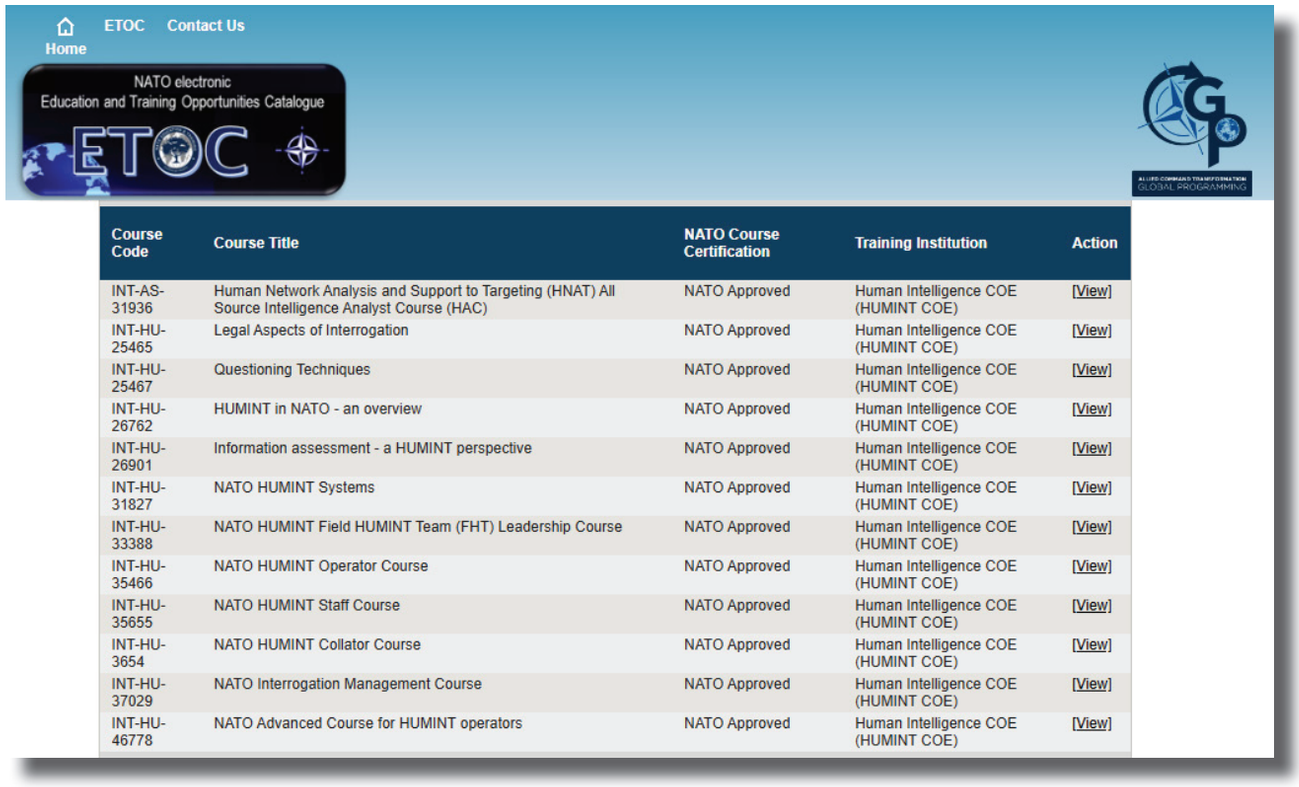
altor discipline sau funcțiuni și relevanța lor pentru HUMINT;

- popularizarea aspectelor fundamentale legate de HUMINT, ca disciplină de colectare a informațiilor pentru structurile de stat major și de comandă din cadrul NATO (cursul online „*HUMINT in NATO – an overview*” și filmul educativ pentru promovarea disciplinei HUMINT în NATO);
- asigurarea continuumului *instruire individuală – instruire colectivă*, prin sprijinirea activităților de instruire colectivă și a exercițiilor NATO, atât în domeniul de specialitate (unde Centrul acționează ca *Officer Directing the Exercise*, asigurând poziții cheie în cadrul structurilor de management și control instrucțional), cât și în exerciții întrunite de mare amploare, unde integrează elementul de răspuns HUMINT/ în acest spectru, în perioada 2022-2023 Centrul a participat cu experți la exercițiile NATO „Steadfast Jupiter”, „Steadfast Jackal” și „Loyal Leda”.

Conținutul cursurilor Centrului de Excelență NATO este elaborat în baza metodologiei NATO („*systems approach to training*”), care asigură cerințele de calitate și conformitate a soluțiilor educaționale cu nevoile NATO, fiind evaluat și revizuit frecvent în baza feedback-ului colectat și a direcționării strategice, pentru a-și păstra actualitatea și relevanța. Portofoliul de cursuri al Centrului cuprinde 12 cursuri certificate NATO (urmând ca la sfârșitul anului 2024 să fie lansate încă două cursuri în format pilot) și este disponibil pe platforma NATO Education and Training Opportunities Catalogue/ ETOC (*figura 1*). Accesul beneficiarilor la cursurile de nivel și de specializare este prioritizat în baza standardelor NATO și se realizează prin relație directă cu punctele de contact NATO și naționale pentru domeniul HUMINT.

În schimb, cursurile online sunt disponibile în baza unei politici de securitate mai permisive, acoperind o gamă complexă de subiecte: cursul *Questioning Techniques (QT)*, de bază pentru fundamentarea oricărui tip de interacțiune cu sursele umane în context HUMINT; *Legal aspects of interrogation (LAOI)*, destinat clarificării cadrului legal internațional pentru desfășurarea activității de interogare a persoanelor capturate; *HUMINT in NATO – an overview (HiNo)*, curs destinat personalului din structurile de comandă și stat-major, ce asigură înțelegerea principiilor de bază și cerințele de cooperare pentru integrarea capabilității HUMINT în activitatea operațională;

Foto 2-3: *Aspecte din activitatea de instruire desfășurată la Centrul de Excelență NATO în domeniul HUMINT din Oradea*



Course Code	Course Title	NATO Course Certification	Training Institution	Action
INT-AS-31936	Human Network Analysis and Support to Targeting (HNAT) All Source Intelligence Analyst Course (HAC)	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-25465	Legal Aspects of Interrogation	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-25467	Questioning Techniques	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-26762	HUMINT in NATO - an overview	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-26901	Information assessment - a HUMINT perspective	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-31827	NATO HUMINT Systems	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-33388	NATO HUMINT Field HUMINT Team (FHT) Leadership Course	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-35466	NATO HUMINT Operator Course	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-35655	NATO HUMINT Staff Course	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-3654	NATO HUMINT Collator Course	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-37029	NATO Interrogation Management Course	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]
INT-HU-46778	NATO Advanced Course for HUMINT operators	NATO Approved	Human Intelligence COE (HUMINT COE)	[View]

Figura 1: *Portofoliul de cursuri al Centrului de Excelență NATO în domeniul HUMINT din Oradea, pe platforma NATO ETOC*[7]

și *Information assessment – a HUMINT perspective (IAHP)*, având ca obiectiv dezvoltarea competențelor cognitive ale personalului de specialitate în contextul războiului de tip hibrid.

Totodată, prezența online a reprezentat metoda prin care Centrul a continuat pregătirea în peisajul educațional, în timpul pandemiei de COVID-19, alături de puținele cursuri rezidențiale furnizate în condiții speciale de securitate în domeniul sănătății. Importanța cursurilor online a luat tot mai mult avânt ca expresie a rezilienței în activitatea de formare, marcând o atenție

Figura 2: *Infografic – cursurile online ale Centrului pe platforma NATO e-Learning*[8]

sporită pentru abordările hibride și versiunile concurente, online și rezidențiale[9], chiar dacă există încă limitări serioase în capacitatea de a livra conținut clasificat pe platforme online. În acest sens, în cazul unei crize similare care să împiedice mobilitatea beneficiarilor, modulele introductive în domeniul HUMINT dezvoltate la nivelul Centrului au potențial de înlocuire a unor cursuri rezidențiale, în situația combinării lor cu module online sincronice, care facilitează interacțiunea directă a instructorului cu studenții, indiferent de locația acestora.

Figura 3 evidențiază creșterea constantă a numărului de studenți pentru cursurile în format tradițional (rezident/hibrid), ștacheta urmând să treacă în curând de borna reprezentând 2000 de cursanți instruiți în cadrul Centrului, comparativ cu creșterea exponențială a numărului de studenți pentru cursurile online, odată cu introducerea progresivă a acestora în portofoliul instituției.

Dezvoltarea de cursuri online a dus și la o abordare aplicată a oportunităților pe care tehnologiile educaționale moderne le prezintă. Integrarea acestora în educație și instruire pentru a spori eficiența livrării și a facilita accesul cursanților la soluțiile educaționale permite, de asemenea, transferarea unor părți din fundamentul teoretic ca module de lectură prealabilă, facilitând focalizarea pe abordarea practică pe parcursul părții rezidențiale a cursurilor hibride.

O altă dimensiune inovatoare pentru cursurile HUMINT este strategia de livrare gamificată[10], care antrenează curiozitatea și implicarea tinerelor generații de cursanți. Astfel, lansat în 2023 în colaborare cu Centrul de Pregătire în domeniul Informații pentru Apărare „General Nicolae Condeescu" din București, cursul online *Information assessment – a HUMINT perspective* capitalizează în ceea ce privește integrarea unor principii de gamificare, introducând elemente de joc într-un context non-ludic, cu scopul de a spori implicarea utilizatorilor în produs. Prin urmare, în loc să parcurgă doar diapozitivele cu lecții teoretice, studenții devin membrii unei echipe HUMINT dislocată într-o zonă operațională fictivă. Aceștia pot opta pentru o poziție în cadrul echipei, desfășurând o misiune specifică de culegere de informații pentru a răspunde unor cerințe specifice. Pe parcursul misiunii aceștia își dezvoltă abilități și cunoștințe a căror demonstrație într-un mediu complex, marcat de trăsăturile războiului cognitiv, este recompensată cu insigne de progres. Avansul în joc evoluează în paralel cu atingerea obiectivelor de instruire, într-un cadru stimulativ deosebit de apreciat.

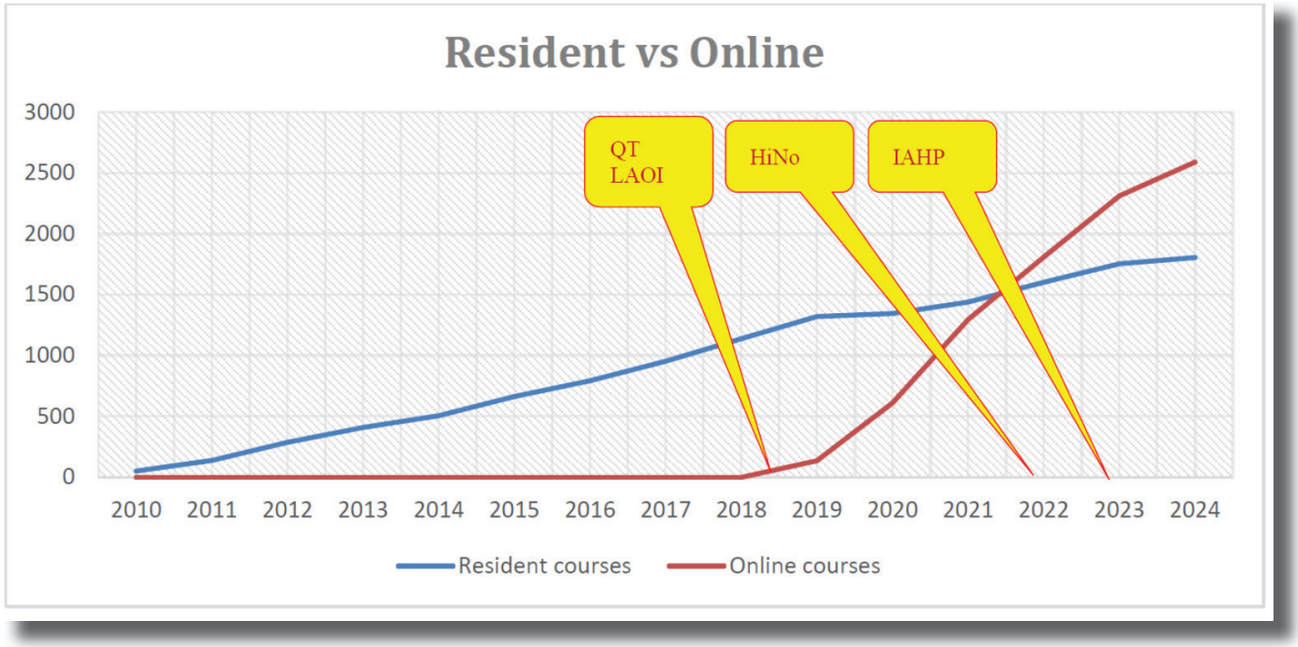


Figura 3: *Infografic – evoluția comparativă a numărului cumulativ de studenți în format rezidențial/hibrid vs. online*

Feedbackul pozitiv obținut a stimulat echipa specializată a Centrului să continue investigarea noilor modalități de îmbunătățire a modului de livrare a cursurilor online, urmând ca aceasta să dezvolte și un proiect de implementare a unui chatbot de simulare a activității de chestionare, urmat de dezvoltarea unei aplicații de realitate augmentată, care să constituie o etapă avansată în instruirea digitală a culegerii de informații din surse umane. În plus, inteligența artificială (dincolo de efectele operaționale generate de utilizarea sa în serviciile de informații[11]) reprezintă un vast domeniu de explorare pentru activitatea de formare. Inteligența artificială oferă avantaje semnificative în optimizarea managementului educațional, sistematizarea informației, generarea de conținut, personalizarea procesului de învățare, accesul la resurse educaționale avansate, feedback în timp real, etc., toate contribuind la o eficiență sporită și la adaptarea instruirii la nevoile individuale ale cursanților.

Mai trebuie să remarcăm faptul că activitatea de formare a Centrului este puternic stimulată de diferite evenimente generatoare de idei inovatoare și soluții științifice pentru o întreagă serie de problematici. Fie că facem referire la participarea la conferințe științifice, dezvoltarea de proiecte de cercetare în cooperare cu mediul academic și experți din industrie sau interacțiuni cu studenți, masteranzi și tineri profesioniști din domenii variate (facilitate de activități de tipul HUMINT Bootcamp[12]), afluxul de idei și informații este de natură să îmbogățească baza de cunoaștere și orizonturile de gândire ale personalului de specialitate, cu efecte certe în activitatea profesională.

CONCLUZII

Centrul de Excelență NATO în domeniul HUMINT din Oradea reprezintă un exemplu concret de aplicare cu succes a principiilor NATO în materie de management educațional și dezvoltarea ca hub de formare profesională, fiind

acreditat ca facilitate de educație și instruire NATO în 2013 și desemnat ca responsabil departamental NATO pentru educația și instruirea în domeniul HUMINT din 2015. Performanțele obținute în acest sens au reprezentat în permanență o adevărată carte de vizită pentru Centru, prin numărul de specialiști instruiți și calitatea pregătirii asigurată printr-o gamă diversificată de cursuri certificate.

Centrul își asumă un rol critic în dezvoltarea curriculei HUMINT în NATO. În acest sens, discuțiile angajate în cadrul comunității de interes HUMINT în NATO, în special la nivelul grupurilor de lucru de specialitate, sunt decisive pentru definirea cadrului general de instruire, asigurarea sprijinului cu instructori cu o largă experiență operațională, proiectarea și implementarea de soluții tehnice în activitatea HUMINT, precum și configurarea parametrilor de avansare în pregătire în cadrul exercițiilor de specialitate.

Asigurarea calității este un aspect central al activităților de formare ale Centrului. Acreditarea acestuia garantează că standardele NATO sunt respectate, iar programele sunt supuse unui proces continuu de îmbunătățire. Prin implementarea unor procese riguroase de evaluare și feedback, Centrul își menține relevanța și eficiența în formarea profesioniștilor HUMINT la toate nivelurile, răspunzând astfel nevoilor dinamice ale Alianței.

Relevanța soluțiilor educaționale ale Centrului este asigurată și prin caracterul complex al competențelor antrenate, orientate prospectiv către cerințele profesionale ale viitorului, profilate în diferite analize și studii. Inovația în instruire, cum ar fi utilizarea gamificării și integrarea tehnologiilor educaționale moderne, a permis Centrului să răspundă preferințelor noilor generații de cursanți. Prin abordarea unor metode interactive și stimulative, Centrul nu doar că îmbunătățește eficiența procesului de învățare, dar și implicarea cursanților, oferindu-le un cadru de dezvoltare profesională adaptat contextului actual.

În concluzie, activitățile de instruire și educație desfășurate de Centrul de Excelență în domeniul HUMINT din Oradea joacă un rol crucial în consolidarea capacităților HUMINT ale Alianței. Acestea nu doar răspund cerințelor operaționale curente, dar pregătesc și terenul pentru viitoarele provocări, asigurând un profil credibil și eficient al capabilităților de Intelligence ale NATO.

BIBLIOGRAFIE

1. DONE Cătălin-Gabriel, „Consolidarea și dezvoltarea capacității de analiză a informațiilor și transformarea paradigmei de securitate a României în contextul provocărilor asimetrice din regiunea Mării Negre“, în *„Gândirea Militară Românească”,* volum dedicat lucrărilor conferinței științifice internaționale „Consolidarea profilului României ca actor proactiv pentru asigurarea securității în regiunea Mării Negre”, noiembrie 2021, p. 34-53, https://gmr.mapn.ro/webroot/fileslib/upload/files/arhivaGMR/2021gmr/2021/4 proceedings 2021/DONE.pdf.
2. ENACHE Petre-Răzvan, „Rolul Intelligence în menținerea capacității de luptă în operații militare contemporane”, în *Buletinul Universităţii Naţionale de Apărare „Carol I”*, Martie, 2022.
3. JURCĂ Adonis, Ostaci Dragoş, Popa Ionuţ, „Informaţiile militare în dinamica teatrelor de operaţii”, în *Infosfera*, nr. 3, 2019 (anul XI).
4. KIS Alexandru, ”HUMINT Bootcamp – the practitioner challenge”, p. 34-37, *NATO HUMINT COE Annual Magazine*, nr. 1, 2023, p. 34-37.
5. KIS Alexandru, „Impactul pandemiei COVID-19 asupra activității de educație și instruire individuală în NATO. Experiența Centrului de Excelență NATO în domeniul HUMINT”*,* în volumul *Implicațiile noilor tehnologii și ale amenințărilor invizibile asupra procesului de adaptare a NATO la noua realitate globală*, (coord. Laviniu Bojor și Alin Cîrdei), Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2021, p. 59-72.
6. KIS Alexandru, Mârza Andrei, *Procesul de transformare a educației și instruirii în NATO. Dezvoltarea capitalului uman și a ecosistemului educațional în domeniul HUMINT*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2024, p. 53-68.
7. SFETCU Nicolae, *Integrarea inteligenței artificiale în serviciile de informații, apărare și securitatea națională*, Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST) al Academiei Române, 21 noiembrie 2023, https://www.crifst.ro/integrarea-inteligentei-artificiale-in-serviciile-de-informatii-aparare-si-securitatea-nationala/
8. SIMION Eduard, Kis Alexandru, ”New features of the NATO Centres of Excellence in support of the North-Atlantic Alliance Transformation”, în volumul ediției nr. 22 a conferinței internaționale ”*The Knowledge-Based Organization*”, Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2016, p. 125-131.
9. SIMION Eduard, Kis Alexandru, ”The NATO HUMINT Centre of Excellence as Department Head for human intelligence education and training in NATO”, în *Defense resources management in the 21st century*, DRESMARA, Editura Universității Naționale pentru Apărare „Carol I”, Braşov, 2015.
10. HQ SACT, *Quality Assurance Unconditional Accreditation for Human Intelligence Centre of Excellence,* scrisoare formală de acreditare*,* 15 octombrie 2013.
11. https://e-itep.act.nato.int/Guest/ETOCindex.aspx
12. https://jadl.act.nato.int/

[1] Petre-Răzvan Enache, „Rolul Intelligence în menținerea capacității de luptă în operații militare contemporane", în *Buletinul Universităţii Naţionale de Apărare „Carol I",* martie 2022, p. 76.

[2] Cătălin-Gabriel Done, „Consolidarea și dezvoltarea capacității de analiză a informațiilor și transformarea paradigmei de securitate a României în contextul provocărilor asimetrice din regiunea Mării Negre", în *„Gândirea Militară Românească",* Proceedings, Conferința Științifică Internațională „Gândirea Militară Românească", p. 37, https://gmr.mapn.ro/webroot/fileslib/upload/files/arhivaGMR/2021gmr/2021/4_proceedings 2021/DONE.pdf.

[3] Adonis Jurcă, Dragoș Ostaci, Ionuț Popa, „Informaţiile militare în dinamica teatrelor de operaţii", în *Infosfera,* nr. 3/2019, p. 47-54.

[4] Eduard Simion, Alexandru Kis, "The NATO HUMINT Centre of Excellence as Department Head for human intelligence education and training in NATO", în *Defense resources management in the 21st century,* DRESMARA, Editura Universității Naționale pentru Apărare „Carol I", Brașov, 2015, p. 97.

[5] Eduard Simion, Alexandru Kis, "New features of the NATO Centres of Excellence in support of the North-Atlantic Alliance Transformation", în volumul ediției nr. 22 a conferinței internaționale *The Knowledge-Based Organization* (iunie 2016), Editura Academiei Forțelor Terestre "Nicolae Bălcescu", Sibiu, 2016, p. 125-131.

[6] HQ SACT, *Quality Assurance Unconditional Accreditation for Human Intelligence Centre of Excellence,* scrisoare formală de acreditare, 15 octombrie 2013.

[7] https://e-itep.act.nato.int/Guest/ETOCindex.aspx

[8] https://jadl.act.nato.int/

[9] Alexandru Kis, „Impactul pandemiei COVID-19 asupra activității de educație și instruire individuală în NATO. Experiența Centrului de Excelență NATO în domeniul HUMINT", în volumul *Implicațiile noilor tehnologii și ale amenințărilor invizibile asupra procesului de adaptare a NATO la noua realitate globală* (Laviniu Bojor și Alin Cîrdei coord.), Editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2021, p. 59-72.

[10] Alexandru Kis, Andrei Mârza, *Procesul de transformare a educației și instruirii în NATO. Dezvoltarea capitalului uman și a ecosistemului educațional în domeniul HUMINT,* Editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2024, p. 53-68.

[11] Nicolae Sfetcu, *Integrarea inteligenței artificiale în serviciile de informații, apărare și securitatea națională,* Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST) al Academiei Române, 21 noiembrie 2023, https://www.crifst.ro/integrarea-inteligentei-artificiale-in-serviciile-de-informatii-aparare-si-securitatea-nationala/

[12] Alexandru Kis, "HUMINT Bootcamp – the practitioner challenge", în *NATO HUMINT COE Annual Magazine,* nr. 1, 2023, p. 34-37.

GEOPOLITICA ȘI GEOSTRATEGIA TAIWANEZĂ

„Poarta închisă cel mai bine este aceea care nu poate fi lăsată deschisă”[1].

Isabela ANCUŢ*

Abstract

Taiwan's geopolitical and geostrategic significance has grown exponentially in recent years, becoming a focal point in the power dynamics between China, the United States, and other global actors. This article examines Taiwan's increasing importance through the lens of geopolitical theories, particularly Nicholas Spykman's Rimland theory and Halford Mackinder's Heartland theory, and how these frameworks help explain China's strategic ambitions. China's claim over Taiwan, rooted in its desire for regional dominance, is central to its broader geopolitical goals, as control of Taiwan would enhance its influence in the Indo-Pacific and beyond, aligning with Spykman's Rimland concept.

Additionally, the article discusses the United States' policy of strategic ambiguity, which plays a critical role in balancing deterrence and diplomacy in its defense of Taiwan, aiming to prevent a direct military confrontation with China while supporting Taiwan's autonomy. By analysing these geopolitical theories and policies, this article provides a comprehensive understanding of why Taiwan remains a potential flashpoint for a major international conflict and how its fate could reshape global power structures.

Keywords: *geopolitical significance; Chinese reunification policy; China-Taiwan relations; power dynamics; Indo-Pacific security; regional dominance; Heartland theory; Rimland theory; strategic ambiguity.*

INTRODUCERE

Despre Taiwan s-a scris, se scrie și se va scrie mult, foarte mult. Simplistic vorbind, foarte multă lume este mirată de faptul că acest stat mic are o valoare geostrategică atât de mare. Totuși, dacă ne amintim de afirmația lui Alfred Thayer Mahan - *„stăpânirea lumii nu se face prin deţinerea de teritorii, ci prin controlul asupra principalelor rute comerciale şi prin stăpânirea principalelor puncte de pe traseul lor – insule, canale, strâmtori, puncte de aprovizionare”*[2], este ușor de înțeles de ce geografia/ suprafața, economia și politica, geostrategia și geopolitica acestui stat sunt de interes pentru marii actori internaționali. Istoria ne oferă cele mai simple exemple în acest sens: Portugalia (marile descoperiri geografice ale lui Vasco da Gama și Alvarez Cabral au instaurat hegemonia portugheză), Anglia (prin înfrângerea Invincibilei Armada a lui Filip al II-lea a fost blocată hegemonia spaniolă), Spania, Turcia/Imperiul Otoman și, mai recent, SUA

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

(„doctrina Monroe” din 1823 a marcat extinderea influenţei americane în întreaga emisferă vestică, iar Oceanul Atlantic a devenit câmpul de bătălie dintre SUA și marile puteri europene pentru obținerea zonelor de influenţă).

A.T. Mahan a observat faptul că, în orice conflict sau competiție pentru supremaţie internaţională, întotdeauna învingător a fost cel care, pe lângă diverse capabilități și avantaje, deţinea și controlul căilor maritime. Numai cu putere navală nu se poate câștiga un război, dar existența unor forțe navale înseamnă protejarea propriilor interese comerciale (chiar câștigarea supremaţiei comerciale), precum şi un element de descurajare strategică a inamicului. Același cunoscut geopolitician a indicat şi punctele strategice de care depinde controlul mărilor: Strâmtorile Gibraltar şi Hormuz, Canalul de Suez şi Portul Aden (pentru ruta Atlantic – Golful Persic prin Mediterana), Canalul Panama (pentru ruta Atlantic-Pacific) şi Strâmtoarea Malacca (pentru ruta Golful Persic – Oceanul Indian – Asia de Sud-Est – Pacificul de Vest)[3].

China își manifestă pretențiile asupra Taiwanului bazându-se pe o istorie veche și complexă, care, în viziunea liderilor de la Beijing, după cum vom vedea în articol, oferă unele fundamentări pertinente. Ceea ce nu dorește China să se afle este faptul că acțiunile sale se bazează puternic pe teoria Heartland-ului[4] și Rimland-ului[5]. Așa cum Rusia dorește să-și prezerve centrul continental prin centura de state slave din jurul său, în mod similar, China continentală dorește să se protejeze printr-o „centură sinică”, unde găsim Vietnamul, Coreea și zonele insulare din mările care înconjoară China, și printr-o „zonă asiatică interioară”, care cuprinde teritoriile populate de alte civilizații și pe care Beijingul încearcă să le controleze, cu scopul de a crea o zonă tampon față de „lumea exterioară”[6]. Concret, astfel de acțiuni chineze pot fi observate în Marea Chinei de Sud, Marea Chinei de Est, Hong Kong și Taiwan. Astfel, geopolitica chineză este aplicată prin „extindere strategică”, respectiv prin controlul unor puncte strategice din care își poate exercita influenţa („șiragul de perle”) și construcţia de insule artificiale în Marea Chinei de Sud[7].

Trebuie menționat că aceste acțiuni chineze „jonglează” cu prevederile dreptului mărilor. Codificarea dreptului mării, deşi abordată treptat de-a lungul istoriei (Lex Rhodia, Bazilicalele Imperiului Bizantin, Codex Amalfitana, Codul Oleron, Marea Liberă a lui Hugo Grotius), a început ca proces definitoriu odată cu perioada de după cel de-al Doilea Război Mondial, sub coordonarea ONU și printr-o serie de trei conferințe[8]. Dreptul mării este inclus în dreptul internaţional public, fiind codificat de către fiecare stat în parte în funcţie de resurse şi necesităţi[9]. Sub prevederile „Convenției de la Montego Bay asupra dreptului mării”, un stat riveran are

suveranitate asupra a 12 mile marine, măsurate de la liniile de bază adiacente ţărmului, și dreptul la o zonă contiguă, care să nu depăşească 24 mile marine măsurate tot de la liniile de bază, precum și o zonă economică exclusivă, care nu poate depăși 200 de mile marine de la liniile de bază.

Taiwanul nu este singura „problemă” din regiune în condițiile în care, urmărind teoriile geopolitice, multitudinea de strâmtori și canale maritime din zonă generează numeroase forme atipice de dileme de securitate[10].

În zonă există Strâmtoarea Malacca, un punct unde găsim un întreg amalgam de vulnerabilități și riscuri, de ambiții individuale și statale, un loc de care depinde traficul și comerțul internațional, precum și existența a trei state riverane (Singapore, Malaezia şi Indonezia), un spațiu

unde SUA, China, Japonia, India și Australia, cele trei puteri riverane, Vietnam, Thailanda, Filipine și Regiunea Administrativă Specială a R.P. Chineză, Hong Kong, joacă o partidă de șah aflată perpetuu în remiză[11].

Totuși, de ce este important Taiwanul pe scena internațională? Din punctul nostru de vedere, dacă Strâmtoarea Malacca este un nod gordian care, momentan, poate fi evitat, Taiwanul are la dispoziție câteva scenarii de evoluție, inclusiv cu potențial de escaladare, dar și de detensionare. Aceasta ar fi partea „pozitivă" a analizei zonei. Trecerea spre partea „negativă" este dată de faptul că istoria se repetă, deja putem vorbi de o reluare a ambițiilor globale maritime pentru puteri europene și transatlantice sau de o combinație a acestora, avantajele aduse de colonialism revenind în memoria statelor din afara regiunii. În plus, considerăm că este foarte interesant să analizăm Taiwanul ca un întreg, în sensul că importanța sa este dată de insulele foarte mici, situate extrem de aproape de coasta de est a Chinei, respectiv insulele fortificate Kinmen/ Quemoy, Matsu și Wuch`iu Yu, și mai puțin Ins. Pescadores (P`enghu) sau Makung.

TAIWAN ȘI CRIZELE STRÂMTORII TAIWAN

Situată la zona de fractură dintre platoul eurasiatic și platoul Mării Filipinelor, Insula Taiwan – cunoscută anterior ca Insula Formosa – a apărut din coliziunea platourilor continentale și continuă să se înalțe cu o rată de aproximativ un centimetru pe an, mai ales în zona muntoasă de centru. În prezent, Taiwanul este o democrație autocrată - Republica Chineză (ROC), teritoriul cuprinzând insula centrală, insulele periferice Penghu (Pescadores), Kinmen (Quemoy) și Matsu[12], dar și o serie de insulițe foarte mici risipite în jurul insulei principale. Toate însumează 36.197 km^2, o suprafață mai mare decât cea a Belgiei, dar mai mică decât cea a Elveției, fiind casa a 23,4 milioane de persoane.

Confuziile în privința Taiwanului încep încă de la numele oficial al statului - *Republica Chineză* (Republic of China - ROC). China, așa cum o știm, are denumirea oficială *Republica Populară Chineză* (People's Republic of China - PRC). În acest caz specific, confuzia joacă în interesul Chinei, istoria „ajutând" și ea Beijingul. De ce? Pe de o parte, avem China care consideră Taiwanul drept parte a sa, iar pe de altă parte, avem guvernul Kuomintang (naționaliștii chinezi) refugiat din China continentală în Taiwan ca urmare a înfrângerii suferite în războiul civil purtat cu mișcarea revoluționară comunistă a lui Mao Zedong și care se consideră a fi descendentul „adevăratului" guvern oficial al Chinei, continuator al Republicii Chineze, care a guvernat China continentală din 1911. Din acest motiv, guvernul Kuomintang dorește să „recupereze" China continentală, Mongolia, Tibetul și toate posesiunile dinastiei Qing, învingând, undeva, cândva și cumva, China comunistă. Cu alte cuvinte, China continentală este a Taiwanului, adică PRC aparține ROC. Cine aparține cui și de ce?

Istoria ne arată că primii coloniști cunoscuți au fost triburile de austronezieni, despre care se crede ca provin din sudul Chinei moderne. Insula apare pentru prima dată, în documentele chineze, în anul 239 î.Hr., când un împărat a trimis o forță expediționară să exploreze zona. Acest mic „amănunt" scris constituie unul din punctele de plecare pentru revendicările Beijingului. De asemenea, există o înregistrare a unei călătorii către Yizhou, presupus a fi Taiwanul, la începutul anului 230 d.Hr.. Apoi, dinastia Sui (581-619) a trimis o expediție armată către Liuqiu, un alt nume presupus a reprezenta Taiwanul. În 1281, guvernul chinez deja stabilise un avanpost/ garnizoană în Penghu.

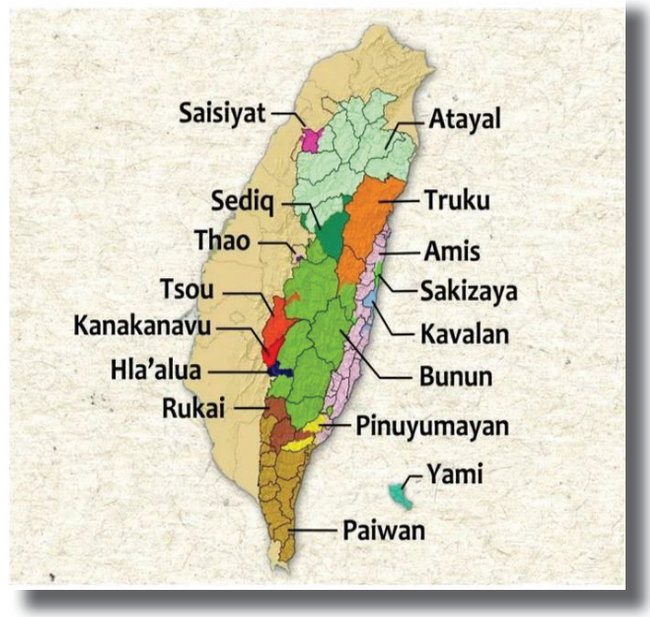
După o perioadă relativ scurtă de colonizare olandeză (1624-1661), Taiwanul a fost administrat de dinastia Qing a Chinei (1683-1895). Din secolul XVII, au început să sosească pe insulă emigranți chinezi: Hoklo din provincia Fujian și Hakka din Guangdong. În 1895, Japonia a câștigat primul razboi sino-nipon, iar guvernul Qing a cedat Taiwanul Japoniei. După cel de-al Doilea Razboi Mondial, Japonia s-a predat și a renunțat la controlul asupra teritoriilor cucerite de la China. Republica Chineză (fondată în 1911 și condusă de către Chiang Kai-shek și Partidul

Naţionalist Chinez/ Kuomintang) a început să conducă Taiwanul cu acordul aliaților săi, SUA și Marea Britanie. În 1949 a izbucnit războiul civil în China, iar trupele liderului de la acel moment, Chiang Kai-shek, au fost înfrânte de armata comunistă a lui Mao Zedong. Chiang, o mare parte a guvernului Kuomintang (KMT) și susținătorii acestora (aproximativ 1,5 milioane de oameni) s-au refugiat în Taiwan.

Momentul din 1949 reprezintă un alt punct de confuzie și dezacord (după denumirea statului) în ceea ce privește Taiwanul. Guvernul în exil al lui Chiang Kai-shek a pretins inițial că reprezintă întreaga Chină, exprimând deschis intenția de a o recuceri. Marii actori internaționali nu au dorit să recunoască noua națiune comunistă[13], motiv pentru care au preferat să accepte „versiunea" lui Chiang Kai-shek privind evoluția situației în zonă, iar Taiwanul a deținut scaunul Chinei/ PRC în Consiliul de Securitate al ONU, fiind recunoscut de mai multe state occidentale drept singurul guvern chinez.

La sfârșitul anilor 70, unele state au început să afirme că guvernul din Taipei nu mai poate fi considerat reprezentantul real al milioanelor de oameni care trăiau în China continentală. În plus, în 1971, ONU a recunoscut Beijingul[14], iar în 1979, recunoscând oportunitățile comerciale, SUA au stabilit oficial legături diplomatice cu acesta. Din acel moment, numărul statelor care au recunoscut diplomatic guvernul ROC a scăzut drastic[15]. Pe de altă parte, Taiwanul a reușit să mențină, neoficial, legături cu principalele state prin așa-numitele „birouri de reprezentare" care funcționează simultan ca ambasade și consulate. Deținătorii de pașapoarte taiwaneze pot intra în 145 de state fără viză.

În timp, evoluția socio-politică a Taiwanului a urmat calea normală și adecvată (istoric vorbind), statul trecând de la autoritarism la democrație. Ceea ce este interesant de menționat este faptul că SUA au insistat să joace rolul de *garant* al securității Taiwanului chiar și după 1979, după recunoașterea oficială a PRC și a conducerii partidului communist (PCC). Astfel, Comunicatul din 1978 menționa că SUA „recunosc poziția chineză cum că există o singură China, iar Taiwanul este parte



a Chinei", document care stă la baza așa-numitei politici „O singură China". Acest concept este deseori confundat cu principiul „O singură China" a PRC, diferențele invocate de specialiști constând în faptul că SUA s-au abținut de la a susține/ aproba pretențiile Chinei de suveranitate asupra Taiwanului. Prin urmare, Actul privind relațiile cu Taiwanul din 1979 menționa faptul că SUA promiteau să furnizeze „arme cu caracter defensiv" și se așteptau ca „viitorul Taiwanului să fie determinat prin mijloace pașnice". Totodată, s-a înființat Institutul American din Taiwan, structură care a funcționat, de facto, ca ambasadă (deși era înregistrată ca organizație non-profit în Washington D.C.).

Caracteristicile populației Taiwanului sunt, la nivel pratic, al treilea aspect de confuzie, identitatea strict etnică întrepătrunzându-se deseori cu identificarea naţională[16]. Deşi aproximativ 70% din populaţia statului se trage din imigranţii chinezi din Fujin, veniți înainte de cucerirea japoneză din 1895, respectivi din *hoklo* – actualii taiwanezi, mulţi dintre aceştia s-au amestecat cu populaţiile indigene, acestea din urmă reprezentând aproximativ 2,28% din populaţia totală. Chinezii *Hakka*, veniţi din Guangdong înainte de cucerirea japoneză, reprezintă aproximativ 15% din populaţie, iar nou-veniţii din China continentală, odată cu retragerea Kuomintang din 1949, reprezintă aproximativ 10% din populaţie. Etnic și genetic, putem afirma

că peste 95% din populaţie sunt chinezi *Han*. Doar când aducem în discuție identificarea națională acești chinezi Han se divid în: cei veniţi înainte de 1949 - denumiţi „*insulari*”; cei veniţi în 1949 - denumiți „*continentali*”; *indigeni* (recunoscute 16 triburi).

Din punct de vedere lingvistic, avem limbile indigenilor taiwanezi, iar limba „*taiwaneză*” oficială este, în realitate, o mandarină care a suferit atât de multe modificări încât a căpătat propria manifestare[17]. Limba *hakka* este și ea originară din China continentală. Distribuția lingvistică pe insulă nu este criteriu în condițiile în care acoperirea teritorială a limbilor indigene este extinsă, dar vorbitorii acestor limbi reprezintă doar 2,28% din populaţia totală și locuiesc în zona preponderent muntoasă. Concentrarea populației care vorbește „*taiwaneză*” se află în jurul capitalei Taipei și a regiunii de nord.

Această analiză se poate aplica și situației economice, dezvoltarea zonelor ocupate de continentali fiind net superioară celor ocupate de indigeni sau chiar insulari, ca urmare a politicilor duse de Kuomintang împotriva populaţiilor indigene şi vechilor imigranţi chinezi. În mod paradoxal, social și politic continuă să se mențină o oarecare suspiciune între *insulari* și *continentali*, aceștia considerându-se, reciproc, „chinezi impuri”, respectiv „taiwanezi impuri”. În ultima perioadă, numărul celor care se consideră *taiwanezi* a crescut, în comparație cu cei care se consideră *taiwanezi şi chinezi* sau doar *chinezi*. Problemele interne de identitate se perpetuează, identitatea chineză şi identitatea taiwaneză neexcluzându-se[18].

La nivel internațional, Taiwanul nu poate fi considerat teritoriu aflat în dispută și nu poate obține un loc de observator în organizațiile internaționale (precum Gaza/ Palestina), așa cum s-ar crede în condițiile în care există o guvernare proprie și funcționează ca un stat suveran.

În ceea ce privește *crizele Strâmtorii Taiwan*, prima a apărut în 1954, imediat după încheierea Războiului din Coreea, când R.P. Chineză a invocat existența și amenințarea venită din partea unor forțe naționaliste, aflate în câteva insule fortificate situate la o distanță apropiată de coasta Chinei continentale, cu precădere în Ins. Kinmen/ Quemoy şi Matsu. Cele două insule au fost bombardate puternic, mai ales după retragerea Flotei a 7-a americane din Strâmtoarea Taiwan și numai poziția fermă a SUA (ca aliat al Taiwanului) a determinat „remiza” situației.

A doua criză s-a derulat în august 1958, când R.P. Chineză a lansat o campanie de bombardamente[19] în apele din jurul Taiwanului, de această dată promovându-se ideea „eliberării Taiwanului”[20]. Total surprinzător, Mao Zedong a fost cel care a decis oprirea atacurilor, iar criza s-a încheiat cu o remiză. De ce? În acest moment, apare clar de ce trebuie să privim Taiwanul și insulițele din jurul său ca un întreg. După cum am menționat, insulele Kinmen/ Quemoy și Matsu au fost puternic fortificate (mai puțin Ins. Wuch`iu Yu), acestea fiind situate extrem de aproape de insulele aflate pe coasta de est a Chinei. Mao Zedong a realizat că cele două insule reprezintă conexiunea KMT cu PRC și că, fără acestea, ROC ar fi trasat granița comună la Ins. Taiwan și/ sau Ins. Pescadores (P`enghu) și Makung, având posibilitatea ideală de a se separa definitiv de continent. Adică dispărea baza pretențiilor PRC și apărea posibilitatea trasării unei granițe maritime între PRC și ROC.

Cea de-a treia criză s-a produs în 1995, când președintele ROC, Lee Teng-hui, a vizitat Universitatea Cornell (SUA) pentru a susține un discurs cu privire la democratizarea Taiwanului. În fapt această vizită fusese inițiată cu mult înainte, odată cu câștigarea alegerilor de către Lee Teng-hui. PRC a reacționat cu ostilitate atunci când SUA au decis să îi acorde viza lui Lee, derulând o serie de teste cu rachetă, exerciții navale complexe (15.07-25.08.1995) și mobilizând forțe în Fujian. SUA au mobilizat în Marea Chinei de Sud portavioanele *USS Independence* şi *USS Nimitz*, acesta din urmă fiind trimis spre Strâmtoarea Taiwan alături de un grup de nave de luptă, parte a Flotei a 3-a americane. Criza s-a finalizat, ca și precedentele, cu remiză, dar aceasta a crescut tensiunile din relațiile sino-americane, precum și vânzările de armament american către Taiwan.

PRINCIPALII ACTORI AI UNEI PERPETUE PARTIDE DE ȘAH: TAIWAN, CHINA ȘI SUA

Taiwan/ ROC

Relațiile R.P. Chineză - Taiwan au început să se îmbunătățească în anii 1980, odată cu recunoașterea Chinei pe plan internațional și cu renunțarea Taiwanului la ideile de „recucerire" a Chinei continentale, dar și cu relaxarea regulilor de conviețuire dintre cele două state (a politicilor privind vizitele și investițiile în China). Cu toate acestea, abia în 1991 Taiwanul a declarat *oficial* că s-a încheiat războiul cu PRC. Aceasta nu era și opinia Beijingului, acesta nerenunțând la politicile promovate de Mao Zedong.

Noua conducere chineză a început să promoveze ideea *„o țară, două sisteme"*, bazându-se pe confuziile generate de denumirile țărilor și comuniunea lingvistică[21]. Beijingul susținea că Taiwanul se va bucura de o semnificativă autonomie dacă ar intra sub controlul său. Strategia chineză, la acel moment, era similară cu cea care a determinat revenirea Hong Kong-ului la China, în 1997 (și a Macao). Taiwan a respins oferta, iar Beijingul a început campania prin care susținea că guvernul Taiwanului este ilegitim. Cu toate acestea, la nivel neoficial, au continuat discuțiile pe teme punctuale, specifice. Președinții taiwanezi care au urmat la conducerea statului - după Chiang Kai-shek și fiul acestuia- Chiang Ching-kuo - Lee Teng-hui și Chen Shui-bian au susținut, în mod deschis, modernizarea și independența statului insular. Relațiile dintre R.P. Chineză și Taiwan/ ROC au început să aibă o evoluție sinuoasă, perioade de îmbunătățire a relațiilor fiind urmate de tensiuni generate de climatul politic care încuraja independența ROC[22].

Beijingul consideră că autoritățile de la Taipei trebuie să respecte „Consensul din 1992", încheiat între Partidul Comunist Chinez (PCC) și Kuomintang (KMT), prin care „cele două părți separate de strâmtoare aparțin unei singure Chine și vor lucra împreună pentru reunificare". Principalul partid rival al KMT este Partidul Democrat Progresist (DPP), care respinge înțelegerea din 1992. De-a lungul timpului, politica Taipeiului a variat între atitudinea adoptată de KMT și cea a DPP[23]. Astfel, după Chen Shui-bian a urmat Ma Ying-jeou (2008, din partea KMT), care a încercat să îmbunătățească relațiile prin acorduri economice cu China, apoi Tsai Ing-wen (2016, 2020) și Lai Ching-te (2024), care oscilează între a obține independența sau a menține statu-quo-ul. Din 2005, după alegerea lui Chen Shui-bian pentru cel de-al doilea mandat, R.P. Chineză a trecut la măsuri dure adoptând *legea anti-secesiune*, unde se afirmă clar dreptul Beijingului de a utiliza „mijloace nepașnice" împotriva Taiwanului dacă acesta ar încerca „separarea" de China. Retorica chineză s-a acutizat în 2018, odată cu reușitele mici, dar constante de separare a ROC de PRC. Faptul că Tsai Ing-wen a câștigat cel de-al doilea mandat (2020) cu un număr record de voturi (8,2 milioane) și mișcările de democratizare din regiune (Hong Kong) au generat intensificarea incisivității retoricilor și acțiunilor PRC (elaborarea unei legi privind securitatea națională în Hong Kong, elaborarea de documente juridice în care se afirmă apartenența ROC la PRC, creșterea durității serviciilor de informații și securitate chineze etc.). Atât în 2019, cât și în perioada următoare, președintele Xi Jinping a reiterat propunerea de încorporare a ROC în PRC sub formula „*o țară, două sisteme*", dar propunerea nu a fost aprobată nici de această dată de taiwanezi, atât președintele democrat, cât și membrii KMT urmărind cu teamă acțiunile dure de represiune angajate de către Beijing în Hong Kong. Nici măcar conceptul *„O familie*", o teorie aplicată punctual și la scară mai mică de PRC în cazul Strâmtorii Taiwan, nu a avut succes, chiar și KMT fiind reticent în ceea ce privește implementarea acestuia[24] (în condiţiile în care „Consensul din 1992" aducea la un loc PRC și ROC, conceptul „O familie" a fost emanația singulară a Beijingului, alături de „o țară, două sisteme", fiind utilizat în media/ propagandă și politic doar atunci când făcea referire la colaborarea PRC-ROC în zona Strâmtorii Taiwan[25]).

Nici constrângerile, nici stimulentele militare, economice, informaționale și diplomatice puse în joc de PRC nu au reușit să schimbe opinia Taipeiului. Paradoxal, nici măcar populația care se consideră „chineză" (din punct de vedere al identității) nu dorește schimbarea condiţiilor curente din Taiwan, așa cum o implică unificarea cu R.P. Chineză. Formațiunea de guvernământ este clar în favoarea independenţei Taiwanului, iar KMT, care, anterior, favoriza o eventuală unificare cu China, a început să oscileze. Politicile chineze (de la nivel social și securitar) tot mai dure atât în China continentală, cât și în Hong Kong au indus teamă chiar și în vechii susținători ai Chinei. Cu toate acestea, opinia noastră este că taiwanezii nu doresc reunificarea cu R.P. Chineză, așa cum nu doresc nici obținerea rapidă a independenței (susținătorii acestor idei extreme fiind foarte puțini ca procent). Marea majoritate a populației, indiferent de culoarea politică, a „împrumutat" politica americană de „ambiguiditate strategică", tradusă, practic, în dorința de a menține *statu-quo-ul* pe termen nelimitat, fără nicio deviație spre independență sau unificare.

Totodată, Taiwanul dorește să păstreze „protecția" americană, în special cea politică și economică, precum și avantajele pe plan militar (dar în condițiile sale). Realitatea este că Taiwanul vrea protecție și asigurări de securitate din partea SUA, dar nu mai mult. Paradoxal, guvernul de la Taipei nu și-a propus să cumpere mai multe capabilități militare decât apreciază că-i sunt necesare, iar capabilitățile militare dorite sunt neapărat cele de ultimă oră. Istoria și timpul ne arată jocul unui foarte fin și interesant echilibru între: „doresc prietenia și protecția ta (SUA), dar nu vreau mai multe arme decât pe cele pe care ți le cer (specificate), astfel încât să pot păstra relații civilizate cu vecinul (China)". Cu alte cuvinte, Taiwanul caută un ajutor dimensionat pe propriile interese geopolitice și geostrategice, simțindu-se confortabil cu poziția-cheie pe care o ocupă în jocul „celor mari", dar fiind foarte atent în a nu deveni pionul de sacrificiu al acestora sau, în alți termeni, „*strategic pion but acceptable casualties in tragic and disperate conditions/situations*"[26].

Mai recent, victoria lui Lai Ching-te (20.05.2024) în alegerile prezidențiale poate fi percepută ca un nou obstacol în fața Bejingului, rezultatul fiind urmarea naturală a identificării (în creștere) a populației ca „cetățeni taiwanezi". Aceasta este a treia victorie consecutivă a DPP la alegerile prezidențiale, KMT rămânând în opoziție, iar politica sa de apropiere față de Beijing păstrându-se în stare latentă. În plus, Beijingul pare să-și pierdut influența și la nivelul KMT, continuându-se lipsa de coordonare și acord între candidații KMT și susținătorii din R.P. Chineză[27]. Singurele pârghii chineze de acțiune rămân spionajul, manipulările, influențările membrilor legislativului taiwanez, operațiunile informaționale și din mass media. În prezent, cel mai important aspect pentru taiwanezi rămâne bunăstarea economică, Taipeiul manifestând anumite temeri în condițiile în care este dependent de Beijing, cel mai mare partener comercial al său. Pe de altă parte, Taiwanul este, în prezent, cel mai mare producător de cipuri semiconductoare[28] din lume, domeniu care se află în plină expansiune, iar acest lucru este puternic vizat de marii actori, în special de R.P. Chineză și SUA, care se află în competiție pentru influență economică.

R.P. Chineză

În ultimii ani, Beijingul a devenit tot mai agresiv, la nivel retoric și acțional, Taiwanul reprezentând pentru liderii chinezi o miză importantă, „reunificarea" fiind unul dintre interesele majore ale regimului Xi Jinping. Pentru R.P. Chineză Taiwanul ridică mai multe dileme de securitate. Din punct de vedere al teoriei Heartland-ului și Rimland-ului, amenințările la adresa Chinei sunt generate de apropierea unor insule care nu se află sub suveranitatea sa, respectiv insulele taiwaneze Kinmen (*Chinmen*) și Matsu, situate în apropierea zonei de coastă a provinciei Fujian. Acestea, în 2001, au devenit primele centre ale legăturii directe de transport, comerț și poștă (*cunoscute drept „Cele trei mici legături"*) între Taiwan/ROC și R.P. Chineză/PRC. După 2020, aceste „Cele trei mici legături" au devenit „Cele patru noi legături"/„Cele patru mici legături", aprofundând coexiunea ROC

- PRC pe furnizarea de apă, electricitate, gaz natural și asigurarea infrastructurii de transport între insulele menționate și provincia Fujian (cu precădere Xiamen)[29]. Este de amintit și faptul că sub conducerea fostului președinte taiwanez, Ma Ying-jeou, Taiwan și China au încercat să dezvolte (2008) „un cerc comun de conviețuire" între insule și provincia Fujian, cu precădere între ins. Kinmen și Xiamen (denumit „Două porți") și între Ins. Matsu și orașul Fuzhou din districtul Mawei (denumit „Doi Cai"); se vorbea chiar de construcția unui pod între Kinmen și Xiamen. Discuțile au fost reinițiate în 2023, când au apărut și mențiunile pentru păstrarea insulelor ca zone demilitarizate.

Acțiunile chineze au insistat, într-o primă fază, asupra aspectului informațional și legal, toate având scopul de a justifica și fundamenta reunificarea ROC cu PRC, respectiv intrarea ROC sub controlul total al PRC. Astfel, documente precum cel intitulat *„Problema Taiwanului și Proiectul de unificare a Chinei în Noua Eră",* din august 2022, menționau, printre altele, că *soluționarea problemei Taiwanului și realizarea totalei unificări a patriei* sunt principalele scopuri ale *Marii Renașteri a Națiunii Chineze*. Totodată, se afirma că *Taiwanul a „plecat" din cauza decăderii naționale și a lipsei de unitate, motiv pentru care o Chină renăscută nu poate tolera statu-quo-ul separării pe timp nedefinit*. Ulterior, în septembrie 2023, insistând în aplicarea conceptului „O familie", liderii de la Beijing au elaborat un document[30] prin care promovau provincia Fujian ca sediu central al dezvoltării zonei de traversare a strâmtorii, respectiv conectarea micilor insule taiwaneze menționate anterior cu China continentală, prin intermediul unor mari proiecte de infrastructură[31]. Nici măcar politica *„puterea ascuțită"* a R.P. Chineze, termen care a definit (2017) acțiunile de manipulare și influențare/subminare masivă a sistemului politic taiwanez, nu și-au atins ținta finală, indiferent dacă la conducerea statului s-a aflat KMT sau DPP.

Odată cu trecerea timpului și cu creșterea rezistenței Taiwanului la propunerile de unificare ale Beijingului, pentru președintele Xi Jinping a devenit un aspect prioritar de politică externă, acesta afirmând, în repetate rânduri, mai mult sau mai puțin direct, că un eventual insucces al reunificării cu Taiwanul independent și pro-american ar putea fi un motiv pentru care *R.P. Chineză ar iniția chiar și un război*. Un indicator al determinării președintelui chinez sunt și patrulările frecvente și de amploare cu bombardiere, avioane de luptă și avioane de supraveghere chineze peste și în jurul Taiwanului, creșterea numerică a navelor de război și a portavioanelor în Strâmtoarea Taiwan, precum și miile de atacuri cibernetice chineze asupra instituțiilor guvernamentale taiwaneze.

În acest caz, putem afirma că se corelează noile abordări cu cele vechi, și anume asigurarea primului și a celui de-al doilea „lanț de insule" care trebuie să protejeze China de orice acțiune externă agresivă. În acest caz, *Rimland-ul* care cuprinde Coreea de Sud, Japonia și Taiwan tinde să „îngrădească" China, închizând-o pe continent. Din acest punct de vedere, China nu mai poate fi o reală putere (pierde puterea maritimă). Astfel, crizele Strâmtorii Taiwan generate de China nu sunt decât manifestări practice ale Beijingului de a „fractura" *Rimland-ul* prin eliminarea unui punct de susținere - Taiwanul[32].

Dacă am corela dorința Chinei de a stăpâni Taiwanul cu deciziile de revendicare teriorială asupra Ins. Senkaku/ Diaoyu și Spratly, atunci putem afirma că PRC consideră mările Chinei de Est și de Sud ca materializarea ambițiilor sale de *„realpolitik"*, zone de manifestare a puterii sale geopolitice și geostrategice în raport cu alte puteri, în special cu SUA (principalul său rival). Pentru Beijing, Taiwan (și Arhipelagul Panhu) sunt obstacole în calea accesului maritim la zonele de coastă ale Chinei continentale și/ sau mijloace de a bloca China și liniile sale de transport din partea estică, elemente necesare asigurării securității statului[33].

Liniile de navigație din Estul Îndepărtat către Mările de Sud, Oceanul Indian și Canalul Suez

trec prin Strâmtoarea Taiwan, unul dintre cele mai mari canale de navigare (350 km lungime, 100-150 km lățime), mărginit de Ins. Taiwan și fortăreața navală din Panhu, aflată la mijlocul drumului dintre Taiwan și Coasta Fukien. Taiwan deține două baze navale importante, Keeling (în nord) și Kaoshung (în sud), ambele având porturi protejate, de mare adâncime, dotate cu facilități moderne și conectate cu infrastructura de cale ferată și șosele. Arhipelagul Panhu cuprinde baza navală Ma Kun, care are condiții excelente pentru derularea de operațiuni în Mările Chinei.

Chiar dacă președintele Xi Jinping a decis ca termen final pentru unificarea ROC cu PRC anul 2049, aceasta este încă în discuție. Tensiunile și epurările recente în rândul elitei militare, reformele în curs de derulare (înființarea de noi categorii de forțe) în cadrul structurilor de securitate[34], cu precădere ale celor din domeniul apărării, fac ca acest termen-țintă să rămână o propunere teoretică, președintele Xi Jinping putând iniția unele acțiuni mai devreme (posibil în 2032[35]). Paradoxal, contrar acțiunilor anterioare, aripa militară este mai puțin „vocală", în prezent, decât președintele chinez în ceea ce privește „pregătirile de război" împotriva Taiwanului, considerând că s-ar putea produce o situație similară celei din Ucraina. Cu alte cuvinte, aripa militară nu crede că este suficient pregătită și nici nu deține capabilitățile necesare obținerii unei victorii rapide și categorice în cazul unui conflict armat deschis.

În plus, în acest caz, s-ar produce o apropiere directă între China, pe de o parte, și SUA și aliații acestora – Japonia, Filipine, Australia etc., pe de altă parte. Oricât de virulente ar fi retorica politică și acțiunile de manipulare, influențare și spionaj chineze, realitatea (în special cea militară) este cu totul altceva. Tensiunile interne, cu precădere cele de ordin social-economic, nu susțin o acțiune militară asupra Taiwanului. Doctrina inițierii și participării la un conflict extern pentru a evita o criză sau detensiona situația internă nu este aplicabilă R.P. Chineze, în pofida numărului mare de militari. Și aceasta în pofida faptului că un Taiwan controlat de Beijing ar deveni o bază militară care ar permite extinderea suplimentară a razei de acțiune a aeronavelor și rachetelor chineze cu 150 de mile marine spre est. Adică ar permite R.P. Chineze să blocheze rutele aeriene și maritime din Marea Chinei de Est și ar crește capacitatea forțelor armate chineze de a lovi ținte din Japonia sau Guam (unde există baze SUA). „Visul chinez" al președintelui, de ridicare a statutului Chinei ca „lider suprem al unei noi ordini mondiale", va trebui susținut de alte acțiuni, pe alte planuri și în alte domenii, chiar dacă la nivelul elitei politice și militare de la Beijing se menține ideea „renașterii Estului și decăderii Vestului".

SUA

În opinia noastră, SUA se află în poziția de „prizonier" al propriului joc geopolitic și geostrategic în regiune. Oficial, Casa Albă a recunoscut *politica „O singură China"* și faptul că *„Taiwan este parte a Chinei",* având legături formale cu R.P. Chineză din 1979. Simultan, deși SUA nu au un tratat de apărare cu Taiwan, cu care nu au relații diplomatice oficiale, există legi[36] care *obligă președintele american să ofere sprijin Taiwanului*, prin vânzări de armament și alte măsuri, în cazul unui conflict[37]. Este ceea ce, în politica externă americană, se numește „ambiguitate strategică". Prin faptul că există documente legale internaționale care îi limitează puterea de a acționa, dar și datorită faptului că a recunoscut legitimitatea PRC și a pretențiilor sale asupra Taiwanului, în prezent Washingtonul preferă să nu clarifice care va fi răspunsul său exact în cazul unui conflict, acționând simultan *pentru descurajarea invaziei chineze și menținerea statu-quo-ului, respectiv oprirea declarării independenței Taiwanului[38].* Dacă luăm în considerare teoria Rimland-ului, SUA acționează ca „limitator" al extinderii PRC, extinderea puterii continentale (Heartland-ul) fiind controlată/ restrânsă prin limitarea (extinderii) puterii maritime (Rimland-ul). Instrumentul prin care SUA implementează aceste politici este Taiwanul, respectiv protejarea „pionului esențial, dar de sacrificiu". Cât timp acest pion este ținut „în viață", în condiții „acceptabile" (limitarea cantității de armament american), cele două puteri

nu se vor ciocni direct, cu efecte dezastruoase pentru statele din regiune și omenire, în general.

Mai recent, a apărut ideea că trebuie revizuită politica de „ambiguitate strategică" față de Taiwan dacă SUA doresc să-și mențină statutul de unic pol de putere, respectiv să elimine actualul echilibru de putere favorabil Chinei. Unele spirite mai „nervoase" ar dori ca SUA să adopte o poziție strategică clară care să descurajeze o eventuală agresiune chineză asupra Taiwanului, apreciind că credibilitatea puterii Americii este în pericol[39]. Istoria și realitatea arată că tocmai acest lucru nu a fost și nici nu este recomandat. În regiune, principiul dominoului se aplică și produce efecte, fără discriminare, pentru toți actorii regionali. Putem să ne gândim că acțiunea SUA va determina susținerea acestora din partea aliaților regionali - Japonia, Coreea de Sud sau Australia și că, similar, inacțiunea SUA ar aduce atingere serioasă încrederii aliaților, respectiv ar demola sistemul de alianțe regionale construite de Washington. Foarte adevărat, dar această abordare ar fi valabilă și în cazul Chinei pentru care pierderea Taiwanului ar însemna diminuarea semnificativă a capacității Beijingului de a influența militar regiunea de dincolo de „primul lanț de insule" (esențiale pentru strategia americană în regiune).

Există și voci în SUA care reamintesc de acțiunile acestora în Irak, respectiv de motivațiile declanșării războiului din Irak sau de luptele din Afganistan, respectiv de ipotezele neclare, confuze, uneori lipsind, de la care s-a pornit în construirea unei strategii de luptă. Chiar dacă unele doctrine au demonstrat eficacitatea eliminării de tensiuni interne prin mobilizarea pentru soluționarea unei așa-zise crize internaționale, noile tehnici, metode și instrumente de luptă au adus confruntările la o situație în care ar fi de preferat să măsurăm de un milion de ori și apoi să tăiem o singură dată.

Paradoxal, mai important decât aplicarea teoriilor de geopolitică și a acțiunilor geostrategice, interesul final al SUA în regiune rămâne unul economic. Așa cum Irakul a fost esențial pentru petrol, Taiwanul este esențial datorită dependenței semnificative a SUA de semiconductorii și cipurile taiwaneze. Războiul Rece dintre SUA şi China este deja concentrat în domeniul supremaţiei tehnologice: inteligenţă artificială, calculatoare cuantice, bioinginerie, posibil o nouă cursă spaţială etc., iar la baza dezvoltării produselor necesare stau tocmai acești semiconductori taiwanezi. SUA au realizat că se bazează pe o singură companie pentru necesarul său și, chiar dacă Administrația Biden a inițiat un plan pentru a consolida industria de profil americană, este prea puțin și prea târziu într-un moment considerat esențial. Washingtonul a presat Taiwanul să nu mai vândă semiconductori companiilor chineze, dar acest fapt este aproape imposibil pentru ROC în condițiile în care economia sa se bazează pe această industrie.

ÎN LOC DE CONCLUZII: DAVID ȘI GOLIAT - TAIWAN ȘI DUELUL GIGANȚILOR ÎN VIITOR

Taiwanul intenționează să dezvolte capabilități militare asimetrice și de descurajare strategică împotriva unei potențiale agresiuni chineze. Prin urmare, va continua acțiunile de dezvoltare și consolidare a aliaților sale utilizând instrumente politice, diplomatice și, cu precădere, economice și tehnologice, accentuând rolul esențial în producerea și comercializarea de componenete necesare industriei de vârf. Taiwanul este conștient de poziția sa, de pion-cheie în regiunea Indo-Pacifică, motiv care este suficient pentru a păstra capabilități de apărare împotriva unei potențiale agresiuni a PRC. Menținerea statu-quo-ului oferă timp de refacere și dezvoltare pentru toți actorii – Taiwan sau China, dar nu în aceeași măsură. În prezent, menținerea DPP la conducerea Taiwanului va determina, cel mai probabil, continuarea răcirii relațiilor ROC-PRC și creșterea numărului exercițiilor militare chineze în Strâmtoarea Taiwan. Chiar dacă PRC nu își permite, în viitorul foarte apropiat, un conflict militar cu ROC[40], aceasta nu oprește retorica incisivă a Beijingului față de Taiwan și aliații săi. Orice problemă economică a Chinei poate permite/genera amplificarea naționalismului și, implicit, dorința de a cuceri Taiwanul. Teoria menționată privind distragerea atenției de la problemele interne se poate aplica, fără discriminare și în cazul Chinei.

BIBLIOGRAFIE

1. BLĂNARU Matei, *Cel mai periculos loc de pe planetă: Taiwanul. Sau când identitatea devine o problemă de securitate*, 02.12.2012, în http://adevarul/blogurile-adevarul/cel-mai- periculos-loc-de-pe-planeta-taiwanul-sau-2136025.html.
2. BRZEZINSKI Zbigniew, *Strategic Vision. America and the Crisis of Global Power*, Basic Books, New York, 2012, 224 p.
3. BUSH C. Richard, ”Taiwan’s democracy and the China challenge”, *Brookings Commentary*, 22.01.2021, https://www.brookings.edu/articles/taiwan’s-democracy-and-the-china-challenge/.
4. FILIP Adrian, *Dreptul maritim internațional*, Ed. Sitech, Craiova, 2017, 249 p.
5. FULCO Matthew, ”Xi Jinping and Taiwan: Change and Continuity with Past CCP Leaders”, The Jamestown Foundation, *China Brief*, vol. 23, nr. 9, 19.05.2023.
6. HO Ming-Sho, *Challenging Beijing’s Mandate of Heaven: Taiwan’s Sunflower Movement and Hong Kong’s Umbrella Movement,* Temple University Press, 2019, 269 p.
7. HSIAO Russell, ”The DPP’s 2024 Presidential Candidate-in-Waiting: William Lai”, The Jamestown Foundation, *China Brief*, vol. 23, nr. 4, 03.03.2023.
8. HUGHES Christopher, *Taiwan and Chinese Nationalism: National Identity and Status in International Society*, Routledge, 1997, 208 p.
9. HUANG Jaw-Nian, ”China’s Propaganda and Disinformation Operations in Taiwan: A Sharp Power Perspective”, *China: An International Journal*, vol. 21, nr. 2, 2023, p.143–170,.
10. HUANG Chih-Jung, *Taiwan’s History and Status: Taiwan Has Never Been a Part of China,* Formosan Association for Public Affairs (FAPA), 28.11.2023, https//fapa.org/taiwans-history-and-status-taiwan-has-never-been-a-part-of-china/.
11. KASTNER L. Scott, *Political Conflict and Economic Interdependence Across the Taiwan Strait and Beyond*, Stanford University Press, 2009, 256 p.
12. LAM Willy Wo-Lap, ”Xi’s Dilemma: The Risk of Waging War Against Taiwan”, The Jamestown Foundation, *China Brief*, vol. 23, nr. 18, 04.10.2023.
13. LIN Hsiao-ting., *Accidental state: Chiang Kai-Shek, the United States, and the Making of Taiwan,* Harvard University Press, 2016, 352 p.
14. LIN Syaru Shirley., *Taiwan’s China Dilemma: Contested Identities and Multiple Interests in Taiwan’s Cross-Strait Economic Policy*, Stanford University Press, 2016, 304 p.
15. LIN Wei-Ping, *Island Fantasia: Imagining Subjects on the Military Frontline between China and Taiwan*, Cambridge University Press, 2021, 250 p.
16. LIU Wen, ”The mundane politics of war in Taiwan: Psychological preparedness, civil defense and permanent war”, *Security Dialogue*, Peace Research Institute Oslo, vol. 55, nr. 1, p. 103-122, 2023, https://doi.org/10.1177/09670106231194908.
17. MAIZLAND Lindsay, ”Why China-Taiwan Relations Are So Tense”, *Backgrounder*, Council of Foreign Relation, 08.02.2024, https//www.cfr.org/backgrounder/china-taiwan-relations-tension-us-policy-biden.
18. MAMCHII Oleksandra, *What Is the Motive of China Behind Its Interest in Taiwan?*, 03.10.2023, https://bestdiplomats.org/why-china-wants-taiwan/
19. MCGUIRE Kristian, ”Taiwan’s Offshore Islands: Assessments Of Support For Integration”, The Jamestown Foundation, *China Brief*, vol. 24, nr. 1, 05.01.2024, p.17-22.
20. MCGUIRE Kristian, ”The PRC’s “One Family” Concept and Taiwanese Views of a Cross-Strait Familial Bond”, The Jamestown Foundation, *China Brief*, vol. 23, nr. 15, 18.08.2023.
21. NACHMAN Lev, *Taiwan shows resilience amid geopolitical uncertainty*, Asia Pacific Peace Research Institute, 19.01.2023, https://eastasiaforum.org/2023/01/19/taiwan-shows-resilience-amid-geopolitical-uncertainty/

22. TING-yu Wang Alex, ”Fortifying Taiwan: Security Challenges in the Indo-Pacific Era”, The Jamestown Foundation, *China Brief*, vol. 24, nr. 4, 16.02.2024, https://jamestown.org/program/fortifying-taiwan-security-challenges-in-the-indo-pacific-era/
23. ROWEN Ian, *One China, Many Taiwans: The Geopolitics of Cross-Strait Tourism*, Cornell University Press, 2023, 200 p.
24. SCHUBERT Gunter (ed.), *Taiwan and the “China Impact”: Challenges and Opportunities*, Routledge, 2016, 334 p.
25. SZONYI Michael, *Cold War Island: Quemoy on the Front Line*, Cambridge University Press, 2009, 328 p.
26. VAN OUDENAREN John S., ”Taiwan’s Dwindling Diplomatic Allies” și Editor’s Note: Special Issue on Taiwan Under Siege, The Jamestown Foundation, *China Brief*, vol 23, nr. 8, 05.05.2023.
27. WENG Dennis LC, Jeter Jared, ”Understanding Taiwan beyond geopolitics”, *East Asia Forum Quartely*, 13.03.2024, https://eastasiaforum.org/2024/03/13/understanding-taiwan-beyond-geopolitics.
28. *** eprs@ep.europa.eu.
29. *** http://www.eprs.ep.parl.union.eu/
30. *** http://www.europarl.europa.eu/thinktank.
31. *** http://epthinktank.eu/
32. *** https://www.geopoliticalmonitor.com/
33. *** https://www.cfr.org/backgrounder.
34. *** https://eastasiaforum.org.
35. *** https://bestdiplomats.org.
36. *** https://www.agora-strategy.com.

[1] Vechi proverb chinezesc.

[2] Andrei Miroiu, cap. „Teoriile geopolitice clasice", în Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), *Manual de relaţii internaţionale,* Editura Polirom, Iaşi, 2006, p. 73-74.

[3] Idem.

[4] Teoria puterii continentale a lui H. Mackinder.

[5] Teoria puterii maritime a lui N. Spykman.

[6] Huntington Samuel, *Ciocnirea civilizațiilor și refacerea ordinii mondiale,* Editura Litera, București, 2019, p. 306.

[7] Kaplan Robert D., *Marea Chinei de Sud şi sfârşitul stabilităţii în Pacific*, Editura Litera, București, 2016, p. 26.

[8] Există Prima Conferință ONU (United Nations Convention on the Law of the Sea-UNCLOS-I) din Geneva, în 1958; A doua Conferință privind Dreptul mării (UNCLOS II) din Geneva, în 1960, și „Convenția de la Montego Bay asupra dreptului mării", din 1982, ultima marcând definitv drepturile teritoriale asupra apelor. Aceasta, prin art.2 alin.(1) arată că „Suveranitatea statului riveran se întinde dincolo de teritoriul său și de apele sale interioare, iar în cazul unui stat-arhipelag, dincolo de apele sale arhipelagice, asupra unei zone a mării adiacente desemnate sub numele de mare teritorială"; prin Art. 3 se statuează că „Orice stat are dreptul de a fixa lățimea mării sale teritoriale; această lățime nu depășește 12 mile marine, măsurate de la liniile de bază stabilite în conformitate cu prezenta convenție".

[9] Manea Constantin, Moșneagu Marian, *Dreptul mării în timp de pace,* Editura Mica Valahie, București, 2011, p. 57-58.

[10] Kenneth Waltz, *Teoria Relațiilor Internaționale,* Polirom, Iași, 2006, p. 252; John H. Herz, "Idealist Internationalism and the Security Dilemma", *World Politics,* vol. 2, ianuarie 1950, p.157-180.

[11] Apud. Vasile Simileanu, *Centre de putere, axe și falii geopolitice,* http/geopolitic.ro/2023/02/centre-de-putere-axe-si-falii-geopolitice, accesat la 12.06.2024.

[12] Cunoscut și drept Districtul Lienchiang.

[13] În perioada 1950-1960, ONU și majoritatea statelor non-comuniste recunoșteau ROC drept singurul guvern al Chinei, teritoriul controlat de PCC fiind denumit „China Roșie".

[14] Rezoluția 2758, din 1971, recunoștea oficial PRC ca reprezentant de drept al populației chineze și „expulza reprezentanții lui Chiang Kai-shek" din organizațiile și întâlnirile internaționale ale Națiunilor Unite.

[15] Doar 13 la nivelul lui 2023.

[16] Blănaru Matei, *Cel mai periculos loc de pe planetă: Taiwanul. Sau când identitatea devine o problemă de securitate,* 02.12.2012, în http://adevarul/blogurile-adevarul/cel-mai-periculos-loc-de-pe-planetă-taiwanul-sau-2136025.html, accesat la 22.07.2024. Matei Blănaru este membru asociat la Centrul de studii sino-ruse din cadrul Institutului de Științe Politice și Relații Internațiionale „Ion C. Brătianu" al Academiei Române.

[17] Idem.

[18] Blănaru Matei, *Op.cit.*

[19] Acțiunile PRC au fost denumite „Războiul de artilerie din 23 August".

[20] Kissinger Henry, *On China,* Penguin Press, New York, 2011, p. 246.

[21] „Consensul din 1992" accepta, implicit, poziția Beijingului cum că Taiwanul este parte a Chinei. Totodată, permitea tacit ca KMT și Beijingul să nu fie de acord cu definiția termenului „China", KMT susținând că acesta se referă la ROC (numele oficial al Taiwanului), iar Beijing susținând că termenul de „China" se referă la PRC.

[22] Blănaru Matei, *Op.cit.*

[23] În trecut KMT era rivalul PCC, iar în prezent este considerat un apropiat al Beijingului, dorind relații mai strânse cu China. La polul opus, DPP susține independența insulei, dar știe că o mișcare atât de radicală ar putea crea un război în Strâmtoarea Taiwan, astfel încât președinții taiwanezi aleși din acest partid preferă să păstreze statu-quo-ul.

[24] Conceptul „O familie" a fost revitalizat după venirea la putere a președintelui Xi Jinping, începând cu 2013. Cartea Albă a PRC din 1993 menționa faptul că acest concept a fost dezvoltat, în 1956, de Mao Zedong, care a afirmat că „toți patrioții reprezintă o singură familie" și „nu este târziu în a aduna toți patrioții". Declarațiile ulterioare, precum cea din 1978 a Comitetului Permanent al celui de-al Cincilea Congres Național al Poporului privind Taiwanul sau declarația lui Zeng Qinghong, membru al Comitetului Permanent al PCC, din 2005, au readus în prim-plan mențiunea că „întotdeauna poziția Bejingului a fost că toți patrioții aparțin unei singure familii".

[25] Huang Jing, „Xi Jinping's Taiwan Policy: Boxing Taiwan In with the One-China Framework", în *Taiwan and China: Fitful Embrace,* Lowell Dittmer (ed.), Berkeley, University of California Press, 2017, p. 239-248; accesat în https://doi.org/10.1515/9780520968707-014, la data de 22.06.2024.

[26] Ca să înțelegem contextul, istoria ne oferă cel mai simplu exemplu în Pen. Coreea: majoritatea războaielor sino-nipone s-au desfășurat pe teritoriul coreean, deși aceasta nu era parte beligerantă a conflictelor.

[27] Hsiao Russell, "The DPP's 2024 Presidential Candidate-in-Waiting: William Lai", The Jamestown Foundation, *China Brief,* vol. 23, nr. 4, 03.03.2023, accesat la 26.07.2024.

[28] Aceste cipuri se găsesc în majoritatea aparatelor electronice, inclusiv în smartphone-uri, computere, vehicule și în sistemele de armament care se bazează pe inteligența artificială. În 2020, companiile taiwaneze au obținut peste 60% din veniturile generate de producătorii de semiconductori de pe piața internațională.

[29] Mcguire Kristian, ”The PRC’s “One Family” Concept and Taiwanese Views of a Cross-Strait Familial Bond”, The Jamestown Foundation, *China Brief,* vol. 23, nr. 15, 18.08.2023, disponibil pe https://jamestown.org/program/the-prcs-one-family-concept-and-taiwanese-views-of-a-cross-strait-familial-bond, accesat la 11.07.2024.

[30] Biroul Consiliului de Stat al PRC, 12.09.2023.

[31] Mcguire Kristian, Taiwan’s Offshore Islands: Assessments of Support for Integration, The Jamestown Foundation, *China Brief,* vol. 24, nr. 1, 05.01.2024, disponibil pe https://jamestown.org/program/taiwans-offshore-islands-assessments-of-support-for-integration/, accesat la 13.07.2024.

[32] Idem.

[33] Blănaru Matei, Op.cit.

[34] Lam Willy Wo-Lap, ”Xi’s Dilemma: The Risk of Waging War Against Taiwan”, The Jamestown Foundation, *China Brief,* vol. 23, nr. 18, 04.10.2023, accesat la 12.07.2024.

[35] Idem.

[36] Trei Comunicate SUA-China/1972, 1978, 1982; The Taiwan Relations Act/1979; Six Assurances”/1982. Mai recent: Taiwan Travel Act (2018), Taipei Act (2020), Six Assurances into law (2021).

[37] Incisivitatea Chinei, în declarații și acțiuni, a determinat Washingtonul să declasifice garanțiile de securitate date de Administrația Reagan Taiwanului referitoare la vânzările de armament. Astfel, în cablograma transmisă în iulie 1982, SUA își manifestau disponibilitatea de a reduce vânzările de armament către Taipei, dar numai în funcție de determinarea Beijingului de a soluționa pașnic conflictul cu Taiwan. În documentul în care detalia cele șase garanții date Taipeiului (august 1982), se menționa faptul că Washingtonul nu-și va schimba poziția în privința suveranității Taiwanului și nu va exercita presiuni asupra acestuia ca administrația de la Taipei să înceapă negocierile cu Beijingul.

[38] Ting-Yu Alex Wang, ”Fortifying Taiwan: Security Challenges in the Indo-Pacific Era”, 16.02.2024, în The Jamestown Foundation, *China Brief,* vol. 24, nr. 4, accesat la 12.07.2024.

[39] Ting-Yu Alex Wang, ”Fortifying Taiwan: Security Challenges in the Indo-Pacific Era”, The Jamestown Foundation, *China Brief,* vol. 24, nr. 4, 16.02.2024, accesat la 12.07.2024.

[40] Blănaru Matei, *Op.cit.;* Lam Willy Wo-Lap, ”Xi’s Dilemma: The Risk of Waging War Against Taiwan”, The Jamestown Foundation, *China Brief,* vol. 23, nr. 18, 04.10.2023, accesat la 12.07.2024.

CONTRACARAREA AMENINȚĂRILOR HIBRIDE/ DEZINFORMĂRII CU AJUTORUL DATELOR GEOSPAȚIALE ȘI A DOMENIULUI GEOINT

Alexandru ZAMFIR*
Aurel MIHAI
Cătălin CONDURACHE
Manuela MOGA
Georgiana ȘIPOȘ

Abstract

In the contemporary security landscape, hybrid threats represent a complex and multifaceted challenge, blending conventional military tactics with unconventional methods such as disinformation and cyber attacks. Through this article, we propose to identify and present the nature of hybrid threats, exploring their various forms and the way they undermine national security. GEOINT (Geospatial Intelligence) helps countering hybrid threats using geospatial data to provide critical insights and enhance situational awareness.

This article examines how GEOINT techniques are employed to combat disinformation, highlighting the role of geospatial data in verifying information, tracking the spread of false narrative and supporting strategic responses.

Keywords: *hybrid threats; disinformation; cyber attacks; Geospatial Intelligence; geospatial data; information; imagery.*

INTRODUCERE

Recentele evoluții de securitate înregistrare în proximitatea estică a spațiului euroatlantic, caracterizate mai ales de agresiunea armată a Federației Ruse asupra Ucrainei, au evidențiat relevanța și aplicabilitatea capabilității GEOspatial INTelligence (GEOINT), în contextul ciclului informațional, încă din faza de pregătire a operațiilor ofensive. Pe lângă avantajele operaționale conferite de capabilitatea GEOINT, materializate în principal prin monitorizarea activităților militare, o altă valență este reprezentată de aportul în efortul de contracarare a unor amenințări hibride.

Din perspectiva cadrului conceptual, potrivit Agenţiei Naţionale pentru Informaţii Geospaţiale a SUA (National Geospatial Intelligence Agency – NGA), GEOINT constă în analiza şi exploatarea

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

imaginilor şi informaţiilor geospaţiale pentru a descrie, evalua şi a evidenţia vizual detaliile fizice şi activităţile referenţiate geografic de pe suprafaţa Pământului[1]. Astfel, GEOINT este o disciplină care a evoluat prin integrarea imaginilor, a IMagery INTelligence (IMINT), a datelor şi informaţiilor geospaţiale, fiind astfel o capabilitate de intelligence de natură tehnică. Localizarea geografică a datelor și informațiilor reprezintă principalul atribut funcțional al acestei capabilități, care permite optimizarea analizei multisursă, fiind utilizată ca integrator și platformă suport pentru celelalte capabilități de culegere de informații[2].

Pe de altă parte, amenințările hibride combină acțiuni militare și non-militare, precum și mijloace de culegere acoperite sau discrete, inclusiv dezinformarea, atacurile cibernetice, presiunea economică, dislocarea de grupări armate paramilitare și utilizarea forțelor convenționale. Metodele hibride sunt utilizate pentru a estompa delimitările dintre război și pace, în vederea creării unor îndoieli în mentalul colectiv al țintei. Scopul este de a destabiliza și submina societatea-țintă[3]. GEOINT contribuie la contracararea unor amenințări hibride, precum propaganda și dezinformarea, prin punerea la dispoziția beneficiarilor a unor produse informative cu o veridicitate ridicată.

Cu toate acestea, pe lângă aspectele pozitive menționate, câteva provocări pot fi atribuite disciplinei GEOINT în contextul combaterii amenințărilor hibride. Pe termen scurt, în lipsa unei verificări detaliate, datele geospațiale pot amplifica efectele dezinformării. Mai mult, datele geospațiale pot fi falsificate, fie prin manipularea celor existente, fie prin crearea unui nou context narativ.

CLASIFICAREA AMENINȚĂRIOR HIBRIDE ȘI TIPURI DE DEZINFORMARE ÎN PRIVINȚA DATELOR GEOSPAȚIALE

Amenințarea la adresa securității unui stat poate fi văzută ca o combinație între capacitate, intenție și oportunitate. Caracterul hibrid, din acest punct de vedere, rezultă din tipul de instrumente folosite.[4] De altfel, în era tehnologiei, războiul convențional tinde să fie transpus într-un plan secund, posibilii agresori recurgând la amenințări hibride.

Amenințarea hibridă reprezintă o combinație de tehnici convenționale și neconvenționale, militare și non-militare, menite să exploateze vulnerabilitățile unui stat sau organizații, într-o manieră integrată, coordonată și bine planificată.[5] Scopul principal este destabilizarea și subminarea, aceste tipuri de amenințări fiind greu de identificat și contracarat, incluzând tactici multiple și complementare, desfășurate în mod sincronizat.

Într-o analiză[6] realizată de Centrul de studii a amenințărilor asimetrice din cadrul Universității Naționale de Apărare din Suedia și de Centrul european de excelență pentru contracararea amenințărilor hibride de la Helsinki/Finlanda au fost definiți o serie de factori care stau la baza generării amenințărilor hibride:

- *globalizarea, dezvoltarea accelerată a mediului şi avansul tehnologic* – aceste fenomene au creat un mediu interconectat, dar vulnerabil, în care actorii statali/non-statali pot exploata tehnologii moderne pentru destabilizare (interferențe politice și economice, acces la resurse și rețele globale, dezvoltarea unor noi tehnologii utilizate în operații militare);
- *apariția unor noi domenii de confruntare, care nu sunt reglementate* – aceste domenii oferă oportunități de a desfășura operațiuni diverse de atac, fără ca posibilii inițiatori să se confrunte cu consecințe legale imediate (folosirea spațiului cibernetic, utilizarea inteligenței artificiale, dominarea spațiului informațional și social media);
- *exploatarea potențialului oferit de tehnologiile media noi* – aceste metode de exploatare a serviciilor online au transformat spațiul mediatic într-un instrument de influență, destabilizare și manipulare a diferitelor categorii de audiență (răspândirea propagandei și dezinformării, crearea conceptelor de deepfake, microtargeting și influențarea

opiniei publice, automatizarea influenței și exploatarea algoritmilor platformelor media);

- *delimitarea neclară dintre pace și război* – este o caracteristică definitorie a amenințărilor hibride deoarece subminează distincția tradițională dintre starea de conflict și non-conflict, operațiunile militare oficiale fiind înlocuite de instrumente neconvenționale (operațiuni ascunse, atacuri economice, război informațional)[7].

Având în vedere factorii enumerați anterior, se poate deduce că amenințările hibride sunt clasificate în funcție de obiectivul vizat pentru a fi destabilizat și modul în care se acționează. Astfel, principalele tipuri de amenințări hibride[8] sunt considerate următoarele:

- *amenințări informaționale* – sunt realizate prin intermediul rețelelor sociale și au ca scop manipularea opiniei publice și influențarea comportamentului social, politic și economic, prin răspândirea de informații false sau distorsionate/metodele cele mai întâlnite în atacul informațional sunt campaniile de dezinformare, propaganda, crearea de conturi false sau operațiuni psihologice (PSYOPS);
- *amenințările cibernetice* – sunt atacuri care vizează infrastructura cibernetică a statelor sau companiilor prin intermediul cărora sunt compromise date sensibile sau operațiuni de securitate și sunt perturbate servicii esențiale/ principalele metode utilizate în cazul acestor amenințări sunt hacking și malware, atacuri DDoS sau phishing;
- *amenințări economice și comerciale* – sunt utilizate acțiuni de destabilizare a economiei pentru a influența politica externă a statului sau pentru a destabiliza societatea/ în acest caz sunt folosite embargourile și sancțiunile economice, manipularea cursului valutar, restricționarea comerțului;
- *amenințări politice și diplomatice* – presupun manipularea proceselor politice și democratice interne ale unui stat/ cel mai des sunt utilizate sprijinirea grupurilor politice extremiste, presiuni externe și intervenții ilegale în procesul electoral;
- *amenințări militare neconvenționale* – implică folosirea unor grupuri paramilitare sau tactici de război neconvențional pentru a destabiliza o regiune fără a implica direct forțele armate/ pentru acest tip de amenințare se recurge la mercenari, tactici de gherilă sau tactici teroriste asupra civililor.

În contextul prezentat, dezinformarea reprezintă un vector al amenințărilor hibride. Această formă de amenințare se definește prin diseminarea deliberată a informațiilor false cu scopul de a manipula percepții, a influența decizii și a genera confuzie sau instabilitate socială, politică și economică. În urma sondajelor realizate de Comisia Europeană a rezultat că dezinformarea devine un motiv de îngrijorare în rândul cetățenilor europeni, 51% dintre aceștia fiind expuși la acest fenomen în mediul online, în timp ce 63% reușesc să descopere știri false de câteva ori pe săptămână[9]. Informația falsă poate fi propagată prin diverse canale, inclusiv mass-media, rețele sociale, agenții de știri sau surse aparent independente. De asemenea, dezinformarea poate fi folosită în orice domeniu, inclusiv în domeniul apărării, cu scopul de a distorsiona realitatea informației.

Un exemplu potrivit în acest sens este *manipularea sau exploatarea datelor geospațiale în cadrul campaniilor de dezinformare*. Datele geospațiale sunt informații critice în analiza și interpretarea evenimentelor globale, precum conflicte armate, crize umanitare, mișcarea populației sau activități cu caracter armat. Astfel, dezinformarea legată de datele geospațiale poate lua multiple forme[10]:

- *manipularea imaginilor satelitare* – datele geospațiale pot fi manipulate prin editarea sau prezentarea parțială a informațiilor, fiind create percepții eronate despre o situație militară sau geopolitică;
- *geolocalizarea falsă a evenimentelor* – asocierea incorectă a unui eveniment/ incident cu o anumită locație geografică,

folosind date geospațiale false sau distorsionate pentru a induce în eroare;
- *distorsionarea hărților* – hărțile pot fi manipulate pentru a reflecta o realitate falsă a terenului prin exagerarea unor elemente (unități de relief, căi de comunicații etc.), omiterea altora sau prezentarea incorectă a poziției informației geografice în teren;
- *falsificarea datelor de mediu/climatice* – implică manipularea unor date despre schimbări climatice, defrișări, poluare sau dezastre naturale pentru a susține anumite agende politice sau economice;
- *dezinformarea legată de migranți sau crize umanitare* – datele geospațiale pot fi folosite pentru a exagera sau minimiza amploarea fluxurilor de migranți sau a crizelor umanitare, modificând implicit percepția asupra unui conflict sau a unei regiuni afectate.

PROVOCĂRI TEHNOLOGICE ȘI RISCURI LA CARE SUNT EXPUSE DATELE GEOSPAȚIALE

Tehnologiile avansate, precum inteligența artificială, sateliții geospațiali sau aplicațiile specializate de analiză și gestionare a datelor geospațiale, au devenit instrumente importante în combaterea amenințărilor hibride și a dezinformării. Aceste inovații tehnologice au capacitatea de a monitoriza și analiza volume masive de date în timp real. Cu toate acestea, trecerea rapidă la era tehnologică aduce în prim-plan un spectru larg de provocări și limitări care necesită o analiză atentă.

Inteligența artificială (AI) este utilizată pe scară largă pentru monitorizarea și analiza volumelor mari de date, inclusiv pentru detectarea unor acțiuni suspecte, tipare anormale și pentru prevenirea dezinformării. AI oferă o serie de oportunități esențiale: *viteză și rezistență* – capacitatea de a colecta informații rapid, pe zone de interes mari și pe perioade lungi de timp, detectând în mod automat nereguli; *scalare* – AI contribuie la îmbunătățirea capacităților de gestionare și analiză, prin utilizarea unor sisteme performante; *superioritate informațională* – crește exponențial cantitatea de date disponibile pentru analiză[11].

Cu toate avantajele sale, inteligența artificială se confruntă cu anumite provocări care influențează eficiența acesteia:
- *manipularea algoritmilor de prelucrare*: actorii ostili pot introduce date corupte sau informații false în sistemele AI, ceea ce poate conduce la interpretări eronate și, în final, la luarea unor decizii greșite;
- *limitări în detectarea dezinformării*: dezinformările geospațiale, cum ar fi manipularea hărților sau a imaginilor din satelit, care conțin deepfake sau geofalsificare, sunt greu de identificat pentru că necesită interpretarea unui context vast și divers;
- *automatizarea atacurilor*: aceleași tehnologii AI care sunt utilizate pentru apărare pot fi folosite de adversari pentru automatizarea atacurilor cibernetice și pentru crearea unor campanii de dezinformare personalizate, mult mai rapide și mai precise.

Geosateliții reprezintă una dintre cele mai importante tehnologii geospațiale utilizate pentru monitorizarea și analizarea activităților. Aceștia au cunoscut o dezvoltare accelerată, oferind imagini și date precise din spațiu esențiale pentru monitorizarea mediului.

Figura 1: *Geosatelit*[12]

Primele generații de sateliți geospațiali au fost dezvoltate în anii 1960 pentru scopuri militare și de supraveghere. Aceștia au evoluat,

în timp, de la simple dispozitive de colectare a datelor la platforme sofisticate care utilizează senzori avansați pentru a obține imagini de înaltă rezoluție ale suprafeței Pământului. Dezvoltările tehnologice au permis ca sateliții să ofere informații esențiale nu doar pentru apărare, dar și pentru activități civile[13]. În perioada anilor 1980–1990 avansul în tehnologia de detecție la distanță și miniaturizarea componentelor au permis creșterea rezoluției și acurateței imaginilor satelitare, iar în ultimele două decenii dezvoltarea sateliților comerciali, cum ar fi cei din programul Landsat, a deschis accesul la date satelitare și pentru organizațiile private, facilitând utilizarea lor într-o gamă largă de aplicații[14].

În contextul amenințărilor hibride și al dezinformării, sateliții geospațiali joacă un rol important, fiind capabili de a monitoriza infrastructurile critice, cum ar fi rețelele de energie sau conductele de gaz, detectând activități suspecte sau întreruperi. De asemenea, sateliții pot fi utilizați pentru a evalua mișcările militare și civile, oferind o sursă de informații independentă care contracarează dezinformările[15].

Deși sateliții geospațiali oferă beneficii enorme, aceștia se confruntă și cu provocări semnificative:

- *manipularea datelor* – imaginile și datele furnizate de sateliți pot fi manipulate sau interpretate greșit pentru a susține campanii de dezinformare: de exemplu, imaginile satelitare pot fi alterate pentru a prezenta o realitate falsă, cum ar fi mișcări militare inexistente sau daune climatice falsificate/această manipulare poate afecta răspunsurile guvernelor și/sau alimenta instabilitatea regională;
- *vulnerabilitatea la atacuri cibernetice* – infrastructurile de satelit sunt vulnerabile la atacuri cibernetice, care pot compromite atât comunicațiile, cât și datele geospațiale colectate: de exemplu, perturbarea rețelelor satelitare sau preluarea controlului asupra acestora poate afecta dramatic capacitățile de monitorizare și poate produce daune strategice semnificative;
- *accesul la date comerciale* – sateliții comerciali oferă posibilitatea publicului larg de a avea acces la imagini, ceea ce favorizează utilizarea acestor date pentru operațiuni de dezinformare și atacuri hibride.

Aplicațiile dedicate pentru analiza geospațială integrează date provenite din surse diverse, cum ar fi drone, sateliți și senzori tereștri, oferind o imagine detaliată și complexă a mediului. Acestea sunt folosite pentru a monitoriza mișcările de populații, schimbările climatice, precum și pentru a analiza potențialele amenințări.

O provocare majoră este interoperabilitatea între diferitele platforme care colectează și procesează aceste date. Sistemele trebuie să fie capabile să colaboreze eficient, iar protecția datelor împotriva atacurilor cibernetice este esențială pentru asigurarea securității naționale.

Dintre cele mai utilizate aplicații pot fi amintite următoarele:

- *Copernicus Emergency Management Service* (CEMS) – platforma face parte din programul Copernicus al Uniunii Europene și oferă sprijin în situații de urgență, oferind imagini din satelit pentru a evalua impactul dezastrelor naturale sau conflictelor[16];
- *Mapbox* – este o platformă pentru vizualizarea și personalizarea hărților digitale, fiind adesea utilizată pentru a crea hărți interactive în aplicații mobile și web[17];
- *Planet Labs* – oferă acces la date satelitare actualizate zilnic, cu rezoluție de până la 3-5 metri/aceste imagini sunt utilizate pentru monitorizarea infrastructurii critice, dar și pentru evaluarea schimbărilor climatice și a impactului economic[18];
- *Sentinel Hub* – este o aplicație care permite accesul la datele din sateliții programului Sentinel al Uniunii Europene, parte a Copernicus, oferind imagini de înaltă rezoluție, și poate fi utilizată pentru monitorizarea terenurilor, mediului și dezvoltării infrastructurii[19].

Cu toate acestea, aplicațiile și platformele dedicate datelor geospațiale prezintă anumite vulnerabilități:

- *interoperabilitatea între diferite tehnologii:* integrarea eficientă a datelor geospațiale din surse multiple (de exemplu, sateliți, drone, senzori terestri) reprezintă o provocare majoră/ lipsa interoperabilității între platforme poate crea lacune în colectarea și analiza datelor, slăbind capacitatea de a răspunde eficient la amenințările hibride;
- *volumul masiv de date:* colectarea de date geospațiale prin sateliți, AI și aplicații dedicate generează un volum enorm de informații care trebuie procesat într-un timp cât mai scurt/gestionarea și analiza acestor date la scară mare este o provocare logistică și tehnologică, necesitând infrastructuri robuste și capacități avansate de big data și AI pentru a extrage informații relevante dintr-o cantitate mare de date neprelucrate;
- *securitatea datelor:* protecția datelor colectate împotriva accesului neautorizat sau atacurilor cibernetice este o provocare critică/ orice breșă de securitate în sistemele care gestionează date geospațiale poate conduce la scurgeri de informații sau la decizii eronate care afectează securitatea națională.

CUM CONTRACAREAZĂ GEOINT DEZINFORMAREA

GEOINT (Geospatial Intelligence) este o formă de culegere de informații care utilizează date geospațiale pentru a analiza și interpreta locații geografice și fenomene asociate. În lupta împotriva dezinformărilor și în remodelarea spațiului geografic și informațional, GEOINT joacă un rol important în următoarele moduri:

1. Contracararea dezinformărilor

Monitorizarea și verificarea evenimentelor în timp real: folosind imagini din satelit și alte date geospațiale, GEOINT poate să verifice rapid dacă o informație este adevărată sau falsă. De exemplu, în timpul unui conflict, dacă o parte publică informații false despre o bătălie sau un atac, imaginile satelitare pot confirma sau infirma evenimentele raportate.

Maparea rețelelor de dezinformare: analizând locațiile geografice din care provine dezinformarea sau zonele unde aceasta are cel mai mare impact, GEOINT ajută la identificarea surselor și la contracararea acestora prin expunerea și demascarea știrilor false.

Identificarea și urmărirea manipulării vizuale: în epoca actuală, imaginile și videoclipurile false pot fi folosite pentru a amplifica dezinformarea; GEOINT poate verifica autenticitatea acestor materiale prin compararea lor cu date geospațiale existente și identificarea discrepanțelor[20].

2. Remodelarea spațiului geografic și informațional

Vizualizarea dinamică a schimbărilor: GEOINT permite vizualizarea dinamică a schimbărilor geografice și sociale, cum ar fi mutările populațiilor sau infrastructura distrusă în zonele de conflict; aceste informații ajută guvernele și organizațiile internaționale să ia decizii bine fundamentate, contribuind la reducerea efectelor negative ale războiului sau crizelor umanitare.

Sprijinirea operațiunilor de securitate și militare: informațiile geospațiale sunt esențiale pentru planificarea și executarea operațiunilor militare și de securitate; prin furnizarea de date exacte despre teren, climă și infrastructură sau forțe armate adverse, GEOINT îmbunătățește capacitatea de reacție și prevenire a conflictelor, minimizând vulnerabilitățile create de lipsa informațiilor clare.

Detecția și prevenția activităților maligne: de exemplu, în cazul unor operațiuni de propagare a minciunilor, cum ar fi crearea de baze fictive sau desfășurarea de activități ilegale (ex: mineritul ilegal sau defrișările), GEOINT poate detecta schimbările fizice care indică astfel de activități, oferind dovezi vizuale concrete.

3. Reconfigurarea contextului geopolitic

Anticiparea mișcărilor strategice: GEOINT poate ajuta la anticiparea și înțelegerea mișcărilor strategice, prin monitorizarea poziționării militare, economice și a fluxurilor migratorii;

acest lucru influențează răspunsurile statelor și organizațiilor internaționale, remodelând alianțele și strategiile globale.

Integrarea datelor multidimensionale: GEOINT nu se limitează doar la imagini satelitare, ci integrează și alte surse de date, cum ar fi datele de mediu, sociale și economice, pentru a oferi o imagine cuprinzătoare asupra unui spațiu geografic; această abordare multidimensională influențează luarea deciziilor la nivel guvernamental și internațional[21].

Prin aceste contribuții, GEOINT joacă un rol critic în combaterea dezinformărilor și în remodelarea spațiului geospațial, permițând o înțelegere mai profundă a contextelor reale și sprijinind acțiuni strategice eficiente[22]. Un exemplu semnificativ de dezinformare contracarată de GEOINT cu ajutorul imaginilor satelitare în timpul conflictului din Ucraina a avut loc în 2022, în orașul Bucea, la nord-vest de Kiev. În contextul retragerii forțelor armate ruse din acea localitate, în martie 2022, au apărut rapoarte și imagini despre masacre în care sute de civili au fost uciși. Imaginile din oraș au arătat cadavrele civililor pe străzi și dovezi ale execuțiilor sumare. Apelând la dezinformare, Rusia a negat responsabilitatea pentru crimele de la Bucea susținând că imaginile incriminante sunt de fapt o punere în scenă realizată de Ucraina pentru a compromite imaginea Rusiei, deoarece trupele sale ar fi părăsit orașul înainte ca respectivele imagini să apară în media. Însă, prin intermediul GEOINT și a imaginilor satelitare realizate de compania Maxar Technologies a fost demonstrat contrariul. Aceste imagini, realizate în prima jumătate a lunii martie 2022, au arătat clar prezența cadavrelor pe străzile din Bucea, cu săptămâni înainte de retragerea trupelor ruse. Cadavrele din imaginile satelitare au fost georeferențiate, acestea corespunzând pozițiilor și locațiilor observate în fotografiile și înregistrările video apărute mai târziu, după eliberarea orașului[23].

Figura 2: *Analiză de imagini*

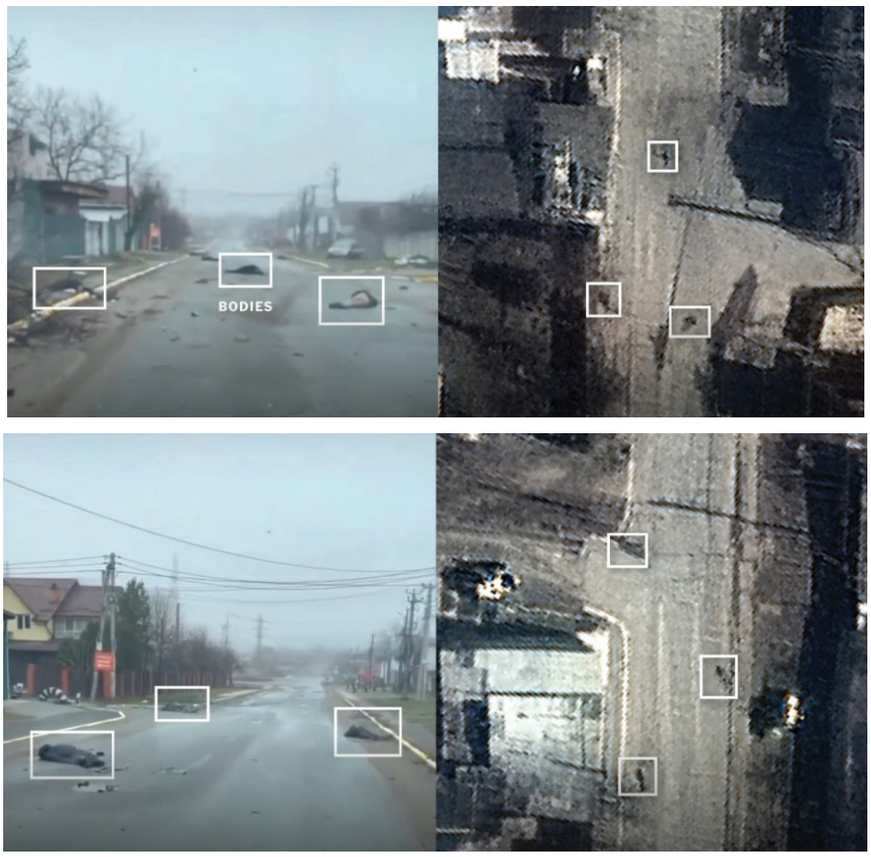


Figura 3: *Analiză de imagini*

Figura 4: *Analiză de imagini*

Astfel, GEOINT-ul a demonstrat că masacrul din Bucea a avut loc în timp ce forțele ruse controlau orașul, contrazicând narativul promovat de autoritățile ruse. Această dovadă vizuală a fost esențială pentru demascarea încercărilor de dezinformare și pentru stabilirea cronologiei reale a evenimentelor.

PROVOCĂRI MAJORE ACTUALE ȘI VIITOARE

Deși GEOINT este un domeniu esențial pentru securitatea națională, oferind informații critice prin analiza datelor geospațiale și a imaginilor satelitare, acesta se confruntă cu provocări majore

actuale și viitoare, care trebuie gestionate pentru a rămâne eficient în fața noilor amenințări globale. Una dintre principalele provocări în domeniu este reprezentată de volumul și diversitatea datelor existente. Odată cu creșterea numărului de sateliți comerciali și militari, drone și alte surse de colectare a datelor geospațiale, volumul de informații colectate a crescut exponențial. Acest lucru creează provocări în gestionarea, procesarea și interpretarea rapidă a acestor date. În plus, această diversitate a surselor de date (imagini satelitare, drone, senzori terești, date de la utilizatori) generează informații geospațiale cu formate și rezoluții diferite, ceea ce face dificilă integrarea și analiza coerentă.

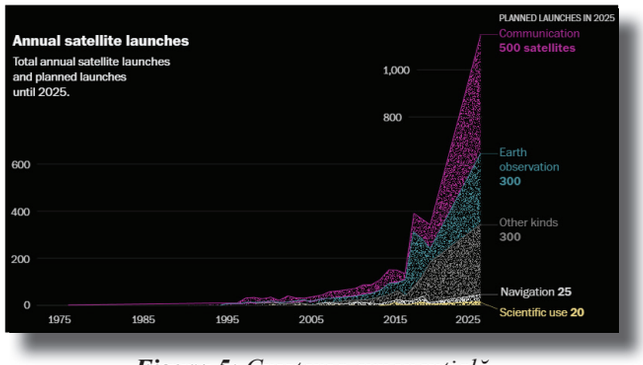


Figura 5: *Creșterea exponențială a numărului de sateliți lansați*[24]

Având în vedere aceste aspecte, intervine necesitatea automatizării fluxurilor de lucru. Cu un volum foarte mare de date avute la dispoziție, analiza manuală devine foarte greoaie. Provocarea constă în dezvoltarea de algoritmi de inteligență artificială și învățare automată, capabili să proceseze rapid și eficient datele, identificând informații relevante pentru îndeplinirea misiunilor specifice de securitate. O altă provocare o reprezintă răspunsul în timp real la nevoile de informații. Multe misiuni de securitate necesită decizii rapide, bazate pe date în timp real. Capacitatea de a procesa și analiza rapid fluxuri continue de date constituie o provocare majoră pentru viitorul GEOINT.

În contextul provocărilor și limitărilor întâlnite în domeniu este de menționat și securitatea și integritatea datelor. Astfel, la fel ca în alte domenii, sistemele GEOINT sunt vulnerabile la atacuri cibernetice care pot compromite sau manipula datele geospațiale. Asigurarea securității acestor sisteme și protecția împotriva interferenței externe reprezintă o prioritate. Este recomandată verificarea autenticității datelor deoarece manipularea acestora, cum ar fi falsificarea imaginilor satelitare (deepfake geospațial), poate duce la dezinformare. Din această perspectivă, verificarea autenticității și integrității datelor este o provocare tot mai importantă.

Deepfake-ul geospațial reprezintă o aplicație relativ nouă și sofisticată a tehnologiilor de inteligență artificială și învățare automată, utilizată pentru a falsifica sau manipula date geospațiale, inclusiv imagini satelitare, hărți și modele tridimensionale ale terenurilor. Acest concept este derivat din tehnologia deepfake, folosită inițial pentru manipularea imaginilor și videoclipurilor cu fețe umane, extins acum la domeniul geospațial. Aplicația folosește algoritmi avansați de AI, cum ar fi rețelele generative adversariale (GAN - Generative Adversarial Networks), pentru a crea imagini și date geospațiale sintetice sau modificate care par realiste. Astfel, aceste tehnologii sunt capabile să modifice caracteristicile geospațiale existente. De exemplu, se poate edita o imagine satelitară pentru a elimina structuri (clădiri, drumuri) sau a adăuga altele noi, care nu există în realitate, sau pot genera de la zero imagini sau hărți complet false ale unor zone, care par autentice, inducând în eroare analiștii și factorii de decizie.

Exemple de deepfake-uri geospațiale:

- *manipularea imaginilor satelitare*: un deepfake geospațial poate modifica imagini satelitare pentru a ascunde infrastructura militară, adăugând clădiri inexistente sau eliminând structuri existente (de exemplu, baze militare, depozite de armament)/ acest lucru poate induce o falsă percepție asupra pregătirii militare sau intențiilor unui stat;
- *crearea de hărți false*: hărțile pot fi modificate pentru a reflecta în mod eronat distribuția geografică a resurselor naturale, a densității populației sau a granițelor, aspecte ce pot fi folosite în conflicte teritoriale sau pentru manipularea deciziilor politice și economice;

- *simularea unor evenimente naturale*: se pot genera imagini false ale unor dezastre naturale (inundații, incendii, cutremure) care nu s-au produs în realitate, dar care pot fi utilizate pentru a dezinforma publicul sau pentru a manipula răspunsul internațional la o criză.

Aceste deepfake-uri geospațiale pot conduce la următoarele riscuri:

- *dezinformare strategică*: aceste falsificări pot fi folosite de actori statali sau non-statali pentru a lansa campanii de dezinformare, influențând opinia publică, instituțiile guvernamentale și organizațiile internaționale/ de exemplu, manipularea datelor geospațiale poate crea percepții eronate despre conflicte teritoriale sau resurse strategice;
- *răspuns militar greșit*: un deepfake geospațial poate induce în eroare analiștii militari, determinându-i să ia decizii strategice eronate bazate pe date falsificate/ de exemplu, manipularea imaginilor satelitare ale mișcărilor de trupe sau ale infrastructurii militare poate duce la o interpretare greșită a amenințărilor reale;
- *pierderi economice și impact asupra afacerilor*: în domeniul industrial, deepfake-urile geospațiale pot manipula date despre locația resurselor naturale (precum petrol, gaze sau minerale), generând investiții greșite sau afectarea piețelor financiare;
- *supravegherea și securitatea națională*: sistemele de supraveghere și securitate care se bazează pe date geospațiale, inclusiv sateliții ISR (Intelligence, Surveillance, Reconnaissance), pot fi vulnerabile la atacuri de tip deepfake, slăbind capacitatea de apărare a unui stat.

Pentru a detecta aceste deepfake-uri este necesară implementarea unor măsuri (ce conduc, la rândul lor, la apariția unor provocări tehnologice) precum dezvoltarea de algoritmi avansați capabili să identifice anomalii subtile în datele geospațiale (cum ar fi neconcordanțele în texturi, umbre sau perspective), utilizarea de surse multiple de date (imagini radar, senzori de la sol, informații din sateliți de diferite tipuri), pentru a verifica autenticitatea imaginilor, datelor geospațiale în timp real, pentru a preveni eventuale decizii greșite

Revenind la principalele provocări în domeniu, trebuie luate în calcul și accesibilitatea și democratizarea datelor geospațiale. Creșterea numărului de sateliți comerciali și accesul public la imagini satelitare de înaltă rezoluție ridică provocări legate de controlul și confidențialitatea datelor. Oricine poate accesa informații care nu cu mult timp în urmă erau disponibile doar pentru instituții guvernamentale. Mai mult decât atât, cooperarea între agențiile de informații, guverne și companii private poate fi dificilă din cauza politicilor diferite de confidențialitate și securitate a datelor.

CONCLUZII

Evoluția tehnologică rapidă, reglementările și problemele legale în vigoare încă nesoluționate, manipularea și dezinformarea realizate de către actori statali sau non-statali și accesul restricționat la date (în contexte geopolitice tensionate accesul la date geospațiale poate fi limitat sau restricționat de anumite state, ceea ce poate afecta capacitatea de răspuns rapid la amenințări) pot influența deciziile politice, militare și economice, iar detectarea și prevenirea lor va necesita o combinație de tehnologii avansate și colaborare internațională între agenții de informații și de securitate.

Nu în ultimul rând, trebuie subliniat faptul că domeniul GEOINT necesită specialiști capabili să integreze și să analizeze date geospațiale complexe. Formarea de experți și actualizarea constantă a competențelor acestora este o provocare continuă.

În acest context, se poate afirma că GEOINT se confruntă cu provocări semnificative, în special din cauza ritmului accelerat al evoluțiilor tehnologice, al volumului și complexității datelor și al amenințărilor cibernetice și geopolitice, iar viitorul acestui domeniu va depinde de capacitatea de a integra noile tehnologii, de a proteja datele și de a forma experți capabili să navigheze aceste provocări complexe.

BIBLIOGRAFIE

1. ALEXANDRESCU Grigore, *Amenințări la adresa securității*, Centrul de Studii Strategice de Apărare și Securitate, Editura Universității Naționale de Apărare, 2004, 24 p.
2. BABER Chris, Ian Apperly, Emily McCormick, „Understanding The Problem Of Explanation When Using AI In Intelligence Analysis", *CREST Report*, Centre for Research and Evidence on Security Threats, Economic and Social Research Council, Marea Britanie, iunie 2021, 68 p., https://crestresearch.ac.uk/resources/understanding-the-problem-of-explanation-when-using-ai-in-intelligence-analysis/, accesat în data de 26.08.2024.
3. BENJAMIN David, "GEOINT and Disinformation – A Tool for Verifying Truth", Geospatial World, 2022, https://www.geospatialworld.net.
4. BESKOW David M., Kathleen M. Carley, "Future Geospatial Disinformation Campaigns", Army Cyber Institute, *The Cyber Defense Review*, nr. 2, vol. 4, West Point Press, 2019, p 131-137.
5. BOTEZATU Ulpia-Elena, "Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-based Vulnerabilities", *Romanian Cyber Security Journal*, vol. 5, nr. 1, 2023, p. 67-76.
6. BROWNE Malachy, David Botti, Haley Willis, "Satellite Images Show Bodies Lay in Bucha for Weeks, Despite Russian Claims", *The New York Times*, 4 aprilie 2022, https://www.nytimes.com/04/04/world/europe/bucha-ukraine-bodies-html., accesat la 05.07.2024.
7. Comisia Europeană, *Cadrul comun privind contracararea amenințărilor hibride*, Comunicare comună către Parlamentul European și Consiliu, 2016.
8. FRUNZETI Teodor, Bărbulescu Cristian, „Reziliența națională la amenințările hibride și cultura de securitate. Un cadru de analiză", *Impact strategic*, nr. 1-2, Centrul de Studii Strategice de Apărare și Securitate, Editura Universității Naționale de Apărare, 2018, p. 16-26.
9. GRĂDINARU Cătălin, „GEOINT – capabilitate specifică secolului XXI", în *Infosfera. Revistă de studii de securitate și informații pentru apărare*, vol. 2, nr. 2, 2010, p. 70-77.
10. HERN Alex, "Satellites images of corpses in Bucha contradict Russian claim", *The Guardian*, 5 aprilie 2022, https://www.theguardian.com/world/2022/apr/05/satellites-images-of-corpses-in-bucha-prove-russian-claim-wrong, accesta la 23.07.2024.
11. LUPULESCU Georgiana-Daniela, „Hibrid - concept definitoriu al războaielor, operațiilor și amenințărilor specific secolului 21", *Buletinul Universității Naționale de Ap*ărare *„Carol I"*, nr. 2, 2023, p. 56-68.
12. McCARTHY Niall, "How Satellite Imagery is Used to Expose Disinformation", *Forbes*, 2020.
13. STEPHENSON Richard, "GEOINT's Role in the Modern Information Environment", National Geospatial-Intelligence Agency (NGA), 2021.
14. TREVERTON F. Gregory, Andrew Thvedt, Alicia R. Chen, Kathy Lee, Madeline McCue, *Addressing Hybrid Threats*, Swedish Defence University, 2018, 92 p., disponibil la adresa https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf., accesat în data de 28.08.2024.
15. WHALEN Jeanne, Robyn Dixon, Mary Ilyushina, "Russia denies and deflects in reaction to Bucha atrocities", *The Washington Post,* 4 aprilie 2022*,* disponibil pe www.washingtonpost.com/world/2022/04/04/russia-bucha-atrocities-war-crimes/, accesat la data de 02.09.2024.
16. *** National Geospatial-Intelligence Agency, *Geospatial Intelligence (GEOINT) Basic Doctrine*, *Publication 1.0*, 2018, 48 p., disponibil on-line la https://www.nga.mil/ProductsServices/Pages/GEOINT-Basic-Doctrine-Publication. Aspx, accesat în data de 28.08.2024.
17. *** https://www.nato.int/cps/en/natohq/topics_156338.htm, accesat în data de 26.08.2024.
18. *** https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european, accesat în data de 28.08.2024.

19. democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_ro, accesat în data de 30.08.2024.
20. https://www.internetmobile.ro/provocari-si-limitari-in-utilizarea-inteligentei-artificiale/, accesat în data de 30.08.2024.
21. https://gisgeography.com/landsat/, accesat în data de 01.09.2024.
22. https://www.nga.mil/, accesat în data de 01.09.2024.
23. https://earth.esa.int/eogateway/missions/landsat, accesat în data de 01.09.2024.
24. https://www.usgs.gov/, accesat în data de 01.09.2024.
25. https://emergency.copernicus.eu/, accesat în data de 02.08.2024.
26. https://www.mapbox.com/, accesat în data de 02.09.2024.
27. https://www.planet.com/, accesat în data de 02.09.2024.
28. https://www.sentinel-hub.com/, accesat în data de 03.09.2024.
29. https://www.washingtonpost.com, accesat în data de 03.09.2024.

[1] Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0, 2018, p. 4, disponibil online la https://www.nga.mil/ProductsServices/ Pages/GEOINT-Basic-Doctrine-Publication. Aspx.

[2] Cătălin Grădinaru, „GEOINT – capabilitate specifică secolului XXI", în *Infosfera. Revistă de studii de securitate și informații pentru apărare,* vol. 2, nr. 2, 2010, p. 70-77.

[3] https://www.nato.int/cps/en/natohq/topics_156338.htm.

[4] Georgiana-Daniela Lupulescu, „Hibrid - concept definitoriu al războaielor, operațiilor și amenințărilor specifice secolului 21", *Buletinul Universității Naționale de Apărare „Carol I"*, nr. 2, 2023, București, p. 60.

[5] Comisia Europeană, *Cadrul comun privind contracararea amenințărilor hibride*, Comunicare comună către Parlamentul European și Consiliu, 2016.

[6] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, Madeline McCue, *Addressing Hybrid Threats*, Swedish Defence University, 2018, disponibil la adresa https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf.

[7] Ibidem.

[8] Grigore Alexandrescu, *Amenințări la adresa securității*, Centrul de Studii Strategice de Apărare și Securitate, Editura Universității Naționale de Apărare, 2004, 24 p.

[9] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_ro

[10] David M. Beskow, Kathleen M. Carley, "Future Geospatial Disinformation Campaigns", *The Cyber Defense Review*, vol. 4, nr. 2, Army Cyber Institute, West Point Press, 2019 și Ulpia-Elena Botezatu, „Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-based Vulnerabilities", *Romanian Cyber Security Journal*, vol. 5, nr. 1, 2023, p. 67-76.

[11] Pentru detalii suplimentare a se consulta site-ul https://www.internetmobile.ro/provocari-si-limitari-in-utilizarea-inteligentei-artificiale/, precum și articolul lui Chris Baber, Ian Apperly, Emily McCormick, „Understanding The Problem Of Explanation When Using AI In Intelligence Analysis", *CREST Report*, Centre for Research and Evidence on Security Threats, Economic and Social Research Council, Marea Britanie, iunie 2021, https://crestresearch.ac.uk/resources/understanding-the-problem-of-explanation-when-using-ai-in-intelligence-analysis/

[12] https://gisgeography.com/landsat/

[13] https://www.nga.mil/

[14] https://earth.esa.int/eogateway/missions/landsat

[15] https://www.usgs.gov/

[16] https://emergency.copernicus.eu/

[17] https://www.mapbox.com/

[18] https://www.planet.com/

[19] https://www.sentinel-hub.com/

[20] Niall McCarthy, „How Satellite Imagery is Used to Expose Disinformation", *Forbes*, 2020.

[21] Richard Stephenson, „GEOINT's Role in the Modern Information Environment", National Geospatial-Intelligence Agency (NGA), 2021.

[22] Benjamin David, „GEOINT and Disinformation – A Tool for Verifying Truth", Geospatial World, 2022.

[23] Malachy Browne, David Botti, Haley Willis, „Satellite Images Show Bodies Lay in Bucha for Weeks, Despite Russian Claims", *The New York Times*, 4 aprilie 2022, https://www.nytimes.com/04/04/world/europe/bucha-ukraine-bodies-html., accesat la 05.07.2024; Alex Hern, "Satellites images of corpses in Bucha contradict Russian claim", *The Guardian*, 5 aprilie 2022, https://www.theguardian.com/world/2022/apr/05/satellites-images-of-corpses-in-bucha-prove-russian-claim-wrong, accesta la 23.07.2024; Jeanne Whalen, Robyn Dixon, Mary Ilyushina, „Russia denies and deflects in reaction to Bucha atrocities", *The Washington Post*, 4 aprilie 2022, disponibil pe www.washingtonpost.com/world/2022/04/04/russia-bucha-atrocities-war-crimes/, accesat la data de 02.09.2024.

[24] ***, Space junk is out of control. Here`s why – and what to do about it, *The Washington Post*, 2 noiembrie 2023, www.washingtonpost.com/opinions/interactive/2023/ space-junk-dbris-removal/

ROLUL SIGINT ÎN CADRUL ARHITECTURII NAȚIONALE DE SECURITATE

George-Daniel BOBRIC*

Abstract

In an era of technological developments that significantly impact every domain, regardless of their nature, the need for knowledge represents a ubiquitous human peculiarity, driving complex, comprehensive, multi-domain and rapid efforts to collect data and information. Though seemingly anachronistic yet whit a potentially illustrious future, SIGINT represents a critical tool providing military and politico-military decision-makers at all the hierarchical levels with the key information needed to support their future decisions and actions.

In this context, the aim of this paper is to offer an overall perspective of the role and place of SIGINT within the national security architecture. Accordingly, notional elements will be presented, as well as its relationship with other intelligence collection domains, the importance of using this resource in order to fulfill the need for strategic knowledge, a retrospection analysis of the role of SIGINT during the Second World War and potential future opportunities and threats to this domain.

Keywords: *SIGINT; electromagnetic environment; information; national security.*

ASPECTE GENERICE

Domeniul SIGINT, cu o istorie bogată și cu o semnificativă relevanță în prezent, constituie una dintre cele mai importante ramuri ale activității de intelligence, într-o perioadă caracterizată de eforturi susținute de inovare a tehnologiilor de comunicații și informatică. Cu primele acțiuni specifice SIGINT înregistrate la începutul secolului anterior, acest domeniu a căpătat o relevanță ridicată pe timpul celor două conflagrații mondiale care au modelat arhitectura de (in) securitate specifică secolului XX, devenind în prezent o modalitate prin care decidenților le pot fi furnizate o serie de informații acționabile, cu un grad ridicat de acuratețe și veridicitate, imposibil a fi obținute prin alte mijloace și metode distincte.

Potrivit literaturii de specialitate, domeniul SIGINT este format din două ramuri principale: COMINT (Comunications Intelligence) - constituie activitatea de culegere, analizare și procesare a comunicațiilor dintre diferite persoane sau grupuri/entități/organizații pentru a sustrage informații referitoare la activitățile desfășurate/ planificate de acestea, și ELINT (Electronic Intelligence) - reprezintă acțiunile de colectare și analizare a emisiilor specifice diverselor sisteme electronice (radare, dispozitive de telemetrie, balize ș.a.). Pe fondul inovărilor tehnologice, în ultimul deceniu se discută și despre o a treia ramură a SIGINT, reprezentată de FISINT

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

(Foreign Instrumentation Signals Intelligence) - culegerea și procesarea emisiilor specifice testării și operaționalizării anumitor sisteme tehnice (precum sistemele de armament aeriene, terestre, navale sau aflate în submersiune)[1].

RELAȚIA DINTRE SIGINT ȘI CELELALTE DISCIPLINE DE CULEGERE A INFORMAȚIILOR

În literatura de specialitate[2] se identifică, alături de SIGINT, alte patru discipline principale de culegere a informațiilor, astfel:

✓ HUMINT – culegerea de informații din surse umane. O disciplină de o relevanță deosebită până la momentul marilor descoperiri tehnologice specifice secolului XX, cu un impact ridicat în arhitectura de ansamblu a intelligence-ului modern, HUMINT se intercalează cu disciplinele tehnice de culegere a informațiilor, inclusiv cu SIGINT, în vederea îndeplinirii cu succes a misiunilor încredințate de comandanții de la diferite niveluri operaționale. În principal, sinergia celor două domenii contribuie la crearea unei imagini integrate asupra mediului operațional și a unei cunoașteri aprofundate a țintelor vizate. Pe de o parte, informațiile obținute prin procedee specifice domeniului HUMINT pot constitui o bază pentru determinarea cursului optim de acțiune în contextul desfășurării de acțiuni în mediul electromagnetic, pentru obținerea de informații SIGINT. Pe de altă parte, informațiile obținute ca urmare a întrebuințării mijloacelor și procedeelor SIGINT pot reprezenta avertizări pentru forțele care desfășoară acțiuni specifice HUMINT. Nu în ultimul rând, informațiile din cele două domenii pot fi utilizate pentru a se completa reciproc sau pentru a fi confirmate/ infirmate.

✓ OSINT – culegerea de informații din surse deschise (Internet, televiziune, cărți etc.). Relația dintre aceste două domenii este una de incluziune reciprocă, OSINT putând fi o potențială sursă de confirmare a unor date obținute prin intermediul SIGINT sau de completare a unor informații SIGINT lacunare. Totodată, prin intermediul OSINT pot fi obținute detalii referitoare la anumite ținte de interes care, ulterior stabilirii nivelului de relevanță operațională, pot fi monitorizate prin intermediul SIGINT în scopul identificării de detalii aparte.

✓ GEOINT – informații geospațiale. Prin intermediul acestei discipline sunt obținute informații referitoare la anumite activități sau ținte de interes, ca urmare a desfășurării unor operațiuni de analiză imagistică și a spațiului geografic natural sau artificial[3]. Ca și în cazurile anterior prezentate, cooperarea dintre cele două domenii poate conduce la completarea imaginii specifice unui anumit eveniment sau la obținerea de detalii suplimentare cu privire la o potențială țintă. Spre exemplu, prin intermediul SIGINT se poate observa o creștere a numărului de emisii electromagnetice într-un anumit raion geografic, fără a fi posibilă obținerea de date suplimentare. Prin intermediul analizei imagistice se pot identifica anumite detalii cu privire la activitățile aflate în desfășurare în respectivul raion, precum și despre țintele vizate.

✓ MASINT – „informația tehnico-ştiinţifică obținută din analiza cantitativă și calitativă a datelor (metrice, angulare, spațiale, de undă, temporare, modulare, plasmatice, magnetice) obținute de senzori creați pentru a observa orice particularități asociate unei surse, unui emițător sau unui transmițător și a permite, ulterior, identificarea și măsurarea acestora”[4]. Ambele fiind domenii cu valență tehnică (depinzând preponderent de mediul electromagnetic), principala diferență constă în profunzimea analizei semnalelor recepționate (pe când SIGINT are la bază emisiunile de comunicații și non-comunicații, MASINT înglobează atât tipologii mai vaste de emisii, cum ar fi cele nucleare și cele acustice, cât și date de telemetrie).

Conform celor prezentate anterior, se poate observa faptul că cele cinci domenii de culegere a informațiilor se intersectează și se completează în vederea creării unei imagini cât mai aprofundate asupra situației operaționale, având la bază date obținute prin surse tehnice și umane. În arhitectura de ansamblu, niciunul dintre aceste domenii nu poate funcționa la parametri optimi în mod solitar, în vederea furnizării de informații complete beneficiarilor, existând o continuă nevoie de coroborare a datelor pentru satisfacerea nevoilor de cunoaștere ale acestora.

IMPORTANȚA DOMENIULUI SIGINT ÎN CADRUL ARHITECTURII NAȚIONALE DE SECURITATE

Rolul SIGINT în cadrul operațiilor militare, indiferent de natura acestora, este direct proporțional cu anvergura misiunilor de specialitate desfășurate și cu nivelul de ambiție al comandanților. La nivel tactic, informațiile obținute prin intermediul SIGINT pot determina rezultatul final al unei anumite operațiuni. De exemplu, în faza de planificare, comandanții de la eșaloanele de nivel tactic pot planifica acțiunile prin identificarea unei zone de concentrare a forțelor inamice, detalii despre aceasta putând fi reliefate de o creștere a numărului de emisii radio dintr-un anumit raion. Suplimentar, prin analizarea comunicațiilor adversarului, pot fi identificate detalii cu privire la echipamentele întrebuințate, organigrama și tipologia forțelor adverse, elemente de planificare a operațiilor sau sprijinului logistic inamic etc. Totodată, prin întrebuințarea sistemelor SIGINT se poate realiza și protecția forței la nivel tactic, prin identificarea dispozitivelor explozive improvizate sau ale echipamentelor de bruiaj, în funcție de aceste informații putând fi adoptate noi cursuri de acțiune. Nu în ultimul rând, există posibilitatea ca, prin intermediul SIGINT, să poată fi angajate sisteme de armament specifice pentru a neutraliza anumite ținte adverse, în baza localizării poziției acestora prin intermediul detectării semnalelor de comunicații și/sau non-comunicații.

Pe de altă parte, la nivel strategic, rolul SIGINT este cu atât mai important, având în vedere relevanța integrării informațiilor veridice în procesul de stabilire a țintelor și de planificare a acțiunilor militare. Mai mult decât atât, sistemele de obținere a informațiilor SIGINT de nivel strategic permit furnizarea de date despre diverse entități guvernamentale sau non-guvernamentale, ce constituie fundamentul identificării situației de securitate specifice și estimării potențialelor evoluții nefaste, cu impact asupra siguranței naționale. În acest fel, decidenții militari și/sau politico-militari pot beneficia de informații acționabile și se pot adapta pentru diverse situații conflictuale, acțiuni cu caracter terorist-extremist sau activități înglobate în sfera criminalității organizate.

Cu toate acestea, domeniul SIGINT nu este specific doar mediului militar, având valențe semnificative pentru întreg spectrul de activități subsumate siguranței naționale și ordinii publice. Spre exemplu, în cadrul unui document[5] elaborat la nivelul Agenției Naționale de Securitate a SUA în anul 2007 (ce conținea o listă cu privire la prioritățile Sistemului SIGINT al SUA pentru următoarele 12-18 luni) a fost reliefat potențialul întrebuințării sistemelor specifice acestui domeniu la nivel strategic. Lista a fost împărțită astfel:

a) *Misiuni regionale* - constituie misiunile prioritare în anumite zone cheie, în cadrul cărora acțiunile SIGINT ar putea avea un rol semnificativ, după cum urmează: terorism (câștigarea luptei globale împotriva terorismului); securitate națională (protejarea teritoriului național de atacuri teroriste și amenințări transfrontaliere); armamente de distrugere în masă și CBRN (combaterea amenințării generate de dezvoltarea și proliferarea armelor de distrugere în masă și CBRN, precum și a vectorilor purtători); sprijin militar pentru trupele SUA; stabilitate politică/ națională (furnizarea de informații despre potențiale mișcări ce ar genera instabilitate la nivel național); amenințări nucleare (furnizarea de avertizări privind un potențial atac cu rachete nucleare strategice împotriva teritoriului național); conflicte regionale și crize (monitorizarea tensiunilor regionale ce ar putea escalada în conflicte/situații de criză); operații informaționale (prevenirea atacurilor cibernetice împotriva infrastructurii critice); modernizare militară (furnizarea de date despre inovațiile străine în domeniul militar); tehnologii emergente strategice (prevenirea surprinderii tehnologice); politică externă (asigurarea avantajului diplomatic pentru SUA); securitate

energetică; combaterea spionajului advers și sprijinirea activității de contrainformații; reducerea riscului generat de rețelele și sindicatele de criminalitate organizată și de trafic de droguri; influențare/ stabilitate economică (asigurarea strategiilor și avantajului economic); cunoașterea spectrului electromagnetic la nivel global (informații cu privire la sistemele și rețelele de comunicații de interes).

b) *Ținte durabile* – ținte ce trebuiau monitorizate holistic, având în vedere importanța acestora, precum R.P. Chineză, Coreea de Nord, Irak, Iran, Federația Rusă și Venezuela.

Din documentul ante-menționat se poate observa faptul că domeniul SIGINT poate fi întrebuințat pentru a satisface nevoia de cunoaștere strategică multi-domeniu, plecând de la misiuni militare de nivel tactic și până la activități specifice dimensiunilor economică, socială, politică, energetică etc. În acest registru, luând în considerare faptul că documentul este datat cu mai mult de o decadă și jumătate în urmă, coroborat cu trendul evolutiv al domeniului tehnologic (ce influențează inclusiv mijloacele și metodele de îndeplinire a misiunilor subsecvente domeniului SIGINT), este intuitiv a opina faptul că, în prezent, rolul acestui domeniu în arhitectura națională și transnațională de securitate este unul deosebit de important.

STUDIU DE CAZ - IMPACTUL SIGINT LA NIVEL OPERAȚIONAL

Primul Război Mondial a constituit punctul de plecare în dezvoltarea domeniului, având în vedere o intensificare a utilizării comunicațiilor pe câmpul de luptă. Deși aflat la un stadiu incipient, primele succese înregistrate în domeniul SIGINT pe timpul celei dintâi conflagrații mondiale au generat o impulsionare a cercetărilor în domeniu, astfel încât, pe timpul celui de-al Doilea Război Mondial au fost semnalate operațiuni SIGINT la nivel strategic care au modelat cursul ulterior al conflictului. De exemplu, informațiile obținute prin intermediul SIGINT au contribuit decisiv la stabilirea planurilor aliate pentru debarcarea din Normandia și bătălia din Franța și la obținerea de detalii cu privire la operații inamice desfășurate în regiunea Balcanilor și în Creta, respectiv în nordul Africii.

Un document[6] declasificat recent și făcut public de către guvernul australian demonstrează rolul SIGINT în cadrul principalelor operații militare desfășurate pe timpul celui de-al Doilea Război Mondial, astfel:

- bătălia de la Midway (1942): armata SUA deținea informații SIGINT despre planurile Japoniei de a ataca Insula Midway cu două luni înainte ca acțiunea în sine să aibă loc/cunoscând detalii despre intenția inamicului, forțele acestuia, locația de dispunere și rutele de apropiere, forțele navale americane au putut pregăti contramăsurile adecvate pentru a neutraliza trupele inamice și pentru a schimba balanța de putere din regiunea Pacificului în favoarea SUA;
- campania din Rusia sovietică: forțele armate britanice au reușit să obțină informații SIGINT cu aproximativ șase luni înainte de declanșarea invaziei naziste în URSS, permițând liderilor politici să analizeze potențiale direcții de acțiune necesar a fi întreprinse în situația materializării incursiunii/ totodată, pe timpul acesteia, britanicii și americanii au avut la dispoziție informații SIGINT cu privire la planurile comandanților germani, operațiile planificate, capabilitățile din înzestrare și ordinea de bătaie a trupelor, care le-au permis ulterior să elaboreze planuri pentru faimoasa operațiune de debarcare din Normandia;
- debarcarea din Normandia (1944): potrivit aceluiași document, înainte de realizarea operațiunii, Aliații au cules cantități semnificative de informații SIGINT cu privire la intențiile armatei germane, dispunerea trupelor și aprecierile acestora față de viitoarele operațiuni aliate/ în ceea ce privește intențiile trupelor germane, subunitățile SIGINT aliate au determinat

faptul că acestea își consolidau poziția defensivă în raport cu estimările referitoare la potențialele acțiuni aliate viitoare; totodată, în perioada dinaintea declanșării operațiunii, subunitățile SIGINT aliate au determinat faptul că estimările inamicului erau eronate, astfel încât Aliații au reușit să-și stabilească direcțiile principale de ofensivă în punctele considerate nevralgice și insuficient acoperite din punct de vedere militar/ prin urmare, la momentul declanșării invaziei, Aliații dețineau informații cu privire la liniile defensive inamice, modul de organizare al trupelor după debutul ostilităților și, în mod primordial, despre planul armatei germane de a încercui diviziile aliate aflate la contact prin flancarea acestora, pe mare, pentru a întrerupe contactul dintre acestea și trupele din eșalonul secund.

Având în vedere faptul că debarcarea din Normandia constituie și astăzi una dintre cele mai emblematice operațiuni ale celei de-a doua conflagrații mondiale, rolul SIGINT în cadrul acesteia se evidențiază prin prezentarea informațiilor puse la dispoziția trupelor aliate înainte de declanșarea operațiunii și pe timpul desfășurării acesteia, astfel[7]:

1. Planurile Germaniei de a face față invaziei aliate: strategia feldmareșalului Gerd von Rundstedt, strategia feldmareșalului Erwin Rommel, strategia forțelor aeriene germane.
2. Estimările conducerii militare germane cu privire la planurile de debarcare ale Aliaților.
3. Modul de angajare în luptă a trupelor germane în Franța (dispunerea forțelor terestre și aeriene în Ziua Z, dezorganizarea din cadrul diviziilor în primele luni după debarcare, motivele angajării defectuoase în luptă a trupelor).
4. Lecțiile învățate înainte de declanșarea operațiunii (eficacitatea tehnicilor de desant aliate, efectul la țintă al artileriei și aviației aliate).
5. Informațiile obținute de trupele germane după declanșarea debarcării din Normandia (identificarea trupelor, determinarea planurilor și stabilirea, în mod eronat, a strategiei generale aliate).
6. Bătălia din Normandia și retragerea către fluviul Sena (încercările feldmareșalului Günther Adolf Ferdinand von Kluge de a-și salva trupele, ordinele lui Adolf Hitler de menținere a liniilor defensive).
7. Zborurile germane peste fluviul Sena, în nord-vestul Franței și în Belgia.
8. Măsurile adoptate de forțele germane împotriva partizanilor francezi și a legiunilor străine.
9. Demolarea porturilor și fortărețelor, respectiv ordinele lui A.Hitler privind distrugerea capitalei franceze.
10. Măsuri pe linie de personal (noi unități create pentru Frontul de Vest, redislocarea de trupe din alte teatre de operații).

Documentul sus-amintit prezintă elemente suplimentare cu privire la rolul SIGINT în cel de-al Doilea Război Mondial: astfel, din aspectele prezentate, se observă rolul primordial al acestui domeniu de culegere a informațiilor în desfășurarea acțiunilor militare la toate nivelurile operaționale, îndeosebi într-o perioadă în care nu ar fi fost posibilă obținerea acestor informații din alte surse disponibile în prezent (de exemplu, prin intermediul GEOINT).

VIITORUL DOMENIULUI SIGINT - PROVOCĂRI ȘI OPORTUNITĂȚI

Evoluțiile tehnologice specifice finalului secolului XX au marcat în mod semnificativ întregul spectru de activități cotidiene, domeniul SIGINT nefăcând excepție. Dacă în trecut mijloacele și metodele de protejare a comunicațiilor erau mult mai rudimentare, în prezent acestea prezintă un trend evolutiv, impactul asupra potențialului de îndeplinire a misiunilor SIGINT fiind unul cu un nivel ridicat de relevanță.

Una dintre cele mai importante provocări viitoare la adresa SIGINT o constituie dezvoltarea continuă a sistemelor responsabile de protejarea semnalelor (modulare, codare, criptare). Spre exemplu, întrebuințarea inteligenței artificiale

pentru realizarea de noi algoritmi de criptare poate constitui o barieră greu de străpuns de specialiști, îngreunând în mod semnificativ potențialul de îndeplinire a misiunilor de către structurile SIGINT. În contrapondere, dezvoltarea inteligenței artificiale constituie, în mod paradoxal, și o oportunitate de dezvoltare a domeniului, prin sprijinirea ansamblului de activități subsumate procesării semnalelor, având în vedere creșterea semnificativă a numărului de semnale disponibile în spectrul electromagnetic. În acest context, automatizarea anumitor procese, precum detectarea anumitor tipare de semnal, filtrarea și analizarea acestora din multitudinea de emisii electromagnetice fără valoare informativă, va facilita soluționarea cu succes și în timp oportun a sarcinilor de culegere[8]. Mai mult decât atât, prin intermediul procesului de învățare automată comprehensivă, pot fi create analize și predicții pe baza informațiilor SIGINT, utilizabile ulterior în cadrul unor produse integrante a mai multor surse de informații distincte.

Pe de altă parte, evoluțiile recente specifice domeniului de calcul cuantic demonstrează faptul că, în viitorul apropiat, tehnologia va modela suplimentar capacitatea operatorilor SIGINT de a-și îndeplini misiunea. Constituind atât o vulnerabilitate, cât și o oportunitate (în funcție de modul particular de raportare), calculul cuantic va permite (în eventualitatea neidentificării unor soluții de atenuare a efectelor) prelucrarea de operații de factorizare a unor numere mari în perioade de timp scurte, ceea ce ar conduce la diminuarea semnificativă a eficienței actualilor algoritmi de criptare. Totodată, calculul cuantic ar putea permite dezvoltarea de mijloace pentru soluționarea problemei privind procesarea semnalelor în medii cu niveluri ridicate de zgomot, prin optimizarea circuitelor cuantice în vederea extragerii semnalului de interes din zgomot, respectiv pentru eficientizarea procesului de analiză a acestuia[9].

Analizând dintr-o altă perspectivă, una din potențialele provocări specifice domeniului SIGINT constă în creșterea accesibilității acestuia pentru diverse entități private. Evocând perspectiva domeniului GEOINT, o capabilitate aparținând, în trecutul nu foarte îndepărtat, doar structurilor guvernamentale, acesta a căpătat o semnificativă valență comercială, prin înființarea de companii ce monetizează informații specifice acestei discipline de culegere. În mod similar, prin comercializarea dispozitivelor de culegere, procesare și analizare a semnalelor, ar putea fi pusă la dispoziția publicului larg o capabilitate care, în procentaj covârșitor, se regăsește în ansamblul de capabilități guvernamentale de culegere a informațiilor.

Un exemplu elocvent îl constituie companiile care și-au dezvoltat constelații de sateliți în vederea detectării, analizării și localizării semnalelor, precum compania HawkEye360. Potrivit site-ului oficial[10] al acesteia, constelația de sateliți pune la dispoziția beneficiarilor informații referitoare la o gamă largă de semnale de radiofrecvență, care ulterior pot fi întrebuințate pentru procesare și analizare suplimentară. Totodată, compania a integrat și soluții GEOINT pentru a furniza detalii cât mai cuprinzătoare din zonele de interes, spre exemplu pentru a identifica potențiale activități ilicite în zonele de graniță, nave suspecte în diverse părți ale globului sau pentru a detecta interferențe ale semnalelor GPS (Global Positioning System).

CONCLUZII

Rolul domeniului SIGINT în arhitectura națională de securitate este unul de necontestat, având potențialul de a furniza informații cu valoare informativă ridicată, acționabile, imposibil de obținut prin intermediul altor discipline de culegere. După cum am prezentat anterior, rolul SIGINT nu rezidă în identificarea de informații doar în scop militar, ci utilitatea acestor date transcende o multitudine de domenii subsecvente securității naționale, precum lupta împotriva terorismului, combaterea proliferării armelor de distrugere în masă și a vectorilor purtători, reducerea riscurilor aferente grupărilor de criminalitate organizată transfrontalieră etc.

Din perspectivă militară, la nivel operațional, rolul SIGINT a fost demonstrat în cursul istoriei recente, unele dintre cele mai mari reușite fiind

înregistrate pe timpul celei de-a doua conflagrații mondiale, în cadrul căreia informațiile obținute prin intermediul acestei discipline au determinat modul de desfășurare a ostilităților și au modelat, într-o anumită proporție, rezultatul final al conflictului. În prezent, acest domeniu rămâne la fel de important, punând la dispoziția decidenților militari și politico-militari date cu privire la diverse dosare de interes din punctele „fierbinți" de pe glob.

La nivel informațional, între disciplinele de culegere există o sinergie accentuată, atât în ceea ce privește mijloacele și metodele de obținere a informațiilor, cât și în ceea ce privește corelarea datelor în vederea completării imaginii generice. În ansamblu, capabilitățile specifice celor cinci discipline de culegere a informațiilor (conform literaturii de specialitate) sunt întrebuințate în comun fie pentru a stimula inițierea culegerii în domenii complementare, fie pentru validarea anumitor date, fie pentru a avea la dispoziție o informație cât mai completă și detaliată, în vederea transmiterii acesteia la factorii decidenți responsabili de securitatea națională.

În ceea ce privește viitorul domeniului SIGINT, există atât provocări, cât și oportunități ce pot determina semnificativ modul în care acesta va evolua. Descoperirile tehnologice, îndeosebi cele specifice inteligenței artificiale și calculului cuantic, au potențialul de a consolida capabilitățile curente, prin creșterea capacității de detecție a semnalelor, prin analizarea unor volume semnificative de date, prin realizarea de corelații și asocieri rapide în vederea furnizării unor analize integrate. Pe de altă parte, evoluțiile tehnologice au potențialul de a limita capabilitățile curente specifice domeniului SIGINT, un exemplu în acest sens fiind utilizarea inteligenței artificiale pentru crearea de algoritmi de criptare mult mai dificil de decriptat decât cei existenți în prezent.

Concluzionând, domeniul SIGINT reprezintă unul din pilonii de bază ai arhitecturii naționale de securitate, atât prin furnizarea, către decidenți, de informații cu grad ridicat de veridicitate, cât și prin unicitatea datelor astfel obținute. Totodată, anvergura informațională specifică, ce transcende o multitudine de misiuni cu caracter militar (de la nivel tactic spre strategic) și de domenii de activitate, constituie laitmotivul pentru care rolul acestui domeniu va continua să fie unul semnificativ și în viitor.

BIBLIOGRAFIE

1. BRENNER Yaghiyah, *"The future of signal processing"*, SoundsReal R&D, martie 2023, https://soundsreal.co.za/2023/03/30/article/
2. KAY Teresa, David McElreath, *Overview of the Intelligence Disciplines*, 2020, https://www.researchgate.net/publication/ 344224551_ Overview_of_the_Intelligence_Disciplines.
3. PARKER Edward, "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret", Commentary, RAND Corporation, 13.09.2023, https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html.
4. ROBU Adrian, "Imaginea amenințării. Senzorii, surse ale cunoașterii", *Revista Intelligence*, Serviciul Român de Informații, martie 2020, https://intelligence.sri.ro/imaginea-amenintarii-senzorii-surse-ale-cunoasterii/.
5. *** "What is SIGINT and how it's maximizing military capabilities", MAG Aerospace, https://www.magaero.com/what-is-sigint-and-how-its-maximizing-military-capabilities/.
6. *** "Documents Show NSA Efforts to Spy on Both Enemies and Allies", *The New York Times*, noiembrie 2013, https://www.statewatch.org/media/documents/news/2013/nov/nsa-sigint-strategic-mission-2007.pdf.
7. *** National Geospatial-Intelligence Agency, *"National System for Geospatial Intelligence. Geospatial Intelligence (GEOINT) Basic Doctrine/ Publication 1-0"*, Washington, septembrie 2006, 52 p.
8. *** HawkEye 360, https://www.he360.com/technology/.
9. *** Australian Signals Directorate, *Role and Effectiveness of Signals Intelligence in World War 2*, aprilie 2021, https://www.asd.gov.au/sites/default/files/2022-03/Role-and-Effectiveness-of-Signals-Intelligence-in-World-War-2.pdf.

---

[1] ***, "What is SIGINT and how it's maximizing military capabilities", https://www.magaero.com/what-is-sigint-and-how-its-maximizing-military-capabilities/, accesat în data de 02.08.2024.

[2] Carl Jensen, David McElreath, Mellisa Graves, *Introduction to Intelligence Studies*, Routledge, New York, 2018; apud. Teresa Kay, David McElreath, *Overview of the Intelligence Disciplines*, 2020, p. 2, https://www.researchgate.net/publication/344224551_Overview_of_the_Intelligence_Disciplines, accesat la 21.07.2024

[3] National Geospatial-Intelligence Agency, "National System for Geospatial Intelligence", 2006, p. 7.

[4] Adrian Robu, „Imaginea amenințării. Senzorii, surse ale cunoașterii", *Revista Intelligence*, Serviciul Român de Informații, martie 2020, https://intelligence.sri.ro/imaginea-amenintarii-senzorii-surse-ale-cunoasterii/, accesat în data de 08.08.2024.

[5] *** "Documents Show N.S.A. Efforts to Spy on Both Enemies and Allies", *The New York Times*, https://www.statewatch.org/media/documents/news/2013/nov/nsa-sigint-strategic-mission-2007.pdf, accesat în data de 02.08.2024.

[6] *** Australian Signals Directorate, *Role and Effectiveness of Signals Intelligence in World War 2*, aprilie 2021, https://www.asd.gov.au/sites/default/files/2022-03/Role-and-Effectiveness-of-Signals-Intelligence-in-World-War-2.pdf., accesat în data de 09.08.2024.

[7] *Ibidem.*

[8] Yaghiyah Brenner, "The future of signal processing", SoundsReal R&D, martie 2023, https://soundsreal.co.za/2023/03/30/article/ accesat în data de 08.08.2024.

[9] Edward Parker, "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret", Commentary, RAND Corporation, 13.09.2023, https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html., accesat în data de 10.08.2024.

[10] *** HawkEye360, https://www.he360.com/technology/, accesat în data de 12.08.2024.

OPERAȚIILE ÎN SPECTRUL ELECTROMAGNETIC – O „NOUĂ" PARADIGMĂ SPECIFICĂ DOMENIULUI MILITAR CONTEMPORAN

George-Daniel BOBRIC*
Emilian TRANDAFIR

Abstract

The effective use of the electromagnetic spectrum has become, in recent years, a sine qua non condition for ensuring superiority at the operational level and meeting the objectives at the tactical level. Through the operational environment, various multi-domain operations achieve effects that are difficult to anticipate by the enemy, thus fulfilling multiple principles specific to the armed conflict such as surprise, manoeuvre, concentration of efforts, etc.

In the last decade, various concepts relevant to the five recognized operational environments (air, land, naval, space and cyber) have influenced military literature, with multiple subsequent efforts to operationalize them being initiated. This is also the case for the electromagnetic spectrum which, under the name of electromagnetic environment, is perceived as another operational environment, thus, facilitates the carrying out of specific operations, augmenting the kinetic effects in the above-mentioned operational environments and contributing to the fulfilment of the final objectives.

In this context, within this article the main aspects related to the operations in the electromagnetic environment will be analysed, starting from a short theoretical review of them. Therefore, elements regarding the relationship between this type of operations with the activities specific to the SIGINT field and the actions performed in the cyber environment will be addressed, respectively, two brief case studies will be carried out: one "conceptual", referring to the theoretical approach of the three big geopolitical actors (NATO, the People's Republic of China and the Russian Federation) towards operations in the electromagnetic environment, respectively an operational one, with the aim of highlighting how the Russian army used the specific capabilities within the conflicts in Ukraine and Syria.

Keywords: *electromagnetic spectrum; electronic warfare; SIGINT; cyberspace.*

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

INTRODUCERE

Începutul secolului XXI a determinat o reorientare a politicilor referitoare la modul de desfășurare a operațiilor și la mediile operaționale existente, spațiul cibernetic fiind luat în considerare drept cel de-al cincilea mediu de efectuare a misiunilor cu caracter militar. Suplimentar, în ultima decadă, o atenție sporită a fost acordată acțiunilor întreprinse în spectrul electromagnetic, îndeosebi de către actorii statali implicați în acțiuni beligerante, pentru a identifica o capabilitate de nișă care să permită consolidarea apărării proprii, cât și sporirea efectului de neutralizare a mijloacelor tehnice inamice.

În ceea ce privește conceptul de *operații în spectrul electromagnetic* (Electromagnetic Spectrum Operations/ EMSO), acestea sunt definite în literatura de specialitate[1] drept acțiuni specifice războiului electromagnetic - „acțiunea militară ce implică utilizarea energiei electromagnetice direcționate pentru a controla spectrul electromagnetic sau pentru a ataca inamicul, respectiv acțiunile de protecție împotriva întrebuințării spectrului electromagnetic pentru degradarea, neutralizarea sau distrugerea capabilităților de luptă aliate", împreună cu acțiunile de management al spectrului electromagnetic – „procedurile operaționale, inginerești și administrative pentru a planifica și coordona operații în mediul operațional electromagnetic".

Spectrul electromagnetic are un rol deosebit de important în ansamblul activităților cotidiene, indiferent de natura acestora, fiind esențial în cadrul conflictelor moderne, din perspectiva facilitării anumitor operații specifice în alte medii operaționale. Astfel, mediul electromagnetic constituie componenta prin intermediul căreia se

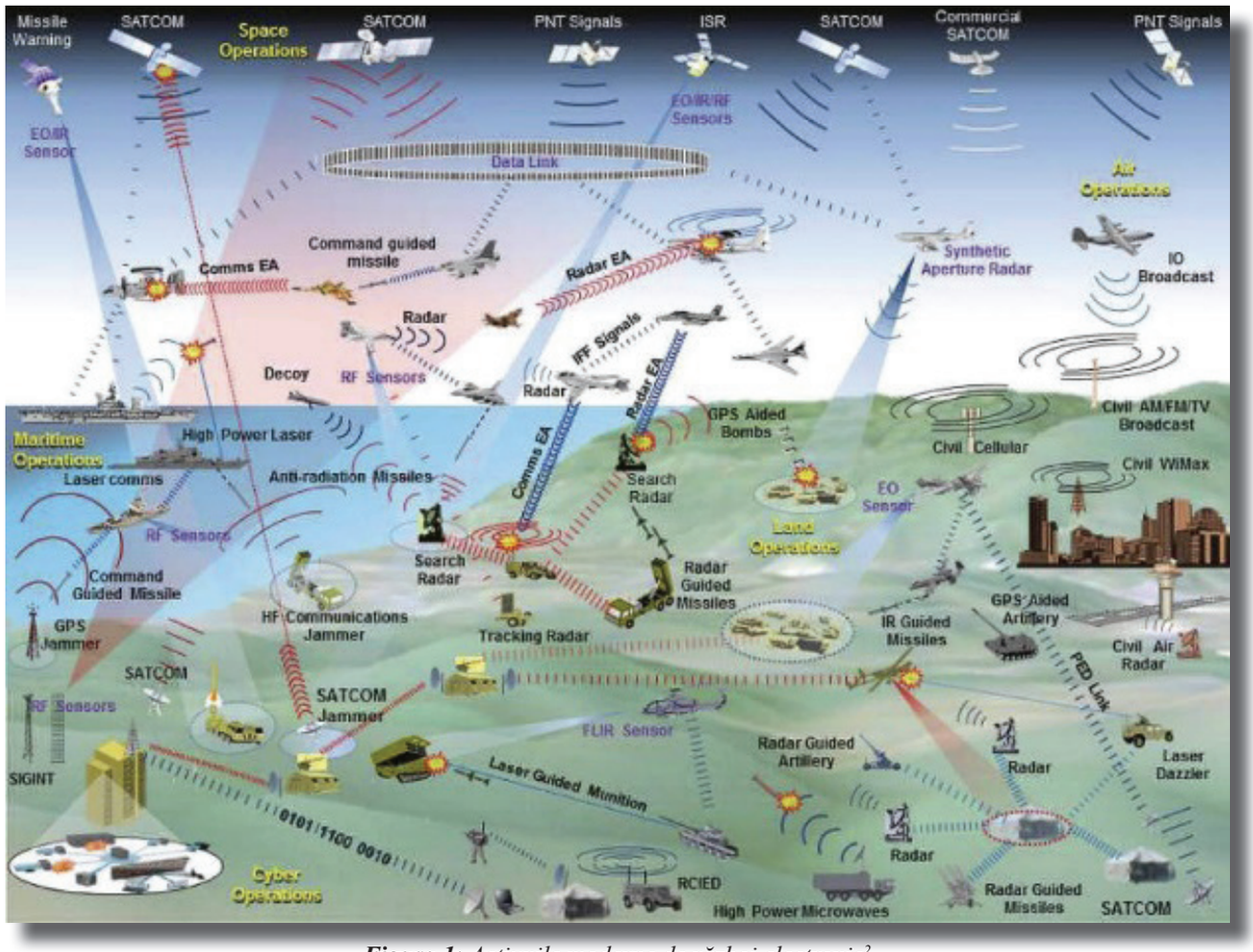


Figura 1: *Acțiunile moderne de război electronic*[2]

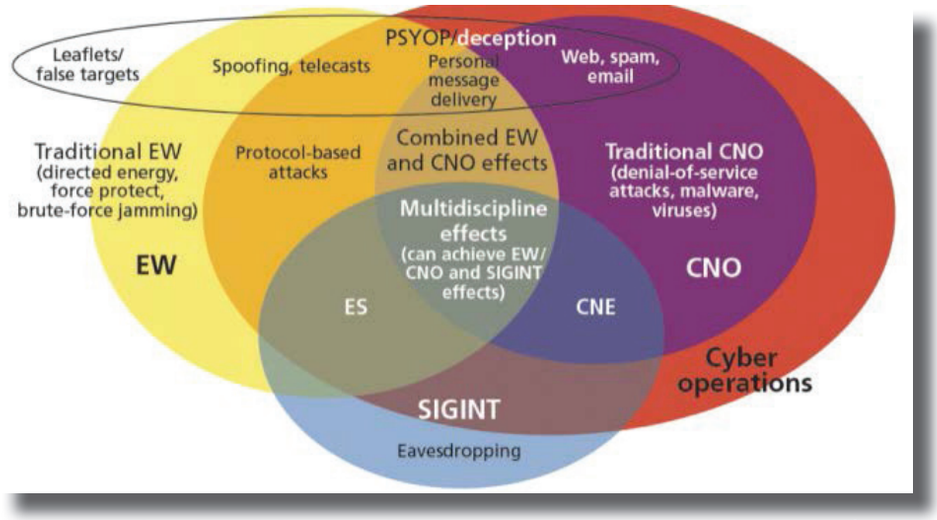


Figura 2: *Relația SIGINT - război electronic - operații în mediul cibernetic*[3]

desfășoară activități de bază precum realizarea comunicațiilor militare, transmiterea de date, navigarea prin intermediul sistemelor de poziționare globală. Mai departe, prin intermediul mediului electromagnetic, echipamente precum radare sau senzori pot detecta, monitoriza, stabili natura și angaja o țintă. În același timp, mediul electromagnetic constituie o sursă de obținere a informațiilor prin intermediul echipamentelor SIGINT și de supraveghere electromagnetică, precum și un catalizator al operațiilor desfășurate în spațiul cibernetic, acestea din urmă exploatând, în unele situații, vulnerabilități specifice echipamentelor fizice.

RELAȚIA RĂZBOI ELECTRONIC - SIGINT - ACȚIUNI ÎN MEDIUL CIBERNETIC

Între cele trei tipuri de acțiuni există o conexiune semnificativă, generată fie de asemănări operaționale, fie de obiective similare realizabile prin acțiuni specifice (figura 2).

La nivel tehnic, componenta de supraveghere electronică (SE) a războiului electronic prezintă suprapuneri cu domeniul de activitate al SIGINT, principalele diferențe înregistrându-se la nivel de misiune specifică, sensibilitate temporală și tip de date ce sunt colectate de sistemele specifice (tabelul 1).

Tabelul 1: *Relația dintre SIGINT și măsurile de supraveghere electronică*[4]

	SIGINT	SE
Misiuni	Interceptarea emisiilor de comunicații și non-comunicații în vederea identificării de informații despre emitent (tipologie, localizare, înzestrare, acțiuni planificate etc.).	Identificarea și localizarea emisiilor de comunicații pentru realizarea bazei de date cu emițătoare și stabilirea priorităților de adoptare de contramăsuri (de exemplu, de bruiaj), respectiv identificarea locației sistemelor radar inamice.
Sensibilitate temporală	Întrucât procesul de decriptare, demodulare, decodare și analizare a conținutului este unul consumator de timp, informațiile SIGINT nu sunt foarte sensibile din punct de vedere temporal.	Informațiile trebuie să fie acționabile, astfel încât timpul de diseminare al acestora este necesar a fi cât mai scăzut.
Date colectate	Volum maxim de date pentru a realiza o analiză cât mai comprehensivă asupra conținutului informațional.	Volum suficient de date cât să permită stabilirea tipologiei țintei, a locației și a mijloacelor/metodelor necesare pentru neutralizarea acesteia.

Totodată, o conexiune strânsă se identifică între SIGINT și operațiile de război electronic din perspectiva sprijinului pentru operațiile militare. La nivel tactic, informațiile SIGINT pot fi utilizate în timp aproape real pentru acțiuni de stabilire a țintelor, care să fie angajate ulterior fie de echipamentele de atac electronic, fie de sistemele de lovire cinetică. Pe de altă parte, semnalele obținute de echipamentele de supraveghere electronică pot fi utilizate pentru analiză ulterioară, informațiile obținute fiind guvernate de regulile specifice domeniului SIGINT.

După cum se poate observa și din figura 2, principalul aspect avut în comun de operațiile în spectrul electromagnetic și acțiunile în spațiul cibernetic îl reprezintă obiectivul operațional de consolidare a efectelor finale și de îndeplinire a misiunilor (ofensive sau de apărare). Pentru realizarea acestui deziderat, se pot avea în vedere aspectele prezentate în tabelul 2:

STUDIU DE CAZ: ABORDĂRI „CONCEPTUALE"

Integrarea conceptuală și operațională a războiului electronic cu domeniul SIGINT reflectă o schimbare recentă de paradigmă privind modalitatea de purtare a acțiunilor militare, punând accent pe desfășurarea de acțiuni multidomeniu.

I. R.P. Chineză

✓ *Războiul electronic integrat în rețea*

Încă de la începutul anilor 2000, strategii militari chinezi au pus bazele unor noi abordări în ceea ce privește modalitatea de desfășurare a operațiilor în „mediul electromagnetic complex (CEME)", având ca punct focal dezvoltarea capabilităților de război electronic și SIGINT. Mai mult decât atât, în aceeași perioadă a luat naștere conceptul de „război electronic integrat în rețea", ce îmbină operațiile specifice

Tabelul 2: *Similarități operaționale specifice acțiunilor cibernetice și electromagnetice*[5]

Obiectiv urmărit	Acțiuni în spectrul electromagnetic	Acțiuni cibernetice
Culegerea de informații despre inamic	Supraveghere electronică (detaliată anterior).	Utilizarea de programe de exfiltrat date și informații (precum spyware) din rețelele adversarului.
Interferarea cu capacitatea operațională a inamicului	Atac electronic - prin intermediul acțiunilor de bruiaj electronic, pentru a reduce sau împiedica capabilitatea de a recepționa semnale emise în spectrul electromagnetic de către inamic.	Atacuri cibernetice ce implică fie utilizarea de viruși (în scopul modificării programelor instalate în calculatorul infectat), fie acțiuni pentru blocarea efectivă a țintei (precum atacuri de tip denial-of-service).
Sabotarea sistemelor inamicului pentru inițierea de acțiuni nedorite	Atac electronic - prin intermediul acțiunilor de dezinformare electronică (crearea de ținte false pentru sistemele de interceptare inamice și inducerea în eroare a inamicului cu privire la posibilitățile reale și la dispunerea trupelor proprii).	Atacuri cibernetice ce implică, spre exemplu, întrebuințarea de programe de tip „cal troian" (aplicații malițioase deghizate în unele legitime, ce pot desfășura o serie de acțiuni ilicite în calculatorul-țintă).
Protecția capabilităților proprii	Protecția electronică a echipamentelor proprii împotriva acțiunilor specifice războiului electronic întreprinse de adversar.	Protecția capabilităților cibernetice proprii în fața amenințărilor din mediul operațional cibernetic.

războiului electronic cu acțiunile întreprinse în cadrul spațiului cibernetic. Ca urmare, în anul 2015, în cadrul Armatei de Eliberare a Poporului a fost înființat[6] un serviciu cu statut instituțional similar categoriilor de forțe, intitulat Forța de Sprijin Strategic, responsabil de managementul capabilităților și acțiunilor specifice de război electronic integrat în rețea. În prezent, după aproximativ o decadă, Forța de Sprijin Strategic a fost desființată, în locul acesteia fiind create trei forțe cu statut similar - Forțele Aerospațiale, Forțele Cibernetice și Forțele de Sprijin Informațional. Deși în anul 2015 Forța de Sprijin Strategic a fost creată pentru a stabili o sinergie între operațiile în spațiul cosmic, spațiul cibernetic și mediul electromagnetic, cele trei componente au fost apoi separate, fiind augmentate în structuri de sine stătătoare, cu misiunile specifice războiului electronic și misiunilor informaționale arondate Forței de Sprijin Informațional[7].

✓ *Tehnologii avansate de procesare a semnalelor*

La începutul anului curent, cercetătorii chinezi au anunțat dezvoltarea unui nou model de convertor analog-digital, ce ar avea capacitatea de a detecta semnale radar cu o viteză de aproximativ 91% mai mare decât versiunile existente aflate în uz, generând o scădere semnificativă a întârzierilor specifice receptoarelor utilizate în echipamentele de război electronic de la nanosecunde la picosecunde. În echipamentele curente, semnalul este transformat din analog, reprezentând unda electromagnetică, în digital - forma binară, recunoscută de calculatoare, iar apoi sunt analizate caracteristicile pentru a identifica dacă semnalul este sau nu de interes. În context, actualul cip reușește să identifice anumite tipuri de semnale înainte de a fi convertite în formă digitală și să determine dacă sunt sau nu semnale radar, doar cele de interes fiind apoi procesate, reducându-se astfel semnificativ timpul de răspuns, puterea de procesare și consumul de energie[8]. In extenso, acest dispozitiv ar putea fi întrebuințat, în mod similar, și în cadrul echipamentelor SIGINT.

✓ *Întrebuințarea inteligenței artificiale*

Fiind unul dintre liderii-cheie ai acestui domeniu, R.P.Chineză investește în dezvoltarea inteligenței artificiale, intenția fiind de a augmenta capabilitățile de confruntare armată în centrul căreia se află informația. Astfel, prin intermediul inteligenței artificiale, armata chineză caută să integreze capabilitățile de distrugere/neutralizare cu cele de obținere, procesare și analizare a informațiilor, astfel încât cantități mari de date să fie procesate în timp cât mai scurt pentru a furniza informații acționabile.

În ceea ce privește operațiile în spectrul electromagnetic, merită precizat faptul că, în ultimii ani, Armata de Eliberare a Poporului a contractat diverse instituții pentru desfășurarea de activități de cercetare-dezvoltare în domeniul războiului electronic. Dintre acestea, cele mai importante fac referire la tehnicile de generare adaptivă a emisiilor electromagnetice, modularea automată în frecvență, bruiajul în benzile de microunde sau separarea semnalelor utile din propagarea multicanal, în vederea producerii de sisteme adaptive, automate. Astfel, aceste sisteme ar avea rolul de a fi întrebuințate în operații specifice „cunoașterii situației de pe câmpul de luptă, recunoașterii țintelor electromagnetice, asigurării contramăsurilor electronice și a protecției electronice și managementului câmpului de luptă”[9].

✓ *Adaptarea strategiilor curente în raport cu cele occidentale*

În strategia privind superioritatea în spectrul electromagnetic, făcută publică în anul 2020 de către Departamentul Apărării al SUA, este stipulat faptul că, pentru asigurarea libertății de acțiune în acest spectru, este necesară îndeplinirea cumulativă a următoarelor obiective: „dezvoltarea de capabilități [de operare] în spectrul electromagnetic, evoluția către o infrastructură specifică mediului electromagnetic agilă și complet integrată, asigurarea disponibilității totale a forței în spectrul electromagnetic, securizarea parteneriatelor solide pentru [obținerea] avantajului în mediul electromagnetic și stabilirea unei autorități eficiente în cadrul acestuia[10]”.

În contrapondere, strategii militari chinezi lucrează la o strategie privind spectrul electromagnetic având aproximativ aceeași viziune ca omologii americani, potrivit căreia spectrul electromagnetic este definit drept un

„catalizator” al operațiilor desfășurate în mediile consacrate de purtare a acțiunilor cu caracter beligerant și nu un domeniu în sine. Suplimentar față de această viziune, specialiștii chinezi militează pentru integrarea operațiilor în spațiul cibernetic cu acțiunile de război electronic, cu scopul de a augmenta efectul final al loviturilor cinetice[11].

II. Federația Rusă

În mod similar, strategii militari ruși acordă o atenție deosebită operațiunilor desfășurate în mediul electromagnetic, capabilitățile de război electronic fiind intens întrebuințate în cadrul conflictelor purtate în estul Ucrainei sau în Siria. Din această perspectivă, rolul acțiunilor în spectrul electromagnetic este unul covârșitor în ceea ce privește cadrul normativ și doctrinar rusesc, între acesta și cel al statelor occidentale (în special celor din cadrul NATO) fiind identificate câteva diferențe de perspectivă (tabelul 3).

STUDIU DE CAZ: PERSPECTIVA OPERAȚIONALĂ A CONFLICTULUI RUSO-UCRAINEAN

Unul dintre cele mai relevante studii de caz, în ceea ce privește operațiile în spectrul electromagnetic, îl constituie conflictul din Ucraina; astfel, în literatura de specialitate există o serie de articole ce relevă rolul deosebit de important al acestora pe timpul desfășurării ostilităților.

În ceea ce privește prima fază a conflictului, perioada februarie-aprilie 2022 (până la retragerea trupelor ruse din proximitatea capitalei ucrainene), cele mai importante acțiuni în spectrul electromagnetic au vizat[16]:

- comunicațiile radio militare și civile, îndeosebi prin întrebuințarea de sisteme tactice de bruiaj a benzilor V/UHF;
- comunicațiile satelitare - sistemele întrebuințate de forțele ucrainene, provenite

Tabelul 3: *Diferențe de abordare a războiului electronic NATO-F.Rusă*

Diferența	Federația Rusă	NATO
Doctrina operațională	Războiul electronic este strâns integrat în cadrul tuturor nivelurilor operaționale, fiind esențial pentru neutralizarea, degradarea sau distrugerea elementelor de comandă-control și ISR inamice[12].	În doctrina SUA, spre exemplu, este făcută clar distincția între componenta de supraveghere electronică, specifică războiului electronic, și SIGINT, domeniu de culegere de informații (detalii suplimentare au fost prezentate într-un capitol anterior)[13]. Totodată, capabilitățile de război electronic sunt realizate în contrapondere la diverse amenințări din mediul operațional.
Tactici specifice	Armata rusă a întrebuințat intens capabilitățile de război electronic în toate fazele conflictelor armate purtate recent, atât în Ucraina, cât și în Siria.	În prezent, NATO se concentrează pe identificarea de lecții învățate din cadrul conflictului ruso-ucrainean pentru a-și adapta propriile proceduri în raport cu noile descoperiri tehnologice și evoluțiile operaționale în domeniu. Totodată, trupele ucrainene au capturat diverse echipamente rusești de război electronic, ce ar putea genera un efort de analiză și fabricare de echipamente de contracarare[14].
Integrare structurală	Capabilitățile de război electronic au fost integrate la toate nivelurile operaționale din mediile naval, terestru și aerian, pentru a consolida eficacitatea operațională și efectul final al acțiunilor cinetice.	NATO menține o abordare modulară, cu capabilități centralizate în cadrul unor unități specializate, subordonate categoriilor de forțe ale armatei[15].

de la companiile Viasat și Starlink, au fost victimele unor acțiuni de atac cibernetic;
- semnalele satelitare de navigație globală, precum cele provenite de la GNSS (Global Navigation Satellite System);
- dronele, indiferent de natura (civilă sau militară) sau misiunea acestora (de cercetare, lovire etc.);
- sistemele radar ucrainene.

În regiunea Mării Negre, echipamentele de război electronic au fost întrebuințate împotriva armamentului ghidat de mare precizie dependent de sistemele de ghidare prin satelit (precum JDAM și HIMARS furnizate de SUA)[17]. Pe de altă parte, bruiajul GPS reprezintă o constantă a acțiunilor întreprinse de forțele armate ruse în prezent, o parte importantă din zona de sud-est a României (Dobrogea) și de sud-vest a Mării Negre fiind afectate de aceste acțiuni.

Astfel, din figura 3 se poate observa intensitatea crescută a interferențelor GPS în zona de sud-est a României, raportate de sistemele de navigație ale aeronavelor care evoluează în zona bazinului Mării Negre, cauzate probabil de acțiunile de bruiaj în benzile GPS executate de mijloace de război electronic dispuse în Peninsula Crimeea.

Una din posibilele rațiuni pentru această acțiune o constituie limitarea libertății de acțiune a navelor ce operează spre porturile ucrainene din regiunea Odesa și cele cu ieșire la Dunăre, utilizând coridorul maritim pentru exportul cerealelor prin Marea Neagră. Pe de altă parte, aceste acțiuni pot fi întreprinse și pentru a proteja anumite acțiuni proprii, aflate în derulare, având în vedere că sistemul rusesc de poziționare globală (GLONASS) operează în alte benzi de frecvență, capabilitățile rusești nefiind afectate de bruiajul GPS. La nivel strategic, nu este exclusă posibilitatea ca astfel de acțiuni să constituie elemente de mesaj pentru NATO, prin prisma faptului că acestea sunt considerate a fi acțiuni ostile, cu caracter ofensiv, împotriva unor state ale Alianței (România, Bulgaria, Turcia), față de care aceasta nu întreprinde nicio contramăsură.

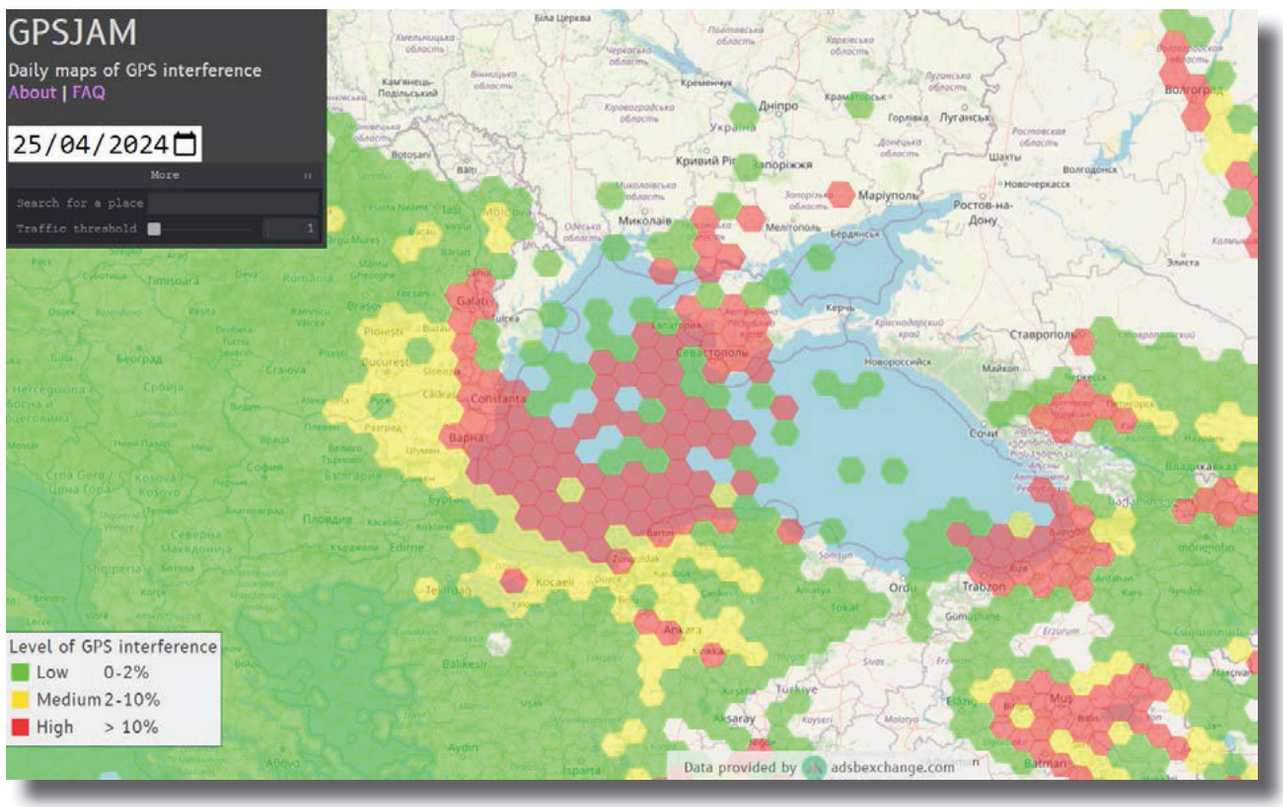


Figura 3: *Bruiaj GPS în regiunea Mării Negre*[18]

CONCLUZII

Mediul electromagnetic constituie o componentă catalizatoare a operațiilor specifice războiului modern, influențând strategiile militare și capabilitățile specifice. Progresele rapide în domeniul tehnologiilor de război electronic subliniază importanța inovării și a integrării în obținerea succesului pe câmpul de luptă. Pe măsură ce operațiile militare se bazează din ce în ce mai mult pe utilizarea eficientă a spectrului electromagnetic, convergența dintre războiul electronic, operațiile în mediul cibernetic și SIGINT vor modela viitorul războiului, necesitând o abordare cuprinzătoare a dominației în spectrul electromagnetic.

Astfel, în cadrul prezentului articol au fost abordate aspecte disponibile în spațiul public referitoare la noțiunea de operații în spectrul electromagnetic, ce reprezintă o schimbare de paradigmă atât la nivel conceptual, cât și operațional. La nivel conceptual, au fost prezentate eforturile întreprinse de principalii actori (îndeosebi SUA și R.P. Chineză) pentru actualizarea cadrului doctrinar specific acestui tip de acțiuni, ca parte a unui efort întrunit de obținere a dominației inclusiv asupra mediului electromagnetic și celui cibernetic. Pe de altă parte, având în vedere că Federația Rusă întrebuințează, de un deceniu, capabilitățile de război electronic în „poligoanele de testare” Siria și Ucraina, se observă că arhitectura legislativ-organizatorică specifică operațiilor electromagnetice este bine consolidată, spre deosebire de statele NATO care se află încă în etapa de aplicare a lecțiilor învățate pe timpul celor două conflicte menționate anterior și de modernizare a capabilităților aferente.

Din punct de vedere operațional, conflictul ruso-ucrainean relevă un aspect imposibil de contestat: obținerea avantajelor tehnologice specifice acțiunilor purtate în mediul electromagnetic reprezintă un deziderat strategic în vederea consolidării capabilităților de neutralizare a inamicului și de augmentare a efectului final al loviturilor cinetice. De exemplu, încă din prima etapă a conflictului, armata rusă a aruncat în luptă capabilități de război electronic utilizate la toate nivelurile operaționale, într-un efort consolidat de asediere a capitalei ucrainene.

Nu în ultimul rând, în regiunea Mării Negre capabilitățile de război electronic servesc la perturbarea operațiilor militare ale inamicului și la manipularea navigației maritime. Această tactică nu afectează doar strategiile militare, dar prezintă și riscuri semnificative pentru transportul comercial, subliniind complexitatea războiului modern în medii contestate.

BIBLIOGRAFIE

1. ADAMY David, *EW 101: A First Course in Electronic Warfare*, Artech House, Boston-London, 2001, 330 p.
2. AMOROSO Antonino, *"Electronic Warfare AKA Electromagnetic Warfare"*, https://www.emsopedia.org/entries/electronic-warfare-aka-electromagnetic-warfare/.
3. BHARDWAJ Abhishek, "China's new warfare chip increases radar detection, response time by 91%", 31.07.2024, https://interestingengineering.com/military/china-fast-chip-radar-detection.
4. BRUZZESE Matt, Peter Singer, "Farewell to China's Strategic Support Force. Let's meet its replacements", *Defence One*, 28 aprilie 2024, https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/.
5. CHIRIAC Olga, Thomas Withington, "Russian Electronic Warfare: From History to Modern Battlefield", Irregular Warfare Initiative, 21.03.2024, https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/.
6. CLAY Marcus, "To rule the invisible battlefield: the electromagnetic spectrum and the Chinese military power", *War on the Rocks.* 22 ianuarie 2021, https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-Chinese-military-power/.
7. DAHM Michael, *Electronic Warfare and Signals Intelligence. South China Sea Military Capability Series - A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea*, Johns Hopkins Applied Physics Laboratory, 2020, 35 p.
8. DANGWAL Ashish, "Russia's 'Most Advanced' Electronic Warfare (EW) Jamming Pod Mounted On Su-30 Fighter Seized By Ukraine", *The EurAsian Times*, 13.09.2022, https://www.eurasiantimes.com/russias-electronic-warfare-ew-jamming-pod-ukraine/.
9. FEDASIUK Ryan, Jennifer Melot, Ben Murphy, *Harnessed Lightning. How the Chinese Military is Adopting Artificial Intelligence*, Center for Security and Emerging Technology, Georgetown Walsh School of Foreign Service, octombrie 2021, 84 p.
10. SCOTT Richard, "NATO Confronts the Challenge of a Congested and Contested Spectrum", *Journal of Electromagnetic Dominance*, vol. 44, nr. 5, Mai 2021, https://www.jedonline.com/2023/11/30/from-the-jed-archives-nato-confronts-the-challenge-of-a-congested-and-contested-spectrum/.
11. UPPAL Rajesh, "Military Race for Integrated Cyber, Space, EW, Signals Intelligence and Communications Capability for Information Dominance", 3 aprilie 2023, https://idstch.com/cyber/military-race-for-integrated-cyber-space-ew-signals-intelligence-and-communications-capability-for-information-dominance/.
12. VON SPRECKELSEN Malte, "Electronic Warfare - The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict?", *Journal of the Joint Air Power Competence Center*, NATO Joint Air Power Competence Center, nr. 27, 2018, p. 41-45, https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/.
13. WITHINGTON Thomas. "The Underwhelming Performance Of Russian Land Forces Electronic Warfare - Watt Happened?", *The Defense Horizon Journal*, 18.08.2022, https://tdhj.org/blog/post/watt-happened/.
14. *** United States Government Accountability Office (GAO), *Electromagnetic Spectrum Operations,* Report to the Committee on Armed Services, House of Representatives, decembrie 2020, 66 p., https://www.gao.gov/assets/720/711469.pdf., accesat în data de 26.08.2024.
15. *** *Joint Publication 3-85. Joint Electromagnetic Spectrum Operations*, Chairman of the Joint Chiefs of Staff, 22 May 2020, 148 p., https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.
16. *** Department of Defense, *Electromagnetic Spectrum Superiority Strategy,* October 2020, 28 p. https://www.airandspaceforces.com/app/uploads/2020/10/ELECTRO MAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.pdf.
17. *** https://gpsjam.org/?lat=44.26282&lon=33.82718&z=5.6&date=2024-04-25, accesat în data de 04.09.2024.

[1] United States Government Accountability Office (GAO), *Electromagnetic Spectrum Operations,* Report to the Committee on Armed Services, House of Representatives, decembrie 2020, https://www.gao.gov/assets/720/711469.pdf., accesat în data de 26.08.2024.

[2] Malte von Spreckelsen, "Electronic Warfare - The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict?", *Journal of the Joint Air Power Competence Center,* NATO Joint Air Power Competence Center, nr. 27, 2018, https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/, accesat în data de 26.08.2024.

[3] Rajesh Uppal, "Military Race for Integrated Cyber, Space, EW, Signals Intelligence and Communications Capability for Information Dominance", 3 aprilie 2023, https://idstch.com/cyber/military-race-for-integrated-cyber-space-ew-signals-intelligence-and-communications-capability-for-information-dominance/, accesat în data de 05.08.2024.

[4] David Adamy, *EW 101: A First Course in Electronic Warfare,* Artech House, 2001, p. 42.

[5] Antonino Amoroso, "Electronic Warfare AKA Electromagnetic Warfare", https://www.emsopedia.org/entries/electronic-warfare-aka-electromagnetic-warfare/, accesat în data de 28.08.2024.

[6] Michael Dahm, *Electronic Warfare and Signals Intelligence. South China Sea Military Capability Series - A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea,* Johns Hopkins Applied Physics Laboratory, 2020, p. 2-3.

[7] Matt Bruzzese, Peter W. Singer, "Farewell to China's Strategic Support Force. Let's meet its replacements", *Defence One,* 28 aprilie 2024, https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/, accesat în data de 28.08.2024.

[8] Abhishek Bhardwaj, "China's new warfare chip increases radar detection, response time by 91%", 31.07.2024, https://interestingengineering.com/military/china-fast-chip-radar-detection, accesat în data de 29.08.2024.

[9] Ryan Fedasiuk, Jennifer Melot, Ben Murphy, *Harnessed Lightning. How the Chinese Military is Adopting Artificial Intelligence,* Center for Security and Emerging Technology, Georgetown Walsh School of Foreign Service, 2021, p. 31.

[10] *** Department of Defense, *Electromagnetic Spectrum Superiority Strategy,* October 2020, https://www.airandspaceforces.com/app/uploads/2020/10/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.pdf., accesat în data de 01.09.2021.

[11] Marcus Clay, "To rule the invisible battlefield: the electromagnetic spectrum and the Chinese military power", *War on the Rocks,* 22 ianuarie 2021, https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-Chinese-military-power/, accesat în data de 17.08.2024.

[12] Olga Chiriac, Thomas Withington, "Russian Electronic Warfare: From History to Modern Battlefield", 21.03.2024, Irregular Warfare Initiative, https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/, accesat în data de 01.09.2024.

[13] *** Joint Publication 3-85. Joint Electromagnetic Spectrum Operations, Chairman of the Joint Chiefs of Staff, 22 May 2020, p. 1-6, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf., accesat în data de 01.09.2024.

[14] Ashish Dangwal, "Russia's 'Most Advanced' Electronic Warfare (EW) Jamming Pod Mounted On Su-30 Fighter Seized By Ukraine", *The EurAsian Times,* 13.09.2022, https://www.eurasiantimes.com/russias-electronic-warfare-ew-jamming-pod-ukraine/, accesat în data de 03.09.2024.

[15] Richard Scott, "NATO Confronts the Challenge of a Congested and Contested Spectrum", *Journal of Electromagnetic Dominance,* vol. 44, nr. 5, Mai 2021, https://www.jedonline.com/2023/11/30/from-the-jed-archives-nato-confronts-the-challenge-of-a-congested-and-contested-spectrum/, accesat în data de 02.09.2024.

[16] Thomas Withington, "The Underwhelming Performance Of Russian Land Forces Electronic Warfare - Watt Happened?", *The Defense Horizon Journal,* 18.08.2022, https://tdhj.org/blog/post/watt-happened/, accesat în data de 03.09.2024.

[17] Olga Chiriac, Thomas Withington, Op. cit.

[18] Online: https://gpsjam.org/?lat=44.26282&lon=33.82718&z=5.6&date=2024-04-25, accesat în data de 04.09.2024.

SISTEMELE AERIENE FĂRĂ PILOT ȘI DEPENDENȚA DE SPECTRUL ELECTROMAGNETIC

Dragoș DRĂGOI*

Abstract

The recent conflicts have brought to the forefront, on a large scale, a successor to the RCIEDs extensively used in Iraq and Afghanistan wars, namely commercial and military drones. They approach the target with assigned ISR, BDA, fire correction, personnel recovery or strike missions and act as force multipliers, as equipment costing a few thousand euros with an attached explosive device can damage or destroy platforms worth hundreds of thousand or even millions of euros. Drones are highly dependent on the use of specific portions of the electromagnetic spectrum to carry out their mission, more precisely to ensure survivability of their critical core elements, meaning the C2 link, data streaming and GNSS.

Therefore, fighting against drones, from a broader perspective than countering each individual unmanned system, becomes mostly a matter of controlling or dominating the electromagnetic spectrum, both achievable through electronic warfare actions.

Keywords: *drones; UAV; electronic warfare; electromagnetic spectrum.*

INTRODUCERE

Conflictele care au marcat începutul secolului XXI (cele din Afganistan și Irak, menționate împreună datorită unor caracteristici comune și a prevalenței caracterului de contra-insurgență, și conflictul din Ucraina) au generat schimbări importante asupra modului în care lumea, mai ales europenii, privesc binomul apărare-securitate și au readus în prim-plan războiul convențional, în condițiile evoluției tehnologice specifice acestui secol.

În cazul primelor două conflicte, forțele unei coaliții internaționale s-au lovit de un tip nou de amenințare, mai puțin evocat în manualele de instruire pentru luptă a forțelor armate regulate, respectiv dispozitivele explozive improvizate (DEI), termenul „improvizat” fiind probabil cel definitoriu în caracterul de noutate al amenințării. Acest nou tip de amenințare a schimbat modul de planificare și desfășurare a operațiilor și a instruirii, precum și al sprijinului logistic și de informații etc. DEI-urile erau amplasate astfel încât să maximizeze probabilitatea de a produce victime și daune materiale, indiferent dacă ținta era reprezentată de militari sau civili.

Modalitățile de inițiere a DEI-urilor au fost diverse și dependente de materialele avute la dispoziție, de caracteristicile zonei de operații și de locul de amplasare ales. Dintre acestea, DEI-urile comandate prin radio (Radio Controlled Improvised Explosive Devices - RCIED) au

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

avut o pondere importantă, datorită diversității, disponibilității și costului redus de achiziție al echipamentelor de emisie-recepție utilizate[1]. În mod natural, forțele armate s-au adaptat situației și au dezvoltat soluții de contracarare a acestora, mașinile de luptă și autovehiculele militare utilizate în aceste campanii fiind echipate cu dispozitive de bruiaj destinate să blocheze legătura de comandă-control dintre persoana care acționa dispozitivul și dispozitivul respectiv.

La rândul său, conflictul din Ucraina a adus în prim-plan un nou tip de amenințare, prin utilizarea pe scară largă a unui succesor al RCIED-urilor și anume sistemele fără pilot[2] comerciale și militare (denumite, pe scurt, drone). Acestea evoluează către țintă fie terestru (Unmanned Ground Vehicle/System – UGV/S), fie prin aer (Unmanned Air Vehicle/ System - UAV/ UAS), fie pe apă (Unmanned Surface Vehicle/ System – USV/ USS) sau sub apă (Unmanned Underwater Vehicle/ System – UUV/ UUS) și reprezintă multiplicatori de forță, întrucât acest echipament relativ accesibil din punct de vedere al costurilor (sumele vehiculate fiind doar de ordinul câtorva mii de euro) și care are atașat un dispozitiv exploziv poate avaria, neutraliza sau distruge echipamente/ platforme de sute de mii sau chiar milioane de euro. Utilizarea tot mai frecventă a dronelor în conflictele actuale a influențat modul de ducere a acțiunilor militare, exemple în acest sens fiind acțiunile de luptă din estul Ucrainei, Fâșia Gaza, acțiunile rebelilor Houthi în Yemen și Marea Roșie. Din nou, utilizarea unor mijloace neconvenționale, respectiv a dronelor, în conflict reprezintă un punct de inflexiune cu efecte asupra modului de ducere a acțiunilor militare și de asigurare a instruirii, sprijinului logistic, sprijinului de informații, sprijinului cu foc etc.

Constatăm, așadar, că tehnica utilizată pe scară largă are o însemnătate aparte, generând modificări ale modului de planificare/ ducere a acțiunilor de luptă, iar pentru cineva specializat în exploatarea din punct de vedere militar a spectrului electromagnetic relevă un alt aspect extrem de important, respectiv cât de mare poate fi diferența între un „părinte” și „succesorii” săi. Mediul operațional în care prevala RCIED a fost considerat de comunitatea de SIGINT și război electronic ca fiind unul simplu, ușor gestionabil din ambele perspective specifice comunității, respectiv *exploatare* și *contracarare*. Introducerea în ecuație a dronelor, în contextul unui conflict convențional, a complicat foarte mult mediul operațional din perspectiva aceleiași comunități.

Vom încerca, în continuare, să evidențiem de ce și unde apar principalele provocări, concentrându-ne asupra UAS-urilor, în special, întrucât ponderea utilizării acestora pe câmpul de luptă este covârșitoare comparativ cu UGS, USV și UUS.

RELAȚIONAREA ÎN MEDIUL ELECTROMAGNETIC: SIGINT ȘI RĂZBOI ELECTRONIC

Operațiile militare se bazează tot mai mult pe spectrul electromagnetic (Electromagnetic Spectrum - EMS) pentru comunicarea pe verticală și orizontală, pentru cunoașterea situației, detecția, urmărirea și angajarea țintelor. Acest spectru cuprinde toate radiațiile electromagnetice, separate în benzi de frecvențe. În același timp, mediul electromagnetic (Electromagnetic Environment - EME) este mediul geofizic în care radiațiile electromagnetice se propagă, influențate de factori precum terenul, vremea și condițiile atmosferice. Cu alte cuvinte, EME reprezintă mediul de confruntare care reunește toate celelalte medii și în care operează inclusiv UAS-urile. De vreme ce majoritatea UAS-urilor sunt dependente de EMS pentru a putea funcționa, întreruperea sau interzicerea accesului la EMS poate limita semnificativ posibilitățile de utilizare eficientă a acestora[3].

Războiul electronic (RE) reprezintă totalitatea acțiunilor desfășurate în mediul electromagnetic pentru controlul spectrului electromagnetic. Scopul războiului electronic este să reducă capacitatea adversarului de a folosi spectrul electromagnetic, simultan cu asigurarea folosirii neîngrădite a acestuia de către forțele proprii[4]. Acest deziderat este pus în practică prin acțiuni de supraveghere electronică (monitorizarea spectrului, goniometrarea și analiza semnalelor

de interes), atac electronic (sau bruiaj – pentru neutralizarea semnalelor de interes) și apărare electronică (măsurile luate de forțele proprii astfel încât să reducă probabilitatea de a fi detectate în EME și eficiența acțiunilor de bruiaj executate de inamic).

La rândul său, SIGINT reprezintă o ramură a activităților de informații, orientată pe culegerea de date și informații din comunicații (COMINT) și din parametrii semnalelor care nu conțin comunicații (ELINT - de exemplu semnale radar). Există o serie de asemănări între RE și SIGINT, unele state tratând chiar unitar cele două concepte, neexistând diferențe în ceea ce privește echipamentele sau procedurile folosite. În alte state, această comunitate este separată în două entități distincte, SIGINT fiind orientată specific spre culegerea de informații, iar RE către componenta activă, de tip ofensivă – bruiaj.[5]

În esență, diferența majoră dintre SIGINT și RE este reprezentată de modul în care este folosită informația obținută prin supraveghere electronică/ COMINT&ELINT. SIGINT se concentrează pe exploatarea informativă a mesajelor interceptate și a meta-datelor semnalelor de interes, pe când RE este orientat pe neutralizarea semnalelor de interes.

POSIBILITĂȚI DE DETECȚIE ȘI CONTRACARARE A DRONELOR

Majoritatea dronelor sunt dependente de utilizarea unor porțiuni ale spectrului electromagnetic pentru a-și putea îndeplini misiunea în ceea ce privește asigurarea legăturii de comandă-control (pentru pilotarea dronei, inclusiv cu sisteme redundante precum 4G/ 5G, STARLINK), a navigației GNSS[6] (care poate fi mono sau multi-constelație) și a legăturii de comunicații pentru transmiterea datelor culese către operator.

În acest context, este necesar să evidențiem principalele avantaje ale utilizării dronelor în acțiuni militare:

- dificultatea în a fi detectate și urmărite prin radiolocație, din cauza suprafeței efective de reflexie mici, ceea ce impune utilizarea unor radare specializate sau adaptarea radarelor existente;
- dificultatea și mai mare în a fi detectate și urmărite prin radiolocație în situația zborului la înălțimi mici;
- dificultatea neutralizării acestora cu ajutorul sistemelor de lovire dirijate în spectrul infraroșu (Infra Red - IR), din cauza amprentei termice reduse;
- saturația sistemelor radar de descoperire, în cazul în care dronele operează în număr mare sau roiuri;
- efectul de multiplicator al forței pe care îl generează, prin prisma raportului cost/ beneficiu;
- prețul redus de achiziție, procurarea facilă, posibilitatea producerii pe scară largă a dronelor, comparativ cu soluțiile de contracarare a acestora.

Datorită acestor avantaje, în conflictul ruso-ucrainean dronelor le-au fost alocate misiuni complexe, dintr-un spectru larg de acțiuni militare, de la cunoașterea situației, cercetare, identificarea și distrugerea țintelor până la coordonarea și corecția focului altor sisteme de lovire și evaluarea efectului la țintă a acestora. Dronele au căpătat o importanță majoră în desfășurarea acțiunilor militare, fiind utilizate de forțele armate ale celor două state, cu diferite rate de succes, iar ambii combatanți sunt interesați, pe de o parte, de dezvoltarea acestei capabilități proprii și, pe de altă parte, mult mai important, de consolidarea unor soluții pentru detecția și neutralizarea dronelor adversarului.

În îndeplinirea acestui obiectiv, cele două părți combatante iau permanent în calcul principiile de funcționare și caracteristicile specifice dronelor, în așa fel încât să se asigure că aceste amenințări sunt descoperite la momentul și pe aliniamentul optime și angajate cu mijloacele hard sau softkill cele mai eficace. Principalele caracteristici ale mijloacelor de detecție a dronelor care pot fi luate în calcul sunt cuprinse în tabelul următor:

Tip senzor	Avantaje	Dezavantaje	Posibile evoluții/ dezvoltări
Radar	- principalul senzor pentru detecție și urmărire; - rază mare de descoperire; - poate transmite date către sisteme hardkill/ softkill, inclusiv de tip PGM (Precision Guided Munition).	- preț relativ mare de achiziție; - detecție dificilă la altitudini joase; - senzor activ.	- dislocare pe platforme aflate la înălțime (inclusiv UAV).
Supraveghere electronică/ COMINT	- senzor pasiv; - rază mare de descoperire; - poate detecta locația pilotului/operatorului; - poate transmite date către sisteme hardkill/ softkill; - poate identifica ținta; - flexibilitate constructivă (portabil, mobil, staționar).	- preț mare de achiziție; - asigură localizare 2D a țintei, insuficientă precizie pentru dirijarea sistemelor hardkill de tip PGM (Precision Guided Munition); - mai puțin eficient față de dronele cu navigație sau operare autonomă, precum și față de dronele comandate prin GSM/ SATCOM/ STARLINK.	- dezvoltarea de versiuni portabile pentru avertizare timpurie, integrate în rețea; - instalare pe majoritatea platformelor de luptă.
EO/IR	- senzor pasiv; - poate identifica și urmări ținta.	- distanță eficace relativ redusă; - eficiență dependentă de condițiile meteo.	- utilizare conjugat cu radar sau senzori RF; - utilizare cu software de recunoaștere ținte bazat pe inteligență artificială.
Acustic	- senzor pasiv; - într-o rețea de senzori poate identifica și urmări ținta; - cost și factor Size Weight and Power (SWaP) reduse.	- distanță eficace redusă; - eficient împotriva țintelor zgomotoase; - eficiență redusă în mediu urban.	- dislocare în număr mare, integrate în rețea.

***Tabelul 1**: Mijloace de detecție ale dronelor*

Ținând cont de aceste caracteristici specifice mijloacelor de detecție a dronelor, putem considera că principalele elemente de care ar trebui să se țină cont în stabilirea unei metode de combatere a acestora sunt următoarele:

Metode combatere	Avantaje	Dezavantaje	Posibile evoluții/ dezvoltări
Bruiaj/ ECM	- eficient împotriva dronelor dependente de navigația GNSS și de comunicații pentru C2 și transmitere date.	- echipamentul de bruiaj poate fi detectat și localizat; - necesită redislocare repetată pentru supraviețuire; - poate afecta frecvențe civile; - dependent de date primite de la alte surse; - eficiență redusă dacă ținta folosește metode de protecție electronică.	- proliferarea dronelor ca echipamente de bruiaj/ momeală pentru activarea apărării aeriene inamice și mascarea pachetelor aeriene proprii de lovire.
Cyber	- preluarea legăturii C2 și aterizarea controlată a dronei; - eficientă mai ales asupra dronelor comerciale, cu protocoale de comunicații cunoscute.	- necesită actualizări ale bazei de date cu protocoale de comunicații asociate dronelor; - ineficientă asupra dronelor care folosesc protocoale de comunicații necunoscute.	- integrare cu senzori RF pentru detecția C2, identificarea protocolului de comunicații și preluarea controlului.
Hardkill cu arme de calibru mic	- disponibilitate vastă; - cost redus; - poate fi instalat pe platforme mobile.	- probabilitate redusă de lovire a țintelor cu dimensiuni reduse; - rază relativ mică de acțiune; - dependență de senzor precis de detecție și urmărire.	- integrare cu sisteme automate de avertizare și conducere a focului.
Hardkill cu rachete	- probabilitate mare de lovire a țintei.	- cost de achiziție posibil mai mare decât al țintei; - dependență de senzor precis de detecție și urmărire.	- echiparea dronelor cls. II și III cu sisteme de protecție electronică (dipoli pasivi și/sau capcane termice).
Microunde de putere mare	- eficiente împotriva roiurilor de drone; - cost redus de utilizare pe „lovitură”.	- rază mică de acțiune; - poate afecta echipamente proprii; - factor SWAP mare.	- reducerea factorului SWAP; - instalarea de arme cu microunde pe drone.
Laser de putere mare	- cel mai mic cost per lovitură comparativ cu alte soluții hardkill.	- rază mică de acțiune; - eficiență dependentă de vreme; - poate angaja o singură țintă simultan; - dependent de sisteme performante de urmărire a țintei; - factor SWAP mare; - preț mare de achiziție.	- progresul tehnologic va favoriza reducerea SWAP și a costului de achiziție.

***Tabelul 2**: Metode de contracarare a dronelor*

De asemenea, pentru reducerea posibilităților de detecție și contracarare a dronelor pot fi aplicate măsuri precum:

- utilizarea de receptoare GNSS multi-constelație, pentru utilizarea alternativă a unor sisteme satelitare de poziționare globală diferite, în caz de bruiaj;
- folosirea de antene rezistente la bruiaj (de exemplu, antene CRPA[7] sau antene cu câștig mic la unghiuri de elevație mici), care reduc semnificativ influența bruiajului asupra sistemelor de navigație[8];
- utilizarea unor sisteme de navigație inerțială sau hibridă (inerțială/GNSS), care permit dronelor evoluția către țintă în lipsa semnalului satelitar sau cu corecții periodice, bazându-se pe componentele interne pentru determinarea poziției, analizând viteza de deplasare, timpul și profilul terenului;
- utilizarea de sisteme alternative de navigație bazate pe sateliți LEO (Low Earth Orbit)[9], rețele de telefonie mobilă, SDR (Software Defined Radio);
- utilizarea unor sisteme redundante de comunicații;
- utilizarea unor sisteme de navigație asistate de inteligența artificială: compararea imaginilor înregistrate dinamic cu imagini prestocate și cu modelul digital al terenului.

ROLUL RE ÎN CONTRACARAREA DRONELOR ÎN CONFLICTUL DIN UCRAINA

Potrivit publicației de specialitate *Journal of Electronic Dominance*[10], Federația Rusă a dislocat cel puțin un echipament de bruiaj la fiecare 10 km de front, iar, de partea cealaltă, Ucraina ar fi primit „mii de sisteme de bruiaj" prin intermediul programului de asistență externă. De asemenea, conform aceleiași surse, 90% dintre acțiunile de război electronic executate pe frontul ucrainean sunt îndreptate împotriva dronelor[11]. Densitatea de drone comerciale este atât de mare încât pe nici un segment de front nu există canale de comunicații (frecvențe) libere, operatorii dronelor ajungând uneori să piardă temporar conexiunea cu platforma aeriană și să primească date video de la o altă platformă aeriană din vecinătate. De asemenea, potrivit unui studiu al Royal United Services Institute din Londra (RUSI)[12], în fiecare lună pe front sunt distruse aproximativ 10.000 drone[13]. Pe acest fond, contracararea dronelor depinde mult de controlul sau dominarea spectrului electromagnetic, motiv pentru care războiul electronic are un rol important în acest sens.

Acțiunile de bruiaj din partea beligeranților pentru contracararea dronelor sunt omniprezente. Cum pe frontul ucrainean sunt folosite pe scară largă drone comerciale, care utilizează aceleași benzi de frecvențe, fratricidul în spectrul electromagnetic este, am putea spune, omniprezent. Pentru operarea dronelor FPV (First Person View – vedere directă prin camera dronei) forțele ucrainene utilizează, în mod premeditat, frecvențele de lucru ale dronelor utilizate de F.Rusă pentru a crește șansele de supraviețuire ale propriilor echipamente.

Dronele operate în roiuri nu sunt exceptate de efectele bruiajului. Prin bruiaj sunt perturbate legăturile de comunicații dintre drone, făcând dificilă sau imposibilă comunicarea dintre drone sau între drone și operatori. În consecință, dispare coordonarea roiului, apar erori de navigație și coliziuni între drone.

EFECTE COLATERALE ALE BRUIAJULUI

Întrucât propagarea semnalelor radio nu ține cont de limitele administrative ale țărilor, efectele bruiajului se manifestă și în afara zonelor de operații. Navele de transport din Marea Neagră și Marea Mediterană au fost afectate atât de bruiajul sistemelor de navigație, cât și de pozițiile false raportate de aceste sisteme. De asemenea, bruiajul a afectat și navigația aeronavelor care tranzitează spațiul aerian aferent acestor zone și țărilor riverane. În plus, manipularea semnalelor de identificare ale navelor (AIS) poate fi folosită la ocolirea sancțiunilor economice vizavi de exportul de bunuri și produse din statele supuse acestor restricții. În consecință, bruiajul

sistemelor de navigație afectează tranzitul navelor comerciale, precum și al aeronavelor, ducând atât la pierderi economice importante pentru armatori, cât și la posibilitatea apariției unor accidente sau incidente. La nivel local au fost semnalate situații în care sistemele de navigație ale autovehiculelor au fost afectate de bruiaj.

CONCLUZII

Conflictul din Ucraina, operațiile israeliene din Gaza și acțiunile rebelilor Houthi din Yemen reliefează importanța tot mai ridicată a dronelor în operațiile militare, acestea fiind utilizate în misiuni complexe și într-un spectru larg de acțiuni militare, ca mijloace de lovire, ISR, de corecție și dirijare a focului, de recuperare personal sau evaluare a efectului la țintă. Asistăm la proliferarea unor categorii de echipamente ușor de produs în cantități mari și cu efect multiplicator foarte important pe câmpul de luptă. În același timp, dronele au devenit echipamente consumabile. În ambele tabere ale frontului din Ucraina se consumă mii de bucăți în fiecare lună. Astfel, cantitatea devine calitate, ambele forțe combatante investind masiv în aceste echipamente, precum și în tactici noi de utilizare a acestora și în metode de contracarare a lor.

Devine tot mai clar că viitoarele conflicte vor fi dominate de echipamentele fără pilot, fie acestea UAV-uri, UGV-uri, USV-uri sau UUV-uri, datorită caracteristicilor menționate, cât și scăderii numărul militarilor expuși focului direct sau indirect, implicit al victimelor. Numitorul comun al acestor echipamente este reprezentat de mediul electromagnetic, care le facilitează operarea, dronele utilizând o resursă finită pentru îndeplinirea misiunilor – frecvențele radio. Chiar dacă este de așteptat ca progresul tehnologic să producă schimbări majore în tacticile și procedurile de utilizare/ contracarare a dronelor, limitările actuale ale propagării radio nu vor permite, pe termen mediu, implementarea unor măsuri prin care dronele să opereze în zone mai libere ale spectrului electromagnetic.

În concluzie, contracararea dronelor depinde, în mare măsură, de controlul sau dominarea, temporare și în areale geografice limitate, a spectrului electromagnetic, deziderate realizabile prin acțiuni de război electronic. Aceste două *statu-quo*-uri sunt „vii”, se află permanent în dinamică, se manifestă în zone limitate și pe perioade de timp variabile, fapt care impune reanalizarea modului de desfășurare a acțiunilor militare din punct de vedere al doctrinei, operațiilor, instruirii, materialelor, programelor de înzestrare, logisticii necesare, a personalului specializat și liderilor performanți, a infrastructurii și informațiilor necesare (DOTMLPFI[14]).

[1] John Knowles, ”EMSO Strategies”, *Journal of Electromagnetic Dominance*, vol. 47, nr. 5, mai 2024, p.6, https://www.jed-digital.com/jedm/0524_may_2024/MobilePageArticle.action?articleId=1970745#articleId1970745, accesat la data de 11.08.2024.

[2] John Knowles, ”Drones, Drones, Drones”, *Journal of Electromagnetic Dominance*, vol. 47, nr. 6, iunie 2024, p. 6, https://www.jed-digital.com/jedm/0624_june_2024/MobilePagedArticle.action?articleId=1982081#articleId1982081, accesat la data de 28.07.2024.

[3] Panagiotis Stathopoulos, ”Electromagnetic Operations”, în *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, NATO Joint Air Power of Competence Center, Ianuarie 2021, p. 167-183, https://www.japcc.org/chapters/c-uas- electromagnetic-operations/, accesat pe data de 13.06.2024.

[4] Electromagnetic warfare, https://www.nato.int/cps/en/natohq/ topics_80906.htm., accesat la data de 24.06.2024; a se vedea și Don E. Gordon, *Electronic Warfare. Element of Strategy and Multiplier of Combat Power*, Pergamon Press, 2014, https://www.sciencedirect.com/ topics/engineering/electronic-warfare, accesat pe data de 24.06.2024.

[5] David L. Adamy, *EW 101: A First Course in Electronic Warfare*, Artech House, Boston-London, 2001 https://indianstrategicknowledgeonline.com/web/ Sigint%20vs%20ES.pdf., accesat pe data de 24.06.2024.

[6] Global Navigation Satellite System: în prezent există patru sisteme importante GNSS – GPS (SUA), Galileo (UE), Glonass (F.Rusă) și Beidou (R.P. Chineză).

[7] Controlled reception pattern antennas.

[8] The Latest in Machine Learning, online, https://paperswithcode.com., accesat în data de 20.07.2024.

[9] Will Barrett, Sharbel Kozhaya, Zak (Zaher) M. Kassas, *Session E6: Sensor Network and cooperative Navigation*, https://www.ion.org/gnss/abstracts.cfm?paperID=13918, accesat pe data de 24.06.2024.

[10] John Knowles, ”Drones, Drones, Drones”, *Journal of Electromagnetic Dominance*, vol. 47, no. 6, iunie 2024, p.6.

[11] Thomas Withington, *Clear Channels*, accesat la https://www.armadainternational.com/2024/03/secure-drone-communications-milcom/#:~:text=Armada%20has%20learned%20that%20around% need%20RF%2C%20are%20another%20option, accesat pe data de 10.06.2024.

[12] Royal United Services Institute/ RUSI - unul dintre cele mai vechi și mai recunoscute think-tank-uri, la nivel internațional, în domeniile politicii externe și securității internaționale.

[13] Jack Watling, Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*, https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine, accesat pe data de 10.06.2024.

[14] În limba engleză – *doctrine, operations, training, materiel, leadership, personnel, facilities, infrastructure, information.*

IMPLICAȚIILE NOILOR REGLEMENTĂRI EUROPENE ASUPRA MODELELOR DE INTELIGENȚĂ ARTIFICIALĂ OPTIMIZATE PENTRU RECUNOAȘTEREA IMAGINILOR

Florin SPOIALĂ*
Daniel-Sabin ȘTEFAN
Cornel ARGINT

Abstract

This article addresses the impact of the artificial intelligence/ AI regulations, specifically the AI Act adopted by the European Union, on the development and use of AI in various fields. The article defines fundamental AI concepts, such as Machine Learning (ML) and Deep Learning, explaining the differences between them as well as how these technologies are applied across different sectors. It explores the risks associated with AI, including mass surveillance and data manipulation, providing examples and case studies.

The article highlights the necessity of the AI act for regulating the use and development of AI, particularly in the context of security and ethics. It emphasizes both on the opportunities and challenges that these regulations bring, focusing on the balance between innovation and public protection.

Keywords: *artificial intelligence (AI); machine learning (ML); deep learning; AI regulations; YOLO, vulnerabilities; opportunities; European Union; AI Technologies.*

În ultimii ani, inteligența artificială (AI) a devenit un element central în diverse domenii, iar recunoașterea imaginilor reprezintă una dintre aplicațiile cele mai avansate și răspândite ale acestei tehnologii. Progresele rapide în dezvoltarea AI au condus la utilizarea pe scară largă a modelelor de recunoaștere a imaginilor, precum YOLO (You Only Look Once) și Google Vertex AI, care sunt esențiale pentru detectarea și clasificarea obiectelor în timp real. Aceste tehnologii sunt utilizate în domenii critice precum securitatea națională, supravegherea video și industria auto.

ASPECTE INTRODUCTIVE ÎN AI

AI reprezintă un domeniu al informaticii care se concentrează pe crearea de sisteme capabile să execute sarcini care, în mod normal, necesită inteligență umană. Aceste sarcini includ recunoașterea vorbirii, luarea deciziilor și procesarea limbajului natural.

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

Pentru a înțelege pe deplin implicațiile AI în dezvoltarea tehnologiilor, este esențială cunoașterea diferențelor dintre AI, machine learning (ML) și deep learning, astfel[1,2,3]:

» Inteligența Artificială (AI) este un termen general care se referă la sisteme informatice capabile să imite comportamentele umane pentru a efectua sarcini complexe, cum ar fi recunoașterea vorbirii, luarea deciziilor și traducerea limbilor. AI include orice algoritm sau sistem care poate percepe mediul înconjurător, poate învăța din date și poate lua decizii pentru a atinge un obiectiv specific[4].

» Machine Learning (ML) este o subcomponentă a AI care se concentrează pe dezvoltarea de algoritmi ce permit unităților de calcul să învețe din date. Algoritmii ML analizează datele și fac predicții, îmbunătățindu-se în timp fără a fi programați explicit pentru fiecare sarcină specifică. Exemple de algoritmi ML includ regresia liniară, arborii de decizie și rețelele neuronale de bază.[5,6]

» Deep Learning este o subcomponentă a ML și utilizează rețele neuronale artificiale cu multiple straturi pentru a analiza date complexe și a obține rezultate precise. Aceste rețele, inspirate de structura creierului uman, sunt utilizate în recunoașterea imaginii, procesarea limbajului natural și alte sarcini avansate.[7]

Utilizând aceste definiții, se poate realiza o clasificare mai detaliată a modelelor AI, explorând tipurile și specializările acestora cu scopul de a identifica modul în care sunt influențate de AI Act.

CLASIFICAREA MODELELOR DE AI

Inteligența Artificială este un domeniu vast care include o varietate de modele utilizate în scopuri diverse, de la recunoașterea imaginilor la generarea de text sau imagini. Modelele AI pot fi clasificate în funcție de tipul lor și de specializarea acestora.[8,9]

Modele de AI

În continuare, vor fi prezentate principalele tipuri de modele de inteligență artificială (AI) utilizate în diverse aplicații. Fiecare tip de model este explicat pe scurt, împreună cu exemple relevante din domeniul respectiv:[10,11,12,13,14]

a) ***Modele generative:*** Aceste modele sunt utilizate pentru a genera noi exemple de date, cum ar fi imagini, text sau muzică. Modelele învață distribuția datelor dintr-un set de antrenament și pot crea noi instanțe care urmează acea distribuție.

» *GANs (Generative Adversarial Networks):* GAN-urile sunt rețele care implică două modele - un generator și un discriminator - care se antrenează unul împotriva celuilalt. Generatorul încearcă să creeze date care să fie confundate cu date reale, iar discriminatorul încearcă să distingă între datele reale și cele generate. Exemplele din acest domeniu includ StyleGAN pentru generarea de fețe umane realiste și BigGAN pentru generarea de imagini de mare rezoluție.

» *VAEs (Variational Autoencoders):* Sunt modele generative care combină autoencoderele cu teoria probabilităților pentru a genera noi exemple de date. De interes, în acest context, sunt modelul VAE pentru generarea de imagini MNIST și utilizarea VAEs în generarea de molecule noi pentru cercetarea farmaceutică.

» *GPT (Generative Pretrained Transformer):* Acesta este unul dintre cele mai cunsocute modele generative pentru text, având capacitatea de a înțelege și ge a genera limbaj natural.

b) ***Modele Autoregresive:*** Acestea prezic următorul element dintr-o secvență bazându-se pe elementele anterioare din acea secvență. Exemplele includ GPT pentru generarea de text și PixelRNN pentru generarea de imagini.

c) ***Modele Discriminative:*** Sunt folosite pentru a clasifica sau a face predicții pe baza datelor existente, concentrându-se pe învățarea frontierei (threshold-ului) care separă clasele de date.

» *SVM (Support Vector Machines):* Algoritmi de învățare automată utilizați pentru clasificare și regresie, care funcționează prin identificarea unei frontiere optime care separă diferitele clase de date în spațiul caracteristicilor. Această frontieră, cunoscută sub numele de hiperplan, este determinată astfel încât să maximizeze distanța (marginea) dintre cele mai apropiate puncte de date ale claselor opuse, asigurând o clasificare cât mai precisă. Exemplele includ clasificarea spam-urilor în emailuri și clasificarea imaginilor în seturi de date precum CIFAR-10.

» *CNNs (Convolutional Neural Networks):* Rețelele neuronale convoluționale sunt utilizate în principal pentru recunoașterea imaginilor, aplicând filtre pentru a extrage caracteristici relevante din datele vizuale. Ca exemple pot fi amintite AlexNet pentru clasificarea de imagini și ResNet pentru recunoașterea de imagini complexe.

» *Random Forest:* Algoritm de clasificare și regresie bazat pe o colecție de arbori de decizie. Exemplele includ clasificarea utilizatorilor în analize de credit și clasificarea speciilor în analize de date biologice.

d) ***Modele de Învățare Reforțată:*** Aceste modele sunt utilizate pentru a învăța agenții să ia decizii secvențiale prin interacțiunea cu un mediu, având ca scop maximizarea unei funcții de recompensă.

» *Q-learning:* Algoritm de învățare prin recompensă care facilitează o politică optimă pentru luarea deciziilor. Exemplele includ jocuri de tipul "grid world" pentru agenți simpli și probleme de optimizare pentru managementul traficului.

» *Deep Q Networks (DQN):* Combină Q-learning cu rețele neuronale adânci pentru a învăța politici optime în medii complexe. Exemplele includ AlphaGo, pentru jocul de Go, și aplicații în controlul roboților.

» *Policy Gradient Methods:* Aceste metode sunt folosite pentru a învăța politici care să optimizeze direct o funcție de recompensă, fără a folosi un model Q. Exemplele includ REINFORCE pentru jocuri de Atari și PPO folosit în robotică.

În secțiunea următoare sunt prezentate tipurile de modele de AI specializate în anumite domenii sau sarcini specifice. Fiecare categorie este însoțită de exemple care ilustrează aplicațiile practice ale acestor modele:[15,16,17,18,19]

» *Recunoaștere de Imagini:* Modelele specializate în recunoașterea de imagini sunt optimizate pentru analiza și interpretarea vizuală, recunoscând obiecte, fețe sau texte.

» *CNNs (Convolutional Neural Networks):* Exemplele includ AlexNet, YOLO pentru detectarea obiectelor în timp real și Mask R-CNN pentru segmentarea obiectelor.

» *ResNet (Residual Networks):* Pot fi menționate aici ResNet-50 și ResNet-101, utilizate în competiții precum ImageNet.

» *Inception:* Exemplele includ Inception-v3 pentru clasificarea de imagini complexe.

» *Procesare de Limbaj Natural (NLP):* Modelele NLP sunt utilizate pentru analiza și generarea limbajului natural, având aplicații în traducere automată, analiza sentimentelor și generarea de text.

» *Transformer models:* Ca exemple pot fi incluse BERT pentru înțelegerea limbajului, GPT-3 pentru generare de text și T5 pentru sarcini de tipul text-to-text.

» *RNNs (Recurrent Neural Networks):* Exemplele includ LSTM pentru traducere automată și GRU pentru generarea de limbaj natural.

» *Seq2Seq Models:* În această categorie intră modelul de traducere automată de la Google pentru traducerea textelor în timp real.

» *Analiza Serie Temporală:* Aceste modele sunt specializate în analiza datelor secvențiale, fiind utile în predicțiile bursiere, analiza semnalelor biologice și alte aplicații care implică date temporale.

» *RNNs (Recurrent Neural Networks):* Exemplele includ predicția stocurilor bursiere și analiza comportamentului utilizatorilor în e-commerce.
» *LSTMs (Long Short-Term Memory Networks):* Modele utilizate pentru predicția datelor meteorologice, analiza semnalelor EEG în domeniul medical și predicția cererii în lanțurile de aprovizionare.
» *Generare de Imagini:* Modele generative de imagini utilizate pentru a crea noi imagini bazate pe seturi de antrenament, cum ar fi DALL-E.
» *GANs (Generative Adversarial Networks):* Exemplele includ StyleGAN pentru generare de fețe umane realiste și CycleGAN pentru transformarea stilurilor de imagine.
» *VAEs (Variational Autoencoders):* Aceste modele permit generarea de imagini MNIST și utilizarea VAEs în domeniul medical.

AI ACT ȘI CLASIFICAREA RISCULUI MODELELOR DE AI

Vulnerabilitățile modelelor AI

Modelele AI pot fi vulnerabile la diverse tipuri de atacuri cibernetice, cum ar fi atacurile de tip adversarial, unde atacatorii manipulează datele de intrare pentru a induce erori în predicțiile modelului. Aceste atacuri pot compromite integritatea și disponibilitatea sistemelor AI utilizate în infrastructurile critice, cum ar fi rețelele de energie, transporturi și comunicații. Pentru a proteja aceste sisteme sunt necesare măsuri precum: implementarea de mecanisme de detectare și răspuns la atacuri; îmbunătățirea securității datelor de antrenament; utilizarea tehnologiilor de criptare și autentificare; elaborarea unui cadru legislativ care să reglementeze utilizarea AI.

În acest context, Uniunea Europeană a adoptat *Artificial Intelligence Act*/ AI Act, în 2024, un cadru legislative menit să reglementeze utilizarea responsabilă și etică a AI. În această secțiune vom analiza implicațiile AI Act asupra modelelor AI optimizate pentru recunoașterea imaginilor, subliniind provocările și oportunitățile pe care aceste reglementări le aduc pentru viitorul acestor tehnologii.[20]

AI Act introduce un cadru juridic menit să gestioneze riscurile asociate cu utilizarea AI și să maximizeze beneficiile pentru societate. În acest context, modelele AI sunt clasificate în funcție de riscul pe care îl prezintă, fiecare categorie având implicații specifice, astfel:[21]

1. *Risc inacceptabil*: Modelele AI care prezintă un risc evident pentru siguranța și drepturile fundamentale ale oamenilor sunt interzise. Deși modelele AI optimizate pentru recunoașterea imaginilor nu se încadrează în această categorie, utilizările lor abuzive, cum ar fi supravegherea intruzivă neautorizată, ar putea fi strict reglementate. Este esențială conștientizarea acestor riscuri și implementarea măsurilor de siguranță care să prevină astfel de utilizări abuzive.
2. *Risc ridicat*: Modelele AI utilizate în infrastructuri critice, cum ar fi supravegherea video sau securitatea națională, sunt clasificate ca având un risc ridicat. YOLO v3/v5 și modelele implementate pe Google Vertex AI, care sunt folosite în astfel de contexte, trebuie să respecte cerințe stricte de securitate și conformitate, inclusiv evaluări riguroase și măsuri de protecție împotriva utilizării abuzive. Tranziția către conformitatea cu AI Act va necesita un efort coordonat între dezvoltatori, utilizatori și autorități pentru a asigura că aceste tehnologii rămân sigure și eficiente.
3. *Risc limitat*: Sistemele AI cu riscuri minime, cum ar fi modelele de tip chatbot și asistenții virtuali, trebuie să informeze utilizatorii că interacționează cu o AI și să respecte standarde minime de transparență. Chiar și pentru aceste sisteme, este crucial ca utilizatorii să fie bine informați și ca datele colectate să fie gestionate într-un mod care respectă confidențialitatea.

4. *Risc minim*: Aplicațiile AI fără risc semnificativ, cum ar fi filtrele de spam sau jocurile video, sunt permise fără restricții speciale. Totuși, chiar și în aceste cazuri, conformitatea cu regulamentele de bază este necesară pentru a asigura integritatea și transparența proceselor AI.

Uniunea Europeană a fost activă în promovarea și reglementarea AI pentru a asigura o dezvoltare etică și responsabilă chiar și înainte de apariția acestei legi. Astfel, în 2018, UE a lansat „Strategia pentru Inteligența Artificială", care urmărea să stimuleze investițiile în AI și să promoveze cercetarea și dezvoltarea în acest domeniu. Strategia a pus bazele pentru reglementările ulterioare, culminând cu AI Act, care introduce un cadru legal detaliat și cuprinzător.[22] Legea include și măsuri de transparență, cerințe de documentare și monitorizare continuă pentru a asigura conformitatea cu standardele europene. De asemenea, această lege introduce sancțiuni severe pentru nerespectarea regulilor, inclusiv amenzi substanțiale. Acest aspect subliniază importanța colaborării strânse între sectorul public și cel privat pentru a asigura faptul că modelele AI sunt dezvoltate și implementate în conformitate cu normele stabilite.[23]

De asemenea, în 2019, Comisia Europeană a publicat „Liniile directoare etice pentru o Inteligență Artificială de încredere", subliniind necesitatea transparenței, robusteții și echității în dezvoltarea și implementarea AI. Aceste linii directoare au fost menite să asigure că sistemele AI respectă drepturile fundamentale și să încurajeze responsabilitatea socială a dezvoltatorilor de AI.[24]

IMPLICAȚIILE AI ACT ÎN IMPLEMENTAREA TEHNOLOGIILOR DE AI

Din multitudinea de avantaje pe care le aduce inteligența artificală, se evidențiază capacitatea acesteia de a procesa rapid și eficient cantități uriașe de date, oferind suport esențial în diverse etape ale analizei și evaluării informațiilor. Fie că este vorba despre recunoașterea imaginilor, procesarea limbajului natural sau analiza comportamentelor complexe, AI reușește să ofere soluții inovatoare, precum metodele prin care aceste modele contribuie la prevenirea și gestionarea riscurilor, prin:[25]

- analize predictive: modelele AI pot analiza volume mari de date pentru a identifica tendințe și tipare care pot indica amenințări iminente/ aceste analize sprijină luarea deciziilor și a măsurilor preventive în timp util;
- simulări și scenarii: AI poate fi folosită pentru a crea simulări complexe și scenarii de răspuns la diferite tipuri de atacuri, ajutând la pregătirea și planificarea strategică.

Deși există provocări și dezavantaje asociate cu implementarea acestor tehnologii, ele nu sunt limitatate doar la AI, ci se extind la întregul spectru al sistemelor de calcul. În acest sens, de-a lungul timpului, sistemele AI și-au dovedit utilitatea în ceea ce privește securitatea națională. În contextul reglementărilor AI Act, aceste avantaje sunt dublate de necesitatea unei conformități riguroase. Astfel, AI Act nu doar că impune standarde stricte, dar și încurajează utilizarea responsabilă a AI, mai ales în sectoarele sensibile, cum ar fi securitatea națională. Această reglementare asigură faptul că tehnologiile AI, deși puternice și capabile, sunt utilizate într-un mod care respectă drepturile fundamentale și protejează datele personale.[26,27]

Implicațiile AI Act pentru YOLO v3/v5 și Google Vertex AI

Modelele YOLO v3/v5 sunt adesea utilizate în sisteme de supraveghere video în timp real și în securitatea națională. Datorită aplicabilității lor în infrastructuri critice, acestea sunt considerate modele cu risc ridicat în contextul legislativ adus de AI Act. Implicațiile includ:[28]

- securitate și conformitate: utilizarea YOLO v3/v5 va necesita respectarea unor standarde stricte de securitate, care să asigure că aceste modele nu sunt utilizate în moduri care ar putea compromite siguranța publică;
- transparență și responsabilitate: este necesară documentarea și monitorizarea detaliată a modului în care sunt folosite

aceste modele, inclusiv implementarea măsurilor de protecție împotriva utilizării abuzive în supravegherea publică;
- protecția datelor: supravegherea video implică adesea colectarea de date personale, astfel încât utilizarea YOLO v3/ v5 trebuie să fie conformă cu GDPR și alte reglementări de protecție a datelor.

Google Vertex AI, ca platformă de gestionare a modelelor AI, joacă un rol esențial în facilitarea utilizării la scară largă a tehnologiilor de recunoaștere a imaginilor. Sub AI Act, implicațiile pentru Google Vertex AI includ:[29]

- diminuarea riscului pentru aplicațiile critice: modelele AI de recunoaștere a imaginilor implementate prin Google Vertex AI în infrastructuri critice vor trebui să respecte reglementările stricte ale AI Act, asigurând conformitatea cu cerințele de securitate și protecție a datelor;
- cerințe de audit și transparență: Google Vertex AI va trebui să ofere instrumente de audit și transparență pentru a asigura monitorizarea continuă a performanței și conformității modelelor AI implementate pe platforma sa;
- interoperabilitate și standardizare: fiind o platformă globală, Google Vertex AI va trebui să asigure că modelele AI sunt compatibile cu standardele europene, facilitând cooperarea internațională și integrarea eficientă în diverse aplicații.

Aceste reglementări, în esență, impun un cadru de responsabilitate și securitate, asigurând că utilizarea AI, în special în sectoare critice, nu devine un risc pentru societate. Totodată, aceste cerințe sunt esențiale pentru menținerea încrederii publice în tehnologiile AI și pentru prevenirea unor potențiale abuzuri.[30] YOLO v3/v5 și Google Vertex AI reprezintă doar două dintre cele mai cunoscute exemple de utilizare a inteligenței artificiale pentru analiza datelor și realizarea de simulări complexe. Dacă pentru aceste tehnologii se implementează soluții eficiente care să prevină utilizarea în scopuri malițioase, acest lucru ar putea demonstra nu doar utilitatea AI Act, ci și capacitatea acestui act normativ de a trasa o direcție clară pentru toate modelele AI utilizate în prezent.[31]

STUDII DE CAZ

a) Israel și utilizarea AI în domeniul apărării[32]

Un exemplu notabil al utilizării AI în securitatea națională constă în implementarea modelelor de recunoaștere a imaginilor de către forțele armate israeliene. Israelul a dezvoltat și utilizat tehnologii avansate de AI, inclusiv modele de recunoaștere facială și analiză predictivă, pentru a preveni atacurile teroriste. Succesul acestor tehnologii a fost demonstrat prin reducerea numărului de incidente și îmbunătățirea răspunsului la amenințări. În acest context, modelele YOLO v3/v5 ar putea fi utilizate pentru detectarea și urmărirea automată a suspecților în timp real, oferind un avantaj semnificativ în securitatea națională.

Abordarea israeliană evidențiază modul în care implementarea eficientă a AI poate îmbunătăți capacitățile de apărare națională, dar și necesitatea unor reglementări care să asigure utilizarea etică și responsabilă a acestor tehnologii.

b) Proiectul Maven în SUA[33]

În Statele Unite, armata a utilizat AI pentru a analiza datele de la drone și sateliți din cadrul Proiectului Maven, un proiect menit să identifice și să neutralizeze amenințările înainte ca acestea să devină critice. Modelele AI implementate pe platforme similare cu Google Vertex AI au jucat un rol central în acest proces, permițând analiza rapidă a volumelor mari de date vizuale pentru a detecta obiective de interes. Acest proiect a demonstrat modul în care AI poate îmbunătăți eficiența operațiunilor militare (la nivelul UE sub AI Act, utilizarea unei astfel de tehnologii ar necesita respectarea unor standarde stricte de transparență și securitate). Pe de altă parte, analiza Proiectului Maven a evidențiat importanța transparenței și conformității în utilizarea AI în domeniul apărării, precum și rolul reglementărilor în utilizarea responsabilă a acestor tehnologii.

c) Cazul Cambridge Analytica[34]

Un alt exemplu notabil care subliniază necesitatea reglementărilor stricte în domeniul

AI și al datelor personale este cazul Cambridge Analytica. În acest caz, datele personale ale unor milioane de utilizatori Facebook au fost colectate și utilizate, fără consimțământul lor explicit, pentru a influența procesele electorale. Scandalul a evidențiat modul în care AI și tehnologiile de profilare pot fi utilizate în mod abuziv pentru manipularea maselor, generând un val de preocupări legate de confidențialitate și etică în utilizarea datelor.

Acest incident a accelerat discuțiile privind necesitatea unor reglementări mai stricte și a unor măsuri eficiente de protecție a datelor, cum ar fi GDPR. Cazul Cambridge Analytica servește drept avertisment asupra riscurilor implicate de utilizarea necontrolată a AI în combinație cu datele personale, subliniind importanța respectării principiilor de transparență și responsabilitate.

Cele trei studii de caz amintite mai sus demonstrează în mod clar impactul profund pe care AI îl poate avea în diverse contexte, de la securitate națională și până la influențarea proceselor electorale. În toate aceste situații, AI Act joacă un rol crucial în asigurarea utilizării etice și responsabile a inteligenței artificiale. Studiile demonstrează că utilizarea responsabilă și etică a AI în domeniile Big data, recunoaștere de imagine și procesarea limbajului natural poate fi transformată, cu ușurință, într-o utilizare malițioasă (cazul Cambridge Analytica) în lipsa reglementărilor. Acest vid legislativ a fost acoperit odată cu adoptarea la nivelul Uniunii Europene a AI Act, care ar trebui să încurajeze luarea unor astfel de măsuri la nivel global. Prin impunerea unor standarde stricte de transparență, securitate și conformitate, AI Act nu doar că protejează drepturile fundamentale ale cetățenilor, dar promovează și încrederea publicului în tehnologiile emergente. Fie că este vorba despre prevenirea abuzurilor în utilizarea datelor personale sau despre reglementarea aplicațiilor AI în domeniul apărării, AI Act oferă un cadru legal esențial pentru a naviga provocările complexe ale erei digitale.

CONCLUZII

AI Act reprezintă un pas important pentru reglementarea utilizării Inteligenței Artificiale în Europa, protejând atât drepturile cetățenilor, cât și securitatea națională a statelor membre. Modelele AI optimizate pentru recunoașterea imaginilor, precum YOLO v3/v5, și platforme avansate ca Google Vertex AI sunt utilizate în multe aplicații critice și, în consecință, sunt supuse unor reglementări stricte.

Studiile de caz prezentate din Israel și Statele Unite, alături de cazul Cambridge Analytica, demonstrează atât potențialul benefic al acestor tehnologii în securitatea națională, cât și riscurile semnificative pe care le pot reprezenta în lipsa unor reglementări adecvate. AI Act asigură utilizarea responsabilă și sigură a AI, prevenind riscurile asociate cu utilizările abuzive și protejând confidențialitatea datelor.

În contextul securității naționale, integrarea AI ridică provocări majore, în special în ceea ce privește supravegherea și protecția datelor personale. Din această perspectivă, reglementările GDPR și alte legi privind confidențialitatea datelor impun restricții stricte asupra modului în care datele personale pot fi colectate, stocate și utilizate. Provocările principale includ asigurarea securității și confidențialității, gestionarea datelor sensibile și aplicarea tehnologiilor de anonimizare. În același timp, AI are potențialul de a îmbunătăți semnificativ capacitățile de apărare prin analiza datelor din surse multiple și automatizarea răspunsurilor defensive.

Pentru a sprijini această tranziție către o utilizare responsabilă a AI, este esențial ca în dezvoltarea și utilizarea acestor modele să fie adoptate măsuri proactive care să asigure conformitatea cu reglementările impuse de AI Act, cum ar fi:

- implementarea unui mecanism de audit continuu: crearea sistemelor de audit care să verifice constant conformitatea cu AI Act, asigurându-se astfel respectarea reglementărilor impuse;
- educarea utilizatorilor finali: este important ca utilizatorii finali să fie informați cu privire la modul în care sunt utilizate modelele

AI și la drepturile lor în contextul acestor tehnologii;

- colaborarea strânsă cu autoritățile de reglementare: angajarea într-un dialog constant cu autoritățile de reglementare va ajuta procesul de dezvoltare a domeniului AI;
- promovarea cercetării în domeniul securității AI: investiția în cercetarea modurilor de protejare a modelelor AI împotriva atacurilor cibernetice va fi esențială pentru asigurarea unei utilizări sigure și etice a acestor tehnologii.

În concluzie, AI Act asigură folosirea responsabilă și sigură a AI, prevenind riscurile asociate cu utilizările abuzive și protejând confidențialitatea datelor. Pe măsură ce AI continuă să evolueze, colaborarea dintre dezvoltatori, utilizatori și autoritățile de reglementare va deveni crucială pentru adaptarea la cerințele legale și pentru a maximiza beneficiile acestei tehnologii în societatea modernă.

BIBLIOGRAFIE

1. BISHOP Christopher M., *Pattern Recognition and Machine Learning*, Information Science and Statistics Series, Springer, New York, 2006, 738 p.
2. Comisia Europeană, *Abordarea europeană a inteligenței artificiale*, 2024, online: https://digital-strategy.ec.europa.eu/ro/policies/european-approach-artificial-intelligence, accesat în data de 08.08.2024.
3. Comisia Europeană, *Europe fit for the Digital Age: Artificial Intelligence*, 2021, online: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682, accesat în data de 28.07.2024.
4. GOODFELLOW Ian, Bengio Yoshua, Courville Aaron, *Deep Learning,* Adaptive Computation and Machine Learning Series, Cambridge, MA, The MIT Press, 2016, 800 p.
5. KAUR Ravpreet, Sarbjeet Singh, „A comprehensive review of object detection with deep learning", în *Digital Signal Processing*, vol. 132, ianuarie 2023, online: https://www.sciencedirect.com/science/article/abs/pii/S1051200422004298, accesat în data de 03.08.2024.
6. WEST M. Darrell, John R. Allen, *How artificial intelligence is transforming the world*, Brookings Institution, 2018, online: https://www.brookings.edu/articles/how-artificial-intelligence-is-transfroming-the-world, accesat în data de 25.07.2024.
7. *** *Artificial Intelligence (AI) vs. Machine Learning*, Columbia Engineering, online: https://ai.engineering.columbia.edu/ai-vs-machine-learning, accesat în data de 15.07.2024.
8. *** *The Difference Between AI, Machine Learning, and Deep Learning*, NVIDIA Blog, online: https://blogs.nvidia.com/blog/2021/07/29/ai-vs-machine-learning-vs-deep-learning, accesat în data de 29.07.2024.
9. *** *Machine Learning vs. Artificial Intelligence: What's the Difference*, MIT, online: https://professionalprograms.mit.edu/blog/technology/machine-learning-vs-artificial-intelligence, accesat în data de 16.07.2024.
10. *** *Deep Learning Fundamentals Explained*, NVIDIA Blog, online: https://blogs.nvidia.com/deep-learning-fundamentals-explained, accesat în data de 02.08.2024.
11. *** Towards Data Science, online: https://towardsdatascience.com, accesat în data de 01.08.2024.
12. *** The Latest in Machine Learning, online: https://paperswithcode.com, accesat în data de 20.07.2024.

13. *** Parlamentul European, *Artificial Intelligence Act*, online: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, accesat în data de 05.08.2024.
14. *** *Machine Learning – What Is It and Why Does It Matter?*, NVIDIA Blog, online: https://www.nvidia.com/en-us/glossary/machine-learning/, accesat în data de 02.08.2024.
15. *** *Vertex AI Documentation*, Google Cloud, online: https://cloud.google.com/vertex-ai/docs, accesat în data de 10.08.2024.
16. *** Technology and Innovation, online: https://www.idf.il/en/mini-sites/technology-and-innovation/, accesat în data de 31.07.2024.
17. *** ”Cambridge Analytica: The Data Scandal that Changed the World”, *The Guardian*, The Cambridge Analytica Files, online: https://www.theguardian.com/news/series/cambridge-analytica-files, accesat în data de 26.07.2024.

[1] *** AI vs. Machine Learning, Columbia Engineering, online: https://ai.engineering.columbia.edu/ai-vs-machine-learning/, accesat în data de 15.07.2024.
[2] Christopher Bishop M., *Pattern Recognition and Machine Learning*, New York, Springer, 2006.
[3] Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep Learning,* Cambridge, MA, The MIT Press, 2016.
[4] *** The Difference Between AI, Machine Learning, and Deep Learning, NVIDIA Blog, online: https://blogs.nvidia.com/blog/2021/07/29/ai-vs-machine-learning-vs-deep-learning/, accesat în data de 29.07.2024.
[5] Machine Learning vs. Artificial Intelligence: What’s the Difference, MIT, online: https://professionalprograms.mit.edu/blog/technology/machine-learning-vs-artificial-intelligence/, accesat în data de 16.07.2024.
[6] *** Machine Learning – What Is It and Why Does It Matter?, NVIDIA Blog, online: https://www.nvidia.com/en-us/glossary/machine-learning/, accesat în data de 02.08.2024.
[7] *** Deep Learning Fundamentals, Explained, NVIDIA Blog, online: https://blogs.nvidia.com/deep-learning-fundamentals-explained/, accesat în data de 02.08.2024.
[8] *** Towards Data Science, online: https://towardsdatascience.com/, accesat în data de 01.08.2024.
[9] *** The Latest in Machine Learning, online: https://paperswithcode.com/ accesat în data de 20.07.2024.
[10] Ravpreet Kaur, Sarbjeet Singh, „A comprehensive review of object detection with deep learning”, *Digital Signal Processing*, vol. 132, ianuarie 2023, în Science Direct, online: https://www.sciencedirect.com/science/article/abs/pii/S1051200422004298, accesat în data de 03.08.2024.
[11] Towards Data Science, online: https://towardsdatascience.com/, accesat în data de 01.08.2024.
[12] Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Op. cit.*
[13] Christopher Bishop M., *Op.cit.*
[14] *** The Latest in Machine Learning, online: https://paperswithcode.com/ accesat în data de 20.07.2024.
[15] Ravpreet Kaur, Sarbjeet Singh, *Op. cit.*
[16] Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Op.cit*.
[17] *** The Latest in Machine Learning, online: https://paperswithcode.com/ accesat în data de 20.07.2024.
[18] Christopher Bishop M., *Op.cit*.
[19] *** The Latest in Machine Learning, online: https://paperswithcode.com/, accesat în data de 20.07.2024.
[20] Parlamentul European, *Artificial Intelligence Act,* online: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, accesat în data de 05.08.2024.
[21] *Ibidem.*

[22] Comisia Europeană, *Abordarea europeană a inteligenței artificiale*, 2024, online: https://digital-strategy.ec.europa.eu/ro/policies/european-approach-artificial-intelligence, accesat în data de 08.08.2024.
[23] Parlamentul European, *Artificial Intelligence Act,* online: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, accesat în data de 05.08.2024.
[24] Comisia Europeană, *Abordarea europeană a inteligenței artificiale*, 2024, online: https://digital-strategy.ec.europa.eu/ro/policies/european-approach-artificial-intelligence, accesat în data de 08.08.2024.
[25] Darrell M. West, John R. Allen, *How artificial intelligence is transforming the world*, Brookings Institution, 2018, online: https://www.brookings.edu/articles/how-artificial-intelligence-is-transfroming-the-world/, accesat în data de 25.07.2024.
[26] Parlamentul European, *Artificial Intelligence Act,* online: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, accesat în data de 05.08.2024.
[27] Comisia Europeană, *Europe fit for the Digital Age: Artificial Intelligence*, 2021, online: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682, accesat în data de 28.07.2024.
[28] Ravpreet Kaur, Sarbjeet Singh, *Op.cit.*
[29] *** Vertex AI Documentation, Google Cloud, online: https://cloud.google.com/vertex-ai/docs, accesat în data de 10.08.2024.
[30] Comisia Europeană, *Abordarea europeană a inteligenței artificiale*, 2024, online: https://digital-strategy.ec.europa.eu/ro/policies/european-approach-artificial-intelligence, accesat în data de 08.08.2024.
[31] Ravpreet Kaur, Sarbjeet Singh, *Op.cit.*
[32] *** Technology and Innovation, online: https://www.idf.il/en/mini-sites/technology-and-innovation/, accesat în data de 31.07.2024.
[33] Darrell M. West, John R. Allen, *Op.cit.*
[34] *** ”Cambridge Analytica: The Data Scandal that Changed the World”, *The Guardian*, The Cambridge Analytica Files, online: https://www.theguardian.com/news/series/cambridge-analytica-files, accesat în data de 26.07.2024.