MESAJUL MINISTRULUI APĂRĂRII NAȚIONALE CU OCAZIA SĂRBĂTORIRII A 160 DE ANI DE INFORMAȚII MILITARE

Gabriel Beniamin LEŞ, Ministrul Apărării Naționale

Direcția informații militare aniversează 160 de ani de existență, iar cu prilejul acestui eveniment remarcabil din istoria Armatei Române, mă simt onorat să adresez mesajul meu de apreciere şi de recunoştință uneia dintre structurile de elită ale Ministerului Apărării Naționale.

Prima filă din istoria Direcției informații militare, datată cu 12 noiembrie 1859, surprinde înființarea Corpului de Stat Major General al Armatei Principatelor Unite de către Alexandru Ioan Cuza. Dacă atunci, constituirea primei structuri de informații militare a reprezentat un punct de referință în ceea ce urma să însemne organizarea şi cristalizarea Armatei României, treptat, serviciul de informații militare a devenit un răspuns ferm la cerințele de securitate din perioada consolidării statului român şi s-a impus ca un element esențial în apărarea şi promovarea intereselor naționale de-a lungul istoriei României.

Structurile de informații militare au avut un rol esențial în momente critice de pe scena globală care au configurat, treptat, identitatea statului român, începând cu Războiul de Independență şi cu cele două războaie mondiale. Dinamica continuă a mediului de securitate global a determinat extinderea spectrului de provocări, care nu au făcut decât să amplifice gradul de adaptabilitate al structurilor de informații militare – trăsătură definitorie pentru întreaga Armată română, manifestată tot mai intens după aderarea României la Organizația Tratatului Atlanticului de Nord (NATO) şi la Uniunea Europeană (UE).

Implicarea României în teatrele de operații din Balcani, Orientul Mijlociu, Asia sau Africa reprezintă dovada că statul nostru este parte componentă activă în mecanismele de instaurare şi menținere a unui climat de securitate global şi prioritizează importanța respectării angajamentelor internaționale asumate. În acest context, îmi revin obligația şi onoarea de a aprecia efortul militarilor aflați în misiuni, care dau dovadă permanent de profesionalism şi devotament.

Participarea cu experți din rândul personalului de informații militare în comandamentele NATO sau UE este unanim apreciată, experiența acumulată în domenii din sfera activității de informații militare fiind şi promotorul înființării Centrului de excelență NATO în domeniul HUMINT în România.

Subsumat eforturilor continue de a consolida statutul de furnizor de securitate al României în regiune şi în zonele de criză şi de a gestiona dinamica provocărilor de securitate, Direcția informații militare a reuşit să exceleze prin profesionalism atât în teatrele de operații, cât şi în domeniul diplomației militare.

Rolul crucial al diplomației militare în prevenirea surprinderii strategice a României devine tot mai evident în contextul politic şi militar internațional actual, extrem de complex, marcat de tendința de multiplicare a spectrelor conflictuale, scăderea coeziunii în formatele tradiționale de cooperare şi asigurare a securității şi, în multe cazuri, de revenire a elementului militar în prim-planul relațiilor internaționale.

Astăzi, mai mult ca oricând după momentele accederii României în NATO şi UE, suplimentar rolului esențial în consolidarea dialogului strategic în planul apărării cu statele partenere, corpul ataşaților apărării are sarcina dificilă de a identifica primele semnale ale reconfigurării relațiilor dintre actori statali sau non-statali şi ale transformărilor de natură militară, politică şi de securitate care pot afecta interesele naționale ale țării noastre.

În aceste momente aniversare şi reiterând complexitatea mediului de securitate din proximitatea României, adresez mulțumiri corpului ataşaților apărării din Direcția informații militare pentru implicarea în promovarea imaginii Armatei Române şi a intereselor de securitate ale României pe scena internațională, asigurarea nivelului optim al cooperării pe linie militară şi pentru întreaga activitate specifică desfăşurată în țările de acreditare.

De ziua dumneavoastră, domnilor generali, ofițeri, maiştri militari, subofițeri, gradați şi soldați profesionişti, funcționari publici, personal civil contractual, vă mulțumesc pentru întreaga activitate desfăşurată şi vă felicit pentru profesionalismul şi devotamentul cu care acționați, vă urez succes în îndeplinirea misiunilor încredințate şi îmi exprim convingerea că veți onora blazonul dobândit în cei 160 de ani de existență, expertiză şi experiență!

La mulți ani, Direcția informații militare!

MESAJUL ŞEFULUI STATULUI MAJOR AL APĂRĂRII CU OCAZIA ANIVERSĂRII A 160 DE ANI DE LA ÎNFIINȚAREA INFORMAȚIILOR MILITARE

General Nicolae-Ionel CIUCĂ, Şeful Statului Major al Apărării

Este o onoare pentru mine să mă adresez, la ceas aniversar, personalului Direcției informații militare, instituție care aniversează 160 de ani de existență, în vremuri dificile ale istoriei neamului românesc, care stau drept mărturie a importanței structurii de informații a Armatei României de-a lungul timpului.

„Omnia incipit cum notitia” („Totul începe cu informația”) – deviza sub care vă desfăşurați activitatea – nu este decât o sintetizare a primei misiuni pe care a primit-o Secția a 2-a din cadrul Statului Major General al Armatei Principatelor Unite, în ziua înființării acesteia, ziua de 12 noiembrie 1859, aceea de a acționa *„pentru tot ce se atinge de lucrările statistice şi tot ce priveşte lucrările tactice şi strategice precum recunoaşteri şi itinerare militare, combinarea sau dirijarea manevrelor, alegerea pozițiilor şi întărirea taberelor militare”*.

Trecerea anilor a supus structura de informații militare mai multor încercări şi transformări, iar conflagrațiile mondiale prin care a trecut țara noastră au reprezentat dovada eficienței, profesionalismului şi dedicării cu care personalul militar a slujit sub Drapelul de luptă pentru cunoaşterea celor 1.400 km de front în Primul Război Mondial şi, ulterior, pentru cunoaşterea inamicului, indiferent de natura acestuia, precum şi pentru identificarea amenințărilor externe, militare şi non-militare, la adresa securității naționale.

Datorită celor care au fost şi, în egală măsură celor prezenți azi, în această zi de importanță istorică pentru Direcția informații militare, sărbătorim 160 de ani de continuitate într-un cadru mereu supus schimbărilor. Aniversăm o vârstă care ne permite să analizăm matur parcursul istoric al Direcției informații militare şi care ne oferă o înțelegere profundă asupra mediului de securitate actual, ca parte a celei mai puternice alianțe politico-militare din lume.

Sprijinul cu informații destinate elaborării planurilor de apărare, dezvoltarea capabilităților de culegere de informații şi transmiterea oportună şi standardizată a produselor informative de la structurile de nivel tactic la eşaloanele de nivel operativ şi strategic reprezintă o prioritate pentru Statul Major al Apărării şi se constituie într-un efort conjugat la care participă categoriile de forțe, comandamentele operaționale şi de sprijin. Expertiza Direcției informații militare în domeniile de competență a sprijinit permanent demersurile Armatei României, care este parte a unui amplu proces de modernizare şi adaptare la standardele NATO, atât din perspectivă tehnică, cât şi din perspectivă procedurală.

Transformarea Armatei României a dus la reconfigurarea şi adaptarea permanentă a DIM la evoluția mediului internațional pentru a răspunde cerințelor de securitate şi provocărilor

pe care le înfruntăm în activitatea curentă. Astfel, au fost dezvoltate capabilităţi moderne de HUMINT, SIGINT, GEOINT şi alte structuri de culegere de informaţii, care contribuie la îndeplinirea misiunilor direcţiei.

Folosesc acest prilej pentru a remarca modul în care DIM şi-a exercitat comanda operaţională asupra structurilor de informaţii din teatrele de operaţii, fapt ce demonstrează o legătură puternică între elementele de conducere şi cele de execuţie şi asumarea responsabilităţii de a confirma încrederea şi aprecierea partenerilor de misiune, fie că este misiune NATO, a Uniunii Europene sau de tip coaliţie.

Cei 160 de ani de istorie pe care îi aniversăm astăzi au fost marcaţi de eforturi şi sacrificii, care au mers, în multe situaţii până la sacrificiul suprem. Este datoria noastră istorică să ne cinstim eroii care au scris file din istoria Direcţiei informaţii militare, plătind pentru aceasta cu vieţile lor. Eroii noştri, prin sacrificiul suprem, vor rămâne mărturii ale devotamentului şi responsabilităţii pe care instituţia dumneavoastră şi le asumă permanent.

Informaţiile militare reprezintă astăzi un vector al politicii externe a României, contribuind la realizarea unor obiective naţionale din sfera securităţii şi la consolidarea rolului României şi Armatei României în cadrul organismelor internaţionale. În acest sens, Direcţia informaţii militare şi-a asumat responsabilităţile specifice ce derivă din calitatea României de membru NATO şi UE, acţionând într-un context geopolitic şi militar complicat şi imprevizibil.

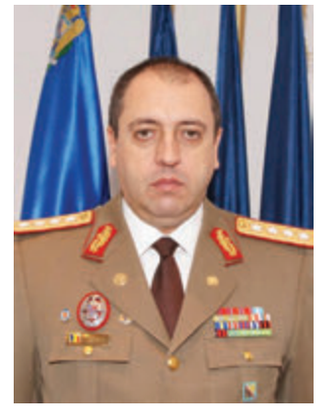
Prin informaţiile şi evaluările de securitate furnizate către NATO şi UE şi prin întreaga activitate a reprezentanţilor săi în cadrul comandamentelor şi altor entităţi de informaţii ale acestor organizaţii, Direcţia informaţii militare contribuie la asigurarea securităţii aliate şi a descurajării oricărei acţiuni convenţionale sau hibride din partea adversarilor statali sau non-statali.

Dragi camarazi,

Vă felicit cu ocazia împlinirii a 160 de ani de informaţii militare şi vă mulţumesc în numele Statului Major al Apărării pentru modul în care vă executaţi misiunile încredinţate şi pentru modul în care asiguraţi continuitatea valorilor promovate de instituţia dumneavoastră!

La mulţi ani!

MESAJUL DIRECTORULUI GENERAL AL DIRECȚIEI GENERALE DE INFORMAȚII A APĂRĂRII CU PRILEJUL SĂRBĂTORIRII A 160 DE ANI DE LA ÎNFIINȚAREA PRIMEI STRUCTURI DE INFORMAȚII MILITARE



General Marian HĂPĂU, Directorul general al Direcției generale de informații a apărării

Anul acesta sărbătorim 160 de ani de la înființarea primei structuri de informații militare în Armata Română. Momentul constituie mai mult decât celebrarea unei instituții; este o recunoaştere a misiunilor îndeplinite, a rolului Direcției informații militare în acțiunile Armatei României şi a meritelor oamenilor care au contribuit la scrierea istoriei acesteia. Aniversarea Zilei Direcției informații militare îmi oferă prilejul de a vă transmite, în numele comandamentului Direcției generale de informații a apărării, întreaga recunoaştere şi apreciere față de activitatea pe care o desfăşurați.

Direcția informații militare îşi are rădăcinile şi tradițiile în istoria poporului român şi este indisolubil legată de momentul naşterii României moderne, în anul 1859. Înființarea Secției a II-a în cadrul Statului Major al Armatei Principatelor Unite, prin înaltul Ordin de Zi nr. 83 din 12 noiembrie 1859, a fost determinată de necesitatea asigurării sprijinului informativ al nou înființatei Armate moderne române, iar acest act a fost pe deplin justificat, ulterior, în toate momentele de vârf, cumpănă şi jertfă ale poporului nostru.

De-a lungul timpului, profesionalismul, dedicația şi patriotismul personalului Direcției Informații militare au contribuit decisiv la gestionarea situațiilor de criză şi succesul operațiilor militare. Ca urmare, în acest context, la sărbătorirea a 160 de existență a informațiilor militare, trebuie să omagiem eforturile şi jertfa de sânge a tuturor camarazilor noştri, de pe ”fronturile văzute şi nevăzute” pentru apărarea Neamului şi Patriei.

În actualul context geopolitic, cu un mediu de securitate complex şi impredictibil, cu riscuri şi amenințări din ce în ce mai greu de identificat şi o gamă largă de actori care pot amenința securitatea națională a României, nu putem să nu remarcăm eforturile Direcției informații militare de adaptare continuă la tendințele şi cerințele actuale de sprijin cu informații a proceselor decizionale la nivel strategic, operativ şi tactic.

Direcția informații militare contribuie decisiv la efortul Direcției generale de informații a apărării în cadrul Comunității naționale de informații şi se situează la un nivel ridicat de expertiză. Direcția generală de informații a apărării, prin aportul Direcției informații militare, are o contribuție esențială la asigurarea intereselor naționale şi aliate de securitate, prin misiunile desfăşurate în afara teritoriului național, în domeniul diplomației militare şi în teatrele de operații, fiind deosebit de apreciată de partenerii externi.

În domeniul operațional, național şi aliat, Direcția informații militare are o contribuție definitorie în procesul de analiză strategică a apărării şi al revizuirii şi adaptării planurilor permanente de apărare la noile provocări de securitate.

Şi în viitor, Direcția informații militare trebuie să acționeze pro-activ şi anticipativ la provocările de securitate, adaptându-se continuu şi prioritizându-şi resursele şi efortul pentru furnizarea de intelligence strategic decidenților militari şi politico-militari.

La acest moment jubiliar, am deosebita bucurie de a transmite personalului Direcției informații militare, expresia celei mai înalte aprecieri. Mă simt onorat, cu prilejul aniversării a 160 de ani de existență, să vă felicit pe fiecare dintre dumneavoastră!

Vă urez multă sănătate, putere de muncă şi împlinirea idealurilor profesionale şi personale şi vă asigur de sprijinul meu în activitatea dumneavoastră!

La mulți ani!

Direcția generală de informații a apărării

INFOSFERA, anul XI, nr. 3, 2019

Revistă de studii de securitate şi informații pentru apărare

DIRECȚIA INFORMAȚII MILITARE – 160 DE ANI DE ISTORIE

General-maior Marian SIMA,
Şeful Direcției informații militare

Abstract

November 12th, 2019 marks the 160th anniversary of the Military Intelligence Directorate. It is more than the celebration of an institution; it is a celebration of its missions that have been accomplished, its role in the Romanian military operations, as well as a celebration of every soldier who wrote a chapter of its history.

The Romanian military intelligence has continuously reformed its organization and tasks throughout its 160 years of existence, depending on the historical context, the operational environment and the security risks and threats the Romanian military had to face. We learned from every challenge and we adapted to our adversaries' way of war, while representing the Romanian national and military interests abroad in every key-moment of our country's modern history.

What did not change, however, are the core values of the military intelligence professionals, who perform their missions selflessly, alongside the other branches of the Romanian military, serving the higher purpose of defending our country.

Keywords: *military intelligence, history, decision-makers, Romanian War of Independence, World War, NATO, EU.*

Regăsim istoria informațiilor militare la intersecția dintre două domenii: istoria militară şi istoria structurilor informative instituționalizate. Primul domeniu este foarte bogat şi la fel de vechi ca războiul, în timp ce al doilea este mai recent, în România apărând imediat după formarea statului român modern. Intersecția dintre cele două este complicată; este o serie de provocări şi reuşite, care au condus la o continuă adaptare şi la maturizarea Direcției informații militare de astăzi.

Anul acesta sărbătorim 160 de ani de la înființarea primei structuri de informații militare în Armata Română. Este mai mult decât celebrarea unei instituții; este o celebrare a misiunilor îndeplinite, a rolului său în acțiunile Armatei Române şi a oamenilor care au contribuit la scrierea istoriei Direcției informații militare.

Aceasta începe odată cu istoria Statului Major al Apărării, imediat după ce Alexandru Ioan Cuza declara la Focşani *„Unirea pentru vecie a celor două Principate"*, iar reformele începute pe timpul scurtei sale domnii puneau bazele statului român modern. Prima structură cu responsabilități în domeniul informațiilor militare, Secția a II-a, a fost înființată la data de 12 noiembrie 1859, prin Înaltul Ordin de Zi nr. 83, ca parte integrantă a Statului Major al

Principatelor Unite. La acel moment, Secția a II-a sprijinea conducerea Forțelor Armate române cu *„tot ce se atinge de lucrările statistice şi tot ce priveşte lucrările tactice şi strategice precum recunoaşteri şi itinerare militare”* într-o perioadă în care statul român nou format îşi definea locul pe harta Europei în plină reconfigurare.

Prima structură de informații militare înființată după unirea Principatelor române a fost condusă de sublocotenentul Gheorghe Slăniceanu, ajutat de sublocotenentul Ştefan Fălcoianu. Sistemul informativ de la acea vreme avea principalele componente ale unui serviciu de informații, desfăşurând activități de culegere, prelucrare şi transmitere a informațiilor.

Telegraful era, în perioada respectivă, mijlocul cel mai rapid de informare a factorilor de decizie, iar structurile informative din cadrul Ministerul de Război au beneficiat de sprijinul Telegrafului pentru a transmite puterii statale informații necesare actului de decizie. Informațiile erau obținute în mare parte prin activități specifice lucrului cu agentura.

În pofida dezvoltărilor tehnologice şi apariției unor noi discipline de Intelligence de-a lungul timpului, lucrul cu sursele umane este încă indispensabil unui serviciu de informații, iar structurile de informații militare române au continuat să îşi dovedească profesionalismul în acest tip de misiuni. Astăzi, contribuția militarilor români în domeniul HUMINT (Human Intelligence) în teatrele de operații, pe timpul misiunilor pe care armata română şi le-a asumat, este recunoscută la nivelul NATO, iar România găzduieşte Centrul de Excelență NATO în domeniul HUMINT la Oradea.

Un alt punct de reper istoric pentru activitatea de informații militare este legat de Războiul de independență (1877-1878), rămas în memoria colectivă datorită eroismului Armatei Române. Iminența războiului ruso-turc, obiectivul societății româneşti de obținere a independenței şi conjunctura internațională de la acel moment au condus la mobilizarea armatei şi intrarea în război.

Pierderile suferite de armata română au depăşit 4.000 de oameni, iar costurile financiare au fost suportate cu dificultate. *„Trupele sunt obosite nu numai de marş, dar şi de privaţiuni şi lipsă de hrană mai cu seamă. Este mai mult decât urgent trimiterea de pesmeţi (...) căci marşurile se vor face, dar oamenii vor cădea de osteneală fără hrană“*, scria Ştefan Fălcoianu, acum Şeful Statului Major al Armatei, către ministrul de Război, în decembrie 1877[1]. Localitățile Nazâr-Mahala, Novoselcea, Inova şi Capitonovcea, aflate pe căile de acces spre cetatea Vidinului, fuseseră puternic fortificate de către forțele otomane. În acel moment, organizată pentru apărare, cetatea Vidin era pregătită pentru o rezistența de lungă durată, dispunând de suficiente cantități de alimente şi muniții.

După încheierea Războiului de independență şi-au început activitatea primii ataşați militari ai României. La sfârşitul anilor 1870 era, astfel, acreditat primul ataşat militar român la Paris, căpitanul Pavel Stătescu, care a reînnoit relația bilaterală româno-franceză. Într-un timp scurt, statul român trimite ataşați militari în Germania (1884) şi Austro-Ungaria (1889), până în 1916 fiind deja înființate posturi de ataşați militari ai României în 11 capitale. Aceştia au avut un rol major în crearea premiselor cooperării bilaterale şi multilaterale a statului român care îşi proclamase independența, precum şi în informarea factorilor de decizie din țară despre potențialul şi intențiile altor state care puteau amenința în domeniul militar securitatea României. Nu multe lucruri ilustrează mai bine angajamentul față de țară decât îndeplinirea misiunii, oriunde şi oricând este nevoie, pentru promovarea şi apărarea intereselor României. Astăzi, Ministerul Apărării Naționale este reprezentat de ataşați ai apărării având reşedința sau extindere de acreditare în peste 60 de state.

Structura de informații a armatei s-a adaptat continuu în perioada care a urmat noilor realități regionale şi globale. Intrarea României în război alături de Puterile Antantei în 1916 a reprezentat începutul unei noi etape, trecerea de la starea de pace la cea de război determinând o serie de schimbări organizatorice la nivelul structurilor de informații ale Marelui Stat Major, care la momentul respectiv aveau o serie de deficiențe şi vulnerabilități. Primul Război Mondial urma

să arate că superioritatea capabilităților militare pe câmpul de luptă nu este suficientă, iar *„un serviciu secret nu se poate improviza”*[2], după cum remarca mai târziu Mihail Moruzov. Acțiunile desfăşurate de state „pe frontul secret” în secolul XX (spionaj, contraspionaj, diversiune, influență, propagandă, contrapropagandă) au determinat înființarea unor structuri specializate şi elaborarea unor *„Instrucțiuni asupra organizării”* acestora, care stabileau, între altele, *„cu mai multă exactitate misiunile aviației de recunoaştere (...) şi coordonarea activității agenților secreți”*, schițând practic doctrina activității de informații militare.

Tot experiența conflictelor ne-a arătat cel mai bine că amenințările se manifestă pe toate palierele puterii naționale şi a demonstrat necesitatea coordonării activității de informații desfăşurate în domeniul militar şi în alte domenii, în țară şi în afara teritoriului național. Astfel, decretele emise în perioada celui de-al doilea Război Mondial, prin care serviciul de informații a fost transferat în subordinea conducătorului statului şi transformat succesiv, precizau între altele că acesta *„conlucrează cu celelalte ministere si cu Marele Stat Major al Armatei”*[3].

Astăzi, Direcția informații militare cooperează cu serviciile naționale de informații şi structurile departamentale cu atribuții în domeniu şi este parte a Comunității Naționale de Informații.

Istoria recentă a fost marcată de o revoluție în domeniul militar, determinată în mare parte de descoperirile ştiințifice şi dezvoltările tehnologice, precum şi de creşterea relevanței amenințărilor de natură asimetrică în spațiul euro-atlantic. Statele europene au recunoscut importanța cooperării pentru prevenirea şi combaterea amenințărilor transfrontaliere şi faptul că securitatea națională este condiționată şi de securitatea regională.

Aderarea României la NATO şi UE, precum şi asumarea participării la coaliții multinaționale în teatre de operații din Balcani, Orientul Mijlociu, Asia de Sud-Vest sau Africa au prezentat noi provocări pentru Direcția informații militare, care s-a adaptat treptat standardelor euro-atlantice. Astăzi, Direcția informații militare răspunde cerințelor informative naționale şi aliate, contribuind la fundamentarea deciziilor care influențează securitatea României şi a aliaților săi în domeniul militar.

Evoluțiile tehnologice au determinat, pe de o parte, creşterea complexității amenințărilor, însă au permis şi dezvoltarea capabilităților militare de răspuns şi a celor de culegere de informații.

În prezent, Direcția informații militare este autoritate națională în ceea ce priveşte capabilitățile SIGINT (Signal Intelligence) şi război electronic, iar dezvoltarea domeniilor IMINT (Imagery Intelligence) şi GEOINT (Geospatial Intelligence) este parte a eforturilor continue de modernizare a capabilităților de culegere de date privind evenimente care pot afecta securitatea României.

În anul 2019, privim înapoi la cei 160 de ani de istorie şi ne amintim de progresele pe care instituția le-a făcut şi de misiunile îndeplinite. Ne amintim de contribuția informațiilor militare la decizii care au schimbat cursul destinului României în momente-cheie, precum cele două Războaie Mondiale, semnarea Pactului Ribbentrop-Molotov şi a Dictatului de la Viena sau invazia Cehoslovaciei. Ne amintim de eforturile depuse pentru ca România să fie parte a unor alianțe ale căror valori şi obiective le-am împărtăşit şi de devotamentul şi dedicarea personalului Direcției informații militare, dovedite pe timpul misiunilor externe pe care instituția şi le-a asumat. Profesionalismul acestor militari contribuie direct, alături de celelalte structuri din Armata Română, la afirmarea României ca partener serios şi capabil în relațiile bilaterale şi în cadrul Alianței Nord-Atlantice.

Nimic din ceea ce ne face acum să ne mândrim cu istoria Direcției informații militare nu s-a făcut însă fără sacrificii. Ne amintim de sublocotenenții post-mortem Samuilă Mihail Anton, Fogoraşi Iosif Silviu şi Şonei Narcis, căzuți la datorie în teatrul de operații Afganistan şi de toți cei care au plecat prea devreme dintre noi şi suntem recunoscători că astfel de oameni au ales să îşi dedice cariera activității de informații militare. Avem datoria şi privilegiul de a continua eforturile lor, pentru un scop mai presus decât interesele personale.

În prezent, mediul de securitate regional şi global şi complexitatea ameninţărilor asupra securităţii României cu impact în plan militar sunt foarte diferite de cele din secolele trecute, iar Direcţia informaţii militare nu mai este Secţia a II-a. Instituţia s-a adaptat permanent de-a lungul istoriei. A păstrat şi a perfecţionat, pe baza experienţei acumulate, capabilităţile care şi-au dovedit eficacitatea şi a dezvoltat altele noi, în funcţie de evoluţiile tehnologice şi ca urmare a diversificării ameninţărilor cărora Armata Română trebuie să fie în măsură să le răspundă.

În continuare, natura ameninţărilor se va modifica din nou, iar Direcţia informaţii militare se va adapta şi răspunde cerinţelor informative care vor apărea, asigurând un suport realist pentru fundamentarea deciziilor comandanţilor de la toate nivelurile. Vom reuşi acest lucru, pentru că istoria nu ne va permite să eşuăm.

---

[1] Raport al Colonelului Ştefan Fălcoianu, Şeful Marelui Stat Major al Armatei, către Ministrul de Război privind situaţia din sectorul Nazir-Mahala-Belogragic, 22 decembrie 1877, în Academia R.P.R. - *„Documente privind istoria României - Războiul de Independenţă“*, Bucureşti, 1952-1955, vol. VIII, doc. nr. 511

[2] Mihail Moruzov, şeful Serviciului S., EXPUNERE ASUPRA SERVICIILOR DE INFORMAŢII ALE ARMATEI, 1934, în Biblioteca Arh. S.R.I. dosar nr. 4/311, f. 15-37

[3] Decretul-lege nr. 3/083, art.2, emis la data de 8 septembrie 1940

DIRECȚIA INFORMAȚII MILITARE LA 160 DE ANI

*Dan NICULESCU**

Abstract

In the 160 years of existence of the Military Intelligence Directorate a few features have been highlighted that have continuously enlightened/marked this elite structure of Romanian Armed Forces. It is a red wire which could not be interrupted by the crises, tragedies, ups and downs during the state being/ existence/evolution and his army. In the current security environment, where intelligence services are facing a context of information overload and distortion, every day, the Military Intelligence Directorate provides fast and reliable intell that supports the decision making process.

Keywords: *Independence War, The Romanian Scouts, The First World War, The Second World War, Military Joint Staff.*

Acum 160 de ani, la 12 noiembrie 1859, domnitorul Alexandru Ioan Cuza, prin Înaltul Ordin de Zi nr. 83, a creat Statul Major General şi odată cu acesta a fost înființată şi structura de informații militare - Secția a II-a. Principalele atribuții funcționale ale noii structuri de informații a Armatei prevăzute în ordin erau: „(…) adunarea documentelor privitoare la statistica militară, procurarea şi studierea lucrărilor şi operelor publicate în străinătate şi studierea armatelor străine”.

Acesta a fost punctul de plecare spre o evoluție modernă a serviciului de informații militare, pe baze instituționalizate şi cu misiuni stabilite prin instrucțiuni şi decrete semnate de domnitor.

Drumul parcurs de la înființare până în prezent a fost unul sinuos, cu urcuşuri şi coborâşuri, cu dificultăți interne şi externe, cu succese şi eşecuri, cu invidii şi tendințe de a subordona această structură sau, cel puțin, de a o controla. Din fericire, toate aceste obstacole au fost depăşite şi au făcut serviciul de informații militare mai puternic, mai apt să-şi îndeplinească misiunile şi să reziste următoarelor atacuri ce nu vor întârzia să apară, dată fiind complexitatea actualului sistem politic internațional.

Pentru ca aceste afirmații să nu rămână cumva doar la nivel declarativ, voi încerca să trec în revistă cele mai importante evenimente care au marcat cei 160 de ani ai informațiilor militare în istoria modernă a României.

Astfel, imediat după înființarea Secției a 2-a, Marele Stat Major a apreciat că principala sursă de procurare a datelor de interes o constituie promovarea relațiilor de colaborare militară cu alte armate. Astfel, prin „Regulamentul asupra serviciului ofițerului de stat major”, apărut în baza Decretului 181 din 1870, a fost legiferată, pentru prima dată, acreditarea unor ofițeri din Corpul de stat major în funcții de ataşați militari sau alte funcții diplomatice.

Următorul pas major făcut de informațiile militare în procesul de transformare într-o structură eficientă, indispensabilă luptei armate,

* ***Preşedinte al Asociației Diplomaților Militari în Rezervă şi în Retragere „Alexandru Ioan Cuza“.***

s-a înregistrat după Războiul de Independență (1877-1878). Pe baza experienței acumulate pe timpul luptelor purtate în război şi analizându-se unele nereuşite pe linia prevenirii surprinderii, au fost făcute o serie de modificări privind modul de folosire în luptă a structurilor însărcinate cu cercetarea la nivel operativ şi tactic.

Perioada premergătoare Primului Război Mondial a marcat o amplificare a atribuțiilor structuri de informații militare, prin adăugarea unor responsabilități noi: studierea, încă din timp de pace, a teatrelor probabile ale unor acțiuni de luptă în vederea stabilirii celor mai potrivite aliniamente de apărare; zone propice pentru construirea unor sisteme de fortificații; studierea căilor de comunicații şi a caracteristicilor topografice ale terenului pe direcțiile probabile de acțiune; procurarea de hărți şi planuri operative ale statelor ce ne puteau deveni inamice.

Complexitatea sporită a sarcinilor, dar şi iminența războiului au impus efectuarea unor îmbunătățiri în ceea ce priveşte structura informațiilor militare. Astfel, în 1916 a fost înființat, în cadrul Secției a II-a din Marele Stat Major, Biroul de Informații. Instrucțiunile de funcționare ale acestui Birou prevedeau că „pentru culegerea ştirilor un rol foarte mare îl au agenții de spionaj şi agenții secreți, care trebuie să funcționeze în două zone şi anume: în spatele frontului inamic şi în zona operațiilor, adică pe linia fronturilor".

Tot în anul 1916 se dezvoltă structurile de cercetare tactică prin înființarea birourilor de cercetare - la nivelul diviziilor şi corpurilor de armată - şi numirea ofițerilor cu cercetarea - la nivelul brigăzilor şi regimentelor. Totodată, anul 1916 marchează şi folosirea pentru prima dată în Armata României a cercetării radio ca mijloc de culegere de informații despre inamic. De asemenea, a crescut importanța executării cercetării cu mijloacele mobile nou apărute, în primul rând cu cele aeriene (avioane şi baloane), completându-se astfel acțiunile de cercetare ce se executau de către unitățile şi subunitățile de cavalerie.

O inițiativă remarcabilă a perioadei Primului Război Mondial a fost aceea a creării unui cadru organizat de pregătire a tineretului pentru apărarea țării, cu predilecție fiind atraşi către activitățile de cercetare. Răspunsul tinerilor a fost pe măsura inițiativei, aceştia înscriindu-se masiv în structurile nou înființate. Astfel a luat ființă asociația „Cercetaşii României" (înființată în anul 1913 şi legiferată în 1915), care şi-a adus o însemnată contribuție la pregătirea ca cercetaşi a tinerilor şi la educarea lor patriotică. Mulți dintre cei care au activat în această asociație au luptat în Marele Război, unii dintre ei ca voluntari, unii au prins momentul astral al României - Marea Unire din 1 Decembrie 1918 -, alții s-au bucurat de sus.

Poate că momentul înființării Cercetaşilor României, poate războiul sau jertfa, poate insuflarea în sufletele acelor copii a celor mai sincere şi profunde sentimente patriotice pe care, la rândul lor le-au transmis mai departe, poate toate aceste motive la un loc au contribuit la întipărirea adânc în memoria poporului român a ceea ce a însemnat mişcarea cercetaşilor, mişcare ce a continuat pentru o bună bucată de timp şi care astăzi este, practic, inexistentă.

Probabil că acum tinerii trebuie învățați altceva, dar memoria colectivă nu poate fi ştearsă… deocamdată.

Perioada interbelică a fost pentru țară una de mare avânt, de progres, de modernizare a instituțiilor statului. Armata şi, în cadrul acesteia, serviciul său de informații, au urmat acelaşi curs al modernizării, al folosirii experienței dobândite într-un război în care soarta statului român a fost pe muchie de cuțit pentru eliminarea disfuncționalităților.

Astfel, numărul ataşaților militari acreditați în străinătate a crescut, se înființează centre de informații teritoriale (1923) şi două posturi radio–gonio, se stabilesc protocoale de cooperare pe linie informativă cu anumite instituții de stat precum poşta, căile ferate, vama, marina comercială şi comandamentul trupelor de grăniceri.

În anul 1930 se organizează serviciul de informații tehnice în interiorul țărilor vecine (Rusia, Ungaria şi Bulgaria), iar în 1938 s-a elaborat un nou regulament privind atribuțiile ataşaților militari români acreditați în străinătate. De asemenea, apar instrucțiunile de organizare şi funcționare a serviciului de curieri diplomatici pentru nevoile Marelui Stat Major.

Întrucât după anul 1918 Secția a II-a a început să primească tot mai multe sarcini contrainformative, a apărut necesitatea separării informațiilor militare de contrainformațiile militare, fapt ce s-a realizat în anul 1920 când biroul de contrainformații din cadrul Secției a II-a a fost transformat într-o secție independentă a Marelui Stat Major.

Perioada de liniște necesară pentru reorganizarea și modernizarea structurilor informative ale Armatei României nu a fost prea mare fiindcă tensiunile acumulate, dorința de revanșă a învinșilor Primului Război Mondial, apariția fascismului și a bolșevismului au determinat începerea unei noi catastrofe pe „bătrânului continent" – Al Doilea Război Mondial.

Pe toată durata războiului, Secția a II-a și-a concentrat forțele și mijloacele pentru a informa conducerea statului și a Armatei cu date cât mai veridice privind capacitatea de luptă a armatelor statelor vecine, dislocarea marilor unități și unități, situația de pe diferite fronturi ale acțiunilor de luptă etc.

După întoarcerea armelor de către armata română împotriva Germaniei hitleriste, serviciul de informații al Marelui Stat Major a organizat o puternică rețea informativă care a acționat în spatele frontului german pe toată durata operațiilor, până la eliberarea Ungariei și Cehoslovaciei.

Evenimentele ce au urmat după război, plasarea României în categoria țărilor învinse, cedările Occidentului în fața pretențiilor URSS și schimbarea forțată a regimului politic din România au avut urmări grave atât pentru țară, cât și pentru instituțiile acesteia. Pentru serviciul de informații militare a urmat o perioadă de declin, de restrângere a activităților, de reducere a personalului și de control politic extern, dar mai ales intern.

Astfel, în anul 1951 Secția a II-a a fost transformată în Direcția Informații a Marelui Stat Major, iar sarcinile contrainformative au fost transferate către Ministerul de Interne.

Atmosfera a devenit puțin mai respirabilă abia în anul 1958, când trupele sovietice au fost nevoite să părăsească România. Se pare că la această reușită și-a adus contribuția și structura de informații militare.

Pentru Direcția informații militare plecarea rușilor din țară a însemnat o scădere a presiunii acestora asupra deciziilor în urma înlăturării consilierilor sovietici, ceea ce a dus la îmbunătățirea activităților în toate compartimentelor sale, mai cu seamă a celor cu caracter informativ, al cercetării radio, al reprezentării și dezvoltării relațiilor cu alte armate.

Presiunea externă s-a redus, în schimb a crescut presiunea internă asupra Direcției Informații. Aceasta s-a materializat prin hotărârea luată, la inițiativa Ministerului de Interne, de a se stabili o „colaborare" cu Ministerul Apărării Naționale. Această colaborare însemna ca Direcția informații militare să devină dependentă de Ministerul de Interne, mai cu seamă pe problemele operative și ale încadrării cu personal. Abia în anul 1968 această situație a luat sfârșit, dar unele cicatrici au rămas.

Ca de obicei, lucrurile bune nu sunt de durată. Pentru Direcția informații militare perioada 1970 – 1989 a fost una de intensificare a controlului politic exercitat prin structurile de partid și ale Ministerului de Interne.

Revoluția din Decembrie 1989 a însemnat începerea unei noi etape pentru Direcția informații militare, cu noi misiuni și provocări, cu noi transformări, ajustări și modernizări. O astfel de măsură, care în mod categoric trebuie menționată, este apariția pe scena informațiilor militare a Direcției generale de informații a apărării (1999).

În încheiere, doresc să subliniez că în cei 160 de ani de existență ai Direcției informații militare au fost evidente câteva trăsături ce au particularizat continuu această structură de elită a Armatei României. Este un fir roșu care nu a putut fi întrerupt de crizele, tragediile, suișurile și coborâșurile care au marcat existența țării și a Armatei sale.

Poate că vă așteptați să încep să le enumăr. Nu o să fac așa ceva. O să vă las să priviți singuri în cele mai adânci cotloane ale conștiinței dumneavoastră și să le descoperiți singuri.

Cred că este un exercițiu folositor.

La Mulți Ani, Direcție de informații militare, și f*ii pregătită fiindcă intemperiile istoriei nu se termină niciodată!*

ATAŞATURA APĂRĂRII – TRADIȚIE ŞI ACTUALITATE

Col. dr. Dumitru NEACŞU
Mr. Lucian ENE*

Abstract

In the 160 years of existence, military diplomacy proved to be a representative pillar of the Romanian Diplomacy. The transformations recorded in the international political environment, in the last century and a half, have pointed out the national military structures to a continuous process of adaptation to the reality of the security context, a process, to which the Military Intelligence Directorate has made its full contribution.

Keywords*: defense diplomacy,*

Cine este bine şi la timp informat, învinge"[1]

În cei 160 de ani de existență, Ataşatura Apărării s-a evidențiat a fi un pilon reprezentativ al diplomației române. Transformările de substanță înregistrate în mediul politic internațional, în ultimul secol şi jumătate, au supus structurile de forță naționale la un proces de adaptare continuă la realitatea contextului de securitate.

Un moment reprezentativ al evoluției instituției Ataşaturii Apărării îşi are izvorul la 12 noiembrie 1859, când domnitorul Alexandru Ioan Cuza, prin Înaltul Ordin de Zi nr. 83, înființează Secția a II-a Statistică şi Studiul Armatelor Străine. Misiunea primei structuri de informații militare a Statului Major al Armatei Principatelor Unite era despre „*tot ce se atinge de lucrările statice şi tot ce priveşte lucrările tactice şi strategice precum recunoaşteri şi itinerare militare, combinarea sau dirijarea manevrelor, alegerea pozițiilor şi întărirea taberelor militare"*[2]. Şeful structurii era sublocotenentul Gheorghe Slăniceanu, având ca locțiitor pe sublocotenentul Ştefan Fălcoianu[3].

Misiunile îndrăznețe ale structurii de informații nou înființate *(studiul şi pregătirea manevrelor de amploare, studiul teatrelor de război, studiul armatelor străine, regulamente tactice străine, studii statice generale şi speciale)*[4] au fost greu încercate încă de la început de nenumărate provocări de subminare a intereselor noului stat balcanic, concretizate în încercările Turciei şi Austriei de a destabiliza statul român, în care vedeau un pericol pentru propriile interese în Europa Centrală.

Cu privire la originea funcției de ataşat militar se poate afirma că aceasta a apărut în secolul al XVII-lea, în timpul Războiului de 30 ani, atunci când ducele de Richelieu a trimis reprezentanți militari în afara țării pentru a realiza legătura cu puterile aliate, să supravegheze inovațiile din domeniul militar şi, totodată, să furnizeze informații despre intențiile adversarilor.

În România, în anul 1860, diplomația română a apărării, ca parte distinctă a diplomației, ia naştere în momentul în care domnitorul Cuza

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

hotărăşte trimiterea primului „diplomat militar" al Armatei Române în Franţa, în persoana căpitanului Ioan Alecsandri, fratele poetului Vasile Alecsandri. Pentru a-i creşte vizibilitatea pe lângă Napoleon al III-lea, tânărul şi deosebit de capabilul căpitan este avansat succesiv la gradele de maior şi locotenent–colonel. În poziția sa, locotenent-colonelul Ioan Alecsandri a reuşit nu numai să consolideze internațional actul Unirii, în care Franța a avut un rol deosebit, dar să şi dezvolte relațiile militare româno-franceze.

Ulterior, declarareaîn 1877a independenței de stat deschide calea pentru realizarea unei diplomații statale la nivelul celorlalte state europene. Chiar dacă declararea unilaterală a independenței de stat a românilor nu a fost agreată de majoritatea puterilor europene[5], diplomația activă din perioada imediat următoare, prin intermediul tuturor componentelor, inclusiv cea militară, a reuşit să obțină consensul politic dorit.

În anul 1882, pentru perfecționarea pregătirii profesionale a personalului Secției a II-a, a fost elaborat Regulamentul ataşaților militari în care au fost specificate, pentru prima dată, şi misiunile ataşatului român al apărării, astfel:

- întreținerea de relații cordiale cu armata şi statul acreditar şi corpul diplomaților din acel stat;
- cunoaşterea în amănunt a armatei şi țării în care este acreditat;
- desprinderea concluziilor utile pentru modernizarea înzestrării şi introducerii de noi acte normative în armata română;
- identificarea oportună a intențiilor de prietenie din partea unor state şi armate şi, cu prioritate, a celor cu gânduri ascunse (duşmănoase), mai ales dacă sunt vecine, şi comunicarea urgentă a acestora ministrului de război român, distingând în rapoartele sale ceea ce a văzut şi ceea ce a auzit[6].

De-a lungul celor 160 de ani, dispozitivul ataşaturii apărării a cunoscut atât etape exponențiale de dezvoltare, dar şi perioade de declin profund, procesul de transformare fiind în strictă legătură cu evoluțiile mediului de securitate internațional şi situația politico-militară națională.

De exemplu, în anul 1914 România avea opt ataşați ai apărării[7] cu reşedința în țările de acreditare, doi dintre aceştia având extindere diplomatică în alte două țări.

Directa dependență dintre dimensiunea dispozitivului ataşaturii apărării şi situația politico-militară națională este foarte bine surprinsă la sfârşitul Primului Război Mondial, când România avea ataşați ai apărării în 14 state[8], reprezentare care era considerată, pentru acea perioadă, foarte bine conturată. Acelaşi efect, dar data aceasta în sens invers, este observat şi 27 de ani mai târziu, la finele celui de-al Doilea Război Mondial, când dispozitivul a fost redus la zero[9].

Pentru diplomația militară românească, perioada 1930-1940 a constituit cea mai mare provocare din istoria ei de 160 de ani, perioadă în care ofițerii Secției a II-a/ Marele Stat Major şi ataşații apărării de pe lângă misiunile diplomatice ale României din străinătate au participat activ pentru fundamentarea şi semnarea convențiilor militare ce au însoțit Pactul de apărare româno-polon şi pactele de organizare ale Micii Înțelegeri şi Înțelegerii Balcanice.

Totodată, deceniul al treilea al secolului XX s-a constituit, într-o perioadă de adaptare organizatorică, economică, financiară şi administrativă a statului român la noile condiții postbelice, etapă de adaptare resimțită din plin şi la nivelul structurii Ataşaturii Apărării care din punct de vedere numeric, a înregistrat o evoluție sinusoidală continuă.

Cel mai important rol de informare al Marelui Stat Major român, dar şi al Casei Regale a României, cu privire la situația politico-militară a Europei din ajunul celui de-al Doilea Război Mondial, a revenit ataşaților militari. Cu toate acestea, analizele prospective şi rapoartele redactate, în mare măsură relevante, nu au putut asigura un alt deznodământ la şirul de evenimente dezastruoase ce au urmat. Politica ezitantă a celor două mari puteri ale Europei de la acea vreme, Franța şi Marea Britanie,față de acțiunile hotărâte ale Germaniei au făcut ca, în cele din urmă, Mica Înțelegere şi Antanta Balcanică să devină două tratate inoperabile.

Ulterior dureroasei lovituri înregistrate de structura Ataşaturii Apărării la sfârşitul celui de-al Doilea Război Mondial,atunci când toate birourile ataşaților apărării au fost desființate, în anul 1948 dimensiunea dispozitivului ataşaturii a fost restabilită la numărul de 14 reprezentanțe[10].

Bineînțeles că noul dispozitiv al Ataşaturii Apărării şi misiunile informative ale structurii serveau noilor orientări ale politicii de stat dintr-o Românie aflată sub o puternică influență a politicii externe sovietice. Creşterea rapidă a numărului de ataşați ai apărării a fost determinată şi de apariția celor două blocuri militare antagoniste, NATO (1949) şi Tratatul de la Varşovia (1955).

Inițial, în alegerea viitorului ataşat al apărării nu s-a ținut cont de calitățile strict necesare unui diplomat militar de carieră, criteriul hotărâtor rămânând cel politic (originea socială), dar după anul 1960 baza de selecție a reuşit să se îmbunătățească considerabil atât în ceea ce priveşte pregătirea militară, cât şi din punct de vedere al culturii generale, cunoaşteriilimbilor străine etc. Pentru următorii 30 de ani, diplomația română a apărării a înregistrat o perioadă de relativă constanță atât din punct de vedere al misiunilor, cât şi al acoperirii diplomatice, cu observația că în perioada menționată politicul şi ideologicul au dominat atitudinea autorităților vis-à-vis de foştii ataşați ai apărării. Mulți dintre ei, ofițeri cu merite deosebite în activitățile specifice, au suferit, nu de puține ori, acțiuni de defăimare şi/sau compromitere doar pentru că făceau parte din „elita" Armatei Române - structura Ataşaturii Apărării.

După sfârşitul Războiului Rece, Armata României a fost nevoită să facă față unei noi arhitecturi naționale şi internaționale. Odată cu schimbările survenite în mediul de securitate, rolul ataşatului apărării a devenit mult mai complex, acestuia revenindu-i o poziție cheie în diplomația națională. În această perioadă, dispozitivul Ataşaturii Apărării a fost fundamental regândit şi dezvoltat, iar la nivelul anului 2006 România deținea ataşați ai apărării în 58 de state (42 de birouri ale ataşaților apărării cu reşedință permanentă în țările de acreditare, respectiv 16 state acoperite prin extinderi de acreditare)[11].

Acesta este momentul în care Ataşatura Apărării cunoaşte o transformare radicală, efortul activității de culegere a informațiilor concentrându-se pe noile zone de criză şi conflict, cu eventual potențial de a aduce atingere intereselor naționale ale României (spațiul ex-sovietic şi Balcanii).

În prezent, structura Ataşaturii Apărării reprezintă expresia schimbărilor succesive survenite în cadrul structurii Direcției Informații Militare şi Armatei României, dispozitivul Ataşaturii Apărării acoperind 62 de state (35 de birouri ale ataşaților apărării cu reşedință permanentă, respectiv 27 de state acoperite prin extinderi de acreditare).

Din punct de vedere al acoperirii nevoilor cu informații ale beneficiarilor, actualul dispozitiv al Ataşaturii Apărării răspunde în mod adecvat solicitărilor. Realitatea reflectă faptul că misiunile Ataşaturii Apărării au devenit tot mai dinamice, diversificate, complexe şi mai direcționate,pe de o parte, pentru a face față, cerințelor naționale şi internaționale din ce în ce mai cuprinzătoare şi, pe de cealaltă parte, pentrua păstra cu onoare şi demnitate imaginea celor 160 de ani de istorie măreață a Direcției Informații militare.

Astfel, misiunile[12] clasice ale ataşatului apărării, militar, aero şi naval al României s-au transformat şi s-au adaptat la contextul şi mediul de securitate, astfel:

- reprezentarea Ministerului Apărării Naționale şi a Armatei României față de autoritățile militare şi civile, corpul diplomatic militar şi populația din țara de acreditare;
- promovarea intereselor industriei române de apărare;
- culegerea, exploatarea, analiza şi transmiterea de informații;
- consilierea ambasadorului în chestiuni legate de apărare.

În conformitate cu documentele politico-militare de planificare a apărării şi cerințele cuprinse în Țintele de Capabilități asumate de România în Cadrul procesului NATO de planificare a apărării, dar şi cu angajamentele de modernizare a Armatei Române, Direcția Informații Militare

prin intermediul Ataşaturii Apărării pune mare accent, cu medierea ataşatului apărării, pe întărirea colaborării dintre România şi statul acreditar în domeniul industriei de apărare şi al cercetării tehnico-ştiinţifice în domeniul militar.

Se urmăreşte (în colaborare cu Departamentul pentru Armamente) dezvoltarea programelor ce asigură soluţii pentru realizarea, în primul rând, a compatibilităţii tehnice militare româneşti cu standardele NATO, dar şi de a: dezvolta noi programe de achiziţie de tehnică de luptă pentru Armata României, întări parteneriatele tehnologice între marile companii producătoare de armament şi industria naţională de profil;relansa producţia internăde tehnică de luptă ca urmare a proiectelor strategice de înzestrare pe care Armata României le are în vedere;relansa exportul de armament şi, nu în ultimul rând, de a întări parteneriatele strategice.

Întreaga activitate de reprezentare diplomatică a Ataşaturii Apărării se desfăşoară în scopul promovării în străinătate a României, a istoriei patriei şi poporului român, a valorilor culturale naţionale şi a Armatei Române.

În evoluţia sa, Ataşatura Apărării a reuşit să seadapteze la condiţiile politico-militare ale fiecărui moment şi a fost gata să răspundă provocărilor prezentului.

Acum, poate mai mult ca niciodată, în actualul context de securitate regional şi global, structura Ataşaturii Apărării va fi utilizată la un nivel din ce în ce mai ridicat pentru a aduce noi elemente de cunoaştere şi de a urmări, sesiza, stimula şi raporta iniţiativele şi sugestiile autorităţilor statului acreditar pentru dezvoltarea relaţiilor militare.

Este cert că, în contextul noului mediu de securitate al secolului XXI (surprinzător şi dinamic, cu evoluţii aparent contradictorii generatoare de incertitudini), diplomaţia militară va continua să găsească soluţii de transformare şi adaptare pentru a răspunde corespunzător misiunilor de azi, dar mai ales de mâine ale Direcţiei informaţii militare.

IN MEMORIAM
Cornel Gheorghe TRIFU
– fost ataşat al apărării în Republica Algeriană Democratică şi Populară – decedat în misiune
2019

Bibliografie:

1. PLĂVIŢU, Dan, Ilie Ovidiu FRĂŢILĂ, *Serviciul de informaţii al Armatei Române – Tradiţie şi continuitate,* Editura AXIOMA PRINT, Bucureşti, 2009;
2. MEDAR, Sergiu T., *Diplomaţia apărării*, Editura CTEA, Bucureşti, 2006;
3. *Diplomaţia Română a Apărării,* Editura Medro, Bucureşti, 2007.

[1] Dictonul Secţiei a II-a/Marele Stat Major – *Diplomaţia Română a Apărării,* Editura Medro, Bucureşti, 2007, p. 181;
[2] Dan PLĂVIŢU, Ilie Ovidiu FRĂŢILĂ, *Serviciul de informaţii al Armatei Române – Tradiţie şi continuitate,* Editura AXIOMA PRINT, Bucureşti, 2009, p. 19.
[3] Sergiu T. Medar, *Diplomaţia apărării,* Editura CTEA, Bucureşti, 2006, p. 19.
[4] Ibidem, p. 217.
[5] Turcia şi Anglia erau net împotrivă, iar Franţa, Germania, Italia şi Austro-Ungaria primeau cu rezervă nota diplomatică de înştiinţare;
[6] Sergiu T. Medar, *Diplomaţia apărării,* Editura CTEA, Bucureşti, 2006, pp. 223-224.
[7] Turcia, Franţa, Austro-Ungaria, Germania, Bulgaria, Italia, Rusia, Serbia şi extinderi de acreditare în Grecia şi Belgia;
[8] România, în anul 1914, de la o ţară care avea o întindere teritorială de aproximativ 130.000Km^2 şi o populaţie de cca. 7.000.000 locuitori, în anul 1920, a ajuns la o suprafaţă uşor până în 300.000 km^2 şi o populaţie dublă;
[9] ***, *Diplomaţia Română a Apărării,* Editura Medro, Bucureşti, 2007, p. 1;
[10] Ibidem, p. 182;
[11] Ibidem, p. 2;
[12] Sergiu T. Medar, *op.cit*, p. 19.

SPRIJINUL INFORMATIV LA NIVEL STRATEGIC PE TIMP DE CRIZĂ

Vasile-Cristian ONESIMIUC
Vasile-Iulian ALISTAR[*]

Abstract

The current security environment remains characterized by volatility, while the continuous changes entail adaptive measures by the decision makers in order to convey the appropriate response to a specific crisis. Intelligence support was and it will remain of paramount importance in any crisis management process. In order to reduce the unknown and prevent strategic surprise intelligence support must be timely and permanent thus facilitating appropriate decisions in crises avoiding dangerous escalations and supporting pacification to the best solutions. The intelligence support related activities at strategic level should firstly lead to enhaced situational awareness and constantly development of leaders` knowledge in relation to factors of disturbance and their effects that foment crisis.

Keywords*: information support, crisis, cooperation, crisis management.*

Prin dinamica riscurilor şi ameninţărilor prezente, mediul actual de securitate obligă factorii de decizie la o continuă adaptare şi consolidare a capacităţilor de apărare şi de răspuns în situaţii de criză.

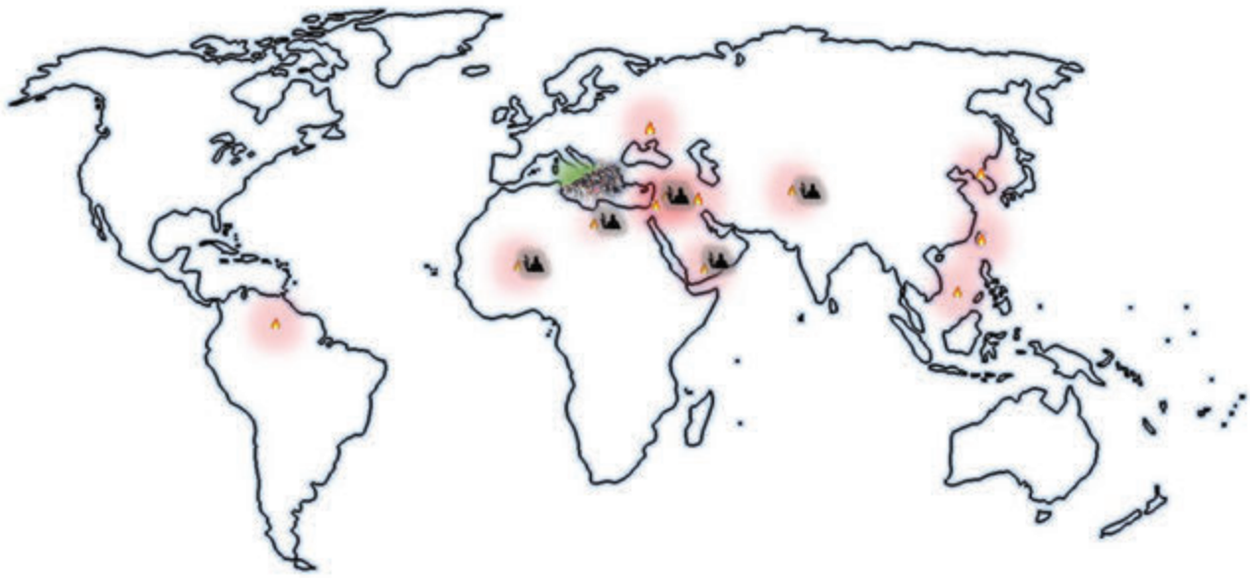
Structurile cu atribuţii în managementul crizelor se confruntă cu situaţii din ce în ce mai complexe, generate de factori cât mai diverşi. În raport cu dinamica mereu în schimbare şi complexitatea ameninţărilor, a factorilor multivectoriali generatori de crize, instituţiile de securitate şi sistemul naţional de management al crizelor trebuie să desfăşoare acţiuni adaptative, de cunoaştere şi dezvoltare permanentă a expertizei şi capacităţii de intervenţie, context în care rolul structurilor informative este unul esenţial. Evitarea surprinderii la nivel strategic se realizează prin aportul structurilor de intelligence, respectiv prin sprijinul continuu cu informaţii pentru identificarea şi cunoaşterea naturii ameninţărilor. Deşi acest lucru reprezintă, în esenţă, un truism, această iteraţie apreciem că este astăzi binevenită în contextul unor evoluţii complexe în spaţiul european şi la Marea Neagră (ex. Brexit-ul,emergenţa F.Ruse, situaţia din Marea Azov, Ucraina) care pot genera schimbări ale paradigmei de securitate regională, cu implicaţii pentru România pe termen lung.

Evoluţia complexă a mediului de securitate implică analiza şi regândirea constantăa procesului de răspuns la situaţii criză în cadrul sistemului naţional de securitate.

Strategia Naţională de Apărare a României identifică faptul că „mediul de securitate va continua să fie influenţat de provocări multiple, unele cu manifestări previzibile şi liniare, reprezentând consecinţe ale unor strategii urmărite de diverşi actori statali şi non-statali pe termen lung, iar altele, dimpotrivă, cu caracter impredictibil, neliniar şi profund perturbator, care pot genera surprize strategice.”[1]

Evoluţiile recente ale mediului de securitate şi imperativul răspunsului la o situaţie de criză - răspuns aşteptat la nivelul societăţii, dar şi la

[*] ***Autorii sunt experţi în cadrul Ministerului Apărării Naţionale.***



nivelul conducerii politice - trebuie să determine structurile cu atribuții în domeniul managementului crizelor să procedeze la adaptarea continuă a modalităților de abordare, a instrumentelor de intervenție, dar şi la pregătirea perpetuă a personalului pe diferite domenii de competență şi întrunit, pentru răspunsul în situații de criză. Această adaptare este de dorit şi trebuie să producă efecte în plan acțional față de situațiile de criză anticipate şi/sau clasice, istoric repetitive, însă la fel de important sunt şi efecteleadaptărilor specifice în situațiile de criză care au aspect de noutate, care se desfăşoară pe coordonate noi impuse de transformările multiple şi accelerate generate de societatea modernă. În această situație, răspunsul trebuie să fie caracterizat de multă flexibilitate, o interoperabilitate crescută între structuri şi celulele de intervenție, creşterea vitezei de procesare a datelor şi analiză multidimensională şi, nu în ultimul rând, pentru ridicarea şanselor de succes este posibil a se impune regândirea procedurilor existente şi/sau a sistemului, în ansamblu, de management al crizelor.

Pentru a putea reacționa în mod eficient se impune ca sistemul de management al crizelor să beneficieze de suportul informativ din partea structurilor de intelligence. Sprijinul informativ trebuie să pună la dispoziția decidenților atât constantele identificate, cât şi elemetele noi care pot defini o situație de criză potențială sau în desfăşurare, precum şi o analiză privind anticiparea posibilelor efecte legate de dezvoltările ulterioare ale crizei şi care pot afecta securitatea națională. De asemenea, în sprijinul factorilor de decizie, a managementului crizei, anticiparea efectelor unui model sau altul de intervenție la o situație de criză credem că poate fi realizată cu sprijinul structurilor de intelligence.

Definirea crizei/situației de criză

Termenul *criză* apare din ce în ce mai des în viața de zi cu zi, în diferite domenii şi este definit într-o mare varietate de forme.

Charles Herman consideră criza „o situație care amenință obiectivele cu prioritate ridicată pentru unitatea decizională; restrânge timpul disponibil pentru un răspuns, înainte ca situația să fie modificată; când se produce, îi surprinde pe membrii unității decizionale.”[2] Autorul sesizează caracterul impredictibil al desfăşurării crizei, identifică scurtarea timpului aflat la dispoziție pentru reacția factorilor de decizie;drept urmare, suportul informativ trebuie să fie cu atât mai rapid şi anticipativ, încât să se producă în timp oportun pentru asigurarea datelor necesare formulării unui răspuns eficient.

Michael Brecher arată că o criză este „o situație caracterizată de patru condiții necesare şi suficiente, aşa cum sunt ele percepute de către decidenții de la nivelul maxim al actorilor implicați: o mutație în ambientul extern sau intern; o amenințare a valorilor de bază; o

probabilitate înaltă de implicare în ostilităţi cu caracter preponderent militar; un răspuns la ameninţarea valorilor."[3]Autorul este de acord cu cele enunţate de către Charles Herman în ceea ce priveşte ameninţarea valorilor/obiectivelor, în plus introduce riscul dezvoltării situaţiei de criză şi escaladării acesteia spre o situaţie de conflict militar, în lipsa unui răspuns eficient care să dezamorseze situaţia de criză.

Ioan Crăciun consideră criza drept „manifestarea unor dificultăţi temporare sau cronice ale modului de organizare a unui sistem, exprimând incapacitatea sa de a funcţiona în modalitatea existentă."[4] Din această perspectivă, atragem atenţia că şi sistemul de management al crizelor poate fi expus unei situaţii de criză.

Manualul de planificare al operaţiilor defineşte criza/situaţia de criză ca „acea stare în care se poate afla un sistem/sistem de sisteme - un grup organizat, o parte a unei naţiuni, o naţiune, un grup de naţiuni, actori statali/non-statali etc. - delimitată în timp şi spaţiu, alta decât starea de pace. În sistemul nostru de drept există o definiţie legală pentru următoarele stări, altele decât starea de pace: starea de urgenţă, starea de asediu, starea de mobilizare, starea de război."[5]

Unul din elementele comune definiţiilor de mai sus este acela că situaţia de criză creează riscuri pentru securitatea naţională, ameninţă existenţa sistemului de valori acceptat şi, în mod implicit, reacţia este aşteptată la nivel intituţional în timp oportun.

Importanţa anticipării evoluţiei mediului de securitate către situaţii de criză

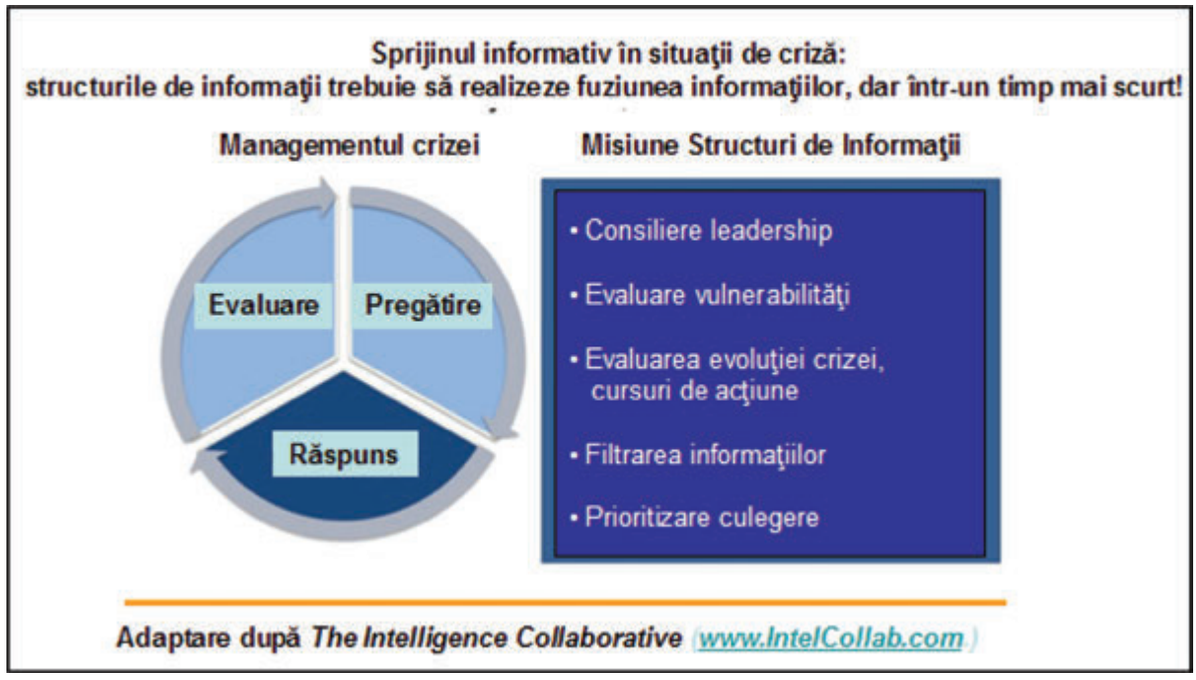
Din punct de vedere procesual, monitorizarea mediului de securitate trebuie să conducă la identificarea indicilor unei situaţii potenţiale de criză şi formularea clară a avertizărilor.

Cunoaşterea situaţiei iniţiale care a stat la baza unei crize este importantă pentru realizarea oricărui plan de intervenţie, iar aceasta se realizează cu sprijinul informativ al structurilor de intelligence. În procesul de monitorizare sunt importante identificarea tendinţelor în spectrul evoluţiilor semnificative şi evaluarea potenţialului de materializare, pe unităţi de timp, a unor riscuri şi ameninţări. În egală măsură, anticiparea evoluţiilor mediului de securitate trebuie să conducă, în paralel, la identificarea unor potenţiali parteneri/aliaţi/structuri de suport care pot sprijini şi/sau contribui la reacţia de răspuns pe dimensiunea managementului crizei şi punerea în aplicare a unui plan de colaborare şi acţiune în sprijinul dezvoltării opţiunilor de răspuns la nivel strategic, naţional.

Anticiparea evoluţiilor mediului de securitate contribuie la iniţierea pro-activă a demersului de planificare pentru gestionarea unei crize, în special atunci când aceasta poate fi o consecinţă directă a deteriorarii situaţiei de securitate din perspectivă militară. Crizele de natură economică, de exemplu, politică sau în relaţie cu dezastrele naturale pot, de asemenea, atunci când ating anumite dezvoltări extreme, să conducă la efecte în planul deteriorării mediului de securitate în accepţiunea unor escaladări de ordin militar.

În cadrul Strategiei Naţionale de Apărare a României sunt identificate potenţiale crize şi conflicte care sunt în măsură să afecteze, direct sau indirect, interesele naţionale de securitate.[6]. Din acest punct de vedere, suportul şi activitatea informativă trebuie să aibă în vedere evoluţiile din zonele identificate a fi generatoare de riscuri şi ameninţări, atât din perspectivă naţională, cât şi din perspectiva de membru al organizaţiilor internaţionale la care România a aderat şi faţă de care avem obligaţia de informare, avertizare şi realizarea schimbului de informaţii. Pe de altă parte, anticiparea evoluţiei situaţiei de securitate, în sensul degradării mediului de securitate şi tranziţieispre situaţia de criză, trebuie să fie abordatăcomprehensiv, holistic şi fără limitări. Pe acest principiu trebuie să fie construit suportul informativ şi informarea la nivel strategic.

Armata României îşi propune „să dispună de capabilităţi în măsură să prevină surprinderea strategică, din perspectiva obţinerii, integrării şi prelucrării de informaţii şi furnizarea de produse finite (intelligence) către autorităţile decizionale naţionale, aliate şi partenere."[7] Deteriorarea situaţiei de securitate la nivel regional şi internaţional impune evaluarea constantă a principalelor ameninţări, riscuri şi vulnerabilităţi



cu care se confruntă România, atât în contextul în care se pot dezvolta situații de risc pornind de la amenințările şi vulnerabilitățile deja cunoscute, cât şi prin sesizarea apariției de vulnerabilități noi şi/sau de noi forme de manifestare a riscurilor de securitate.

Asigurarea sprijinului informativ la nivel strategic

Necesitatea fuzionării informațiilor de la toate sursele de informare disponibile, atât militare, cât şi non-militare, va rămâne o prioritate pentru înțelegerea în întregul ei a situației de securitate şi/sau potențial generatoare de criză.

În asigurarea sprijinului informativ la nivel strategic, resursa umană continuă să fie un factor decisiv, resursă care, în contemporaneitate, poate fi susținută prin dezvoltări pe linia inteligenței artificiale şi exploatarea bazelor de date extinse.

Sprijinul informativ în situații de criză are ca obiectivobținerea de informații relevante în scopul asigurării de evaluări pertinente care să sprijine procesul de decizie la nivel strategic.

Comunitatea Națională de Informații (CNI) asigură „cadrul pentru dezvoltarea cooperării interinstituționale între structurile componente prin crearea şi dezvoltarea de facilități şi instrumente comune pentru coordonarea planificării informative şi elaborarea integrată a produselor analitice şi evaluărilor informative de interes național”[8]. În cadrul CNI[9] se realizează cooperarea dintre structurile de informații naționale, în vederea realizării suportului informativ la nivel strategic.

Deşi pentru elaborarea sprijinului informativ la nivel strategic colaborează, în cadrul CNI, principalele structuri de informații, factorii de decizie trebuie să aibă o imagine de ansamblu şi o înțelegere a limitărilor, vulnerabilităților şi performanțelor structurilor implicate. Sprijinul informativ poate lămuri anumite aspecte, dar trebuie precizat faptul că informațiile nu pot fi întotdeauna complete, iar resursele avute la dispoziție pentru culegere sunt, uneori, limitate. Suportul informativ nu va putea oferi certitudini în toate situațiile şi, în acest context, devine importantă prioritizarea anumitor domenii, optimizarea alocării şi utilizării resurselor, dar şi extinderea cooperării cu alți actori care pot sprijini obținerea de date. Acest proces ar trebui să cuprindă un ansamblu de măsuri în diferite domenii (diplomatic, informații, militar şi economic), precum şi reunirea specialiştilor pentru integrarea datelor şi analiză.

Managementul crizelor are la bază un proces național de planificare în situații de criză[10], proces care cuprinde şase faze:

1. Indici şi avertizări. Cunoaşterea situației implică analizarea informațiilor provenite din surse multiple, în mod continuu;

2. Evaluarea crizei, extinderea evaluării inițiale a unei crize în dezvoltare sau potențiale;
3. Evaluarea opțiunilor de răspuns, stabilirea modalității de abordare a crizei şi starea finală dorită a fi atinsă la finalul crizei;
4. Planificarea/Elaborarea concepției militar-strategice, dezvoltarea planurilor, în colaborare cu alte structuri implicate, pentru atingerea stării finale dorite;
5. Executarea operației, pe timpul acesteia continuând procesul de evaluare şi coordonare a acțiunilor informative;
6. Tranziția, transferul atribuțiilor către structurile care aveau responsabilități înainte de declanşarea situației de criză.

Etapele ciclului informațional pentru elaborarea suportului informativ trebuie să se desfăşoare ciclic, astfel încât să asigure informații oportune, verificate şi actualizate permanent, pentru a satisface nevoile de informații ale beneficiarului.

Atât la nivel național, cât şi la nivelul NATO, în principal şase domenii de analiză pe spațiul geografic de angajare/interes asigură sprijinul informativ la nivel strategic, conform modelului PMESII[11].Astfel, pe măsura evoluției activității de evaluare a situației, suportul informativ trebuie să asigure înțelegerea profundă a crizeiprin analiza următoarelor domenii:

- Politic/diplomatic: actorii principali ai mediului civil, organizații internaționale şi regionale şi instituții centrale şi locale, care exercită autoritate sau impun respectarea legii într-o zonă geografică stabilită sau organizație, prin aplicarea puterii sau influenței politice/diplomatice;
- Militar: forțele armate dotate, antrenate, dezvoltate şi susținute, precum şi infrastructura de sprijin pentru îndeplinirea şi protejarea obiectivelor naționale sau aliate;
- Economic: totalitatea producției, distribuției şi consumului de bunuri şi servicii ale unui stat sau organizații;
- Social: religia, structura socială, sistemul legal şi juridic, politicile de infrastructură pentru sprijin, umanitar;
- Infrastructura: facilitățile de bază, serviciile şi instalațiile necesare pentru buna funcționare a comunității, organizației sau societății;
- Informații: infrastructura specifică, sistemele de organizare, personalul şi componentele care planifică, colectează, procesează, diseminează, stochează, operează şi gestionează date şi informații, sistemele de comunicare, mass-media.

Trebuie avut în vedere faptul că informațiile care prezintă situația curentă la nivel strategic se bazează pe informațiile provenite din cadrul procesului de monitorizare, însă,de regulă, acestea se modifică în timp şi devin,astfel,perisabile;ca urmare, este necesară actualizarea permanentă a informațiilor şi înțelegerea limitărilor privind obținerea acestora. În consecință, sprijinul informativ la nivel strategic trebuie să surprindă evoluțiile pe domeniile menționate în dinamica lor, evaluând tendințele şi corelațiile sau acțiunile complementare care pot sugera anumite dezvoltări în perspectivă.

Evaluarea mediului operațional trebuie să asigure informații relevante, oportune şi predictive. Suportul informativ se desfăşoară pe parcursul tuturor fazelor de management al crizelor (enumerate mai sus), este un proces continuu, dinamic şi trebuie să se adapteze în funcție de cerințele beneficiarului. Este necesar ca suportul informativ să asigure o înțelegere corectă a situației şi evitarea dezinformării,condiție sine-qua-nonîn vederea prevenirii surprinderii strategice şi oferirii avantajului decizional pentru autoritățile politico-militare naționale.

În context, trebuie înțeles faptul că natura crizelor moderne este caracterizată de interdependențe complexe, conflictele având loc ca urmare a unei combinații de neînțelegeri de natură istorică, politică, militară, socială, culturală şi economică, cu evoluții adesea imprevizibile. Sistemele moderne de comunicații şi informatică au crescut semnificativ rapiditatea diseminării informațiilor în rândul populației, lucru care pune o presiune crescută asupra structurilor de informații, pentru a informa cu aceeaşi

repeziciune factorii de decizie în managementul crizei. Informarea în acest sens, din perspectiva serviciilor de intelligence, înseamnă fuziunea datelor şi elaborarea de analizeîn timp real, în paralel cu circulația cu o viteză din ce în ce mai mare a fluxurilor informaționale care, de multe ori, se întâmplă sau pot fi intenționat manipulative.

Asigurarea sprijinului informativ la nivel strategic trebuie să lupte astăzi mai mult ca oricând împotriva dezinformării, iar pericolul este dublu: pe de o parte, scurtarea timpului de analiză sub presiunea fluxurilor crescute de informații, a vitezei acestoraşi nevoii de informare în timp real a beneficiarului poate produce informări sumare, cu valoare acțională imediată scăzută, lucru de evitat în situații de criză şi, pe de altă parte, dezinformarea, care afectează astăzi din ce în ce mai mult gradul de înțelegere a unei situații, poate influențacalitatea analizei la nivelul serviciilor de informații şi, implicit, suportul informativ pentru nivelul decizional strategic pe timpul unei crize.

Suportul informativ şi pericolul dezinformării

Evaluarea mediului operațional trebuie să asigure informații relevante, oportune şi predictive în fiecare etapă din cadrul ciclului informațional şi să aducă plus-valoare în scopul realizării unui produs final relevant, în funcție de nevoile de cunoaştere ale beneficiarului.

Dezvoltarea generală a societății, la nivele mult mai complexe decât în trecut, din cauza interconectărilor existente, determină ca şi efectele situației de criză să se reflecte la nivele de magnitudine care în trecut nu erau posibil de prevăzut şi atins. Beneficiile dezvoltării au crescut vulnerabilitatea generală în cazul situațiilor de criză, un singur domeniu de manifestare a crizei putând avea consecințe la nivel global.

Globalizarea a generat o interdependență atât a aspectelor economice, a sistemelor de transport, a serviciilor etc., cât şi a amenințărilor şi riscurilor la adresa securității statelor. O criză care afectează unul dintre elementele unui lanț cu dezvoltare globală poate crea efecte în cascadă asupra unor domenii care, la prima vedere, nu ar avea motive

să fie afectate de situația de criză. Managementul crizelor trebuie să fie un proces evolutiv, adaptat situației în continuă schimbare. Astfel, se impune ca structurile cu atribuții în domeniu să fie în măsură să furnizeze produse informative pertinente, să nu scadă nivelul de acurateţe al informărilor şi să nu deformeze realitatea. Din acest acest ultim punct de vedere pericolul este unul major.

Pericolul dezinformării este unul foarte real, având în vedere multitudinea surselor de informații şi a structurilor implicate în procesul sprijinirii procesului decizional. Diseminarea informațiilor cu ajutorul rețelelor de socializare, a Internetului în general, precum şi varietatea surselor care vehiculează informații mai mult sau mai puțin veridice, generează o presiune suplimentară atât pe structurile de informații, cât şi pe factorii de decizie. Factorii de decizie trebuie să fie în măsură să elaboreze deciziile pe baza informațiilor disponibile, în condiții de incertitudine, cu rapiditate, mai ales pe timpul situațiilor de criză cu impact crescut asupra populației.

Riscul dezinformării creşte nivelul de dificultate al procesului decizional şi acesta se poate manifesta în toate etapele unei situații de criză. Începerea procesului de management al crizelor la nivel național printr-o cunoaştere deformată a situației inițiale, ca urmare a identificării eronate a riscurilor şi amenințărilor, atât în sensul supraevaluării sau al minimalizării acestora în perspectiva evoluției crizei, va conduce la elaborarea unor modalități neconforme de răspuns şi la vulnerabilizarea sistemului de management al crizei. Ignorarea unor date sau asumarea unor premise false la baza planificării intervenției pot conduce la situații de escaladare a crizei şi/sau la costuri mult mai mari de remediere a situației şi revenire la starea de normalitate.

Realizarea de planuri premergătoare situației de criză pe baza analizei predictive a informațiilor disponibile la un moment dat poate oferi factorilor de decizie obținerea unui timp de reacție suplimentar în situația materializării crizei, atât pentru compararea şi refacerea analizelor şi evaluărilor informative, cât şi pentru a discerne cu privire la acțiunile posibile de dezinformare manifeste.Prin urmare, este indicat ca suportul informativ să fie realizat având în vedere posibilitățile de dezinformare executate cu intenție, în mod conştient, de către actori cu interese diverse raportate la situația de criză.

Dezvoltarea capacităților şi instrumentelor de răspuns la criză necesită a fi dimensionată în concordanță cu nivelul real de manifestare al crizei, context în care analiza sau pericolul dezinformării trebuie supus atenției decidenților prin suportul informativ dezvoltat de structurile de intelligence. Această dimensionare corectă se poate realiza pe baza experienței, pe modelul unor crize cunoscute, repetitive, care au mai putut fi evaluate sub diferite aspecte, situație în care suportul informativ poate să fie suficient pentru elaborarea unei modalități eficiente de răspuns. Există însă situații când factorii de decizie iau hotărâri pe timpul desfăşurării crizei având la bază informații mai mult sau mai puțin suficiente, fiindsupuşi efectelor sau fiindchiar ținte ale dezinformării.

Colaborarea dintre factorii de decizie şi structurile care asigură suportul informativ poate conduce la diminuarea riscurilor, dar nu va fi suficient pentru eliminarea în totalitate a pericolului adoptării unei decizii mai puțin inspirate. Colaborarea continuă, anticipativă şi clarificarea aspectelor urmărite pe timpul unui proces de management al crizei cu structurile de informații este necesară, scurtează timpul de răspuns la solicitările de actualizare a produselor informative şi diminuează, în egală măsură, riscul dezinformarii, legat în principal de posibilitatea nefiltrăriicorespunzatoare a datelor în ritmul alert al petrecerii evenimentelor.

Concluzii

Noile crize, ce se vor desfăşura în contextul interconectării societății la nivele neatinse anterior, vor solicita beneficiarilor de produse informative şi structurilor de informații o capacitate de adaptare crescută pentru a răspunde performantşi oportun pe timpul unor astfel de situații.

La rândul lor, structurile de informații trebuie să-şi dezvolte capacitatea de evaluarepredictivă a evoluțiilor pe linie de securitate, să îmbunătățească capacitatea de avertizare şi evaluare pe baza analizei domeniilor de risc, acum interconectate, pe termen mediu şi lung. Procesul de adaptare se impune a fisusținut de o viziune de pregătire adecvată, care să ofere suportul teoretic atât pentru lideri, cât şi pentru elementele de execuție implicate în elaborarea suportului informativ. Analiza pro-activă de către decidenți a răspunsului instituțional la situații potențiale de criză, cu sprijinul structurilor şi competențelor structurilor de informații, a simulărilor şi jocurilor de rol, poate răspunde cu succesnevoii crescute de adaptare la condițiile mereu în schimbare ale mediului de securitate şi ale societății, în general.

Modul tradițional de răspuns la o situație de criză pe baza structurii organizaționale existente şi/sau a istoricului unor situații similare cunoscute, credem căse impune a fi permanent pus în discuție pentru diminuarea expunerii în cazurireale la riscuri şi amenințări,care în contemporaneitate se conturează în mod permanent şi diferit.

Bibliografie:

1. *Strategia Națională de apărare a țării pentru perioada 2015-2019, O Românie puternică în Europa şi în lume, Bucureşti,* 2015;
2. *Strategia Militară a României*, 2016;
3. *Manualul de planificare a operațiilor*, Bucureşti, 2016;
4. *Doctrina Informațiilor pentru apărare*, Bucureşti, 2017;
5. *Doctrina pentru proceduri de informații*, Bucureşti, 2018;
6. BRECHER, Michael, *Studies in crisisbehavior,* Special Issue: The Jerusalem of International Relations, 1978;
7. CRĂCIUN, Ioan, *Prevenirea conflictelor şi managementul crizelor*, Editura UNAp "Carol I", Bucureşti, 2006;
8. HERMAN, Charles F., *Crises in Foreign Policy. A SimulationAnalysis*,1969;
9. www.administratie.ro/articol.php?id=4921.

[1] Strategia Națională de Apărare a Țării pentru perioada 2015-2019, O Românie puternică în Europa şi în lume, Bucureşti, 2015, Cap.II, Evaluarea Mediului Internațional de securitate, aliniat 27.

[2] Herman F. Charles, *Crises in Foreign Policy. A SimulationAnalysis*, Indianapolis, 1969.

[3] Brecher Michael, *Studies in crisisbehavior Special Issue The Ierusalim of International Relations*, 1978.

[4] Crăciun Ioan, *Prevenirea conflictelor şi managementul crizelor*, Editura UNAp„Carol I", Bucureşti, 2006, pag.32.

[5] Manualul de planificare a operațiilor, Bucureşti, 2016, pag.187.

[6] Evoluțiile din Vecinătatea Estică, Orientul Mijlociu şi Nordul Africii, instabilitatea din Bacanii de Vest,emergența grupărilor teroriste, Strategia Națională de apărare a țării pentru perioada 2015-2019, O Românie puternică în Europa şi în lume, Bucureşti, 2015, Cap.II, Evaluarea Mediului Internațional de securitate.

[7] Strategia Militară a României, 2016, subcapitolul 3, punctul 1f.

[8] Doctrina Informațiilor pentru apărare, Bucureşti, 2017, pag. 11.

[9] www.administratie.ro/articol.php?id=4921, accesat la data de 23.04, ora 22.04.

[10] Doctrina pentru proceduri de informații, Bucureşti, 2018, pag. 14-17.

[11] Manualul de planificare a operațiilor, Bucureşti, 2016, pag.10, în original, în limba engleză: *Political, Military, Economic, Social, Infrastructure, Information*.

CENTRUL DE EXCELENȚĂ NATO ÎN DOMENIUL HUMINT – PROVOCĂRI ŞI OPORTUNITĂȚI PENTRU O NOUĂ DECADĂ ÎN SPRIJINUL ALIANȚEI*

Vasile-Cristian ONESIMIUC
Vasile-Iulian ALISTAR**

Abstract

The North-Atlantic Allianceis at time of radical changes, from the enhanced defensive posture in its Eastern flank, to the NATO Command Structure adaptation and functional optimization. This process includes a re-thinking of the way NATO Centres of Excellence (COEs) respond to the Alliance's requests for support, challenging their institutional resilience. Furthermore, any transformational direction – standardization, concept development, lessons learned and an alysis, or education, training, exercises, and evaluation – have specific probe stopass, making use of the best the NATO COEscanoffer as human capital.

The NATO HUMINT Centre of Excellence (HCOE) from Oradea is near to celebrate a decade of active contribution to NATO, shaping important landmarks in the HUMINT capability development with in the full spectrum of DOTMLPFI domain: doctrine, organization, training, materiel, leadership and education, personnel, facilities, and interoperability. From the perspective of the aforementioned challenges to the NATO organization and functioning, the paper provides a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis for the COEs' next decade, pointing out vision elements that will further drive HCOE's program of work.

Keywords: *NATO HUMINT Centre of Excellence, HCOE, transformation, human capital, HUMINT capability*

Centrul de Excelență NATO în domeniul HUMINT, bilanț pentru un deceniu de activitate

Activitatea Centrelor de excelență NATO are o importanță multidimensională, atât din punct de vedere al spectrului de discipline şi capabilități acoperite, cât şi pentru nivelul de deservire a cerințelor de sprijin ale NATO, aliniat intereselor națiunilor participante. Pe de o parte, Centrele gestionează proiecte şi programe în sprijinul îmbunătățirii capabilităților existente sau dezvoltării de noi capabilități, dintr-o perspectivă inovativă, antrenând în acest sens activitatea de standardizare (ca reper al interoperabilității), managementul şi analiza lecțiilor învățate/ bunelor practici, dezvoltarea şi validarea de noi concepte, şi asigurând oportunități deosebite pentru procesul de educație şi instruire. Pe de altă parte, participarea națiunilor la Centrele de excelență, **dincolo de contribuț**ia asumată, are rațiuni şi interese bine justificate, avantajele imediate incluzând: asigurarea implementării viziunii şi reprezentării intereselor naționale în produsele specifice, asigurarea accesului nemijlocit la evoluțiile de

* ***Opiniile şi ideile exprimate în acest articol sunt ale autorilor şi nu reflectă neapărat politica NATO.***

** ***Col. Florin-Vasile TOMIUC este directorul Centrului de Excelență NATO în domeniul HUMINT, iar lt. col. dr. Alexandru KIS este expert în cadrul aceleiaşi instituții.***

ultimă oră în domeniul respectiv şi la produsele specifice ale Centrului, în condiţii preferenţiale. În plus, pe lângă vizibilitatea internaţională şi la nivelul Alianţei, relaţia cu partenerii din cadrul Centrului permite dezvoltarea de proiecte comune, facilitând interacţiunile bilaterale între naţiunile participante.

România este foarte bine reprezentată în acest cadru, în primul rând ca naţiune gazdă pentru Centrul de Excelenţă NATO în domeniul HUMINT (HCOE), dar şi prin contribuţia cu experţi în multe alte Centre de excelenţă ale Alianţei.Prin înfiinţarea HCOE, Româniaa exploatat o oportunitate deosebită de a pune în valoare un corp de cadre experimentat, în condiţiile dezvoltării unor capacităţi de lucru în comun cu structurile militare NATO în diferite teatre de operaţii (Kosovo, Bosnia, ulterior Irak şi Afganistan) şi dispunând de o abordare coerentă a Direcţiei Generale de Informaţii a Apărării în cadrul grupurilor de coordonare şi a demersurilor lucrative în sfera informaţiilor militare în NATO.

Materializarea negocierilor preliminare privind participarea naţiunilor la HCOE a venit odată cu semnarea,la 16 decembrie 2009, la Norfolk (SUA), a acordurilor formale de constituire a Centrului de către reprezentantul Comandamentului Aliat pentru Transformare (ACT)şi cei aiprimului grup de naţiuni participante – România (naţiune-cadru), Grecia, Slovenia, Turcia şi Ungaria. Ulterior, acestora li s-au adăugat, succesiv: Slovacia, Polonia, Cehia şi SUA, procesul de aderare fiind în continuare deschis altor state membre NATO.

În paralel cu procesul de negociere, prin efortul asiduu al echipei de proiect au fost puse bazele funcţionale ale instituţiei şi, în urma evaluării nivelului de operaţionalizare de către ACT, aceasta a obţinut statutul de Centru de Excelenţă NATO - organizaţie militară internaţională în virtutea prevederilor Protocolului de la Paris din 1952[1], statut ce urmează să fie reconfirmat în cursul anului 2019, în conformitate cu procedurile NATO.

La un deceniu de la acest eveniment, misiunea Centrului de Excelenţă NATO în domeniul HUMINT rămâne în continuare racordată la nevoile Alianţei, furnizând un punct de referinţă unic în NATO în ce priveşte activităţile de standardizare, dezvoltare conceptuală, analiza experienţei operaţionale, educaţie şi instruire, în procesul de conturare a evoluţiei capabilităţilor sale în domeniul HUMINT.

În acest sens, transpunerea în realitate a obiectivelor se realizează prin produsele şi serviciile rezultate ca urmare a unui program de lucru întocmit în baza cererilor de sprijin ale NATO şi aprobat de către Comitetul Director (forul decizional al Centrului), antrenând şi resurse din cadrul comunităţii de interes largi, reprezentate de Grupurile de lucru NATO pentru HUMINT (NATO HUMINT Working Group/ NHWG) şi tehnologie în domeniul HUMINT (NATO HUMINT Technology Working Group/ NHTWG), a căror preşedinţie şi secretariat sunt asigurate de către HCOE din 2011.

La atingerea unui nivel de excelenţă în activitatea Centrului contribuie în mod decisiv şi baza de relaţionare largă pe care instituţia a construit-o şi consolidat-o în timp, printr-o politică proactivă, prin disponibilitatea de angajament şi prioritizarea judicioasă a resurselor, asigurându-şi prezenţa şi fiind reprezentată la nivelul principalelor entităţi decizionale şi acţionale în domeniul de interes. Astfel, pe lângă structurile de coordonare din cadrul comandamentelor strategice ale Alianţei, au fost stabilite relaţii de lucru, în primul rând, cu naţiunile aliate (în special în cadrul NHWG şi NHTWG, dar şi în relaţie cu grupurile de lucru NATO din domeniilestandardizării, educaţiei -instruirii şial lecţiilor învăţate), cu structuri din cadrul comandamentelor operaţionale şi tactice, cu centre de instruire NATO şi cu alte centre de excelenţă a căror activitate se interconectează la diferite niveluri de interes.Structura organizatorică a Centrului este ea însăşi concepută astfel încât să asigure o conectare specializată, corespondentă pilonilor transformării în NATO, cu branşele responsabile din cadrul comandamentelor strategice şi cele operaţionale, precum şi cu alte structuri angrenate în procesul de dezvoltare a capabilităţilor militare ale Alianţei – Joint Warfare Centre (Norvegia), Joint Force Training Centre

(Polonia), Joint Analysis and Lessons Learned Centre (Portugalia), NATO Communication and Information Agency, etc.

Pe lângă sfera de interacțiune militară, deschiderea şi interrelaționarea cu mediul academic, dezvoltarea de parteneriate cu universități, institute de cercetare, dialogul cu entitățile din industria de securitate, asigură schimbul de experiență şi varietatea perspectivelor necesare inovării şi dezvoltării parametrilor calitativi ai resursei umane de care Centrul dispune.

Implementarea unor politici coerente de management instituțional (reflectate în principiile de elaborare a programului de lucru, în materia gestionării informației şi a cunoaşterii, în politicile de securitate, suportul de comunicații şi informatică, suportul logistic şi cu servicii, angajarea resurselor umane şi financiare, un sistem solid de management al calității legat de activitatea didactică şi sprijinul instituțional al acesteia, etc.) fac din HCOE o instituție modernă, adaptabilă, pe deplin capabilă să servească nevoile în continuă schimbare ale Alianței.

Adesea menționată ca exemplu de bună practică în NATO, maniera de abordare sistematică a dezvoltării capabilității HUMINT în NATO prin stabilirea unor ținte de progres ce acoperă întreg spectrul DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership andeducation, Personnel, Facilities, Interoperability) constituie cadrul planului de acțiune general al grupurilor de lucru NATO pentru HUMINT – indisolubil interconectat cu programul de lucru al HCOE – şi ilustrează în mod elocvent modalitatea în care această capabilitate a evoluat în ultimul deceniu, cu efecte concrete în ce priveşte resursa umană, organizarea şi procesele funcționale ale disciplinei, precum şi implementarea de soluții tehnologice.

În acest sens, este necesar să evidențiem şi principalele repere ce au marcat evoluția HCOE şi contribuția acestuia pentru NATO timp de un deceniu:

- custodia doctrinei şi a standardului pentru tacticile, tehnicile şi procedurile HUMINT în NATO, odată cu preluarea acestor sarcini de la Marea Britanie în 2011; pe lângă aceasta, Centrul sprijină cu experți revizuirea politicii NATO pentru HUMINT şi a directivei pentru HUMINT a Comandamentului Aliat pentru Operații (ACO) şi pune la dispoziția specialiştilor în domeniu publicații suplimentare (manuale şi ghiduri) utile atât în activitatea operativă, cât şi în sprijinul activității educaționale;
- acreditarea de către NATO, în 2013, ca furnizor de educație şi instruire în sprijinul cererilor Alianței; acest statut a fost dobândit ca recunoaştere a calității infrastructurii, sistemelor, proceselor şi procedurilor de lucru, a managementului şi standardelor academice aplicate (instituția urmează să parcurgă procesul de reacreditare pentru managementul calității în cursul anului 2019); totodată, HCOE este principalul furnizor de soluții de instruire individuală certificate pentru specialiştii HUMINT la toate nivelurile funcționale[2] şi sprijină, în mod constant şi consistent, integrarea disciplinei HUMINT în instruirea colectivă şi exerciții, în conformitate cu standardele NATO;
- tot în 2013 are loc preluarea inițiativei în domeniul lecțiilor învățate prin constituirea Comunității de interes NATO pentru lecții învățate şi bune practici în domeniul HUMINT, gestionată de către Centru, în relație directă cu Centrul NATO pentru analiză întrunită şi lecții învățate (Joint Analysis and Lessons Learned Centre/ JALLC) din Portugalia;
- în 2015, Centrul este desemnat de către Comitetul Militar NATO ca responsabil departamental pentru educația şi instruirea în domeniul HUMINT în NATO (*HUMINT Department Head/DH*); prin structura specializată creată în cadrul Centrului a fost elaborată viziunea de reformare a instruirii de specialitate şi au fost puse bazele unei comunități de interes a furnizorilor de soluții educaționale, urmărindu-se atât construirea unui program educațional accesibil şi sustenabil în sprijinul Alianței, cât şi îmbunătățirea calității acestuia;

- dezvoltarea conceptuală şi experimentarea unor noi dimensiuni teoretice şi tehnice în sprijinul capabilității HUMINT, în cadrul unor proiecte de cercetare de certă valoare pentru operatorii şi personalul de stat major din domeniul HUMINT.

Aceste elemente poziționează HCOE într-un onorant top al performanței în toate dimensiunile cuantificate în procesul de transformare, fiind un indicator complex al capacității instituției de a se implica în mod sustenabil în evoluția disciplinei HUMINT în NATO şi oferind un model recunoscut de bună practică în ce priveşte abordarea integrată a dezvoltării unei capabilități în domeniul informațiilor militare.

Repere ale transfomării în NATO

În cuvântul său introductiv pentru ediția din 2005 a revistei NATO (”NATO Review”), dedicată transformării Alianței, secretarul general din acel moment, Jaap de HoopScheffer, arăta că transformarea este un proces continuu ce trebuie să urmărească sporirea gradului de folosire a forțelor, disponibilitatea şi sustenabilitatea acestora pentru operații în afara teritoriului Alianței, în condițiile armonizării deciziilor politice cu cele operaționale (prin îmbunătățirea proceselor de planificare a apărării şi de generare a forțelor, precum şi prin crearea unei mai mari clarități în privința asigurării resurselor pe baza unui echilibru mai bun între finanțarea la nivel național şi cea în comun). Pe lângă dimensiunea militară a transformării, cea politică presupune întărirea dezbaterii politice pentru a întruni şi susține consensul transatlantic, care a fost şi va rămâne esențial în cazul oricărei acțiuni intreprinse de Alianță.[3]

Dihotomia transformării raportată la rolul dual al organizației, de alianță militară şi organizație politică, este privită de către Mark Joyce, fost responsabil cu Programul Transatlantic în cadrul Royal United Services Institute din Londra, din perspectiva cuantificării succesului celor două dimensiuni, urmând indicatori şi repere de performanță aparte[4].

Robert G. Bell, fost secretar general adjunct NATO (între 1999 şi 2003) pentru investițiile în domeniul apărării, evalua transformarea Alianței din perspectiva agendelor lansate succesiv în cadrul summit-urilor NATO, considerând acest proces mai mult o problemă de cultură şi atitudine decât una ce ține de tehnologii şi mijloace.[5] Planurile de acțiune elaborate în urma summiturilor configurează obiective ce decurg din necesități distinct raportate la axele *spațiu-timp-amenin*țări de securitate, generând şi o dimensiune geopolitică prin extinderea Alianței. În general, acestora le transced probleme legate de finanțare, schimbul de informații, dialogul politic la nivel strategic în cadrul NATO, decalajul dintre dorința aliaților de a participa la desfăşurarea unor noi misiuni şi de a crea noi capabilități şi cea de a angaja personalul, echipamentul şi resursele necesare etc.

Cu toate acestea, nu putem să nu remarcăm importanța critică pe care dezvoltarea capabilităților o are în acest context. Mai mult, pentru centrele de excelență NATO, universul transformării este focalizat tocmai în această direcție: susținerea, promovarea şi dezvoltarea unor capabilități existente sau emergente.

Transformarea capabilităților militare este mai uşor de cuantificat, evaluat şi explicat decât sunt produsele programelor politice ale Alianței, pentru multă vreme implicit conținute de reformele militare ale Alianței. Trecerea de la o postură defensivă la forțe mai suple, dislocabile şi expediționare a indicat determinarea Alianței de a aborda amenințările la sursa acestora. Experiența dobândită în operații a acționat ca un catalizator pentru reformele în domeniul capabilităților, marcând saltul de la capacități de luptă convenționale către cele neconvenționale/ hibride şi facilitând abordarea comprehensivă în materie de planificare şi conducere a operațiilor.

Transformarea pe baza capabilităților este un proces continuu, ce implică o serie de elemente menite să le asigure avantajul competitiv raportat la mijloacele similare aflate la dispoziția adversarilor. Spectrul DOTMLPFI antrenează evoluțiainterdependentă a organizațiilor, proceselor, tehnologiilor şi a capitalului uman, contribuind atât la adaptarea capabilităților existente, cât şi la inițierea dezvoltării de noi capabilități în baza rezultatelor procesului

(retrospectiv) de lecţii învăţate şi a abordărilor analizei predictive (ca proces proactiv).

În prospectarea stării de securitate, modelarea ameninţărilor trebuie să ţină cont de evoluţiile revoluţionare, cu impact radical (”game changer”) în ce priveşte principiile şi definirea ameninţărilor şi în domenii critice pentru infrastructura de securitate (vulnerabilităţi emergente asociate evoluţiei tehnologice, noi surse de putere, etc.). Estimări în acest sens, precum şi conturarea tabloului probabil al spectrului de ameninţări cu care Alianţa se va confrunta în viitor se regăsesc în analiza de previziune strategică (Strategic ForesightAnalysis/SFA), completată de raportul privind cadrul operaţiilor viitoare ale Alianţei (Framework for FutureAllianceOperations/ FFAO). Ideea centrală este aceea că succesul în operaţiile viitoare sunt garantate de evoluţia, adaptarea şi inovaţia continuă a structurilor de comandă şi de forţe ale NATO; transformarea, din această perspectivă, trebuie să asigure credibilitatea forţelor, interconectarea acestora, un nivel ridicat de informare, agilitate şi reziliență.[6]

Raportul anual pentru 2018 al Secretaruluigeneral al NATO evidenţiază, în secţiunea dedicată modernizării Alianţei[7], măsurile materializate în ultimul an privind adaptarea şi întărirea structurii de comandă a NATO, atât din punct de vedere al relevanţei geopolitice, cât şi al responsabilităţilor funcţionale alocate, cu deschidere către noul domeniu operaţional reprezentat de spaţiul cibernetic şi cu o nouă abordare în dezvoltarea capabilităţilor şi contribuţia naţiunilor la efortul comun de dezvoltare.

Esenţializat, transformarea în domeniul militar, înţeleasă ca evoluţia capabilităţilor curente către cele necesare operaţiilor viitoare, într-o manieră eficientă şi economică, urmăreşte să producă: capabilităţi îmbunătăţite (abilitatea de a îndeplini misiunile încredinţate de Alianţă), interoperabilitate crescută (abilitatea naţiunilor aliate şi, după caz, a celor partenere de a opera unitar) şi întărirea valorilor comune (NATO funcţionează prin consensul membrilor şi se bazează pe valorile comune ale acestora).

Reţeaua de transformare a NATO reprezintă, din acest punct de vedere, pe lângă cadrul asigurat de structurile de comandă şi control consacrate, şi o extensie a efortului de gestionare a fenomenului transformării în NATO, bazată pe oportunităţile oferite de prezenţa voluntară şi/ sau cointeresată, sub diferite forme şi formule participative, a statelor membreNATO, partenerilor Alianţei, precum şi a unei serii de organizaţii internaţionale guvernamentale şi neguvernamentale, instituţii academice şi ştiinţifice, şi chiar a publicului larg (în câmpul de interacţiune asigurat de formula comunicării strategice).

Această conexiune este un model original de completare a resurselor necesare procesului continuu al transformării, de care NATO, ca organizaţie, beneficiază din plin. Se realizează astfel transferuri semnificative de abordare a problemelor din perspective culturale diferite, experienţă operaţională, bune practici, lecţii învăţate, resurse tehnologice şi de know-how ce reprezintă un important bagaj de valoare adăugată, în conformitate cu normele Alianţei.

Toate aceste aspecte trebuie luate în considerare la nivelul conducerii unei organizaţii menite să sprijine procesul de transformare şi dezvoltare a capabilităţilor NATO în diferite domenii. Acestea se reflectă nu numai în misiunea şi sarcinile asumate la nivelul centrelor de excelenţă, ci şi în modalitatea prin care acestea sunt puse în operă – iar aici intervine talentul managerial al echipelor de conducere. Astfel, un aspect critic al transformării este reprezentat de componenta umană – lideri capabili să conducă schimbarea şi să creeze o cultură organizaţională deschisă schimbării, care să sprijine inovarea, învăţarea şi asumarea de riscuri[8].

Transformarea în domeniul Intelligence

În NATO, disciplina Intelligence este abordată ca parte a unui set de capabilităţi integrate – Intelligence, Supraveghere şi Cercetare Întrunite/Joint Intelligence, Surveillance and Reconaissance (JISR) – spectru ce întruneşte elementele de planificare şi operare ale tuturor mijloacelor de colectare a informaţiilor cu procesarea, exploatarea, şi

diseminarea informației rezultate în sprijinul direct al planificării, pregătirii şi execuției operațiilor. La dezvoltarea şi integrarea capabilității JISR a NATO au avut o contribuție deosebită statele din cadrul proiectului MAJIIC (Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition)[9], atât prin standardele promovate, cât şi prin exercițiul comun (MAJEX[10]), inițial limitat la disciplinele tehnice de colectare a datelor şi informațiilor, dar care a căpătat noi dimensiuni odată cu inițierea, planificarea şi derularea seriei de exerciții-test „Unified Vision", unde o contribuție semnificativă în segmentul de implementare şi testare a capacităților tehnologice din domeniul HUMINT o are HCOE.

Cel mai mare exercițiu aliat de tip întrunit, Trident Juncture, reprezintă corolarul experimentării, validării şi integrării capabilităților din multiple domenii. Astfel, în cadrul simulat al unor operații militare complexe, ediția din 2018 a exercițiului a facilitat experimentarea unor capabilități viitoare legate de sisteme autonome, mijloace avansate de manufactură (printarea 3D) în câmpul tactic, sisteme de comandă şi control modernizate, capabilitatea de evaluare a mediului informațional, capacități de răspuns la amenințări biologice, dar şi procese şi mijloace pentru schimbul de informații, supraveghere şi cercetare în operațiile întrunite[11].

Testarea unor astfel de proceduri şi sisteme vine într-un context aparte, în condițiile în care schimbul de informații secrete între națiuni este determinat de o serie de factori specifici, ce fac nivelul de cooperare în domeniul Intelligence să fie unul particular în cadrul oricăror forme de parteneriat: interesul național, încrederea în parteneri, protecția surselor şi a mijloacelor/ metodelor de colectare, nivelul de credibilitate (evaluarea informației şi a sursei), mecanismele de gestionare a riscurilor şi reciprocitatea („*quid pro quo*"). Găsirea unor formule de conlucrare eficientă este deosebit de importantă pentru NATO, care nu dispune de un angrenaj complex de mijloace de culegere a informațiilor[12] şi se bazează, în primul rând, pe contribuția statelormembre/partenere.

Totuşi, putem face trimitere la abordări experimentale – cum ar fi AMIB (AlliedMilitary Intelligence Battalion/ Batalionul Aliat pentru Informații Militare) în misiunea NATO din Bosnia-Herțegovina – sau la proiecte multinaționale ce au devenit poveşti de succes ale NATO – Centrul NATO pentru Fuziunea Informațiilor (NATO Intelligence Fusion Centre/ NIFC), cu atribuții în a răspunde cererilor de informații ale NATO/ națiunilor aliate, dar şi cu funcție de sprijin (*reachback*) pentru planificarea şi conducerea operațiilor[13].

Transformarea în domeniul Intelligence a cunoscut un nou impuls după summitul NATO de la Varşovia, în 2016, prin înființarea Diviziei pentru Intelligence şi Securitate (Joint Intelligence andSecurity Division/ JISD, sub conducerea Asistentului pentru Intelligence şi Securitate al Secretarului General NATO - AssistantSecretary General for Intelligence andSecurity/ ASG-I&S), compusă din doi piloni: Intelligence (prin comasarea structurilor militare şi civile în domeniu) şi Biroul NATO pentru Securitate. ArndtFreytag von Loringhoven, primul ASG-I&S al NATO, urmăreşte îndeaproape modalitatea în care capabilitatea Intelligence se adaptează şi se transformă astfel încât să asigure unitatea de efort şi gradul necesar de acoperire cu capabilități de monitorizare, analiză şi avertizare timpurie, în condițiile în care mediul de securitate actual (marcat de asertivitatea militaristă a Rusiei şi de larga panoplie a amenințărilor *hibride, de amenințările din spațiul* cibernetic, de pericolul terorismului internațional - cu potențial distructiv ce ajunge până la folosirea de mijloace de nimicire în masă - dar şi de provocările legate de fluxurile masive de migranți/refugiați) necesită capacități multiple şi specializate de abordare simultană a unui larg spectru de indicatori[14].

Raportul secretarului-general al NATO pe anul 2018 evidențiază importanța JISD pentru procesul decizional, printr-o creştere imediată cu 40% în producția de rapoarte şi o ajustare a calității analizei pentru domeniile acoperite de noile structuri specializate subordonate (amenințări hibride, terorism, amenințări în mediul cibernetic). JISD are o contribuție aparte şi din perspectiva

coordonării civili-militari şi relația de colaborare cu UE în domeniul Intelligence[15].

Caracterul hibrid şi globalizat al amenințărilor împinge limitele ariei de interes informațional dincolo de reperele regionale tradiționale şi necesită o abordare integrată a capacităților de informații civile şi militare, dar şi formule largi de parteneriat (ce iau în considerare interesele strategice ale națiunilor)[16], astfel încât să fie generată o imagine coerentă şi completă a tabloului riscurilor şi amenințărilor la adresa securității. Astfel, competitivitatea în domeniul Intelligence, dată de superioritatea informațională şi de calitatea componentei de securitate, cu includerea capacităților contrainformative, este de natură să contribuie la un nivel superior de avertizare timpurie, protecție a forței şi flexibilitate generală a organizației, după cum apreciază Joseph S. Gordon, expert în cadrul National Intelligence University[17].

Inițiative precum comasarea elementelor de Intelligence militare şi civile la nivelul Cartierului General al NATO, crearea de structuri specializate pentru analiza amenințărilor hibride sau pentru gestionarea informațiilor în lupta împotriva terorismului, ori dezvoltarea de noi standarde de securitate pentru protecția informațiilor şi sistemelor clasificate sunt doar câteva măsuri menite să îmbunătățească performanța viitoare a JISD, în cadrul larg a ceea ce ASG-I&S denumea ”*NATO'swider intelligence enterprise*” (cuprinzând NIFC, centrele de excelen**ță din domeniile relevante, comitete** şi grupuri de lucru ce întrunesc reprezentanți naționali din sfera Intelligence, etc.). Mai mult, lansarea proiectului Academiei NATO pentru Intelligence vine să completeze un element cheie în cadrul capabilității - educația şi instruirea individuală - abordată dintr-o perspectivă unitară.

Particularizat pentru domeniul HUMINT, acesta se găseşte ancorat în toate programele şi proiectele ce privesc genul proxim al disciplinei (Intelligence), HCOE fiind, aşa cum îşi şi propune în cadrul misiunii asumate şi a viziunii comenzii, vârf de lance în efortul de dezvoltare a capabilității informațiilor din surse umane în NATO[18].

Strategia transformării şi rețeaua centrelor de excelență NATO

Pornind de la premiza că evoluția tehnologică în domenii precumtehnicacibernetică modernă în echiparea capabilităților strategice, inteligențaartificială, robotica, managementul bazelor de date, război cibernetic, etc. nu mai reprezintă o exclusivitate, comandantul ACT, generalul André Lanata, caracterizează toate aceste evoluții sau schimbările revoluționare în respectivele domenii ca fiind „disruptive”, insistând pentru o politică a inițiativei caresă asigure relevanța ACT în postura de comandament strategic responsabil pentru dezvoltarea modului de ducere a luptei (”warfaredevelopment”). Acest concept subsumează şase dimensiuni interdependente ce constituie cadrul viitoarei contribuții,inclusiv a centrelor de excelență, la transformarea NATO:[19]

1. *înțelegerea şi influențarea viitorului* (analiza predictivă a evoluției vulnerabilităților şi amenințărilor prin formule avansate în cadrul SFA/FFAO);
2. *transformarea prin dezvoltarea de capabilități finanțate în comun* (ACT are o nouă atribuție ca Autoritate a cerințelor de capabilități/Capability Requirement Authority);
3. *experimentarea şi demonstrarea*, facilitate de modelare şi simulare ca translatori ai ideilor şi inovației în capabilități concrete în sprijinul luptei;
4. *doctrină şi concepte*, ca repere ale interoperabilității;
5. *educația şi instruirea*, pentru asigurarea resurselor umane adecvat pregătite;
6. *lecțiile învățate şi analiza*, ca garanție a acumulării experienței şi învățării din greşelile trecutului.

Conferința din 2018 a liderilor implicați în procese de reformă/ transformare la nivel național şi în cadrul NATO (Chiefs of TransformationConference/ COTC)[20], activitate ce cointeresează mediul academic şi industria de securitate, a avut ca subiect principal modalitatea în care evoluțiile de impact în diferite domenii de referință (abordări, tehnici, tactici, proceduri şi

tehnologii „disruptive") îşi pun amprenta asupra calităţii capitalului uman şi a modului de planificare, pregătire şi ducere a luptei. Astfel, reperele pivotale în jurul cărora NATO urmăreşte să construiască noi dimensiuni ale transformării sunt:

- perspectivele alternative de consolidare a pregătirii personalului în exploatarea oportunităţilor oferite de evoluţiile disruptive în diferite domenii de referinţă;
- locul central al informaţiei în activitatea de comandă şi control şi în cadrul procesului decizional;
- îmbunătăţirea cooperării şi a schimbului de informaţii între NATO şi parteneri în baza exploatării evoluţiilor disruptive;
- considerarea provocărilor pe termen lung a evoluţiilor disruptive în cadrul SFA/ FFAO.

Toate aceste abordări reclamă inovaţie în procese, metode, mentalităţi, tehnologie, dar şi o aliniere a modului în care transformarea este promovată de către ACT şi înţeleasă la nivelul actorilor implicaţi în transformarea capabilităţilor – în cazul de faţă Centrele de excelenţă NATO, care se bazează în mod predilect pe orientarea primită din partea comandamentelor strategice ale Alianţei. Un concept revizuit al Comitetului Militar NATO pentru centrele de excelenţă[21] urmăreşte ajustarea relaţiei ACT cu aceste instituţii sub auspiciile unui nivel crescut al contribuţiei cu produse şi servicii orientate predilect către nevoile Alianţei, în condiţii ce încurajează relaţionarea şi interacţiunea centrelor cu structurile NATO la diferite niveluri, pornind de la structurile de comandă şi de forţe şi continuând cu grupurile de lucru şi comitetele NATO, agenţiile şi facilităţile de educaţie şi instruire ale Alianţei, naţiunile partenere şi entităţi non-NATO, cu precădere din mediul academic şi al industriei de apărare.

În condiţiile în care cea mai importantă resursă a Alianţei este personalul ce deserveşte structurile acesteia, viziunea Conceptului NATO pentru *Capitalul uman* promovează augmentarea valorii corpului de cadre prin dezvoltarea cunoaşterii, abilităţilor şi atitudinilor necesare operării într-un mediu complex, cu multiple provocări şi în continuă schimbare. În acest context, NATO asociază capitalului uman o serie de elemente, dincolo de clasica resursă umană:

- doctrina, organizarea şi leadershipul, ca referinţe directoare şi de suport; şi
- instruirea, tehnologia, baza materială şi informaţia, ca facilitatori ai sarcinilor specifice[22], practic, întreg spectrul DOTMLPFI refocalizat către individ.

Aprofundând analiza factorilor specifici subsumaţi de către acest spectru, observăm că trendul actual în NATO în ce priveşte dezvoltarea capitalului uman se leagă, indisolubil, de cultura inovaţiei, atât în materie de gândire critică, exploratorie, cât şi în ce priveşte tehnologia (inteligenţa artificială, sisteme de suport pentru procesul decizional sau sisteme autonome) şi interfaţa om-sistem tehnic. În acest context, avansul tehnologiilor comerciale trebuie tratat ca oportunitate şi adaptat şi exploatat cu prioritate, în condiţiile în care aceste tehnologii sunt accesibile tuturor actorilor relevanţi în domeniul securităţii. Mai mult, centrele de excelenţă trebuie să vină în întâmpinarea oportunităţilor de cercetare şi dezvoltare oferite de mediul academic şi industria specializată, asigurând exclusivitatea unor soluţii originale de rezolvare a unor problematici specifice.

Liderii de la toate nivelurile sunt cei aşteptaţi să direcţioneze şi să fie parte a procesului de dezvoltare şi perfecţionare continuă, proces ce nu poate fi disociat de responsabilitatea naţională pentru formarea corpului de cadre şi dezvoltarea profilului de lider, adaptarea şi diversificarea cunoaşterii şi a mijloacelor operaţionale pentru a răspunde la provocările de securitate actuale şi la particularităţile zonelor de interes, precum şi interconectarea şi parteneriatele cu alţi actori relevanţi, din diferite medii: organizaţii guvernamentale şi neguvernamentale, academic, industria de securitate etc.

Elemente de viziune pentru o nouă decadă de contribuţie a HCOE în serviciul NATO

Noile provocări ale mediului de securitate, impactul evoluţiilor disruptive din diferite medii, cerinţele privind capitalul uman şi reziliența instituţională, inovaţia şi transformarea la nivelul capabilităţilor, dar şi eforturile adaptative ale Alianţei la toate nivelurile sunt elemente ce îşi

pun amprenta asupra modului în care centrele de excelență își organizează activitatea şi contribuie la dezvoltarea de produse şi servicii în sprijinul NATO.

HCOE nu face excepție de la acest trend, grupul de comandă al instituției fiind pus în situația de a aborda cu atenție o serie de elemente cheie ale analizei SWOT[23] pentru configurarea viziunii şi strategiei de urmat în vederea păstrării relevanței Centrului ca facilitator al dezvoltării capabilității HUMINT.

Pornind de la statutul actual al organizației (prin prisma capitalului uman de care aceasta dispune, a sistemului de proceduri interne consolidat în mai mult de zece ani de activitate, a portofoliului de activități şi bazei relaționale cu alte entități) marcăm – prin atributul maturității instituționale – punctul forte al Centrului de excelență NATO din Oradea. Toate aceste realizări sunt tributare leadershipului modern, rezilienței instituționale şi sprijinului de care Centrul se bucură, cu precădere din partea României, în calitate de națiune-cadru.

În ceea ce privește provocările externe, nevoia de transformare rezultă dintr-o serie de curente distincte:

a) modificări ale priorităților strategice ale NATO şi nevoia asigurării superiorității Alianței în domeniile relevante pentru mediul de securitate (de natură să afecteze orientarea eforturilor de sprijin ale Centrului);
b) transformarea capabilităților NATO (în cazul obiectului de activitate al HCOE – cu precădere Intelligence şi HUMINT), proces ce reclamă alinierea şi armonizarea cu trendul general al schimbării, focalizat pe adaptarea la mediul operațional în continuă schimbare şi la procesele tehnologice disruptive de natură să interfereze în mod negativ cu activitatea specifică;
c) transformarea NATO în ceea ce priveşte resursa umană, procesele şi tehnologia; acest fenomen afectează HCOE din multiple perspective:
   - modificări în procesele funcționale ale NATO din sfera dezvoltării doctrinare şi conceptuale, a educației şi instruirii, a analizei bazate pe lecții identificate şi a celei predictive, etc., care antrenează adaptarea proceselor interne;
   - modificări în comportamentul beneficiarilor produselor şi serviciilor HCOE (de unde rezultă nevoia de adaptare a acestora la noile cerințe);
   - modificări în comportamentul entităților partenere, în baza obiectivelor reprioritizate ale acestora (fapt ce necesită flexibilitate şi deschidere instituțională din partea HCOE).

Analiza elementelor specifice ne ajută să putem prefigura câteva dintre prioritățile de viitor ale Centrului, corespunzător pilonilor transformării ce stau la baza activității acestuia.

Astfel, în domeniul dezvoltării doctrinare şi al standardizării, se impune o deschidere mai largă către optimizarea tehnicilor, tacticilor şi procedurilor specifice disciplinei prin abordarea integrată a metodologiei specifice culegerii de informații din surse umane şi exploatării acesteia în mediul militar şi în cel civil, dar şi prin fructificarea oportună a lecțiilor învățate şi a recomandărilor ce decurg din analiza predictivă. Dincolo de contribuția la standardele NATO, produsele adiacente carevin în sprijinul beneficiarilor Centrului (ghiduri, manuale, tutoriale, etc.) trebuie aliniate unei viziuni de educație şi instruire caresă asigure eficiența transferului de cunoaştere, abilități şi atitudini către utilizatorii finali.

Un aport important la dezvoltarea capacităților specifice domeniului HUMINT îl are inițierea, experimentarea şi validarea de noi concepte teoretice şi tehnologice, aliniate nevoilor ce decurg din noile realități ale vieții (translatate în mediul operațional) şi adaptate specificului capabilității. Acest deziderat reclamă o bună înțelegere a transformărilor societății şi a psihologiei individuale şi colective prin perspectiva numitorului comun şi a diferențelor specifice raportate la coordonate culturale, istorice, socio-psihologice, de geografie umană, etc. Centrul a dezvoltat, în acest sens, o bază de relaționare cu mediul academic şi cu industria, contribuind la abordarea sistematizată a unor aspecte relevante (ex. proiectul privind

Aspectele umane ale mediului operațional); în viitor, ne propunem o sensibilitate crescută la concluziile analizei impactului evoluțiilor disruptive în procesele şi tehnologia ce afectează rutina relațiilor interumane, (micro-)mediul de securitate, supremația procedurală/tehnică, cunoaşterea şi înțelegerea, educația şi instruirea, analiza datelor şi informațiilor, etc. În acest sens, urmărim ca relația cu mediul academic şi cu industria să fie orientată predilect către cercetare şi inovare în toate aceste domenii.

Procesul lecțiilor învățate şi al analizei este unul decisiv în orientarea nevoilor de schimbare. Dacă orizontul de colectare a observațiilor este bine stabilit şi valorificat, acesta trebuie să îşi sporească relevanța prin folosirea resurselor de tip ”push” în relația cu beneficiarii (specialiştii în standardizare şi dezvoltare conceptuală, dar nu numai), să identifice trenduri şi puncte/momente critice ale evoluțiilor disruptive şi să formuleze recomandări atât pentru remedierea deficiențelor, cât şi pentru asigurarea avansului procedural şi tehnologic în competiția cu adversarii.

Toate aceste aspecte ajung să fie fructificate în relația cu beneficiarii soluțiilor de educație şi instruire ale Centrului. În calitate de responsabil departamental pentru instruirea în domeniul HUMINT în NATO, Centrul a elaborat o nouă viziune menită să asigure dezvoltarea unui portofoliu de cursuri în cadrul unei abordări structurate, aliniate nevoilor specifice pentru fiecare palier şi specializare necesară în cadrul structurilor HUMINT[24]. Totodată, această abordare urmăreşte creşterea numărului de contributori cu soluții educaționale certificate, complementare ofertei de instruire a HCOE. Înființarea Comunității de interes pentru educația şi instruirea în domeniul HUMINT în NATO este un facilitator atât pentru curricula, cât şi pentru modernizarea metodelor de instruire şi implementarea de tehnici moderne în activitatea de învățământ, un mare avantaj reprezentându-l schimbul de bune practici cu instituțiile partenere.

Pentru a veni în sprijinul experimentării unor astfel de metode şi tehnici, Centrul a înființat un laborator dedicat domeniului educațional, urmărind depăşirea stadiului de inițiere în domeniul e-Learning şi adaptarea soluțiilor educaționale (*„ce predăm”* - spectrul de cunoaştere teoretică, aptitudini/abilități, atitudini şi *„cum predăm”* - opțiunea de livrare şi metoda didactică) la caracteristicile şi aşteptările noilor generații de studenți („mileniali”), cu o motivație şi modalitate de a învăța diferită de cea clasică. Astfel, urmărim să îmbinăm cu creativitate diferite soluții de modelare şi simulare, virtualizare, jocurile educaționale (*seriousgames*[25]), tutoriale inteligente, inteligență artificială, etc., însă cu păstrarea primatului liniei directoare marcate de obiectivele de performanță urmărite şi de obiectivele de învățare/instruire corespondente.

Prin noua directivă internă pentru educație şi instruire, Centrul îşi asumă certificarea unui număr de instructori specializați în domeniul HUMINT în NATO, selectați în baza unor criterii bine definite, ce acoperă atât cerințe de experiență şi cunoaştere în specialitate, cât şi pregătirea necesară în domeniul pedagogic; crearea unui corp de instructori internaționali (calificați şi recunoscuți ca atare) este de natură să permită dezvoltarea calității actului de instruire. Mai mult, urmărind asigurarea accesului cursanților la cunoaştere validată în mediul academic specializat, intenționăm să dezvoltăm baza de referință pentru recrutarea conferențiarilor din mediul civil pentru acoperirea unor teme cuprinse în programa cursurilor rezidente oferite de Centru.

Un mediu de instruire sintetic (Synthetic Learning Environment/ SLE[26]) în cadrul HCOE (cu potențial de cuprindere a întregii comunități de interes din domeniul educațional) urmăreşte îmbinarea elementelor cheie ale teoriei pedagogice şi ale tehnologiei în vederea creării contextului optim pentru învățare şi instruire, materializat în caracteristicile mediului educațional şi parametrii trăirilor beneficiarilor – specialişti în domeniul HUMINT ce urmează să execute activități specifice în cadrul comandamentelor Alianței sau în operații.

*

* *

Dacă elementele descrise mai sus vin în sprijinul direct al pilonilor transformării, direcționarea, controlul şi armonizarea activității este asigurată prin efortul grupului de comandă

şi structurile de stat major. Dincolo de apelul la tehnici şi instrumente manageriale moderne (standarde şi instrumente de management a fluxului informaţiuonal şi a cunoaşterii, planificarea şi conducerea activităţii, controlul calităţii, stabilirea şi măsurarea indicatorilor de performanţă, managementul pe bază de proiecte, gestionarea suportului logistic şi cu servicii, managementul resurselor umane, etc.), ne propunem adaptarea continuă, multidimensională,la vectorii schimbării promovaţi în cadrul Comandamentului Aliat pentru Transformare, astfel încât contribuţia Centrului la efortul de transformare şi la cerinţele Alianţei să fie corect reprezentate.

Totodată, o relaţie intensificată cu Comandamentul Aliat pentru Operaţii şi comandamentele operaţionale şi tactice subordonate va asigura racordarea HCOE la procesele decizionale şi de planificare a operaţiilor (inclusiv prin folosirea de instrumente de realitate virtuală), mizând pe o reflectare corespunzătoare a acestora – în ceea ce priveşte prezenţa şi contribuţia disciplinei HUMINT – în soluţii educaţionale şi medii de dezbatere.

Reanalizarea priorităţilor de sprijin aleHCOE pentru şi în cadrul procesului complex de transformare a Alianţei se află într-o etapă iniţială. În 2020, Centrul de excelenţă NATO în domeniul HUMINT sărbătoreşte zece ani de la acreditare şi va fi pe deplin pregătit pentru asumarea unui nou deceniu de activitate în sprijinul NATO la cele mai înalte standarde de calitate.

Bibliografie

Documente şi rapoarte oficiale

1. HQ Supreme Allied Commander Transformation, *Framework for Future Alliance Operations - 2018 Report*, content provided by Strategic Plans & Policy, Norfolk VA., în https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf.
2. HQ, SACT, Joint Force Trainer Directorate, *Human Capital Focus Area – Concept Paper*, Norfolk VA, USA, 2018.
3. NATO HQ, *Protocol on the Status of International Military Headquarters Set up Pursuant to the North Atlantic Treaty*, Paris, 28 August 1952, în http://www.nato.int/docu/basictxt/b520828a.htm.
4. NATO HQ, *The Secretary General's Annual Report 2018 - Fit for Purpose: Modernising NATO*, 14 Mar. 2019, în https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf#page=41.
5. NATO Military Committee, *MCM-236-03 MC Concept for theCentres of Excellence*, 04 December 2003.
6. Transformation Network Branch/HQ SACT, *2018 Chiefs of Transformation Conference. Analysis Report*, February 2019.

Cărţi şi articole

7. Arndt Freytag von Loringhoven, *Adapting NATO Intelligence in support of "One NATO"*, în NATO Review 08/09/2017, https://www.nato.int/docu/review//2017/Also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/EN/index.htm?utm_medium=email&utm_campaign=NATO%20Review%20Adapting%20NATO%20intelligence&utm_content=NATO%20Review%20Adapting%20NATO%20intelligence+CID_adbce305abebbe57c153524f899812f1&utm_source=Email%20marketing%20software&utm_term=Read%20more.
8. Florin-Vasile Tomiuc, Alexandru Kis, *Centrul de excelenţă* NATO în domeniul HUMINT la schimbul de generaţii, în INFOSFERA – Revistă de studii de securitate şi informaţii pentru apărare, Anul X nr. 3/2018, Centrul tehnic-editorial al armatei, Bucureşti.
9. Jaap de HoopScheffer, *Cuvânt înainte al secretarului general*, în NATO Review – Analiza transformării în NATO, primăvara 2005, https://www.nato.int/docu/review/2005/issue1/romanian/foreword.html.
10. Jan Ballast, *Trust (in) NATO; The Future of Intelligence SharingwithintheAlliance*, ResearchPaper, Research Division – NATO Defense College, Rome – No. 140 – September 2017, înhttp://www.ndc.nato.int/news/news.php?icode=1085.
11. Janis Cannon-Bowers, Clint Bowers, *Synthetic Learning Environments. Handbook of research in educational communications and technology*, University of Central Florida, Orlando, Florida, 2008.

12. John J. Garstka, *The transformation challenge*, în https://www.nato.int/docu/review/2005/NATO-Transformation/transformation-challenge/EN/index.htm.
13. Joseph S. Gordon, *Intelligence sharing in NATO*, în https://www.atlcom.nl/ap_archive/pdf/AP%202017%20nr.%206/Gordon.pdf.
14. Mark Joyce, *Ducând mai departe agenda de transformare a NATO*, în NATO Review – Analiza transformării în NATO, primăvara 2005, în https://www.nato.int/docu/review/2005/issue1/romanian/foreword.html.
15. Robert Bell, *Fişa transformării NATO*, în NATO Review – Analiza transformării în NATO, primăvara 2005, https://www.nato.int/docu/review/2005/issue1/romanian/foreword.html.

Websiteuri

16. http://www.nato.int/docu/update/2007/pdf/majic.pdf, accesat în martie 2019.
17. http://www.ncia.nato.int/news/Pages/20122112-MAJEX12-%E2%80%93-NATO-Agency-hosted-exercise-puts-NATO%E2%80%99s-Joint-ISR-Smart-Defence-initiative-into-practice.aspx, accesat în martie 2019.
18. https://e-itep.act.nato.int/Guest/ETOCindex.aspx, accesat în martie 2019.
19. https://www.act.nato.int/serious-games-beyond-training, accesat în martie 2019.
20. https://www.nato.int/docu/review/2018/Also-in-2018/trident-juncture-and-the-information-environment/EN/index.htm, accesat în martie 2019.
21. www.natohcoe.org, accesat în februarie 2019.

---

[1] *Protocol on the Status of International MilitaryHeadquarters Set upPursuanttotheNorth Atlantic Treaty*, Paris, 28 August 1952, în http://www.nato.int/docu/basictxt/b520828a.htm

[2] Oferta educațională a Centrului este disponibilă atât pe websiteul instituției, www.natohcoe.org, cât şi în catalogul electronic al NATO – Educationand Training OpportunitiesCatalogue/ ETOC, disponibil la https://e-itep.act.nato.int/Guest/ETOCindex.aspx

[3] Jaap de HoopScheffer, *Cuvânt înainte al secretarului general*, în NATO Review – Analiza transformării în NATO, primăvara 2005, https://www.nato.int/docu/review/2005/issue1/romanian/foreword.html

[4] Mark Joyce, *Ducând mai departe agenda de transformare a NATO*, în NATO Review – Analiza transformării în NATO, primăvara 2005, https://www.nato.int/docu/review/2005/issue1/romanian/foreword.html

[5] Robert Bell, *Fişa transformării NATO*, în NATO Review – Analiza transformării în NATO, primăvara 2005, https://www.nato.int/docu/review/2005/issue1/romanian/foreword.html

[6] HQ Supreme AlliedCommanderTransformation, *Framework for FutureAllianceOperations - 2018 Report*, content providedby Strategic Plans&Policy, Norfolk VA., înhttps://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf

[7] NATO HQ, *The SecretaryGeneral'sAnnual Report 2018 - Fit for Purpose: Modernising NATO*, 14 Mar. 2019, p. 42, în https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf#page=41

[8] John J. Garstka, *The transformationchallenge*, în https://www.nato.int/docu/review/2005/NATO-Transformation/transformation-challenge/EN/index.htm

[9] http://www.nato.int/docu/update/2007/pdf/majic.pdf

[10] http://www.ncia.nato.int/news/Pages/20122112-MAJEX12-%E2%80%93-NATO-Agency-hosted-exercise-puts-NATO%E2%80%99s-Joint-ISR-Smart-Defence-initiative-into-practice.aspx

[11] https://www.nato.int/docu/review/2018/Also-in-2018/trident-juncture-and-the-information-environment/EN/index.htm

[12] O excepție notabilă o reprezintă componenta de supraveghere a JISR în NATO, asigurată prin mijloace proprii: flota de aeronave Boeing E-3A Sistem aerian de avertizare şi control/ AirborneWarning& Control System (AWACS), căreia i se adaugă Sistemul Aliat pentru Supraveghere Terestră/ AllianceGroundSurveillance (AGS), format din sisteme aeriene fără pilot şi elemente de sprijin, comandă şi control la sol, în măsură să permită Alianței supravegherea zonelor de interes şi a obiectivelor statice sau în mişcare de la mare altitudine în sprijinul unui larg spectru de misiuni – operații de răspuns în caz de criză/ managementul crizelor, securitate maritimă, contraterorism, asistența umanitară, asistența în caz de dezastre naturale, etc. În 2035, flota AWACS va fi înlocuită de o suită de mijloace moderne, dezvoltate în cadrul programului AllianceFutureSurveillanceand Control.

[13] Joseph S. Gordon, *Intelligence sharing in NATO*, în https://www.atlcom.nl/ap_archive/pdf/AP%202017%20nr.%206/Gordon.pdf

[14] ArndtFreytag von Loringhoven, *Adapting NATO Intelligence in support of "One NATO"*, în NATO Review 08/09/2017, https://www.nato.int/docu/review//2017/Also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/EN/index.htm?utm_medium=email&utm_campaign=NATO%20Review%20Adapting%20NATO%20intelligence&utm_content=NATO%20Review%20Adapting%20NATO%20intelligence+CID_adbce305abebbe57c153524f899812f1&utm_source=Email%20marketing%20software&utm_term=Read%20more

[15]NATO HQ, *The SecretaryGeneral'sAnnual Report 2018 - Fit for Purpose: Modernising NATO*, 14 Mar. 2019, p. 60, în https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf#page=41

[16] Jan Ballast (expert în ministerul apărării olandez) recomandă o serie de priorități pentru noul ASG-I&S, insistând asupra continuării aranjamentelor bilaterale între NATO şi statele membre pentru schimbul de informații/ dezvoltarea unor procese în acest sens, dar şi recunoaşterea rolului dominant al SUA, în virtutea capacităților operaționale de colectare și a sistemelor/ platformelor de facilitare a schimbului de informații.
(Jan Ballast, *Trust (in) NATO; The Future of Intelligence SharingwithintheAlliance*, ResearchPaper, Research Division – NATO Defense College, Rome – No. 140 – September 2017, înhttp://www.ndc.nato.int/news/news.php?icode=1085)

[17] Joseph S. Gordon, *Op. Cit.*

[18] Florin-Vasile Tomiuc, Alexandru Kis, *Centrul de excelen*ță NATO în domeniul HUMINT la schimbul de generații, în INFOSFERA – Revistă de studii de securitate şi informații pentru apărare, Anul X nr. 3/2018, Centrul tehnic-editorial al armatei, Bucureşti

[19] TransformationNetworkBranch/ HQ SACT, *2018 Chiefs of TransformationConference. Analysis Report* (PubliclyDisclosed), February 2019

[20] *Ibidem*

[21] Versiunea curentă - *MCM-236-03 MC Concept for theCentres of Excellence*, 04DEC03

[22] HQ SACT, Joint Force Trainer Directorate, *Human Capital Focus Area – Concept Paper*, Norfolk VA, USA, 2018

[23] Strengths, Weaknesses, Opportunities, andThreats/ Puncte tari, Puncte Slabe (deficiențe, vulnerabilități), Oportunități şi Amenințări

[24] Dorim să remarcăm, în acest context, faptul că HCOE şi-a asumat un rol important în pregătirea liderilor în domeniul HUMINT la nivel tactic (prin dezvoltarea unui curs dedicat elementelor de comandă din cadrul echipelor HUMINT – *NATO Field HUMINT Team Leadership Course*), dar şi formarea cadrelor de stat major specializate, cu atribuții bine determinate în procesul de planificare şi consiliere a factorilor de decizie (*NATO HUMINT Staff Course*)

[25] https://www.act.nato.int/serious-games-beyond-training

[26] Janis Cannon-Bowers, Clint Bowers, *SyntheticLearningEnvironments. Handbook of research in educationalcommunicationsandtechnology*, University of Central Florida, Orlando, Florida, 2008

PROVOCĂRI ALE DOMENIULUI INFORMAȚIILOR LA NIVELUL UNIUNII EUROPENE

Robert CĂLINOIU*

Abstract

The European Union Global Strategy 2016 announced new challenges and established specific goals for the policy of the European Union in the fields of diplomacy and security. In order to meet these goals, EU decisions have to be backed by effective intelligence support. In this respect, the EU intelligence community, composed primarily by four agencies–EU Intelligence Center (INTCEN), EU Intelligence Division/EUMS (EUMS Int), Satellite Center (SATCEN) and European Union Agency for Law Enforcement Cooperation (Europol) –, represents the backbone for the information and policy making support of the EU governance.

In this articleit will be presented the challenges of the EU intelligence domain andpossible future developments of the EU intelligence community. In a world in a rapid change in which the EU has to find its way to maintain the status of a significant player, the development of its intelligence becomes crucial, to understand the classic and hybrid types of threats and to provide the much needed intelligence to the leadership.

Keywords*: European Union, intelligence domain, challenges, EU Intelligence Center, EU Intelligence Center*

Aspecte generale privind cultura de informații

Una dintre principalele provocări ale dezvoltării domeniului informațiilor la nivel european o constituie cultura specifică aferentă, care, deşi matură la nivelul fiecărui stat, este cvasi-absentă la nivelul integrat al instituțiilor şi conştiinței europene.

Cultura în domeniul informațiilor este determinată de patru elemente majore.Primul, capacitatea de funcționare ca entitate de sine stătătoare sau, altfel spus, independența sa pe toate componentele ciclului informațional versus dependența de resursele altor structuri. Al doilea, istoria comunității de informațiipe care se construieşte, de obicei, cultura de informații. Relația dintre comunitatea de informații şi decidentul politic, precum şi societate în ansamblul său, reprezintă al treilea aspect al culturii în domeniul informațiilor,iar ultimul element luat în considerare îl constituiecultura organizațională care stă la baza funcționării agențiilor/structurilor de informații.

Cultura de informații în SUA – elemente comparative

Pentru a sublinia situația improprie în care se află cultura de informații la nivel european, poate fi realizată o scurtă analiză a modelului american şi, apoi, expuse câteva elemente de comparație.

Cultura de informații în SUA a început o dată cu emiterea legislației (National Security Act) de constituire a comunității de informații

* ***Expert în cadrul Ministerului Apărării Naționale.***

(CI), în anul 1947. CI americană cuprinde astăzi 17agenţii specializate, care se află în coordonarea Directorului pentru Informaţii Naţionale (Director of National Intelligence – DNI), şi care sunt organizate astfel încât să răspundă nevoilor de informaţii din domeniile apărării, securităţii interne, energiei, justiţiei, finanţelor etc. Această organizare permite CI americane să fie independentă în funcţionarea ei de partenerii externi naţionali sau terţe organizaţii.

Cel mai important element al culturii de informaţii americane este **culegerea**, bazat pe convingerea că „faptele vorbesc de la sine" (*factsspeak for themselves*[1]), precum şi pe **contextul geopolitic istoric stabil** timp de 50 de ani, în care Uniunea Sovietică a fost principalul inamic, o **ameninţare statică**, acesta neschimbându-şi practicile prea mult în decursul timpului şi generând prin amploarea lui o nevoie continuă de a obţine cât mai multe date şi informaţii, pentru a-l înţelege mai bine. Demersul asiduu de a obţine informaţii a condus la căutarea unor soluţii tehnice din ce în ce mai performante, ceea ce avut un impact deosebit în **dezvoltareatehnologiei** aferente. Avansul tehnologic îi permite şi în prezent CI americane să găsească soluţii mai rapide în domeniul informaţiilor, fie că este vorba de culegere, de transmiterea datelor rapid către centrele de analiză, de analiza unor mari volume de informaţii sau de luarea unor decizii informate şi punerea lor în aplicare.

Birocraţia ierarhică a CI americane, unde agenţiile componente sunt subordonate DNI, iar acesta preşedintelui SUA, este un alt element caracteristic culturii de informaţii americane. Aceasta permite coordonarea eforturilor structurilor de informaţii şi evitarea duplicărilor şi alocării nejustificate a resurselor în proiecte dezvoltate deja de alte agenţii. Cooperarea interinstituţională la nivelul structurilor din cadrul CI s-a dezvoltat continuu, în mod accelerat după atentatele de la 11 septembrie 2001, când s-a constatat că agenţiile deţineau informaţii disparate, care, integrate şi interpretate corect, ar fi putut conduce la evitarea atacurilor teroriste.

Importanţa domeniului informaţiilor şi a funcţionării eficiente a ierarhizării stricte este relevată şi de faptul că preşedintele SUA îşi începe ziua de lucru cu un briefing de informaţii produs de CI, care include elemente de importanţă strategică, relevante pentru procesul decizional specific.

Legăturile solide cu partenerii strategici sunt o altă caracteristică a culturii de informaţii, având rădăcinile în cooperarea dezvoltată, în principal la nivel militar, pe timpul celor două războaie mondiale şi consolidată pe timpul Războiului Rece. În prezent, globalizarea solicită o cooperare şi mai accentuată între agenţiile de informaţii ale diverselor state, volumul uriaş de informaţii provenite din surse deschise (OSINT) necesitând abilităţi de înţelegere şi interpretare pe care un singur stat, oricâte resurse ar deţine, nu le poate acoperi singur.

Valorificarea informaţiilor culese şi analizate prin operaţii specifice reprezintă o altă latură importantă a culturii de informaţii americană. Astfel, de-a lungul timpului, detectarea unei ameninţări majore la adresa intereselor strategice americane a fost urmată deseori de măsuri care au îmbrăcat un spectru larg, de la acţiuni diplomatice, economice, antiteroriste punctuale până la acţiuni militare de mare anvergură.

Cultura de informaţii la nivelul UE. Cultura specifică domeniului informaţiilor la nivel european este în stadiu incipient, situaţie cauzată de mai mulţi factori. Primul este continua transformare a Uniunii Europene (UE), ajunsă succesiv la un număr de 28 de state, fiecare cu o identitate şi cultură proprii. În egală măsură, domeniile apărării şi politicii externe la nivelul UE se află în responsabilitate naţională[2], structurile de la Bruxelles având misiunea de a media armonizarea intereselor statelor, atunci când acestea sunt divergente, şi nu de a lua decizii care să fie aplicate de naţiunile componente. Ca urmare, statele susţin poziţii bazate pe informaţiile primite de la structurile naţionale, care pot fi, în funcţie de resursele la dispoziţie şi interesele regionale, incomplete sau cu un pronunţat caracter de subiectivitate.

Consecințele faptului că responsabilitatea securității naționale revine fiecărui stat membru sunt multiple, mergând de la alocări de resurse naționale pentru obținerea de informații privind aceeaşi amenințare identificată (exemplu: migrația ilegală) până la lipsa unei strategii comune europene de contracarare a acesteia, precum şi reticența de a dezvolta structuri de informații comune.

Un alt impediment major în dezvoltarea unei culturi de informații la nivelul UE este chiar **reticența statelor de a crea structuri de informații comune independente**, care să aibă resursele necesare obținerii, analizării şi furnizării unor produse informative relevante liderilor Uniunii. Inexistența unor structuri solide, a căror activitate să devină apreciată în timp prin impactul major resimțit în domeniul securității europene, contribuie la menținerea culturii actuale, unde informațiile clasificate sunt mai degrabă generatoare de îngrijorări administrative privind accesul la ele şi protejarea confidențialității lor decât aducătoare de clarificări pe subiecte de interes strategic.

Inadecvarea structurilor europene cu atribuții în domeniul informațiilor la amenințările curente reprezintă, în egală măsură, un factor decisiv în menținerea reticenței față de viabilitatea dezvoltării acestora. Imigrația ilegală, care a constituit un factor destabilizator major la adresa securității europene şi o sursă de divergențe politice şi economice între statele membre, a fost percepută târziu ca o amenințare cu caracter strategic.

Amenințările domeniului cibernetic, având ca vectori de propagare entități greu detectabile, sunt de asemenea contracarate cu mijloace insuficiente la nivel european integrat iar centrul de greutate fiind transferat către națiuni, în timp de modul de acțiune este transnațional.

Dezvoltarea conflictelor militare prin interpuşi, fără asumarea de către o națiune a sponsorizării acțiunilor destabilizatoare şi generatoare de instabilitate, sunt, de asemenea, insuficient contracarate în mod unitar, coerent, la nivelul UE.

De asemenea,recrudescența fenomenului terorist transfrontalier necesită o abordare integrată, deplasarea facilă a teroriştilor pe teritoriul UE dintr-un stat în altul pentru a executa atacuri fiind evidentă în ultimele decenii (atacurile de la Madrid, Paris sau Bruxelles).

Fenomenul extremismului internațional îndreptat împotriva instituțiilor naționale sau europene, în continuă expansiune în perioadele de criză politică sau economică, solicită şi el o atenție sporită, fiind totodată un argument în plus pentru crearea unor instituții capabile să informeze la timp despre riscurile asociate unor decizii naționale.

Cooperarea îndomeniul informațiilor

Conceptul de Politică Externă şi de Securitate Comună (CFSP) a fost introdus în dezbaterile europene începând cu anul 1993, odată cu Tratatul de la Maastricht, devenind unul dintre pilonii cooperării în cadrul UE. Ulterior, cu ocazia Summit-ului Consiliului European de la Koln, din iunie 1999, UE a lansat conceptul de „Politică de Europeană de Securitate şi Apărare (Eu*ropean Securityand Defence Policy* – ESDP)", iar la finele anului următor, prin Tratatul de la Nisa, s-a creat baza legală privind cooperarea europeană în domeniul securității şi apărării prin definirea competențelor, structurilor şi mijloacelor necesare dezvoltării Politicii de Securitate şi Apărare Comună (*Common Securityand Defence Policy* – CSDP). La crearea şi dezvoltarea structurilor formale cu atribuții în domeniile CFSP şi CSDP au contribuit, în mare măsură, pe lângă acumulările progresive descrise anterior, şi situația de securitate din Europa, marcată de războaiele din fosta Iugoslavie, dezintegrarea Uniunii Sovietice şi apariția unor republici autonome sprijinite de Federația Rusă pe teritoriul unor state independente, precum şi recrudescența fenomenului terorist, evidențiatăprin atentate cu un număr mare de victime pe teritoriul unor state având sisteme de securitate solide. Ca urmare, obiectivul principal al CSDP l-a constituit managementul

crizelor în afara teritoriului UE, deziderat care a condus în 2001 la apariţia ca structuri formale a Comitetului Politic şi de Securitate (Political SecurityCommittee – PSC), a Comitetului Militar al UE *(EU MilitaryCommittee* – EUMC) şi a Statului Major Militar al UE (*EU Military Staff* – EUMS) – în cadrul Secretariatului General al Consiliului UE şi, ulterior, parte a Serviciul European de Acţiune Externă (*European ExternalAction Service* – EEAS). În cadrul EUMS funcţionează Direcţia informaţii (*EUMS Intelligence Directorate* – DINT), ale cărei misiuni sunt: furnizarea contribuţiilor specifice în procesul de avertizare timpurie, întocmirea evaluărilor privind situaţiile de criză, participarea cu informaţii la planificarea misiunilor, furnizarea de informaţii în procesul de planificare a răspunsului la crize şi de produse specifice pentru operaţii şi aplicaţii.

La nivel civil, în anul 1999 a fost înfiinţat Centrul Întrunit pentru Informaţii (*JointSituation Center* – SITCEN), având misiunea de a întocmi analize din surse deschise. În 2002 acesta a devenit un forum destinat schimbului de informaţii clasificate între SITCEN şi şapte state membre UE (Franţa, Germania, Italia, Olanda, Spania, Suedia şi Marea Britanie). SITCEN s-a dezvoltat progresiv prin accederea reprezentanţilor mai multor state membre şi a devenit, începând cu 2012, Centru de Informaţii (*Intelligence andAnalysis Centre* – INTCEN), structură civilă de informaţii aflată, de asemenea, în cadrul EEAS şi cu care DINT cooperează strâns în cadrul formatului Single Intelligence AnalysisCapacity – SIAC.

De asemenea, parte a arhitecturii de informaţii la nivel european este şi Centrul Satelitar (*EUSatellite Center* – SATCEN). Acesta a fost înfiinţat în 1993 sub denumirea Centrul Satelitar al Uniunii Europei de Vest (*Western European Union Satellite Center*), denumirea actuală (adoptată în 2002) fiind expresia dezvoltării Uniunii în ansamblul său.

Coordonat operaţional de Serviciul European de Acţiune Externă, SATCEN furnizează avertizări privind crize potenţiale (*earlywarning of potentialcrises*). Produsele şi serviciile furnizate se bazează pe exploatarea mijloacelor spaţiale şi date colaterale, incluzând imagini satelitare şi aeriene (GEOINT şi IMINT)[3].

O altă componentă a comunităţii de informaţii europene este EUROPOL (*European Union Agency for Law Enforcement Cooperation* – EUROPOL). Acesta a fost înfiinţat în 1999, având ca scop creşterea securităţii cetăţenilor UE prin sprijinirea autorităţilor naţionale de impunere a legii din statele membre ale Uniunii.

Cooperarea în domeniul informaţiilor între structurile UE

Cooperarea INTCEN/EUMS Int cu serviciile naţionale din statele membre. Structurile civile şi militare de informaţii ale UE cooperează îndeaproape, în diverse forme, cu structurile naţionale. Astfel, personalul celor două structuri provine în cea mai mare parte din serviciile naţionale, oferind astfel expertiza necesară domeniului. Acesta reprezintă, de altfel, şi canalul de comunicare bidirecţională dintre serviciile menţionate, solicitând sau transmiţând informaţiile necesare. Nedispunând de capacităţi de culegere proprii, INTCEN/ EUMS Int se bazează fundamental pe contribuţiile cu informaţii provenite de la statele membre. De asemenea, pe aspecte de interes punctuale sunt organizate întâlniri între experţi la Bruxelles sau în capitalele statelor membre UE, expertiza specifică fiind împărtăşită în beneficiul celor implicaţi.

Pentru coordonarea activităţilor, anual au loc la Bruxelles conferinţe la nivelul coordonatorilor structurilor de politici şi planuri în domeniul informaţiilor ai serviciilor de informaţii civile (SIC) şi militare (SIM), la nivelul directorilor pentru analiză, precum şi la nivelul liderilor SIM ale statelor membre. Ulterior, deciziile luate sunt puse în practică, contribuind la adaptarea şi perfecţionarea cooperării multilaterale.

Cooperarea INTCEN – EUMS Int. Cooperarea INTCEN – EUMS Int se derulează în cadrul formatului oferit de Capacitatea unicăde

analiză a informațiilor (Single Intelligence AnalysisCapacity – SIAC). În acest format are loc partajarea informațiilor primite de la SIC şi SIM, pe canalele protejate naționale, se stabilesc prioritățile informative şi se constituie echipe de lucru mixte (Task Force) pe dosarele de criză, îmbinându-se expertiza militară cu cea civilă.

Un astfel de exemplu este Celula de fuziune a informațiilor privind amenințările de natură hibridă (*HybridFusionCell*), constituită pentru analizarea informațiilor şi acțiunilor specifice îndreptate împotriva intereselor UE şi întocmirea de produse informative caracteristice acestui nou spectru de amenințări.

Produsele informative sunt diseminate atât liderilor instituțiilor Uniunii Europene, cât şi serviciilor naționale de informații, militare şi civile, din acest punct de vedere SIAC funcționând ca un centru de fuziune a informațiilor (Intelligence Fusion Center). Avantajul acestui format constă înfaptul că orice stat membru poate beneficia de expertiza altui stat pe domenii de interes temporar (situații de criză, pregătire misiuni UE/multinaționale etc.).

De asemenea, SIAC organizează grupuri de lucru unde invită analişti ai serviciilor de informații naționale ale statelor membre, ai unor state partenere sau membri ai diverselor organizații non-guvernamentale cu expertiză relevantă în domeniul de interes.

Tot în format mixt sunt organizate misiuni specifice în zonele de interes (*Fact Finding Missions*), pentru a maximiza fluxul de informații pe teme de interes.

Atât cooperarea în cadrul SIAC, cât şi transmiterea produselor informative la beneficiari ar cunoaşte o îmbunătățire exponențială după realizarea sistemului de comunicații care va permite schimbul electronic de informații clasificate între entitățile UE, precum şi între acestea şi instituțiile statelor membre sau delegațiile permanente ale UE în străinătate.

Cooperarea SIAC cu SATCEN. Cooperarea SIAC cu SATCEN are loc în formatul oferit de Serviciul European de Acțiune Externă, Centrul Satelitar fiind singurul mijloc de culegere de informații la dispoziția Uniunii Europene. Având în vedere nivelul strategic la care SIAC îşi desfăşoară activitatea, SATCEN reprezintă un sprijin important în procesul elaborării produselor informative în măsura în care poate furniza informațiile solicitate, răspuns grevat de inexistența unei rețele de sateliți proprie şi apelarea la furnizarea de imagini satelitare de la operatori privați.

Concluzii

Domeniul informațiilor la nivelul UE se dezvoltă şi consolidează în ritmul dictat de decidenții statelor membre. Configurația actuală a sistemului instituțional european al informațiilor oferă atât avantaje, cât şi dezavantaje. Păstrarea centrului de greutate al interesului informativ la nivel național este favorizat de cultura de securitate europeană actuală şi de prevederile Titlului I, Articolul 4 Alineatul (2) din Tratatul privind Uniunea Europeană şi a Tratatului privind funcționarea Uniunii Europene, care menționează fără echivoc faptul că „securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru”.

Pe de altă parte, un sistem instituțional specific, subordonat UE, ar putea oferi elementele strategice necesare evitării surprinderii Uniunii Europene, direct sau indirect, cu acțiuni care să-i afecteze securitatea, precum valuri migraționiste masive, acte teroriste ale unor structuri cu ramificații transnaționale, schimbări de granițe prin forță armată care să afecteze grav echilibrul de securitate în proximitatea sa, influențarea negativă a alegerilor libere şi democratice sau a referendumurilor naționale cu impact la nivelul UE, devoalarea dezinformărilor privind politicile şi acțiunile europene sau evitarea recrudescenței naționalismului extremist.

Bibliografie

1. *Tratatul de la Maastricht*, Titlul V – Provisions on a common Foreign and Security policy;
2. Declarația franco-britanică de la Saint-Malo;
3. SALMI, Ilkka, fost director al INTCEN, interviu în publicația MoondialNieuws din Belgia;https://www.mo.be/en/interview/ilkka-salmi-eu-s-007
4. Prezentare a lt. col. Francisco Rodriguez Berbel-Lopez (EUMS) la cursul CSDP organizat de Colegiul European pentru Securitate şi Apărare cu sprijinul Universității Naționale de Apărare la Bucureşti, în perioada 05-09.02.2018.Broşura de prezentare a EUMS,https://www.cvce.eu/en/obj/information_brochure_on_the_european_union_military_staff_eums-en-1bcbd497-c5e3-4b7a-ab54-9e392e0c1483.html;
5. LASSCHE, Deborah, articol în revista Militaire Spectator;https://www.militairespectator.nl/thema/internationale-samenwerking/artikel/eu-military-staff-frog-boiling-water;
6. Site-ul oficial al EEAS; https://eeas.europa.eu/headquarters/headquarters-homepage_en/3602/Organizationchart.

[1] J.Palacios, „Intelligence Analysis Training: A European Perspective", *The International Journal of Intelligence, Security, and Public Affairs*, 18 (1), 2016, pp. 34-56.

[2] Titlul I,a Articolul 4 Alineatul (2) din Tratatul privind Uniunea Europeană şi a Tratatul privind funcționarea Uniunii Europene: *„Uniunea respectă egalitatea statelor membre în raport cu tratatele, precum şi identitatea lor națională, inerentă structurilor lor fundamentale politice şi constituționale, inclusiv în ceea ce priveşte autonomia locală şi regională. Aceasta respectă funcțiile esențiale ale statului şi, în special, pe cele careau ca obiect asigurarea integrității sale teritoriale, menținerea ordinii publice şi apărarea securități naționale.* În special, securitatea na***ţională rămâne responsabilitatea exclusivă a fiecărui stat membru***.*"*

[3] https://europa.eu/european-union/about-en/agencies/satcen-en

INFORMAȚIILE MILITARE ÎN DINAMICA TEATRELOR DE OPERAȚII

Adonis JURCA
Dragoş OSTACI
Ionuț POPA[*]

Abstract

Military intelligence is one of the most important branches in the military system and even if in the most cases the particular activity of this section is not visible for the untrained eyes, their products participate actively in shaping the military commanders decisions.

First of all, from the perspective of military planning and strategy'sthe intelligence support recently has become more and more often one of the most important key factors for the leaders in order to reduce the level of incertitude - the most challenging issues for a military planner. Military intelligence personnel collect and generate information and in the same, based on the surrounding environment analysis approaches to provide guidance and directions to assist commanders in their decisions. This aim is achieved by providing an assessment of data from a range of sources, directed towards the commander's mission requirements as part of operations and campaign planning.

More and more often in the recent of the new hybrid military approaches, the role of the intelligence assets has become crucial also for offering to the political leaders guidance regarding the level of the security risk towards home land security.

Last but not the least the army's military intelligence is responsible for all collected intelligence during army missions and one of the most important role is to provide essential Intel that often save the solders lives fighting in front lines.

In the future, it can be predicted that the military intelligence system will become more and more complex with a wide range of missions corroborated with the new world wide strategical orientation. So, it may be concluded that this branch will develop even more implicated in every military and political aspect.

Keywords: *NATO, intelligence, stabilization, integration*

Încă de la începuturile istoriei sale, omul a luptat pentru supraviețuire şi se poate spune că a făcut-o cu succes. Acest deziderat se datorează, în mare măsură, capacității sale de a-şi folosi abilitatea minții în scopul multiplicării forței, iar acest lucru nu a însemnat doar descoperirea focului, a armelor şi uneltelor şi perfecționarea continuă a acestora ci, mai ales, căutarea continuă în scopul cunoaşterii adversarului, amenințărilor, punctelor forte ale acestora - pentru a fi evitate - şi a punctelor slabe - pentru a fi atacate decisiv.

Odată cu dezvoltarea societății, au fost generate noi necesități care se doreau a fi satisfăcute astfel încât să poată fi realizate condițiile de perpetuare şi dezvoltare a mediului socializant, nevoia de informații, de cunoaştere, reprezentând o condiție de bază a dezvoltării acestui sistem complex. Una dintre cele mai importante nevoi identificate ca fiind din spectrul celor de bază este cea de apărare şi securitate. În acest context, odată cu dezvoltarea capabilităților şi creşterea gradului de complexitate a amenințărilor şi sistemelor

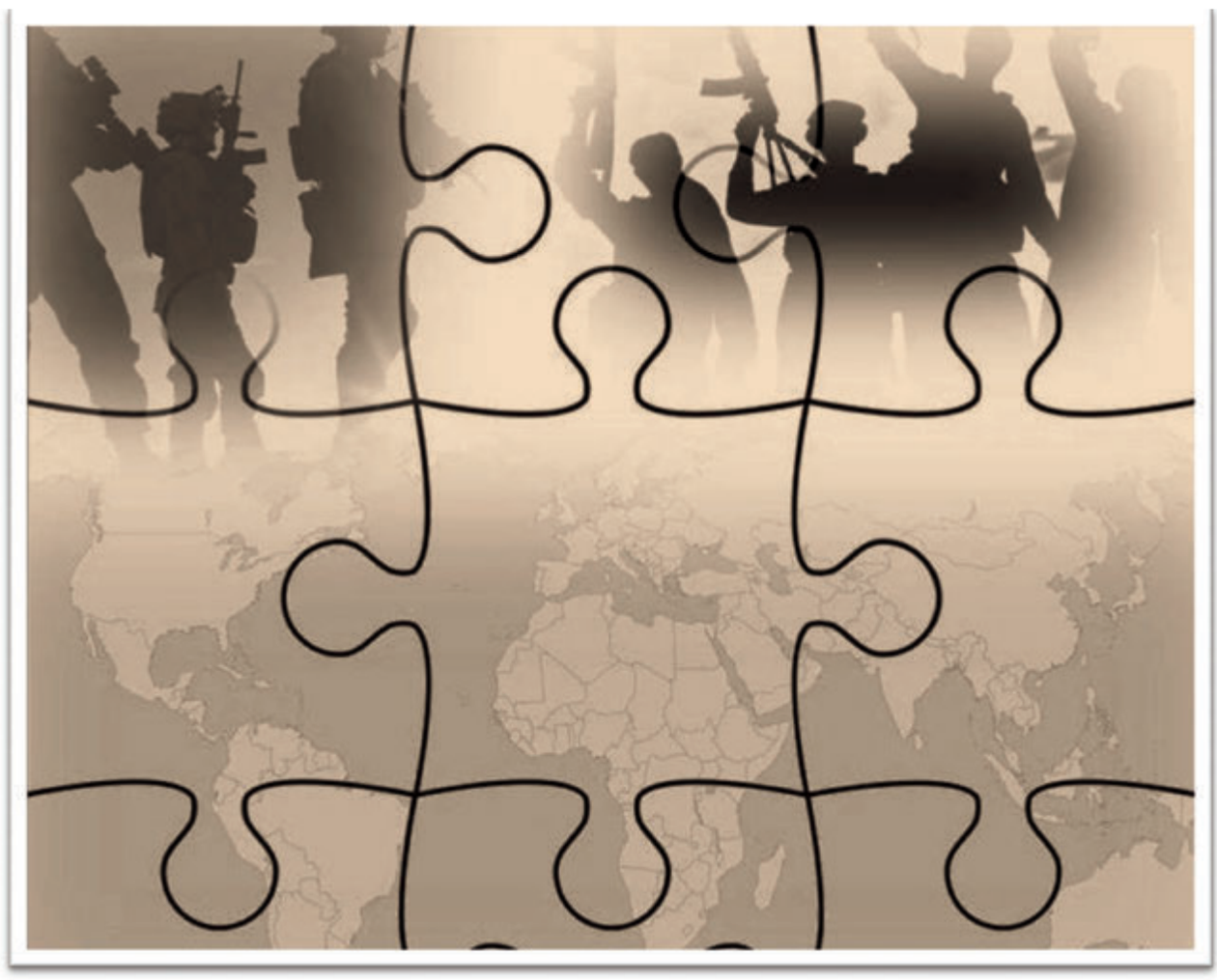
[*] ***Autorii sunt experți în cadrul Ministerului Apărării Naționale.***

militare a apărut necesitatea liderilor de a primi informații despre mediul de luptă în care urmează să își planifice acțiunile militare. Astfel,activitatea decizională impune o consistență sporită a bazei informaționale, iar în domeniul militar nu este doar punctul de pornire al procesului de luare a deciziei, dar şi un real multiplicator al forței în planacțional.

Odată cu apariția actualelor teatre de operații în care misiunile forțelor militare sunt de impunere/menținere a păcii, combatere a terorismului, răspuns la crize, operații umanitare sau, mai pe scurt, Operații Altele Decât Războiul (*MilitaryOperationsOtherThan War*), a reintrat în actualitate necesitatea existenței unor capabilități de culegere de informații care să fie la dispoziția comandanților forțelor luptătoare de la nivel operațional şi tactic.

Actualul mediu de securitate include o combinație de provocări militare şi nemilitare din partea unor actori statali şi nestatali, cu războiul hibrid ca formă favorită. Particularitateaacestor noi tipuri de misiuni (în care capabilitățile militare sunt utilizate şi în alte scopuri decât cele combatante) care implică folosirea forței militare în luptă, dar nu împotriva unei alte forțe militare regulate, ci împotriva unui adversar asimetric, aşa cum se întâmplă în operațiile de combatere a terorismului, a condus la necesitatea oferirii unor noi tipuri de răspunsuri liderilor militari.

În faza de inițiere a planurilor de acțiune, comandanții au identificat nevoia de a defini mediul de confruntare. Din cauza amenințărilor de tip asimetric, acest mediu de confruntare nu poate fi descris doar din punct de vedere militar, ci trebuie analizat din perspectiva unui cumul de factori de tip social, politic, multicultural etc. Nevoile de informații necesare comandanților pentru fundamentarea deciziilor militare nu pot fi satisfăcute întotdeauna prin intermediul forțelor regulate de tip cercetare, fiind necesară implicarea unor capabilități de informații (unice



sau multidisciplinare) prin care să poată fi oferite răspunsuri, analize şi, în general, să sprijine comandantul şi statul major al structurilor militare centrale în buna cunoaştere a mediului de confruntare. Astfel, a fost generată necesitatea apariţiei şi funcţionării unor structuri flexibile şi agile, capabile să acţioneze în medii urbane, aglomerate, şi împotriva metodelor multiple de acţiune teroriste, cu scopul de a obţine informaţii relevante pentru comandanţi.

Totodată, cerinţele operaţiilor multinaţionale dictează abordarea unui spectru larg de misiuni, de la acţiuni pe timp de pace, ca de exemplu asistenţă umanitară, până la zădărnicirea şi prevenirea unui conflict prin acţiuni de menţinere a păcii. În cadrul acestora, informaţiile joacă un rol decisiv. Acestea sunt produsul rezultat din colectarea, prelucrarea, integrarea, analiza, evaluarea, interpretarea şi diseminarea informaţiilor obţinute privind alte naţiuni, forţele ori elementele ostile sau potenţial ostile, zonele operaţiilor actuale sau posibile.

Un alt factor care a condus la apariţia structurilor de informaţii şi a misiunilor de culegere este reprezentat de sporirea ideologiilor extremiste politice, religioase şi etnice care potdeclanşa sau intensifica unele conflicte aflate în stare latentă. Prin intermediul acestor elemente sunt furnizate informaţiide avertizare privind iminenţa declanşării conflictului armat.

În prezent, misiunile principale ale structurilor de informaţii militare în teatrele de operaţii sunt axate, în principal, pe:

- sprijinirea, culegerea, analizarea şi evaluarea informaţiilor necesare structurilor multinaţionale;
- furnizarea deinformaţii privind evenimentele şi fenomenele politico-militare din teatrul de operaţii;
- asigurarea permanentă cu date şi informaţii necesare pregătirii şi executării misiunilor proprii a contingentelor naţionale dislocate în teatrele de operaţii;
- protecţia informativă a contingentelor naţionale dislocate în teatrul de operaţii,prin furnizarea de date privind riscuri şi ameninţări potenţiale la adresa acestora.

Studiu de caz: Teatrul de operaţii (TO) Afganistan

Scurt Istoric

Misiunea ISAF (*International Security Assistance Force*) a fost creată în urma Conferinţei de la Bonn (decembrie 2001), unde s-a convenit, printre altele, ca liderii opoziţiei afgane, care au luat parte la reuniune, să înceapă procesul de reconstrucţie a Afganistanului prin crearea unei structuri guvernamentale denumită Autoritatea Afgană pentru Tranziţie (AAT). Totodată, a fost stabilit conceptul unei forţe internaţionale, sub mandat ONU, care să sprijine AAT şi să creeze un mediu de securitate şi sprijinire a reconstrucţiei Afganistanului. Aceste acorduri au deschis drumul parteneriatului dintre AAT, Misiunea de Asistenţă a ONU în Afganistan - UNAMA (*United NationsAssistanceMission in Afghanistan*) şi ISAF.

La data de 11 august 2003, NATO a preluat conducerea operaţiilor ISAF, Alianţa fiind responsabilă de conducerea, coordonarea şi planificarea forţelor, inclusiv de numirea unui comandant ISAF şicrearea comandamentelor ISAF din Afganistan. Această decizie a rezolvat problema identificării unei naţiuni care să se afle la comanda ISAF şi a permis naţiunilor mai mici, care nu puteau prelua conducerea misiunii, să aibă un rol mai important în cadrul comandamentelor multinaţionale.

Rolul informaţiilor militareeste cu atât mai vizibil din perspectiva particularităţilor acestui teatrude operaţii unde conflictul se desfăşoară între oameni, printre oameni, limitând utilitatea aplicaţiilor convenţionale ale puterii militare. Din acest motiv, comandanţii se confruntă cu lipsa unui inamic, având trupe regulate (având de a face, de această dată, cu adversari de tip asimetric). Din cauza gradului ridicat de impredictibilitate al inamicului nevăzut, capabilităţile militare aflate sub comanda decidenţilor militari şi politici nu pot fi planificate şi utilizate în lipsa informaţiilor. Astfel, informaţiile culese de către structurile responsabile din acest teatru de operaţii sunt folosite pentru a întregi imaginea câmpului de luptă în care acţionează comandantul

forţei multinaţionale.Mai mult decât atât, procesulmilitar de luare a deciziilor nu poate fi derulat şi finalizat în variante corecte în lipsa implicării/furnizării de informaţii obţinute de către ofiţerii de informaţii.

Având în vedere noile concepte doctrinare pe care Alianţa a trebuit să le dezvolte pentru Afganistan, elementele de intelligence au trebuit să participe activ pentru succesul operaţiilor cu efect planificat. Conceptul a condus la multiplicarea cererilor de informaţii solicitate comunităţii de intelligence de către factorii decidenţi, mai ales pe fondul ameninţărilor teroriste. Totodată, din perspectiva mediului dinamic al operaţiilor aflate în derulare, efortul de culegere în Afganistan este concentrat în scopul planificării şi dezvoltării operaţiilor curente.

Din această perspectivă, prin intermediul informaţiilor obţinute se încearcă realizarea superiorităţii de informaţii pentruavertizarea timpurie privind acţiunile insurgente aflate în faza de planificare, realizarea de analize din perspectiva ameninţărilor din domeniul asimetric şi monitorizarea factorilor de risc la adresa forţelor de coaliţie.

Rolul cel mai important al structurilor de informaţii militare dislocate în acest TO este de a transmite în timp util date şi informaţii care conduc la salvarea de vieţi omeneşti. Principala ameninţare este reprezentată de atacurile organizate şi desfăşurate de către diferitele celule sau grupări insurgente/teroriste împotriva militarilor coaliţiei.

Plecând de la fazele de planificare şi pregătire ale unui atac insurgent, comandanţii structurilor de intelligence trebuie să planifice misiuni de culegere care să fie orientate pe obţinerea informaţiilor care pot conduce la interzicerea desfăşurării acestor acţiuni.Astfel, culegerea informaţiilor militare este direcţionată pentru identificarea elementelor specifice fazelor de pregătire a atacului (tranzacţii financiare, întâlniri lideri insurgenţi, aprovizionarea traficarea/ substanţelor explozive, pregătirea specifică a unor autoturisme etc.) şi până la fazele de execuţie a acestor atacuri (lideri implicaţi în coordonarea acestuia, personal implicat în acţiunile directe, data executării, locaţia, etc.). Obţinerea şi diseminarea acestor informaţii în timp oportun conduc la avertizarea timpurie a structurilor şi

microstructurilor militare, fapt ce contribuie decisiv la salvarea de vieți omenești.

Totodată,informațiile militare contribuie și la creșterea nivelului de securitate la nivelul forței de coaliție și prin furnizarea acelor date care contribuie decisiv la capturarea/neutralizarea principalilor lideri insurgenți din TO. În acest sens, direcționarea elementelor de informații se face în modalități dependente de nivelul, ierarhia, precum și rolul liderilor/ membrilorrețelelor teroriste.

O particularitate a acestui tip de misiuni este dată de conlucrarea strânsă dintre structurile de informații militare și structurile de forțe speciale. În situația în care cele douăentități militare nu sunt sincronizate la nivel decizional și acțional, finalitatea procesului de culegere a informațiilor poate fi un eșec. Din acest motiv, este vital ca în cazul existenței unor cereri de informații care pot conduce la capturarea unor lideri insurgenți să poată fi înțelese de către ambele structuri capabilitățile și limitările specifice fiecăreia, astfel încât informațiile furnizate să corespundă nivelului acțional. În același timp, solicitările informative ale elementelor de forțe trebuie adaptate în funcție de capabilitățile și limitările structurilor de informații. Din această perspectivă, este vitală existența/funcționarea unui element comun de comandă care să poată sincroniza toate fazele misiunii (plecând de la furnizarea elementelor declanșatoare pentru planificarea misiunii și până la exploatarea informativă a țintelor de mare valoare capturate de către structurile specializate).

Concomitent cu activitatea specifică ciclului informațional, structurile de intelligence au desfășurat și desfășoară, în continuare, activități specifice de sprijin al forțelor de securitate afgane, precum și al instituțiilor indigene implicate în dezvoltarea capacității de apărare a Afganistanului și cetățenilor afgani.

Astfel, structurile de intelligence au fost implicate și în executarea misiunilor de instruire, consiliere și asistență (TAA/*TrainAdviseAssistant*) a ministerelor afgane din domeniul securității, instituțiilor statului și oficialilor de rang înalt din cadrul forțelor armateși poliției afgane.

Studiu de caz: Teatrul de operații Balcanii de Vest - misiunea KFOR (NATO)

Din perspectiva noilor paradigme de abordare a conflictelor militare, TO Balcanii de Vest reprezintă unul dintre cele mai reprezentative exemple. Schimbările majore privind modul prin care se pot obține efectele scontate (prin producerea schimbărilor din interior, prin de-legitimizarea instituțiilor și a ideologiilor statuluipentru a câștiga, în cele din urmă, sprijinul populației), în lipsa unui conflict militar sau a unor acțiuni directe, au generat transformărișsi în ceea ce privește modul în care sunt utilizate structurile de informații militare. Pentru aceasta, a fost necesară prezența entităților de intelligence pe termen lung, în scopul dezvoltării capacităților necesare și pentru extinderea impactului operațional.

Complexitatea conflictului, izbucnit pe fondul tensiunilor interetnice și prin exacerbarea elementelor cu un profund sentiment național, a generat necesitatea existenței în teren a unor capabilități de informații pentru monitorizarea și transmiterea unor date de tip *atmospherics*. Rolul acestor informări este de a identifica oportun elementele care pot conduce la reizbucnirea unor tensiuni generatore de violență. Astfel, putem concluziona că rolul informațiilor obținute din regiunea Balcanilor de Vest este de a monitoriza atitudinile populațiilor, grupurilor etnice/ minorităților și nu de control al forțelor unui adversar sau al unui teritoriu.

Scurt Istoric

La 10 iunie 1999, Consiliul de Securitate al ONU a adoptat Rezoluția 1244, care a plasat Kosovo sub administrarea UNMIK (*United NationsMission in Kosovo*) și a autorizat dislocarea în zonă a unei forțe militare de menținere a păcii sub comandă NATO, respectiv KFOR (*KosovoForces*).

KFOR menține securitatea și asigură libertatea de mișcare în aria sa de responsabilitate (AOR/*Area of Responsibility*), în strânsă cooperare cu prezența civilă internațională și instituțiile Kosovo, executând operații bazate pe intelligence, utilizând avertizarea timpurie,

dislocarea rapidă şi hotărâtă a forţelor de manevră şi rezervelor pentru a descuraja violenţa şi escaladarea crizelor, concomitent cu asigurarea condiţiilor de trecere la etapa GATE 3.

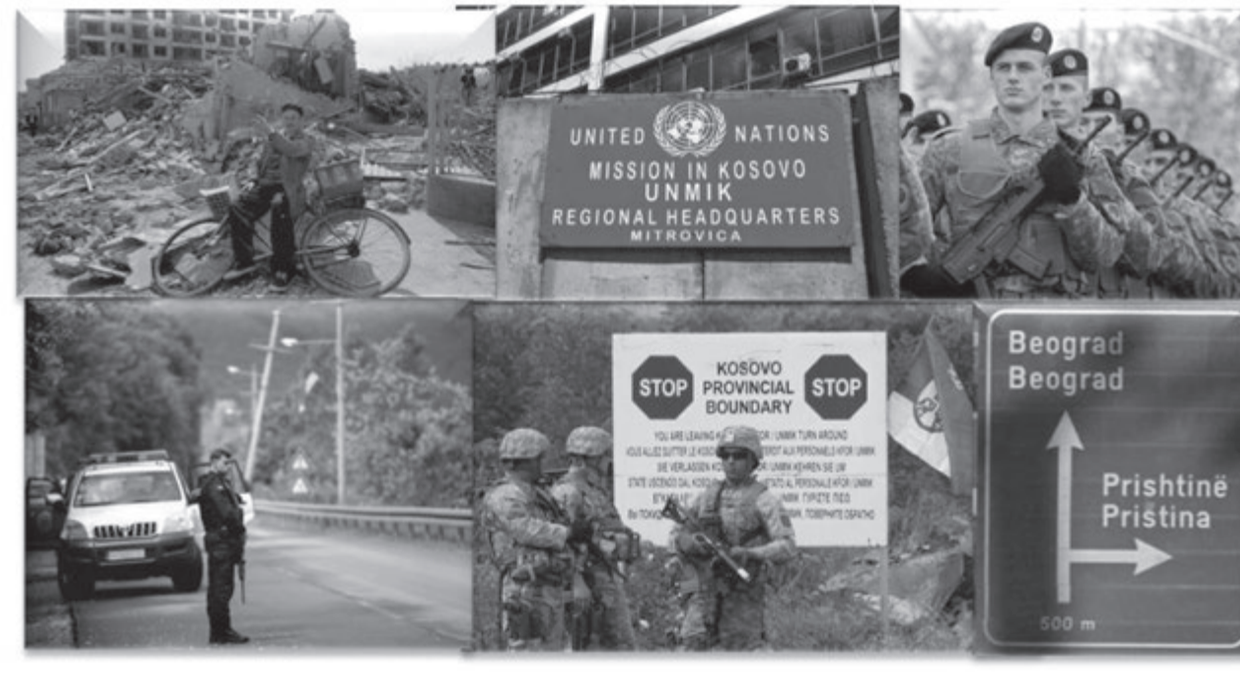
Sprijinul cu informaţii cuprinzător a devenit o cerinţă cheie în cadrul operaţiilor de stabilitate contemporane. Pentru a face faţă provocărilor complexe de securitate, organizaţiile internaţionale sunt nevoite nu doar să îşi dezvolte structuri de informaţii relevante, dar să şi integreze informaţii civile şi militare în cadrul structurilor organice de informaţii. În sprijinul acestei idei este relevantă experienţa de 20 de ani a misiunii KFOR, care, de cele mai multe ori, a fost în măsură să asigure un sprijin cu informaţii complet pentru structura de comandă a misiunii. În momentele în care nu a fost în măsură să prevadă anumite evenimente, misiunea a fost surprinsă şi obligată să se transforme.

Misiunea NATO în Kosovo a fost proiectată ca o operaţie militară bazată pe informaţii (*intelligence drivenoperation*). Iniţial, în perioada 1999-2004, KFOR şi-a dezvoltat, în principal, capabilităţi de culegere a informaţiilor focalizate pe domeniul militar, iar informaţiile civile au fost plasate în plan secund. Din cauza acestui fapt, misiunea KFOR nu a fost capabilă să culeagă informaţii relevante referitoare la tensiunile inter-etnice acumulate între minorităţile sârbă şi albaneză. Ca urmare, escaladarea acestor tensiuni şi, ulterior, transformarea acestora în conflicte deschise au luat prin surprindere KFOR.

Revoltele din Kosovo din anul 2004 au izbucnit la data de 17 martie şi sunt descrise ca fiind cel mai violent incident de la sfârşitul Războiului din Kosovo (1999). Cauza directă a fost un zvon nefondat despre înecarea a trei copii albanezi de către sârbi, ceea ce a determinat ca etnicii albanezi să atace comunităţile sârbe din provincia Kosovo.

Potrivit mass-media sârbe, în urma revoltelor 19 persoane au murit, câteva sute au fost rănite, 4000 de sârbi au fost obligaţi să-şi părăsească casele, 800 de case şi 35 de biserici ortodoxe au fost vandalizate, distruse, profanate. Amploarea violenţelor a determinat KFOR să-şi suplimenteze personalul şi să adopte o nouă paradigmă referitoare la culegere informaţiilor din zona de responsabilitate.

În urma evenimentelor din martie 2004, structura de comandă a KFOR a înţeles utilitatea creării unei structuri specializate pentru culegerea informaţiilor civile referitoare la conflicte interetnice, situaţia economică a municipalităţilor, nevoile cu care se confruntă administraţiile locale, atitudinea populaţiei şi a diferiţilor actori locali faţă de misiunea KFOR, efectele acţiunilor KFOR resimţite la nivelul grupurilor etnice. Aceste categorii de informaţii şi opinii care circulă la un moment dat într-un



areal sunt denumite în literatura de specialitate *atmospherics*. Pentru a gestiona informațiile de tip *atmospherics*, KFOR a planificat şi desfăşurat operații non-cinetice bazate, în special, pe operații informaționale (KLE – keyleadersengagement, COMKFOR Keypoints). În vederea culegerii de informații de tip *atmospherics*, comunicării directe cu instituțiile din Kosovo şi transmiterii către populație a punctelor de vedere ale COMKFOR referitoare la diferite situații şi evenimente, KFOR a dezvoltat şi întrebuințat structuri specializate denumite LMT (Laisonand Monitoring Team).

În prezent, misiunea KFOR se află în faza a II-a operației (*DetterentPresence*)/ etapa a III – a (GATE 3) şi se pregăteşte pentru ultima fază operațională numită MinimumPresence. Transformarea KFOR şi reducerea efectivelor au fost gândite să se desfăşoare în funcție de atingerea unor condiții în mediul operațional, cum ar fi: dezarmarea grupărilor paramilitare, construirea unui mediu sigur, predarea responsabilităților către instituțiile din Kosovo, realizarea dialogului Belgrad – Pristina. Atingerea condițiilor pentru trecerea la următoarea etapă s-a făcut pe baza unor indicatori prestabiliți. Pentru monitorizarea permanentă a indicatorilor şi pentru analiza obiectivă a situației operaționale, misiunea KFOR a fost nevoită să îşi dezvolte structuri proprii de informații care să îi asigure sprijinul informativ în condițiile în care a fost privată de posibilitatea de a solicita sprijin informativ de la alte eşaloane sau misiuni care îşi desfăşurau activitatea în provincia Kosovo. Ca urmare, KFOR şi-a dezvoltat propriile structuri de informații puternice, auto - suficiente şi complexe pentru a acoperi multitudinea de domenii şi solicitări caracteristice unei operații tip *intelligence drivenoperation.*

Un argument puternic în favoarea importanței deosebite a sprijinului cu informații în desfăşurarea misiunii KFOR este faptul că, în procesul dereducere a efectivelor - de la aproximativ 50.000, în faza Focus Engagement, la aproximativ 4000 în prezent - capabilitățile de informații au fost păstrate sau suplimentate. KFOR a utilizat şi utilizează capabilități de informații diverse pentru asigurarea sprijinului de informații propriu, structuri de cercetare, HUMINT, CI, IMINT, SIGINT, LMT, PSYOPS.

Modul în care au fost proiectate inițial structurile de informații ale KFOR, organizarea ulterioară a acestora, modul de acțiune, misiunile executate, lecțiile identificate şi experiența acumulată în 20 de ani de existență recomandă utilizarea arhitecturii sale de informații la nivelul oricărei structuri tactice de nivel divizie din forțele terestre. Arhitectura de informații a KFOR s-a dovedit a fi suficient de complexă pentru a asigura informațiile necesare misiunii şi a arătat că este deosebit de important să se trateze în mod egal domeniul civil şi cel militar. În situația în care misiunea KFOR şi-a concentrat eforturile pe un domeniu în detrimentul altuia, evenimentele din mediul operațional nu au mai putut fianticipate, generând efecte negative, de bumerang, la adresa misiunii. Din cauza particularităților administrative şi etnice din regiunea balcanică, rolul elementelor de informații a fost şi este unul semnificativ, orientat mai ales pentru furnizarea datelor de interes decidenților în ceea ce priveşte identificarea factorilor de risc la adresa stabilității, asigurarea continuării implementării prevederilor acordurilor de pace, precum şi crearea unui climat de securitate în regiune.

Concluzii

În prezent, noile orientări ale strategiilorde politică externă ale marilor actori internaționali combină prevederile doctrinei militare (bazate, în principal,pe asigurarea numărului de militari, a mijloacelor de luptă şi a puterii de foc necesare pregătirii pentru ducerea unui război de uzură) cu rolul dominant al puterii informațiilor. Alături de profesionalismul militarului apare şi necesitatea abilității de a negocia şi atitudinea față de populația locală. Se poate concluziona că actuala filozofie a conflictelor se bazează pe înlocuirea interesului de a ocupa un teritoriu cu interesul de a influența evenimentele, prin renunțarea la ideea necesității de a fi prezenți în favoarea exigenței de a controla, influența şi, eventual, a interveni. De asemenea, observăm caracterul tot mai pronunțat al evitării, pe cât posibil, a confruntărilor armate directe şi schimbarea dezideratului de a-i produce

pierderi substanțiale inamicului, crescând astfel rolul informațiilor întimp real.

Născut odată cu România modernă, în anul 1859, prin înaltul Ordin de Zi nr. 83 emis de domnitorul Alexandru Ioan Cuza, serviciul de informații al Armatei a urmărit cu conştiinciozitate îndeplinirea misiunilor sale: cunoaşterea armatelor străine, identificarea şi analiza pericolelor care pot afecta independența statului, menținerea suveranității, unității şi integrității României şiprevenirea oricăror agresiuni la adresa țării.

În prezent, România participă la efortul comunității internaționale în cadrul misiunilor pentru menținerea păcii şi stabilității în teatrele de operații,atât prin prezența unor subunități militare regulate, cât şi a unor militari care încadrează diferite funcții în cadrul forțelor multinaționale.

Hotărârea de a avea o prezență în aceste teatre de operații a vizat opțiunea factorilor politico-militari naționali de a contribui cu forțe militare şi reprezentanți militari în zone unde au avut loc conflicte, iar în conformitate cu hotărârea organizațiilor internaționale abilitate s-au luat măsuri de a se trece la consolidarea valorilor democrației, apărării păcii şi stabilității pe plan local.

De-a lungul ultimilor ani de prezență militară românească în Afganistan, prin intermediul informațiilor generate de către Direcția de informații militare s-a contribuit la fundamentarea deciziilor liderilor militari, precum şi la salvarea de vieți omeneşti atât în rândul militarilor români, cât şi a partenerilor de coaliție. Din acest motiv culegerea şi diseminarea informațiilor militare reprezintă o capabilitate indispensabilă comandanților din teatrele de operații militare, importanța sa fiind reevaluată în mod continuu.

De asemenea, ca urmare a manifestării tot mai exacerbate a fenomenului migraționist în regiunea Balcanilor de Vest, România, prin intermediul structurilor de informații militare dislocate în acest spațiu, reprezintă un furnizor de securitate prin obținerea informațiilor referitoare despre posibilii luptători din Orientul Mijlociu,care, sub umbrela statutului de refugiat, intenționează să pătrundă pe teritoriul spațiului UE pentru planificarea şi organizarea de noi atacuri teroriste.

Bibliografie

1. Legea nr. 121/2011 privind participarea forțelor armate la misiuni şi operații în afara teritoriului statului român;
2. „Ce este NATO?”, https://www.nato.int/nato-welcome/index_ro.html/;
3. TEODORESCU, Stelian, *„Intelligence-ul multinațional în sprijinul procesului decizional al planificării operațiilor la nivel NATO”- Teză doctorat*, 2016;
4. RETTMAN, Andrew, Eric MAURICE, *EU perspective opposed by Russia in Balkans,* euobserver, https://euobserver.com/foreign/141820;
5. MIREL, Pierre, *The Western Balkans: between stabilisation and integration in the European Union,* European Issues no. 459, Foundation Robert Schuman, The researchand Studies Centre on Europe, https://www.robert-schuman.eu/en/europeanissues/0459-the-western-balkans-between-stabilisation-and-integration-into-the-european-union;
6. „Forțele speciale ale armatei în structuri internaționale”, www.romania-actualitati.ro/fortele_speciale_ale_armatei_in_misiuni_internationale_51591/;
7. https://facebook.com/mapn.ro/;
8. https://jfcnaples.nato.int/kfor/;

RĂZBOIUL HIBRID-FENOMEN AL EVOLUȚIEI ARHITECTURII GLOBALE DE SECURITATE

*Alexandra DAN**

Abstract

As the violent face of power politics has been distorting the international scene, the academia endeavored to translate the harrowing reality into efficient models capable to manage an insecure world. Drawing the lines of future war became a must among strategists who sought to envisage a great formula for devising efficient strategies aimed at tackling tomorrow's unknown. Despite all the efforts, not only the particularities of each scenario hindered the creation of an extensive model, but also, as history reveals, the shaped patterns of war could not stand competing with time.

Following the main events that disturbed the contemporary world scene, the present paper attempts to portray the shape that warfare has taken throughout time. The paper's main objective is to analyze the foremost factors that led to today's nature of warfare depicted into theoretical models whose viability still remains uncertain.

Keywords: *hybrid warfare, global security, hybrid threat, paradigm, stability operation, proxy war.*

1. Debutul conceptului de război hibrid în studiile de securitate euro-atlantice şi direcții de evoluție

Provocările emanate de factorii perturbatori ai sistemului internațional sunt intensificate de accentuarea globalizării prin care fizionomia conflictelor se metamorfozează, înglobând o varietate de actori cu capabilități inovatoare şi strategii flexibile. Arhitectura mediului de securitate edifică, pe fundamentul proeminenței politicilor externe intervenționiste, a schimbărilor geopolitice şi dezvoltării tehnologice, relații marcate de schimbări rapide şi imprevizibile, complexitate accentuată şi antagonism sporit. Documente strategice de referință[1] statuează ineluctabilitatea conflictelor armate într-un mediu lezat de proliferarea armelor de distrugere în masă, ascensiunea statelor competitive, instabilitatea regională, activitatea criminală transnațională şi de concurența pentru resurse. Competițiile politice, economice, militare şi ideologice deformează statu-quo-ul actual.

Conceptul de „război hibrid" a fost adoptatdin necesitatea de a denumi efectele negative ale evoluției sistemice asupra modului de ducere a conflictelor. În opinia lui William J.Nemeth, războiul hibrid reprezintă o adaptare a conflictelor specifice societăților pre-statale, a căror eficiențăeste amplificată de evoluția tehnologiei şia metodelor moderne de mobilizare[2]. Războiul hibrid implică folosirea tehnologiei şi mass-media, tactici specifice luptelor de gherilă şi exploatarea vulnerabilităților forțelor convenționale generate de conformarea la normele legale.

Trăsăturile specifice războiului hibrid se conturează prin inițiativa lui Frank G. Hoffman care, pornind de la bazele arhetipice ale altor şcoli de gândire[3], oferă o demarcare preliminară a amprentelor războiului modern. Hoffman reliefează structura eterogenă a războiului

**Expert în cadrul Ministerului Apărării Naționale.*

hibrid prin fuzionarea unor elemente specifice războiului de generația a patra[4]- pe fondul ambiguității naturii conflictului şi pierderii de către stat a monopolului asupra violenței, războiului nerestricționat[5] - datorită propagării în mai multe sfere, a înglobării unei varietăți de actori şi utilizarea mai multor combinații de metode şi mijloace, războiului compus (*compound warfare*)[6]- datorită adoptării beneficiilor sinergice determinate de amestecul capabilităților convenționale şi neconvenționale. În completarea formulei războiului hibrid, autorul adaugă complexitatea crescută şi natura dezagregată a mediului operațional, dar şi caracterul oportunist al viitorilor adversari[7]. Pe lângă acestea, includerea terorismului şi a comportamentului criminal al forțelor[8] în desfăşurarea acțiunilor definitivează procesul dehibridizare a conflictului.

Definiția lui Hoffman expune complexitatea conflictelor militare care transcende limitele convenționalității prin înglobarea elementelor (forțe, mijloace şi metode) de natură insurgentă, teroristă şi criminală. Actorii hibrizi dețin capacitatea de a-şi metamorfoza caracterul convențional în conformații atipice caracterizate prin celule descentralizate, grupuri tactice în rețea care beneficiază de capabilități militare moderne şi capacități creative, utilizate într-o variabilitate de tactici, cu scopul de a obține un ansamblu de efecte sinergice pentru atingerea unui obiectiv politic. Urmând episodul conflictului din 2006 dintre forțele paramilitare ale grupării Hezbollah şi armata israeliană (Forțele de Apărare Israeliene), Hoffman prezintă o imagine concisă asupra naturii forțelor hibride. Caracterizate de un nivel înalt de disciplină şi pregătire, forțele hibride dețin capacitatea de a restrânge capacitatea operativă a forțelor convenționale prin extinderea arsenalului propriu de metode şi mijloace cu tactici de gherilă şi tehnologie modernă, amplificând gradul de urbanizare al conflictului.

Implicațiile războiului hibrid asupra dimensiunii fizice sunt completate cu cele de ordin psihologic determinate impactul elementelor virtuale şi cognitive, care primesc noi valențe în contextul modernizării tehnologiei informației.

Conceptul de „război hibrid", enunțat de Hoffman, a avut un impact major asupra literaturii de specialitate, devenind un punct de referință al studiilor de securitate. Cu toate acestea, caracterul complex şi polimorf al războiului hibrid a instigat critici din partea comunității academice care au reiterat deficitul de noutate a formei, în ciuda veleității impuse de actualitatea conceptului[9] şi tendința de abstractizare a noțiunii din ambiția de a acoperi o arie largă a formelor de conflict[10], consolidând testimoniul de referință al afirmației că „*dacă toată lumea e un hibrid, atunci nimeni nu este*"[11].

Conturarea modelului specific războiului hibrid, impulsionată de evenimentele violente de pe scena internațională, a determinat mobilizarea comunității academice în direcționarea eforturilor spre aprofundarea modelului teoretic şi identificarea modalităților de optimizare a răspunsului. O primă tentativă de delimitare a originii conflictului hibrid i se atribuie lui Margaret S. Bond care plasează teza statelor eşuate ca nucleu al amenințărilor hibride[12]. Astfel, întregul spectru de metode şi mijloace convenționale şi neconvenționale angrenate de forțe regulate, insurgenți şi teroriști este transpus în efectele caracterului pernicios al statelor eşuate sau aflate în curs de eşuare, hipocentre ale fenomenelor teroriste. Direcția de cercetare vizează impactul războiului hibrid asupra reconfigurării forțelor armate şi necesitatea de a extinde aria de competențe pentru completarea operațiilor de luptă tradiționale cu misiuni umanitare şi operații de stabilitate şi sprijin. Astfel, Bond accentuează importanța acțiunilor profilactice direcționate spre pericolele generate de statele eşuate şi argumentează rolul operațiilor de stabilitate şi sprijin în optimizarea răspunsului la adresa amenințărilor hibride. O bună echipare şi pregătire a forțelor armate oferă posibilitatea de a interveni eficient în toate stadiile conflictului pentru impunerea şi menținerea securității şi a stabilității.

Răspunsul în noul context de securitate, în care prevalează amenințări rezultate din conjugarea convenționalului cu acțiuni teroriste şi criminale, este actualizat prin contribuția lui John

J. McCuen[13] care accentuează rolul populației în extinderea complexității conflictelor militare. McCuen conturează forma războiului hibrid prin integrarea atât a unor elemente de natură militară, cât şi o dimensiune conceptuală în care sunt angrenate eforturi de câştigare a încrederii societății civile aflate în aria de operații. Autorul asociază termenul hibrid unei forme agregate de război simetric şi asimetric prin care actorii desfăşoară operații militare tradiționale împotriva forțelor şi obiectivelor inamice, concomitent cu executarea unor acțiuni de dobândire a controlului asupra populației civile din zona de luptă şi câştigarea suportului acesteia, dar şi al propriului popor şi al comunității internaționale.

Un plus de noutate în definirea războiului hibrid este adus de către Russel Glenn, care înglobează în acelaşi cadru„*mijloace politice, militare, economice, sociale, informaționale şi metode de război convenționale, neregulate, catastrofice, teroriste,disruptive/criminale*”[14]. Amenințarea, determinată de amestecul de instrumente nonviolente cu cele agresive, de ordin cataclismic, este emanată atât din partea actorilor statali, cât şi din partea actorilor non-statali.

În doctrina Armatei Statelor Unite definirea războiului hibrid indică o încorporare sumară a acestuia în tabloul cognitiv şi o abordare generalizată a conceptului. Utilizat în mod diluat, termenul „hibrid” este asociat uzual cu conceptul de „amenințare” pentru a distinge acea „*combinație diversă şi dinamică de forțe regulate, neregulate, teroriste, elemente criminale sau o combinație a acestor forțe şi elemente, unificate pentru obținerea unor efecte benefice mutuale*”[15]. Concepția doctrinară parcurge aceeaşi direcție trasată de cercetătorii domeniului, întărind ideile deja enunțate, conform cărora amenințările hibride sunt generate atât de actori statali care aplică forme specifice războiului de uzură şi războiului de tip *proxy*, cât şi de actori nestatali care utilizează concepte şi capabilități asociate, în mod tradițional, cu statele-națiune şi materializate în medii preponderent urbane care oferă oportunități de exploatare a populației civile.

O formă simplificată a definiției războiului hibrid se regăseşte şi în *Hybrid Warfare. Fighting Complex Opponents from the Ancient World to the Present*[16], aceastafiind delimitată de către autori la sfera forțelor convenționale şi neregulate (forțe de gherilă, insurgenți, terorişti) ale căror acțiuni sunt îndreptate spre obținerea unui scop politic comun. Conceptul de război hibrid, prezentat dintr-o perspectivă istorică, integrează aspecte de natură politică şi militară care oferă profunzime şi intensitate conflictelor moderne. Războiul hibrid prezintă o nouă dimensiune a conflictelor armate prin înglobarea elementelor de intelligence, afaceri civile, operații psihologice şi a capacităților civile interguvernamentale. Rolul semnificativ pe care îl denotă factorul civil în concretizarea războiului hibrid este susținut de aportul societății civile în consolidarea puterii militare şi obținerea victoriei politice. Autorii volumului atrag atenția asupra cunoaşterii adversarului[17] şi înțelegeriiideologiei sale, a angajamentului său, a istoriei şi culturii sale. Cunoaşterea cadrului de operare a inamicului decurge din tabloul istoric ca o condiție stringentă pentru obținerea succesului. Mai mult, Williamson Murray evidențiază tendințele contradictorii dintre cerințele războiului convențional, direcționate spre distrugerea aspectelor fizice şi umane, şi războiul de contra-insurgență orientat spre obținerea încrederii populației civile.

Tendința de limitare a ariei de cercetare a războiului hibrid la domeniul militar a devenit evident eronată odată cu tulburările violente din estul Europei. Agresiunea Rusiei din Ucraina, concretizată în destabilizarea violentă a statu-quo-ului, a consternat comunitatea internațională la fel ca succesul relativ[18] al grupării Hezbollah în fața Forțelor de Apărare ale Israelului, succes datorat îmbinării inovative a capabilităților moderne, abilităților avansate şi organizării descentralizate, creând un precedent al hibridizării conflictului armat. Răspunsul la acest tip de amenințări s-a încadrat într-o arie restrânsă de opțiuni, însă lecțiile învățate au contribuit la completarea literaturii de specialitate.

S-a recurs la utilizarea sintagmeide *război hibrid* pentru a descrie evenimentele din Ucraina

din anul 2014 numai după ce s-a observat cătermeni precum „război special”[19], „război non-linear”[20]sau„război proxy”[21]nu pot surprinde realitatea. Prima utilizare a conceptului de *„război hibrid”*pentru a denotainvaziarusă în spațiul ucrainean a venit din partea generalului în rezervă Frank van Kappen, în aprilie 2014. Acesta a definit războiul hibrid ca fiind *„un amestec al războiului clasic cu utilizarea formațiilor armate neregulate”*[22], în care relațiile dintre actorul statal şi grupurile non-statale se desfăşoară în ascuns.

Lipsa de asemănare a conflictului din Ucraina cu modelele teoretice ale războiului, promovate până la acea dată de comunitatea occidentală, a fost generată de statutul de actor statal al Rusiei care a reformat anvergura războiului hibrid, edificată anterior de actori non-statali. În acest sens, Andras Racz[23]analizează, printr-o lentilă inductivă, războiul hibrid dus de Federația Rusăîn Ucraina pentru a delimita principalele caracteristici şi gradul de aplicabilitate al acestuia. Demersul diacronic al lui Racz etalează, ca element de noutate, modul de implementare a metodelor specifice războiului hibrid de către Rusia şi spectrul vast de instrumente focalizat, în special, pe metode non-militare care vizează inclusiv elitele politice.

În articolul „On Not-So-New Warfare: Political Warfare vs. Hybrid Threats”[24], Frank Hoffman atenționează asupra caracterului restrâns dat de conceptualizarea războiului hibrid şicare exclude instrumentele economice, financiare, actele politice subversive sau operațiile de informații, inclusiv acțiuni de propagandă şi dezinformare. În contextul derulării conflictului din Ucraina, Hoffman critică viziunea îngustă evocată de limitele definirii războiului hibrid care exclud potențialul războiului informațional în concretizarea rezultatelor finale. Pornind de la faptul că prezentul conflict din Ucraina reprezintă o provocare la adresa conceptului occidental tradițional de război, Hoffman avertizează asupra deficitului de utilitate a noțiunii de „război hibrid” în ciuda abuzului de teoretizare a realității războiului.

Mutațiile geopolitice ale actualului context de securitate reliefează o nouă eră a ordinii mondiale şi sporesc necesitatea de a reconfigura strategiile de apărare în conformitate cu aspectele neologice determinate de reafirmarea Rusiei pe plan global, intensificarea violenței şi atacurilor teroriste, transformarea Orientului Mijlociu într-un *hub* al ciocnirilor ideologice şi politice sângeroase, amplificarea fluxului de refugiați, precum şi accentuarea tensiunilor dintre principalii actori internaționali. Avansarea tehnologică, adâncirea interdependențelor şi apariția unor noi actori au alterat natura convențională a războiului, umbrind linia de demarcație dintre pace şi război, dintre adevăr şi ficțiune.

Evenimentele din ultimii ani au evidențiat o transmutare a strategiilor în care forța militară a devenit un apendice al arsenalului de instrumente non-militare, decisive pentru atingerea obiectivelor. Astfel, exemplul ucrainean a confirmat capacitatea populației de a influența deznodământul evenimentului, plasând societatea civilă în *„centrul de greutate”*[25] al războiului hibrid. Acțiunile Rusiei, orientate cu precădere asupra populației, au determinat actualizarea concepției privind războiul hibrid, devenit un epicentru al studiilor de securitate.

În prezent, războiul hibrid utilizeazăo varietate de instrumente subversive şi convenționale. Dacă o primă categorie include instrumente specifice războiului politic, informațional, cibernetic, psihologic şi energetic, cea de-a doua categorie presupune metode şi mijloace specifice războiului convențional, în care autoritatea forțelor militare contribuie decisiv la obținerea unor scopuri de natură teritorială, politică, militară. Diversitatea metodelor aplicate variază de la atacuri cibernetice asupra instituțiilor guvernamentale şi financiare, acțiuni de dezinformare şi propagandă, accentuarea nivelului de corupție în vederea deteriorării stabilității politice, economice şi sociale, până la acte teroriste, acțiuni militare disimulate şi intervenția deschisă a forțelor armate pentru subminarea capacității de apărare a statului vizat. În acest sens, strategia specifică războiului hibrid presupune utilizarea instrumentelor cibernetice, a mijloacelor de informare în masă (mass-media), a mediei de socializare (social media), promovarea

infracțiunilor de corupție, utilizarea la vedere sau în ascuns a echipamentelor militare, prin care hackeri, troli, bloggeri, agenți ai serviciilor de informații, forțe pentru operații speciale şi forțe convenționale contribuie la propagarea intereselor actorului hibrid.

Aceste tipuri de operații, aplicate într-un cadru integrat, sunt relatate într-un raport[26] al Senatului Statelor Unite pentru a delimita paradigma actuală a războiului hibrid al Rusiei. În contextul dezvoltării tehnologiei informației, al comunicării şi intensificării interdependențelor, Rusia şi-a direcționat eforturile spre „înarmarea societății civile, ideologiei, culturii, crimei şi energiei"[27] ca extensie a strategiei de „extindere a controlului asupra vecinătății estice şi restaurare a sferei de influență privilegiată în vecinătatea comună a Uniunii Europene şi Rusiei"[28]. Un „amestec letal al atacurilor militare convenționale, asasinărilor, campaniilor de dezinformare, atacurilor cibernetice, înarmarea energiei şi corupției"[29] definitivează forma hibridă a strategiei Kremlinului pentru erodarea democrației şi fracturarea alianței transatlantice.

Imaginea războiului hibrid pe care o evocă Conceptul NATO privind contribuția militară de contracarare a amenințărilor hibride[30] înglobează o varietate de actori (statali, non-statali sau organizații teroriste) a căror sferă de acțiune devansează domeniul fizic al războiului, penetrând, cu precădere, domeniilecibernetic, informațional şi financiar. Caracterul transnațional al amenințărilor provenitedinOrientul Mijlociu şi Nordul Africii (perpetuarea violenței extremiste, tensiunile arabo-israeliene şi politicile asertive ale Iranului) au determinat amplificarea metodelor şi mijloacelor neconvenționale şi, mai ales, a celor civile în evoluția formulei specifice războiului hibrid. Declarația adoptată la Summitul Alianței din Țara Galilor (2014) aintrodusîn terminologia NATO conceptul de „amenințări ale războiului hibrid" pentru desemnarea unei arii largi de măsuri civile, militare şi paramilitare deschise şi ascunse, înglobate într-un design integrat.

Concepția Uniunii Europene privind amenințările hibride reliefează un tablou comprehensiv care include „acțiuni coercitive şi subversive, metode convenționale şi neconvenționale"[31] menite să exploateze vulnerabilitățile țintei şi să submineze valorile democratice şi libertățile fundamentale.

Îmbinarea dintre convențional şi neconvențional a determinat formarea caracterului hibrid al războiului, însă elementul de noutate este promovat de anvergura operațiilor, de intensitatea şi viteza de desfăşurare a acțiunilor. Amenințările hibride vizează exploatarea vulnerabilităților statelor şi instituțiilor democratice prin utilizarea mijloacelor politice, economice, militare, civile şi informaționale pentru influențarea aparatului decizional în scopul obținerii obiectivelor strategice şi compromiterea şi/sau lezarea țintei[32].

2. Noi repere ale războiului hibrid în strategia Federației Ruse

Caracteruldinamicalrăzboiuluiaobstrucționat generarea unui model adecvat care să ofere previziuni pertinente formelor viitoare de război. Metodele de conflict au evoluat spre dimensiuni non-militare care, conform şefului Statului Major al Federației Ruse, ValeriGherasimov, au devansat ca eficacitate puterea forței armelor, accentuând caracterul asimetric al conflictului. Articolul său, publicat prima dată în revista rusă „Voyenno-Promyshlennyy Kurier", în februarie 2013, a fost tradus în limba engleză („The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations"[33])şi semnalat imediat opiniei publice de Robert Coalson.Ideile prezentate în articol, apărut ulteriorşi în revista americană Military Review (în numărul din ianuarie-februarie 2016), suntconsiderate de unii specialişti ca fiind o „teorie extinsă a războiului modern[34]" sau „o nouă teorie a haosului privind războiul politic"[35], în timp ce alți experți limitează acest articol la un simplu punct de vedere asupra „mediului operațional şi naturii războiului viitorului"[36], descins dintr-o cutumă specifică strategiei ruse[37], reclamând *„Doctrina Gherasimov"* care tentează comunitatea occidentală spre interpretări eronate[38].

Asocierea măsurilor militare cu cele non-militare pe parcursul tuturor stadiilor de

desfăşurare a conflictului şi utilizarea tehnologiei informațiilor în manipularea structurii statului şi a populației definesc formula conflictului evocată de Gherasimov. Concluziile trasate de către Gherasimov privind intervențiile militare occidentale în Africa de Nord şi Orientul Mijlociu şi caracterul dinamic al războiului sunt completate cu lecțiile învățate, sintetizate de către Andrew Korybko în lucrarea „Hybrid Wars: The Indirect Adaptive Approach to Regime Change" (2015) prin raportare la noțiunile de„revoluție colorată"[39] şi „război neconvențional". Analizarea strategiei altor actori prin prisma „lentilei ruse" îl determină pe A.Korybko să delimiteze ontologia războiului hibrid prin includerea exclusivă a metodelor specifice revoluțiilor colorate şi războaielor neconvenționale care conferă o fizionomie neliniară, indirectă, dinamică şi complexă. Trăsătura dialectică evidențiază formula socio-politică a războiului hibrid, al cărui pragmatism este instigat de operațiile psihologice extinse asupra unei societăți în scopuri politice.

Un model similar cu cel al războiului hibrid prezentat de Gherasimov a fostconturat de către S.G. Chekinov şi S.A. Bogdanov. Conform autorilor, *războiul de generație nouă*[40] reprezintă o combinație de metode şi mijloace nonviolente (politice, economice, informaționale, tehnologice şi ecologice) şi militare, în cadrul căreia prevalează importanța superiorității informaționale necesară obținerii succesului final. Tehnologiile informaționale facilitează accesul la o arie largă de opțiuni printre care mass-media, organizații religioase, instituții culturale, organizații neguvernamentale, mişcări publice finanțate din străinătate, persoane din mediul academic. Acțiunile de propagandă sunt stimulate de rețelele de socializare, Facebook şi Twitter, şi de utilizarea unor *războinici ai informației*[41] care conduc războiul informațional împotriva statului țintă.

Faza incipientă a războiului debutează cu inițiereaunuirăzboiinformațional,având cascopuri ascunderea intențiilor proprii, dezorientarea şi inducerea în eroare a adversarului. Războiul informațional presupune utilizarea canalelor diplomatice, a presei, scurgerea intenționată de informații false prin intermediul declarațiilor instituțiilor guvernamentale şi militare, atacuri cibernetice îndreptate împotriva sistemelor de comunicații şi propagandă. Aceasta din urmă vizează declanşarea nemulțumirii, diminuarea moralului şi accentuarea presiunii psihologice în rândul societății civile şi a forțelor armate pentru a dărâma bariera de rezistență a statului țintă. Ca metode de destabilizare a mediului social, autorii evocă utilizarea armelor biologice neletale pentru a accentua starea de haos la nivelul populației, manipularea (prin acțiuni de intimidare, înşelăciune şi mită) elitelor politice şi militare de a se sustrage de la îndeplinirea sarcinilor de serviciu, intensificând iritarea cetățenilor, plasarea de agenți sub acoperire care, prin acțiuni subversive, încurajează nemulțumirea populației, incită la violență şi la comiterea de fapte ilegale. Toate acestea vizează producerea de efecte psiho-cognitive negative asupra populației statului-țintă, prin amplificarea stării de anxietate, panică şi dezordine.

Modelul războiului conceput de către Chekinov şi Bogdanov prevede, pe lângă utilizarea instrumentelor specifice războiului informațional, şi alte metode non-militare care vizează izolarea statului prin impunerea de blocade, instigarea unităților armate de opoziție şi instaurarea unei zone de interdicțieaerianăasupra statului-țintă. Acesta continuă cu faza militară care debutează cu perioada premergătoare lansării atacului, în cadrul căruia statul agresor desfăşoară operații de informații, cu precădere acțiuni de spionaj, pentru a localiza obiectivele guvernamentale şi militare, vitale pentru sustenabilitateaținteiși operații specifice războiului electronic.

Eşafodajul războiului informațional care vizează cetățenii este constituit din ficțiuni, teorii ale conspirației, interpretări voit eronate, difuzate şi intensificate la nivelul populației pentru construirea unor emoții suficient de puternice cât să provoace reacții şi presiuni asupra autorităților. Efectele scontate sunt direcționate spre inocularea anumitor convingeri cetățenilor şi accentuarea nemulțumirii în rândul perdanților. Şansele de reuşită sunt amplificate de gradul de degradare al societății (nivelul scăzut de trai, tensiuni etnice,

religioase, antagonisme de valenţă axiologică) şi de încrederea redusă în instituţii (naţionale şi internaţionale), dar şi de modul subliminal de a conduce ofensiva, astfel încât populaţia ţintă să nu fie conştientă de acţiunile cu caracter psihologic ale atacatorului.

În conflictul din Ucraina, războiul informaţional s-a propagat în toate fazele acestuia (faza pregătitoare, atacul, faza de stabilizare strategică)[42], vizând deteriorarea tuturor elementelor de natură politică, economică şi socială, esenţiale în menţinerea stabilităţii statului. În perioada premergătoare operaţiei de atac, instrumentele specifice războiului informaţional sunt aplicate cu scopul de a câştiga avantajul strategic, iar pe parcursul ofensivei şi fazei destabilizare, pentru consolidarea rezultatelor.

Eforturile F.Rusedebutează cu identificarea vulnerabilităţilor din sistemul administrativ, economic, militar şi stabilirea reţelelor de propagare a acţiunilor de persuasiune. Caracterizată prin lipsa totală a oricărei forme de violenţă, faza pregătitoare se axează pe o campanie informativă asertivă orientată spre compromiterea politică şi socială a statului-ţintă, în scopul comprimării elementelor de rezistenţă prin lansarea de presiuni politice, influenţarea populaţiei şi instigarea mişcărilor separatiste, concomitent cu lansarea unor naraţiuni alternative avantajoase. Trasabilitatea războiului informaţional al Rusiei în Ucraina denotă propagarea unor naraţiuni referitoare la cel de-al Doilea Război Mondial, la Stepan Bandera şi naţionaliştii ucraineni, elogiind totodată perioada sovietică, în timp ce forţele de apărare ale Ucrainei erau comparate cu adepţi ai nazismului, fiind portretizate ca teroriste, criminale, sclave ale juntei de la Kiev[43].

Demonizarea autorităţilor ucrainene s-a realizat prin invadarea spaţiului mediatic cu informaţii false, decontextualizări, interpretări eronate, insinuări, exagerări, cu scopul de a le denigra credibilitatea şi de a suscita reacţii negative din partea populaţiei. Filmul conturat de poziţia oficială a Rusiei înfăţişa o Crimee persecutată de noua guvernare „ilegitimă”[44] şi „radicală”[45], „urmaşă ideologică”[46] a lui Bandera, activist politic cu o istorie complexă, evocat ca fiind „complicele lui Hitler în timpul celui de-al Doilea Război Mondial”[47]. Subminarea puterii de stat a continuat cu înfăţişarea Ucrainei ca stat eşuat, defăimarea autorităţilor de la Kiev ale căror acţiuni sângeroase erau îndreptate spre grupurile de minorităţi, cu precădere, cel rus. De asemenea, se avea în vedere accentuarea dependenţei Ucrainei de Rusia. Astfel, în declaraţia din 18 martie 2014, V. Putin susţinea că Ucraina era victima unei „lovituri de stat” condusă de „naţionalişti, neo-nazişti, rusofobi, şi antisemiţi”[48], accentuând legitimitatea acţiunii de anexare a Crimeei prin extrapolare la independenţa proclamată de Kosovo în anul 2008.

Prin infuzarea spaţiului public cu naraţiuni paralele, atât prin presa scrisă, cât şi prin alternativele create de era Internetului, Moscova viza crearea unei imagini de discreditare a guvernului şi a forţelor de ordine şi apărare, amplificând astfel sentimentele de teamă, confuzie şi revoltă în rândul populaţiei civile. Denigrarea instituţiilor ucrainene viza prezentarea unor naraţiuni de exacerbare a brutalităţii şi violenţei acestora, a incapacităţii de a oferi un răspuns viabil crizei, precum şi infamarea forţelor de apărare, inclusiv prin exploatarea statutului Bisericii Ortodoxe. Valorile creştine aduc un aport semnificativ gradului de influenţă al naraţiunilor plăsmuite de statul rus, fie că acestea sunt direcţionate spre estetizarea imaginii Rusiei, fie că vizează denigrarea statului ucrainean prin emiterea unor poveşti în care membri ai clerului Bisericii Ortodoxe Ucrainene sunt supuşi unui tratament de intimidare de către naţionalişti ucraineni[49].

Pe lângă discreditarea instituţiilor guvernamentale ale Ucrainei şi a forţelor sale de apărare, propaganda rusă a vizat şi denaturarea imaginii statelor occidentale prin difuzarea unor naraţiuni care susţineau prezenţa standardelor duble în politicile europene şi americane[50].

În contrast cu tonalitatea negativă atribuită statelor occidentale, Moscovaa vizat construirea unei reflexii proprii pozitive pe plan internaţional,

aderând la statutul de mare putere care are datoria morală să intervină în sprijinul minorității ruse supuse represaliilor Kievului, oferind în acelaşi timp compasiune față de ucraineni. Pe lângă edificarea imaginii Rusiei ca putere imperială, prosperă şi puternică, eforturile Moscovei erau îndreptate şi spre conceperea unor narațiuni de apoteozare a preşedintelui V. Putin şi de mascare a ambițiilor revizioniste sub reflexia conceptului „responsabilității de a proteja”[51].

Infuzia de realități paralele este susținută, în mare parte, prin intermediul fabricilor de troli, precum cea de la Sankt Petersburg[52], ale căror obiective vizează canalizarea ideilor şi credințelor populației țintă spre narațiuni dictate de către Kremlin şi validarea mesajelor de dezinformare şi manipulare. Penetrarea spațiului virtual cu adevăruri contrafăcute, intens vehiculate prin prezența trolilor în rețelele de socializare şi în secțiunile de comentarii ale diverselor site-uri de ştiri amplifică potențialul de verosimilitate al realităților alternative. Resursele Agenției de cercetare pe internet (*Internet Research Agency* -IRA) facilitează extinderea campaniei de dezinformare a Rusiei prin invadarea platformelor de Facebook, Twitter, Instagram sau YouTube cu troli şi conturi false care răspândesc informații *fake news,* discursuri instigatoare de ură, critici la adresa guvernelor pro-occidentale, elogieri ale preşedintelui V. Putin şi ale politicilor Federației Ruse.

Îmbinarea inovativă a propagandei cu acțiunile forțelor pentru operații speciale a facilitat concretizarea cu succes a operațiunii de dezinformare inițiate de Kremlin. Izolarea peninsulei Crimeea de liniile de comunicații ucrainene şi impunerea de către Moscova a dominației informaționale au generat premise favorabile pentru deturnarea percepției populației. Mai mult, campania de dezinformare a Moscovei a obstrucționat reliefarea unei imagini clare a evenimentelor de către comunitatea internațională, Uniunea Europeană aflându-se aproape un an[53] în imposibilitate de a formula o poziție oficială privind prezența trupelor ruseşti în Ucraina.

Spațiul virtual a facilitat atât campania de dezinformare a Rusiei, cât şi desfăşurarea acțiunilor de spionaj, sabotarea infrastructurii critice şi subminarea capacității cibernetice a statului prin acțiuni de interzicere a accesului cetățenilor la serviciile online (*Denial of Service* – DoS[54]) şi deteriorarea site-urilor web ale instituțiilor. Actele de vandalism care vizau rețelele digitale încă din perioada precedentă crizei ucrainene au crescut în intensitate odată cu amplificarea turbulențelor politice. Încă de la sfârşitul anului 2012, concomitent cu sporirea atacurilor de tip DDoS (Distributed Denial of Service[55]), s-au intensificat şi acțiunile de spionaj cibernetic şi activismul politic, transpus în spargerea rețelelor aferente spațiului guvernamental. Odată cu debutul crizei, războiul psihologic condus prin intermediul platformelor digitale a încorporat noi valențe prin complexitatea atacurilor cibernetice. Tentativelor de perturbare a proceselor politice din rândul cărora se profilează atacul asupra sistemului informatic al Comisiei Electorale Centrale, care s-a soldat cu periclitarea procesării şi transmiterii rezultatelor alegerilor prezidențiale[56] din mai 2014, li se adaugă scurgerea de documente, poze, videoclipuri şi convorbiri telefonice în spațiul virtual, lansate de către utilizatori anonimi sau grupuri de hackeri, precum Cyberberkut, pentru a întreține narațiunea Moscoveişi a submina autoritățile ucrainene şi occidentale.

Utilizarea armelor digitale împotriva autorităților de la Kiev şi infectarea sistemelor informatice cu programe malițioase de tipul Snake[57] deschid oportunități noi pentru operațiunile de supraveghere ale agresorilor, pentru câştigarea şi consolidarea avantajului strategic. Asemănător predecesorului său, Agent. BTZ, cu care împărtăşeşte anumite similitudini[58], arhitectura Snake trădează indicii care au determinat specialişti în domeniu să includă Rusia în lista de suspecți.[59]

Cu toate acestea, reacțiile comunității occidentale, generate de amploarea conflictului din Ucraina, s-au concretizat în numeroase studii de specialitate[60] care argumentează consecvența îndelungată a tacticilor Kremlinului în desfăşurarea conflictului, a cărui noutate este determinată de coordonarea intensă a instrumentelor utilizate, facilitată, la rândul ei, de dezvoltarea tehnologică.

3. Concluzii

În încercarea de a delimita profilurile precise ale războiului, ştiinţele militare sunt asaltate cu aspecte veleitare în reflectarea unei formule concrete, specifice războiului hibrid. Rolul şi locul termenului „hibrid", asociat războiului, denotă o plajă largă de interpretări şi adaptări ale conceptului şi care completează literatura în domeniu. Războiul hibrid este şi asimetric şi neconvenţional şi neregulat, înglobând actori, mijloace şi metode tradiţionale şi netradiţionale ale căror proporţii se află într-o permanentă dezvoltare. În acest sens, strategiile de securitate necesită o redefinire continuă pentru a se adapta la fluctuaţiile din mediul internaţional care amplifică nivelul de complexitate al ameninţărilor.

În literatura de specialitate, dar şi în documente oficiale, noţiunile de *război hibrid* şi *ameninţări* hibride au fost în permanenţă adaptate la evenimentele externe, urmând traiectoria trasată de efectele pernicioase ale globalizării. Cu toate acestea, eforturile eşuate ale specialiştilor în domeniu de a previziona forme veritabile ale războaielor viitorului au obstrucţionat construirea unui model disciplinar adecvat, teoria rămânând mereu în urma practicii.

Caracterul complex şi imprevizibil al provocărilor este determinat de ameninţări teroriste, atacuri cibernetice, proliferare a armelor nucleare şi a armelor de distrugere în masă, tehnologia avansată în domeniul balistic, precum şi de acţiunile subversive ale actorilor de periclitare a valorilor democratice şi a statului de drept. Evaluarea privind acţiunile Rusiei evidenţiază un comportament agresiv al actorului rus care subminează arhitectura securităţii internaţionale, compromite ordinea mondială şi alterează stabilitatea euro-atlantică, prin extinderea spectrului de ameninţări. Rusia este dispusă să îşi utilizeze întreg arsenalul de mijloace şi metode convenţionale şi neconvenţionale (acţiuni subversive, forţa militară) pentru atingerea obiectivelor sale de politică externă. Acţiunile Rusiei de destabilizare a mediului de securitate euro-atlantic vizează atât o direcţie de manifestare a puterii militare, cât şi o strategie disimulată de violare a normelor de securitate internaţionale şi acţiuni subversive. Astfel, anexarea ilegală şi ilegitimă a Crimeii şi continua militarizare a acesteia, destabilizarea din estul Ucrainei, dislocarea de rachete moderne în Kaliningrad, violările spaţiului aerian aliat, modernizarea forţelor sale strategice, desfăşurarea unui număr progresiv de exerciţii militare ample sunt completate cu interferări în procesele electorale, campanii de dezinformare, atacuri cibernetice şi atacuri cu agenţi neurotoxici.

În pofida faptului că modelul teoretic actual al războiului hibrid încorporează întregul arsenal cunoscut şi aplicat de către Rusia în criza ucraineană, trebuie avută în vedere capacitatea Moscovei de adaptare şi surprindere strategică, astfel încât conceptul fragil al războiului hibrid să îşi consolideze utilitatea.

Bibliografie

1. RACZ, Andras, *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist,* Report 43, Finnish Institute of International Affairs, Helsinki, Finland;
2. COHEN, Ariel, *Knowing the Enemy*, 2007, disponibil la https://www.hoover.org/research/knowing-enemy;
3. BOWERS, Christopher O., *Identifying Emerging Hybrid Adversaries,* disponibil la https://ssi.armywarcollege.edu/pubs/parameters/articles/2012spring/Bowers.pdf;
4. SADOWSKI, David, Jeff Becker, *Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare,* disponibil la http://smallwarsjournal.com/jrnl/art/beyond-the-hybrid-threat-asserting-the-essential-unity-of-warfare;
5. European Commission, *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union Response*, Brussels, 06.04.2016, disponibil la https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52016jc0018;
6. HOFFMAN, Frank G., *Conflict in the 21st Century. The Rise of Hybrid Wars,* Potomac Institute for Policy Studies, Arlington, Virgina, decembrie 2007;
7. HOFFMAN, Frank, *On Not-So-New Warfare: Political Warfare vs. Hybrid Threats,* 28.07.2014,

disponibil la https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/;

8. CILLUFFO, Frank J., Joseph R. CLARK, *Thinking About Strategic Hybrid Threats—In Theory and in Practice*, disponibil la http://www.dtic.mil/dtic/tr/fulltext/u2/1042759.pdf;
9. BOND, Margaret S., *Hybrid War: A New Paradigm for Stability Operations in Failing States,* disponibil la http://www.worldinwar.eu/wp-content/uploads/2017/09/ADA468398-1.pdf;
10. COHEN, Michael, *Putin's Dangerous Proxy War*, 17.07.2014, disponibil la https://www.politico.com/magazine/story/2014/07/vladimir-putin-russia-proxy-war-ukraine-crimea-109074;
11. POMERANTSEV, Peter, *How Putin Is Reinventing Warfare*, 05.05.2014, disponibil la https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/;
12. MANSOOR, Peter R., *Introduction. Hybrid Warfare in History* în Wiliamson Murray (ed.), *Hybrid Warfare. Fighting Complex Opponents from the Ancient World tothe Present,* Cambridge University Press, 2012;
13. GLENN, Russel, *Thoughts on "Hybrid" Conflict,* Small Wall Journal, disponibil la http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf;
14. United States Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for*
15. GHERASIMOV, Valery, *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,* în Military Review, ianuarie-februarie 2016;
16. MURRAY, Wiliamson (ed.), *Hybrid Warfare. Fighting Complex Opponents from the Ancient World tothe Present,* Cambridge University Press, 2012.

---

[1] Vezi *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy,* iunie 2016; *National Security Strategy of the United States of America,* decembrie 2017;Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, 10.09.2012.

[2] William J. Nemeth, *Future War and Chechnya: a Case for Hybrid Warfare*, iunie 2002, disponibil la https://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1&isAllowed=y, accesat în data de 10.02.2019

[3] Frank G. Hoffman, *Conflict in the 21st Century. The Rise of Hybrid Wars,* Potomac Institute for Policy Studies, Arlington, Virgina, decembrie 2007, p. 30.

[4] În articolul „*The Changing Face of War: Into the Fourth Generation*" (1989) autorii divid evoluția războiului modern în trei generații specifice. Urmând traiectoria trasată de evoluția ideilor şi a tehnologiei, autorii au generat un nou model al războiului (războiul de generația a patra) care se dispersează în toate domeniile vieții, heteromorfic, descentralizat, cu actori statali şi nestatali ale căror arsenale metodice includ terorismul, criminalitatea transnațională, războiul psihologic şi care are ca scop devastarea fizică şi culturală a inamicului.

[5] Expresie care definește strategii adoptate de către actori aflați în dezavantaj politic şi militar pentru a câştiga inițiativa strategică în războiul cu marile puteri. Conceptul de „război nerestricționat" a debutat în literatura de specialitate odată cu publicarea cărții „*Unrestricted Warfare*" (1999) prin care autorii, col. Qiao Liang şi col. Wang Xiangsui, evidențiază ca trăsătură pregnantă a războiului viitorului dispersia limitei dintre acțiunile militare şi cele nonmilitare, în contextul evoluției tehnologice, a omniprezenței informației şi ubicuității câmpului de luptă.

[6] Sintagmade *război compus* a fost introdus în literatura de specialitate de către Thomas M. Huber, în articolul „*Napoleon in Spain*" (1996) pentru a descrie lupta armată dusă de forțe regulate şi neregulate care acționează sub aceeaşi comandă. În primul capitol al lucrării „*Compound Warfare. That Fatal Knot*" (2002), Thomas M. Huber prezintă un cadru conceptual al războiului compus cu avantaje care decurg din complementaritatea forțelor precum impunerea unei presiuni accentuate asupra inamicului, uzarea forțelor adversare concomitent cu augmentarea capacităților proprii.

[7] În *Conflict in the 21st Century. The Rise of Hybrid Wars*, autorul completează formula războiului hibrid prin adoptarea unor elemente enunțate de cercetători australieni în lucrarea conceptuală a armatei australiene, *Complex Warfighting (*Future Land Warfare Branch, 2004).

[8] Frank G. Hoffman, *Op.Cit.*

[9] Thomas Huber în Brian P. Fleming, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art: a Monograph*, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 2011, disponibil la http://indianstrategicknowledgeonline.com/web/2753.pdf, accesat în data de 05.02.2019; Peter R. Mansoor, *Introduction. Hybrid Warfare in History* în Wiliamson

Murray (ed.), *Hybrid Warfare. Fighting Complex Opponents from the Ancient World tothe Present,* Cambridge University Press, 2012; Frank J. Cilluffo, Joseph R. Clark, *Thinking About Strategic Hybrid Threats—In Theory and in Practice*, disponibil la http://www.dtic.mil/dtic/tr/fulltext/u2/1042759.pdf, accesat în data de 05.02.2019.

[10] David Sadowski, Jeff Becker, *Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare,* disponibil la http://smallwarsjournal.com/jrnl/art/beyond-the-hybrid-threat-asserting-the-essential-unity-of-warfare, accesat în data de 15.02.2019; Christopher O. Bowers, *Identifying Emerging Hybrid Adversaries,* disponibil la https://ssi.armywarcollege.edu/pubs/parameters/articles/2012spring/Bowers.pdf, accesat în data de 15.02.2019.

[11] Christopher O. Bowers, *Op.Cit.*

[12] Margaret S. Bond, *Hybrid War: A New Paradigm for Stability Operations in Failing States,* disponibil la http://www.worldinwar.eu/wp-content/uploads/2017/09/ADA468398-1.pdf, accesat în data de 20.01.2019.

[13] Vezi John J. McCuen, *Hybrid Wars,* în Military Review. Mar/Apr 2008, Vol. 88 Issue 2, 107-113.

[14] Russel Glenn, *Thoughts on "Hybrid" Conflict,* Small Wall Journal, disponibil la http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf, accesat în data de 10.02.2019.

[15] Department of the Army, *ADP 3-0, Unified Land Operations*, octombrie 2011, disponibil la https://www.globalsecurity.org/military/library/policy/army/adp/3-0/adp3_0.pdf, accesat în data de 10.02.2019.

[16] Peter R. Mansoor, *Introduction. Hybrid Warfare in History* în Wiliamson Murray (ed.), *Hybrid Warfare. Fighting Complex Opponents from the Ancient World tothe Present,* Cambridge University Press, 2012.

[17] Wiliamson Murray (ed.), *Hybrid Warfare. Fighting Complex Opponents from the Ancient World tothe Present,* Cambridge University Press, 2012, p. 293.

[18] Ariel Cohen, *Knowing the Enemy*, 2007, disponibil la https://www.hoover.org/research/knowing-enemy, accesat în data de 10.02.2019.

[19] "*Special War" Goes Mainstream*, 21.04.2014, disponibil la https://20committee.com/2014/04/21/special-war-goes-mainstream/, accesat în data de 02.03.2019.

[20] Peter Pomerantsev*, How Putin Is Reinventing Warfare*, 05.05.2014, disponibil la https://foreignpolicy.com /2014/05/05/how-putin-is-reinventing-warfare/, accesat în data de 10.02.2019

[21] Michael Cohen, *Putin's Dangerous Proxy War*, 17.07.2014, disponibil la https://www.politico.com/ magazine/story/2014/07/vladimir-putin-russia-proxy-war-ukraine-crimea-109074, accesat în data de 02.03.2019.

[22] Sofya Kornienko, Пиджакрветсяпошву, 26.04.2014, disponibil la https://www.svoboda.org/a/25362031.html, accesat în data de 02.03.2019.

[23] Andras Racz, *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist,* Report 43, Finnish Institute of International Affairs, Helsinki, Finland.

[24] Frank Hoffman, *On Not-So-New Warfare: Political Warfare vs. Hybrid Threats,* 28.07.2014, disponibil la https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/, accesat în data de 02.03.2019.

[25] Peter Pindják, *Deterring hybrid warfare: a chance for NATO and the EU to work together?,* 18.11.2014,NATO Review, disponibil la https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm, accesat în data de 02.03.2019.

[26] United States Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for*
U.S. National Security, 10.01.2018, disponibil la http://www.gpoaccess.gov/congress/index.html, accesat în data de 02.03.2019.

[27] Idem.

[28] Vira Ratsiborynska, *When Hybrid Warfare Supports Ideology: Russia Today*, Research Paper, Research Division of the NATO Defense College, Nr. 133, noiembrie, 2016.

[29] United States Senate, *Ibidem.*

[30] *Concept for the NATO Military Contribution to Countering Hybrid Threats*, 25.08.2010, disponibil la Concept for the NATO Military Contribution to Countering Hybrid Threats, accesat în data de 02.03.2019.

[31] European Commission, *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union Response*, Brussels, 06.04.2016, disponibil la https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52016jc0018, accesat în data de 05.03.2019.

[32] The European Centre of Excellence for Countering Hybrid Threats, *Countering Hybrid Threats*, disponibil la https://www.hybridcoe.fi/hybrid-threats/, accesat în data de 05.03.2019.

[33] Valery Gherasimov, *The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,* în Military Review, ianuarie-februarie 2016, pp. 21-29.

[34] *James D.J. Brown, Japan woos Russia for its own security*, 11.12.2017, disponibil la https://asia.nikkei.com/Viewpoints/James-D.J.-Brown/Japan-woos-Russia-for-its-own-security, accesat în data de 10.03.2019.

[35] Molly K. McKew, *The Gherasimov Doctrine,* septembrie-octombrie 2017, disponibil la https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538, accesat în data de 26.02.2019.

[36] Charles K. Bartles, *Getting Gerasimov Right*, în Military Review, ianuarie-februarie 2016, pp. 30-38.

[37] Mark Galeotti, *The 'Gerasimov Doctrine' and Russian Non-LinearWar*, 06.07.2014, disponibil la https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, accesat în data de

10.03.2019. Vezi şi Mark Galeotti, *I'm Sorry for Creating the 'Gerasimov Doctrine*, 05.03.2018, disponibil la https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/, accesat în data de 10.03.2019.

[38] Keir Giles, Russia's *'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power,* Research Paper, Chatham House, martie 2016,p.11.

[39] Andrew Korybko, *Hybrid Wars: the Indirect Adaptive Approach to Regime Change*, People's Friendship University of Russia, Moscow, 2015.

[40] *Ibidem.*

[41] *Ibidem.*

[42] Vezi Andras Racz, *Op.cit.*

[43] Vezi Vladimir Sazonov, Kristiina Müür, Holger Mölder (ed.), *Russian Information Campaign Against the Ukrainian State and Defence Force. Combined Analysis*, NATO Strategic Communications Centre of Excellence Estonian National Defence College Tartu, 2016, disponibil la https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf, accesat în data de 12.03.2019.

[44] Address byPresident oftheRussian Federation, Kremlin, Moscova, 18.03.2014, disponibil la http://en.kremlin.ru/ events/president/news/20603, accesat în data de 14.02.2019.

[45] *Ibidem.*

[46] *Ibidem.*

[47] *Ibidem.*

[48] *Ibidem.*

[49] АНАСТАСИЯ НОВИКОВА, Украинские националисты планируют карательную акцию против священников, 14.10.2014, disponibil la https://www.kompravda.eu/daily/26294/3172487/, accesat în data de 15.02.2019.

[50] ОЛЬГА ТУХАНИНА, Почему Запад вступается за Пусси Райот, а не за мертвых девочек из Луганска, 24.08.2014, disponibil la https://www.kompravda.eu/daily/26273.7/3150573/, accesat în data de 12.02.2019.

[51] *Russia reserves right to protect compatriots in Ukraine,* 14.02.2014, disponibil la https://www.reuters.com/article/us-urkaine-crisis-russia-east-idUSBREA2D0M620140314, accesat în data de 12.02.2019.

[52] Keir Giles, *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power,* Research Paper, Chatham House, martie 2016,p. 45.

[53] *Ibidem.*

[54] Cristea Marius Simion, *Atacuri DoS: Taxonomie, Prevenţie, Consecinte şi Atacuri mixte*, Referat 1, 2011, disponibil la http://www.aut.upt.ro/~marius-simion.cristea/pdf/report1.pdf, accesat în data de 26.02.2019.

[55] Cristea Marius Simion, *Idem*.

[56] International Election Observation Mission, *Statement of Preliminary Findings and Conclusions*, Kiev, 26.05.2014, disponibil la https://www.osce.org/odihr/elections/ukraine/119078?download=true, accesat în data de 26.02.2019.

[57] Sam Jones, *Cyber Snake plagues Ukraine networks*, 07.03.2014, disponibil la https://www.ft.com/ content/615c29ba-a614-11e3-8a2a-00144feab7de, accesat în data de 28.02.2019.

[58] BAE Systems, *The Snake Campaign. Cyber Espionage Toolkit*, disponibil la https://www.baesystems.com /en/cybersecurity/feature/the-snake-campaign, accesat în data de 28.02.2019.

[59] Maik Baumgärtner, Matthias Gebauer, Martin Knobbe*, Behörden vermuten russische Hackergruppe "Snake" als Täter*, 01.03.2018, disponibil la http://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-behoerden-vermuten-russische-hacker-gruppe-snake-als-taeter-a-1196089.html; Julian Röpcke**,** "*Snake" is affiliated with Russia's FSB,* 02.03.2018, disponibil la https://www.bild.de/politik/inland/bild-international/cyber-attack-on-germany-54980786.bild.html, accesat în data de 02.03.2019.

[60] Vezi Merle Maigre, *Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO*, 12.02.2015, disponibil la http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato şi Nicu Popescu, *Hybrid tactics: neither new nor only Russian*, 4/2015, disponibil la https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf, accesate în data de 10.03.2019.

RĂZBOI ELECTRONIC – TENDINȚE ŞI PERSPECTIVE

Daniel CHIRIȚĂ
*Dorin CÎRJAN**

Abstract

This article addresses the concept of electromagnetic environment as an operational environment and the role the electronic warfare with its components plays in it. In the end, we present some of the conceptual, technological and operational developments that have the potential to shape the way the electronic warfare is employed in the future military operations. These include concepts like cognitive electronic warfare, collaborative electronic warfare, cyber - electronic warfare integration; technologies like active electronically scanned array antennas, GalliumNitride based monolithic microwave integrated circuits, high energy lasers, solutions against hypersonic missiles and challenges posed by passive radars in suppression of enemy air defenses scenarios.

Keywords: *electronic warfare, electromagnetic environment, electromagnetic spectrum, cognitive electronic warfare.*

1. Mediul electromagnetic

În prezent, lupta armată este caracterizată prin manevrabilitate, dinamism, culegerea şi transmiterea datelor şi informațiilor în timp real sau aproape real, avertizare şi reacție imediată la amenințări sau prin precizie în lovirea țintelor la momentul oportun şi în orice condiții de timp şi stare a vremii. Conflictele militare din ultimii ani au demonstrat că în cadrul operațiilor moderne se produce o deplasare a efortului către confruntarea pe suportul undelor electromagnetice.

Forțele armate moderne şi operațiile pe care acestea le desfăşoară sunt dependente de mediul electromagnetic, acțiunile militare desfăşurându-se în contextul unor cerințe din ce în ce mai numeroase şi complexe privind utilizarea acestui mediu operațional. Toate acestea sunt posibile datorită avansului tehnologic înregistrat şi în domeniul militar, deci a omniprezenței echipamentelor electronice în compunerea armamentului individual, sistemelor de armament şi vectorilor purtători de încărcături de distrugere, sistemelor de comunicații, radarelor şi platformelor militare.

Dezvoltarea considerabilă a mijloacelor militare a căror funcționare nu este posibilă fără utilizarea energiei electromagnetice şi creşterea dependenței acțiunilor militare de aceste mijloace de ultimă generație au creat premisele apariției unui nou mediu operațional şi anume *mediul electromagnetic/(ElectromagneticEnvironment - EME)*. Acest mediu operațional este scena unor intense confruntări desfăşurate în scopul de a asigura controlul acestuia, devenind un domeniu operațional critic la toate nivelurile de ducere a luptei – tactic, operativ şi strategic.

Controlul mediului electromagnetic constituie unul dintre elementele cheie de care depinde supraviețuirea sau victoria într-o confruntare armată. Pentru a avea succes pe câmpul de luptă al viitorului, devine imperativ pentru forțele armate să utilizeze eficient mediul

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

electromagnetic, concomitent cu împiedicarea exploatării sau reducerea utilizării acestuia de către adversar. Operațiile militare sunt executate cu dificultate din cauza existenței unui mediu electromagnetic din ce în ce mai aglomerat şi complex.Necesitatea accesului la/şi utilizareamediului electromagnetic de către forțele militare creează atât vulnerabilități, cât şi oportunități din punct de vedere al războiului electronic în operațiile militare.

Experiența ultimelor conflicte a impus teza conform căreia, în condiții de relativă egalitate a forțelor şi mijloacelor dintre doi adversari, cel care are capacități informaționale şi de control al mediului electromagnetic superioare, *aici intrând şi războiul electronic*, are mai multe şanse să îşi adjudece victoria.

2. Aspecte privind acțiunile de război electronic

Succesul în mediul electromagnetic este deseori un precursor al succesului în celelalte medii operaționale, acest lucru fiind suficient pentru obținerea unui anumit efect. Conform modului general de executare a operațiilor militare, desfăşurarea operațiilor de război electronic începe prin înțelegerea obiectivelor militare şi analizarea efectelor dorite. Din punct de vedere al abordării operației bazate pe efecte, mediul electromagnetic poate fi exploatat, modelat şi folosit pentru atac şi/sau apărare, ca şi celelalte medii operaționale.

Dominația mediului electromagnetic este o componentă crucială a majorității operațiilor militare moderne bazate pe folosirea intensă a sistemelor informatice, de comunicații şi electronice, în general. Dacă aceste sisteme sunt deteriorate sau distruse, un comandant nu poate realiza un act de comandă eficient, fiind, metaforic spus, „orb, surd şi mut”.

Războiul electronic reprezintă o componentă de bază a operațiilor electromagnetice care asigură mijloacele necesare modelării mediului electromagnetic în sprijinul forțelor proprii, simultan cu îngreunarea sau interzicerea folosirii acestuia de către adversar.În literatura de specialitate, războiul electronic este definit ca acțiunea militară desfăşurată în scopul cunoaşterii situației şi obținerii de efecte ofensive şi defensive pe baza exploatării energiei electromagnetice.

Executarea cu succes a acțiunilor de război electronic de către forțele proprii depinde de utilizarea eficientă a mediului electromagnetic în scopul exploatării, împiedicării sau reducerii capacității adversarului de a opera în acest mediu. Aceasta se realizează prin managementul spațiului de luptă al operației electromagnetice cu acțiuni ce presupun:

- utilizarea senzorilor de război electronic, în scopul cunoaşterii situației din mediul electromagnetic;
- deconflictizarea operațiilor electromagnetice proprii în timp, spațiu şi spectrul electromagnetic cu cele executate de adversar şi de actori neutri, în scopul reducerii influenței interferențelor electromagnetice;
- coordonarea acțiunilor de război electronic cu ceilalți utilizatori ai mediului electromagnetic, în scopul reducerii interferențelor electromagnetice;
- stabilirea acțiunilor de război electronic care să reducă vulnerabilitățile electromagnetice ale platformelor, sistemelor şi legăturilor de date;
- executarea acțiunilor de război electronic în scopul influențării negative a capacității adversarului de a utiliza mediul electromagnetic în sprijinul operațiilor;
- analiza efectelor mediului geofizic (terestru, aerian/spațial, maritim) care pot limita sau intensifica efectul operațiilor electromagnetice;
- analiza limitărilor şi luarea în considerare a posibilității operării într-un mediu electromagnetic disputat şi aglomerat.

În definirea şi selectarea cursurilor de acțiune şi a concepțiilor operațiilor este necesar să se înțeleagă modul de aplicare al următoarelor principii de război electronic:

- utilizarea capabilităților de război electronic poate produce efecte la toate nivelurile operației, de la cel tactic până la strategic;

- războiul electronic este utilizat pentru a modela mediul electromagnetic, a facilita cunoaşterea situaţiei, a contribui la managementul operaţiilor electromagnetice, protecţia forţelor proprii şi atacarea adversarului;
- războiul electronic trebuie să fie luat în calcul în toate tipurile şi fazele operaţiilor;
- coordonarea războiului electronic la nivelul spaţiului de luptă modern este vitală pentru a asigura eficacitatea şi eficienţa utilizării capabilităţilor de luptă ale acestuia;
- războiul electronic pune la dispoziţia comandanţilor o varietate de posibilităţi de acţiune în mediul electromagnetic, care produc efecteletale şi non-letale pe tot parcursul conflictului;
- manevra în mediul electromagnetic este asemănătoare manevrei în alte medii operaţionale (geofizice, cibernetic şi informaţional);
- operaţiile de război electronic trebuie să fie planificate centralizat, pentru a asigura unitatea de efort;
- în orice operaţie, execuţia operaţiilor de război electronic trebuie delegată celui mai mic eşalon;
- operaţiile de război electronic vor fi inevitabil influenţate de mediile geofizice.

Accentul pe război electronic înainte, pe timpul şi după conflict, în toată gama de operaţii militare, este esenţial, acesta contribuind la:

- executarea operaţiilor întrunite de informaţii, supraveghere şi cercetare;
- executarea manevrei în mediul electromagnetic, în scopul asigurării protecţiei, exploatării şi atacării sistemelor de comandă-control şi a altor sisteme electronice;
- asigurarea protecţiei zonei, forţei, sistemelor şi platformelor;
- executarea operaţiilor defensive, inclusiv în apărarea împotriva rachetelor anti-navă,lupta contra rachetelor, proiectilelor de artilerie, mortierelor, rachetelor anti-aeriene portabile şi avioanelor fără pilot;
- contracararea ameninţărilor hibride;
- desfăşurarea operaţiilor împotriva terorismului, inclusiv împotriva dispozitivelor explozive comandate prin radio;
- desfăşurarea operaţiilor ofensive, inclusiv suprimarea apărării aeriene inamice, operaţiilor de lovire şi manevrelor tactice terestre, aeriene şi navale;
- reducerea sau interzicerea utilizării eficiente a mediului electromagnetic de către adversar;
- limitarea libertăţii de mişcarea adversarului în utilizarea sistemelor principale de luptă şi determinarea acestuia să recurgă la utilizarea unor sisteme mai puţin performante sau mai uşor de exploatat de către forţele proprii;
- desfăşurarea operaţiilor cibernetice prin controlul, modelarea şi obţinerea de efecte prin intermediul spectrului electromagnetic, element cheie al nivelului fizic al spaţiului cibernetic.

Acţiunile de război electronic (*supravegherea electronică/Electronic Surveillance - ES, atacul electronic/ElectronicAttack -EA şi apărarea electronică/Electronic Defence -ED)*, vârful de lance al operaţiilor electromagnetice, asigură mijloacele necesare intensificării cunoaşterii situaţiei în mediul electromagnetic şi obţinerii efectelor, ofensive şi/sau defensive, stabilite în procesul de planificare al oricărui tip de operaţie militară.

Aceste acţiuni, desfăşurate individual sau împreună cu acţiunile specifice altor specialităţi militare, sunt aplicate la nivel tactic şi produc asupra ţintelor din mediul electromagnetic un spectru larg de efecte non-cinetice şi/sau cinetice în orice tip de operaţie militară.

Într-un scenariu intell/ISR, războiul electronic, prin desfăşurarea de acţiuni de supraveghere electronică,obţine informaţii din detecţia energiei electromagnetice şi măsurarea parametrilor undelor electromagnetice în scopul cunoaşterii situaţiei şi culegerii de informaţii. Cunoaşterea situaţiei[1] este termenul general folosit atunci când un factor de decizie, de la

orice nivel ierarhic, cunoaşte suficiente date şi informaţii dintr-un mediu operaţional pentru a lua decizii şi a desfăşura acţiuni în cunoştinţă de cauză. Astfel, acţiunile de supraveghere electronică sprijină procesul decizional la toate nivelurile ierarhice de comandă, avantajele acestora cuprinzând:

- existenţa opţiunilor de utilizare activă/ pasivă, respectiv ascunsă/la vedere a senzorilor, în scenarii specifice stării de pace, în situaţii de criză sau în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război;
- creşterea relevanţei bazelor de date de război electronic, necesare pentru desfăşurarea operaţiilor de război electronic;
- asigurarea capacităţii de monitorizare a mediului electromagnetic în zona de interes, zi şi noapte, în orice condiţii de stare a vremii, utilizând o capabilitate de nivel tactic de culegere a informaţiilor;
- identificarea, caracterizarea şi localizarea emiţătoarelor;
- achiziţia datelor necesare avertizării automate şi imediate privind ameninţările din mediul electromagnetic.

Supravegherea electronică este separată, dar strâns legată de domeniul SIGINT. Diferenţa o reprezintă scopul utilizării datelor şi informaţiilor obţinute. Datele obţinute prin supraveghere electronică sunt utilizate, în principal, în scop tactic, pentru recunoaşterea ameninţărilor, în procesul de targeting şi pentru obţinerea de informaţii din detecţiile şi măsurătorile emisiilor electromagnetice obţinute dintr-o zonă de interes. De cele mai multe ori, acţiunile de supraveghere electronică şi acţiunile SIGINT pot utiliza echipamente şi resurse comparabile sau identice şi pot primi sarcini de a culege, simultan, informaţii ce îndeplinesc cerinţele operaţionale specifice ambelor domenii. Senzorii de supraveghere electronică pot suplimenta senzorii dedicaţi de informaţii, supraveghere şi cercetare (ISR). Integrarea procesului de planificare a capabilităţilor şi activităţilor de supraveghere electronică în procesul JISR poate aduce următoarele beneficii:

- asigurarea informaţiilor necesare descoperirii, identificării, urmăririi, achiziţiei, angajării, exploatării şi evaluării ţintelor;
- asigurarea răspunsului la un număr crescut de cerinţe de informaţii;
- sprijinul procesului de pregătire informativă a mediului operaţional;
- asigurarea informaţiilor necesare planificării şi desfăşurării acţiunilor de atac electronic în scopul angajării precise a ţintelor sau sprijinirii unei apărări electronice eficiente;
- localizarea ţintelor, în sprijinul acţiunilor de atac electronic, şi identificarea legăturilor de comunicaţii a lanţului C2 pentru sistemele de lovire;
- sprijinul acţiunilor de suprimare a apărării aeriene a inamicului (SEAD2);
- asigurarea, în baza unor indicii specifici, de avertizări cu privire la ameninţările imediate şi intenţiile adversarului;
- realizarea „Imaginii recunoscute din mediul electromagnetic”/REMP[3], componentă a „Imaginii operaţionale comune”/COP[4], care asigură o cunoaştere permanentă a situaţiei operaţionale;
- furnizarea datelor necesare exploatării şi evaluării efectelor la ţintă/BDA[5] asupra sistemelor/echipamentelor electronice vizate;
- evaluări/măsurări suplimentare ale parametrilor undelor electromagnetice, în scopul suplimentării mijloacelor ISR;
- măsurarea gradului de ocupare a spectrului, în scopul reducerii interferenţelor.

Războiul electronic, prin acţiunile de atac electronic/EA, utilizează energia electromagnetică în scopuri ofensive. Atacul electronic utilizează capabilităţi care pot limita sau neutraliza capacitatea adversarului de a opera în mediul electromagnetic. În general, atacul electronic nu se execută în mod izolat, acesta fiind integrat atât cu alte acţiuni de luptă, cât şi cu celelalte acţiuni de război electronic, respectiv supravegherea electronică şi apărarea electronică.

Pentru asigurarea unei eficienţe maxime, atacul electronic se execută numai după înţelegerea modului de utilizare a mediului electromagnetic de către adversar, acesta putând fi utilizat în scopul reducerii, întreruperii, dezinformării, distrugerii sau interzicerii capacităţii adversarului de a executa operaţii electromagnetice, atacării sistemului de comandă-control, împiedicării misiunii senzorilor de informaţii, supraveghere şi cercetare, afectării sistemelor de calculatoare, distrugerii echipamentelor electronice şi diminuării oportunităţilor adversarului de a modela şi exploata mediul operaţional.Există trei moduri tipice de utilizare a atacului electronic, respectiv *bruiajul electronic, dezinformarea electronică* şi *neutralizarea electronică.*

Sistemele de bruiaj electronic includ *sisteme de bruiaj electronic de comunicaţii*, *sisteme de electronic de non-comunicaţii* (radare, sisteme de poziţionare, navigaţie şi sincronizare etc.) şi *sisteme de bruiaj opto-electronic/în infraroşu*.

Sistemele de neutralizare electronică includ a*rme cu microunde de putere mare /High Power Microwave – HPM*, *arme cu laseri de energie înaltă/High Energy Laser – HEL* şi *arme cu fascicul de particule*.

Apărarea electronică, ca acţiune de război electronic,implică folosirea energiei electromagnetice în scopul asigurării protecţiei forţelor proprii şi utilizării eficiente a spectrului electromagnetic de către acestea. Capabilităţile de neutralizare, bruiaj şi dezinformare electronică nu sunt destinate doar scopurilor ofensive asociate atacului electronic, ci şi creării de efecte defensive.Apărarea electronică este organizată pentru a asigura protecţia forţelor, a platformelor, a sistemelor electronice şi a zonelor, de regulă împreună cu alte capabilităţi de luptă. Câteva exemple tipice de acţiuni pentru realizarea apărării electronice în scopul protecţiei forţelor proprii includ:

- împiedicarea detonării dispozitivelor explozive comandate prin radio;
- întreruperea legăturilor de comandă-control utilizate la dirijarea muniţiilor, în scopul reducerii preciziei şi eficienţei acestora;
- saturarea senzorilor de achiziţie/targeting care utilizează spectrul radio, infraroşu şi laser, în scopul ratării ţintei de către armele pe care aceştia le dirijează;
- utilizarea capabilităţilor de dezinformare electronică, precum capcanele tractate şi dipolii pasivi, în scopul asigurării protecţiei platformelor şi personalului;
- transmiterea de ţinte false în receptoarele sistemelor radar, în scopul întreruperii urmăririi ţintei reale;
- utilizarea laserelor la orbirea senzorilor opto-electronici, în scopul limitării/ interzicerii cunoaşterii situaţiei de către adversar.

În timp ce atacul electronic este o acţiune specifică de război electronic, apărarea electronică este o responsabilitate atât a războiului electronic, cât şi a tuturor specialităţilor militare, protecţia platformelor de luptă ale forţelor terestre, aeriene şi navale bazându-se pe echipamente de autoprotecţie necesare pentru a contracara ameninţările din mediul electromagnetic reprezentate de armamentul dirijat prin radar, infraroşu sau laser al adversarului.

3.Tendinţe şi perspective ale războiului electronic

Dinamica evoluţiei tehnologice a determinat, în ultimele decenii, mutaţii majore în toate domeniile activităţii socio-umane, dar cele mai spectaculoase, sau poate doar cele mai vizibile, au fost cele din domeniul militar. Nivelul tehnologic al mijloacelor/sistemelor electronice şi capabilitatea de utilizare a acestora în operaţiile militare determină capacitatea de luptă şi influenţează potenţialul şi puterea de luptă ale oricărei armate. În acest context, mediul electromagnetic al viitorului va fi un complex/ amestec de sisteme interconectate din mai multe ţări/armate.

Sistemele de război electronic şi conceptele de întrebuinţare trebuie să răspundă provocărilor unei lumi marcată de complexitate tehnologică crescândă, din ce în ce mai sofisticată. O tendinţă confirmată este reprezentată de globalizarea tehnologiilor militare, vânzările de echipamente

şi transferul de tehnologie şi expertiză cunoscând creşteri susținute în fiecare an.

Cea mai importantă tendință în evoluția războiului electronic o reprezintă trecerea la *războiul electronic cognitiv*. Aceasta presupune nu doar adaptarea în timp aproape real la amenințările din mediul electromagnetic şi generarea contramăsurilor adecvate fiecăreia, ci utilizarea algoritmilor de inteligență artificială pentru a învăța ce contramăsură este cea mai eficientă şi memorarea acesteia, pentru a putea fi utilizată automat în situații similare. Dacă amenințarea îşi modifică parametrii de emisie, sistemul cognitiv de război electronic identifică schimbările intervenite, generează mai multe variante de contramăsuri, observă efectul acestora, o selectează pe cea mai eficientă şi o memorează în vederea utilizării în viitor.

Necesitatea acestei evoluții este determinată de adoptarea pe scară largă a tehnologiei digitale în realizarea sistemelor de comunicații şi radarelor. Aceasta a permis generarea de semnale cu forme de undă complexe, de bandă largă, uşor de reprogramat. În plus, în condițiile unui spectru electromagnetic din ce în ce mai aglomerat, sistemele moderne radar şi de comunicații pot evalua gradul de ocupare a spectrului electromagnetic, pot identifica benzile libere şi ajusta rapid parametrii de emisie pentru a putea opera eficient.Modul de lucru clasic în care amenințările din mediul electromagnetic erau analizate timp îndelungat de către operatori umani, în scopul identificării unei contramăsuri adecvate, urmat de programarea contramăsurii în sistemele de autoprotecție electronică ale platformelor militare, tinde să nu mai fie valabil. Viteza de evoluție a amenințărilor din mediul electromagnetic depăşeşte capacitatea de adaptare a sistemelor actuale de război electronic, ceea ce impune dezvoltarea de sisteme de război electronic cognitive, care să detecteze, identifice şi contracareze în timp aproape real amenințări noi, pentru care nu au fost programate apriori contramăsuri adecvate de către operatori umani.

Realizarea de sisteme de război electronic cognitive depinde atât de implementarea unor algoritmi software de învățare şi inteligență artificială, cât şi de arhitecturi hardware complexe, care să permită procesarea în timp real a unor volume mari de date rezultate din digitizarea semnalelor interceptate. Arhitecturile hardware se vor realiza pe baza circuitelor integrate programabile(*fieldprogrammable gate arrays/ FPGA*) prevăzute cu interfețe optice, pentru reducerea atenuărilor şi interferențelor, unităților de procesare grafică (*general-purposegraphicsprocessingunits/ GPGPU*), standardelor de interfațare VPX[6] şi sistemelor rapide de stocare a volumelor mari de date.

Implementarea războiului electronic cognitiv poate avea ca efect reducerea numărului de platforme cu echipaj uman la bord şi proliferarea celor nepilotate (terestre – UGV, aeriene – UAV, navale – USV şi subacvatice – UUWV), favorizând implementarea unor noi concepte operaționale precum utilizarea de capabilități distribuite, integrate în rețea şi *manned-unmannedteaming – MUM-T*. Utilizarea platformelor nepilotate permite creşterea gradului de acoperire a zonei de interes grație autonomiei sporite, reducerea probabilității de descoperire de către sistemele de senzori ale adversarului grație dimensiunilor reduse, reducerea puterii de bruiaj necesare contracarării amenințărilor din mediul electromagnetic ca urmare aapropierii de țintă, precum şi creşterea probabilității de interceptare a emisiilor adversarului în scopul contracarării imediate sau analizei şi utilizării datelor parametrice ale acestora în planificarea operațiilor viitoare. O provocare în utilizarea capabilităților distribuite o reprezintă adoptarea de formate standardizate de raportare a datelor interceptate şi dezvoltarea de aplicații software care să fuzioneze aceste date în timp aproape real, în vederea elaborării imaginii recunoscute din mediul electromagnetic.

Un alt concept strâns legat de cele menționate anterior este *războiul electronic colaborativ*. Acesta presupune utilizarea mai multor sisteme de război electronic care îndeplinesc misiuni în comun, în scopul creşterii eficienței acestora. Exemple în acest sens ar putea fi reprezentate de executarea unei acțiuni de bruiaj electronic asupra unei ținte de către mai multe sisteme de

război electronic simultan, în scopul creşterii raportului de puteri zgomot/semnal util la țintă sau stabilirea, într-un sistem distribuit de război electronic, sistemului care să execute bruiaj electronic asupra unei ținte în funcție de criterii multiple, precum apropierea de țintă, caracteristicile acesteia şi capabilitățile sistemului de război electronic desemnat în acest scop. Combinarea unor tipuri diferite de sisteme de război electronic poate asigura avantaje în ceea ce priveşte corelarea acestora cu tipurile diverse de ținte şi îngreunarea misiunii adversarului de a asigura protecția electronică a sistemelor sale de luptă.

Platformele aeriene fără pilot (UAS) pot reprezenta nu doar un suport pentru sistemele de război electronic, ci şi ținte pentru acestea. Proliferarea sistemelor UAS civile şi militare reprezintă o provocare serioasă la adresa securității naționale. Acest tip de amenințare este în continuă creştere atât pentru forțele militare dislocate în teatrele de operații, obiectivele militare, guvernamentale şi industriale, cât şi pentru organizatorii de evenimente publice cu participarea unui număr mare de oameni. Dependența acestora de asigurarea comunicațiilor de comandă-control şi de date, precum şi de sisteme de navigație prin satelit, le face vulnerabile la acțiuni de atac electronic.Soluțiile de contracarare a UAS (C-UAS) dezvoltate variază în funcție de scenariul de utilizare şi de tipul amenințării - de la cele simple la cele complexe, multi-senzor (radar, opto-electronic, război electronic), cu capabilități de contracarare atât cinetice, cât şi non-cinetice. Sistemele de război electronic vor continua să constituie o soluție sau o parte a unei soluții complexe C-UAS pentru viitor. Tehnologiile de război electronic utilizate în sistemele C-UAS se bazează pe cele utilizate de sistemele de contracarare a dispozitivelor explozive improvizate comandate prin radio (C-RCIED) şi, în viitor, din ce în ce mai mult, probabil, pe arme cu laser de energie înaltă şi pe microunde de puteremare.

Testele efectuate în ultimii ani, prin instalarea unor arme cu laser pe diferite platforme (în special navale şi terestre), au permis maturizarea tehnologiei de realizare a laserilor din punct de vedere al miniaturizării, puterii emise (implicit al distanței eficace) şi al calității razei laser. Efectul la ținte de tip UAV a constat în găurirea fuzelajului, aprinderea şi prăbuşirea acestora. Principalele avantaje ale armelor cu laser sunt costul redus pentru o „lovitură" comparativ cu cel pentru o lovitură cu muniție clasică (proiectil de artilerie sau rachetă), precum şi creşterea libertății de mişcare, prin eliminarea nevoii de a transporta unitatea de foc. Este posibil ca în viitor sistemele de autoprotecție cu rază scurtă de acțiune bazate pe artilerie şi rachete să fie înlocuite de lasere de energie înaltă. O soluție în acest sens ar putea fi reprezentată de laserul care are ca element activ un segment de fibră optică dopată cu elemente rare, care asigură reducerea costurilor de operare, creşterea puterii de emisie, creşterea calității razei laser şi a duratei de viață a elementului activ.

O altă aplicație a armelor cu laser o reprezintă contramăsurile directive în infraroşu (*DirectionalInfraRedCounterMeasures – DIRCM*). Acestea sunt integrate deja în sistemele de autoprotecție ale aeronavelor militare şi utilizează o rază laser care bruiază capul de dirijare în infraroşu al rachetei adverse. O provocare specifică rachetelor moderne este faptul că acestea măsoară nivelul radiației termice a țintei în două sub-benzi din gama infraroşu, ceea ce le face mai greu de bruiat sau de dezinformat prin utilizarea de capcane termice. Sistemele DIRCM viitoare vor trebui probabil să genereze raze laser multiple de intensitate mare în toate benzile care ar putea fi folosite de capurile de dirijare în infraroşu ale rachetelor. În plus, sistemele DIRCM viitoare vor avea capacitatea de a interoga capul de dirijare în infraroşu al rachetei în scopul determinării frecvenței sale de modulație, identificând practic acea amenințare. Aceasta va permite sistemelor DIRCM să genereze codurile optime de bruiaj adaptate amenințărilor. Astfel, DIRCM va putea fi considerat omologul în banda infraroşu al unui sistem DRFM[7].

Executarea acțiunilor de atac electronic poate produce interferențe prejudiciabile asupra sistemelor proprii care se bazează pe exploatarea

energiei electromagnetice. O soluție în acest sens este reprezentată de utilizarea în sistemele de război electronic a rețelelor de antene active fazate (*Active ElectronicallyScannedArrayAntenna – AESA*). AESA este o tehnologie matură utilizată pe scară largă în realizarea stațiilor radar, care a început să fie utilizată şi în domeniul război electronic, aceasta asigurând:

- urmărirea precisă simultană a mai multor ținte;
- creşterea câştigului antenei pe o direcție de interes (pentru supraveghere/atac electronic) şi, implicit, creşterea distanței de descoperire/contracarare a țintelor;
- reducerea lobilor secundari şi,în mod direct, a riscului de a fi localizat pe timpul executării atacului electronic;
- creşterea fiabilității de până la trei ori comparativ cu antenele cu explorare mecanică a spațiului;
- generarea semnalelor cu forme de undă complexe.

Tehnologia AESA stă la baza dezvoltării unor module comune de antene, care permit realizarea rețelelor mari de antene, reconfigurabile pentru aplicații diferite, scalabile, fără a fi necesară o reproiectare completă a rețelei de antene. Personalizarea unui modul comun pentru o utilizare specifică se referă la frecvență, bandă, polarizare, nivel de putere, unghi de scanare, geometrie, forma caracteristicii de directivitate şi număr de elemente.

Antenele AESA utilizează din ce în ce mai mult circuite integrate de microunde de tip monolit (*MonolithicMicrowaveIntegrated Circuit – MMIC*),care utilizeazătranzistoare cu nitrură de galiu (GaN) pentru recepția şi generarea semnalelor de radiofrecvență. Comparativ cu tranzistoarele clasice cu arseniură de galiu (GaAs), tranzistoarele GaN pot funcționa la temperaturi mai mari, asigură o densitate de putere de 10 ori mai mare, au dimensiuni de 5 ori mai mici la aceeaşi putere generată şi pot amplifica semnale cu benzi instantanee de 4 ori mai mari la aceeaşi putere generată.

În viitor, se preconizează utilizarea de tranzistoare GaN miniaturizate în dezvoltarea de antene conforme, integrate în fuzelajul aeronavelor, care să înlocuiască radarele aeropurtate şi să execute simultan funcțiile de radar, bruiaj electronic şi sistem de comunicații. MMIC pe bază de GaN pot deveni omniprezente în sistemele viitoare de război electronic, radiolocație şi comunicații.

Unele dintre amenințările în creştere la adresa forțelor proprii sunt reprezentate de rachetele de croazieră, balistice şi hipersonice. Pentru apărarea împotriva acestora, statele dezvoltate au cercetat şi testat inclusiv soluții din domeniul războiului electronic bazate pe:

- acțiuni de bruiaj şi dezinformare electronică, în scopul întreruperii sistemului de dirijare a rachetei pe timpul traiectoriei, pierderii controlului asupra acesteia sau devierii de la ținta stabilită;
- laser de energie înaltă, satelitar sau terestru, în scopul producerii unui efect distructiv asupra rachetei, în orice punct al traiectoriei;
- sistem terestru cu microunde de putere mare, în scopul distrugerii componentelor electronice ale rachetei aflate pe sistemul de lansare sau pe traiectorie.

În viitor, integrarea deplină a capabilităților cinetice şi non-cinetice va reprezenta, probabil, soluția optimă de contracarare a acestor amenințări.

Sistemele de război electronic reprezintă o capabilitate necesară în executarea misiunilor de suprimare a apărării aeriene a inamicului. O provocare în acest context o constituietendința de testare şi chiar implementare în sistemele de apărare aeriană cu baza la sol a stațiilor radar pasive, capabile să localizeze țintele aeriene pe baza reflexiilor la acestea a semnalelor transmise de emițătoare de oportunitate, precum stații radio, TV, de telefonie mobilă etc. În unele cazuri, emițătoarele pot fi dezvoltate special în acest scop şi instalate în locuri care asigură o probabilitate de detecție a țintelor aeriene cât mai mare. Sistemele radar pasive sunt complementare radarelor active şi pot contribui la realizarea imaginii aeriene recunoscute în contextul unui mediu electromagnetic ostil,

caracterizat de utilizarea sistemelor acroşabile de război electronic, rachetelor anti-radiaţie etc. Sistemele radar pasive vor îngreuna misiunea sistemelor de război electronic, contribuind la reducerea capacităţii acestora de a elabora situaţia electronică şi a timpului de reacţie a acestora, prin activarea cu întârziere a sistemelor de dirijare a vectorilor de lovire.

În ultimii ani a crescut dependenţa echipamentelor militare şi civile de sistemele satelitare de poziţionare globală (*Global Navigation Satellite System – GNSS*), capabile să ofere servicii de localizare, navigaţie şi sincronizare în timp (*Position, NavigationandTiming - PNT*), ceea ce le face susceptibile laacţiuni de atac electronic, care pot duce la pierderea semnalului satelitar sau la afişarea eronată a poziţiei echipamentului afectat. Sistemele GNSS au un rol important în dirijarea precisă la ţintă a muniţiilor inteligente, precum şi în determinarea precisă de către senzorii proprii a coordonatelor ţintelor.Costul relativ redus al unor dispozitive de bruiaj împotriva receptoarelor GNSS şi recunoaşterea necesităţii de a opera în situaţii în care serviciile oferite de acestea nu sunt disponibile a determinat unele state dezvoltate să depună eforturi pentru identificarea de soluţii alternative care să ofere servicii PNT sau să asigure funcţionarea receptoarelor GNSS într-un mediu electromagnetic ostil. Câteva dintre acestea sunt sisteme terestre de navigaţie, dispozitive de sincronizare capabile să funcţioneze cu acces discontinuu la GNSS, sisteme inerţiale performante, bazate pe utilizarea unor antene GPS de tip reţea fazată cu orientarea nulurilor caracteristicii de directivitate către sursele de bruiaj etc. Forţele proprii vor trebui să fie pregătite să opereze în condiţiile în care utilizarea receptoarelor GPS este îngreunată sau interzisă, în urma unor acţiuni de bruiaj electronic, precum şi să dispună de sisteme alternative care să ofere servicii de poziţionare, navigaţie şi sincronizare.

Dependenţa crescută de utilizarea energiei electromagnetice pentru exercitarea comenzii-controlului, precum şi transmiterea şi fuzionarea datelor culese de senzori au creat posibilitatea executării de acţiuni cibernetice în reţelele de comunicaţii fără fir. Injectarea software-ului malign în reţelele ţintă se poate realiza în cadrul acţiunilor de atac electronic, utilizate ca suport şi care depind de cunoaşterea detaliată a formatului datelor, standardelor şi protocoalelor utilizate în reţelele ţintă, ceea ce o apropie de o acţiune de dezinformare electronică. Astfel de acţiuni au rol atât ofensiv, în scopul influenţării sau interzicerii capacităţii de luare a deciziei de către adversar, cât şi defensiv, în scopul asigurării protecţiei reţelelor de comunicaţii proprii împotriva ameninţărilor similare.

Executarea cu succes a acţiunilor cibernetice pe suportul undelor electromagnetice necesită o colaborare strânsă între structurile de război electronic şi cele cibernetice. Aceasta a determinat unele state să elaboreze concepţii privind crearea unor structuri multidisciplinare, care pot include înafară de război electronic, război cibernetic şi alte specialităţi care se bazează pe exploatarea energiei electromagnetice (managementul spectrului, SIGINT, comunicaţii, radiolocaţie), să testeze şi implementeze astfel de structuri la toate nivelurile operaţionale, în primul rând la cele de nivel tactic. Unele state au iniţiat chiar programe de dezvoltare a unor sisteme multifuncţionale de război electronic şi cibernetic destinate forţelor terestre şi aeriene. Disciplinele reunite într-o astfel de structură pot contribui la îndeplinirea unor obiective din domeniul mai larg al operaţiilor informaţionale. Este posibil ca, în viitor, acest concept să fie preluat, dezvoltat şi utilizatde mai multe ţări, odată cu implementarea conceptelor războiului bazat pe reţea şi a senzorilor distribuiţi, precum şi cu creşterea ameninţărilor reprezentate de executarea acţiunilor cibernetice pe suportul undelor electromagnetice de către un potenţial adversar.

În final, se poate aprecia că războiul electronic va continua să joace un rol important în operaţiile militare viitoare, succesul depinzând de punerea în parcticăcelor mai noi tehnologii în sistemele de război electronic şi de gradul de interoperabilitate cu celelalte specialităţi care se bazează pe exploatarea energiei electromagnetice.

Bibliografie*:*

1. AJP-3.5C, NATO Joint Electronic Warfare Doctrine (study draft)
2. https://www.crows.org/page/jed
3. https://www.defensenews.com
4. https://www.defenseone.com
5. https://www.c4isrnet.com
6. https://breakingdefense.com

---

[1] Situation alawareness (AJP-2, Allied Joint Doctrine for Intelligence, Counter-IntelligenceandSecurity)

[2] SEAD - Suppresion of Enemy Air Defence/Suprimarea apărării aeriene inamice

[3] REMP – Recognised Electromagnetic Picture/Imaginea recunoscută din mediul electromagnetic - reprezentarea grafică completă a întrebuinţării mediului electromagnetic, realizată în scopul identificării, localizării şi monitorizării continue a emiţătoarelor independente sau asociate sistemelor de armament de pe platformele terestre, aeriene şi navale dintr-o zonă de responsabilitate informativă

[4] COP – Common Operational Picture/Imaginea operaţională comună- situaţie operaţională realizată din integrarea totală sau parţială a informaţiilor specifice unor imagini recunoscute

[5] BDA – BattleDamageAssessment/Evaluarea efectelor la ţintă

[6] VPX - VME and PCI eXtended, standard ANSI care suportă topologii de reţea ce permit împrăştierea traficului de reţea prin legături fizice multiple, având ca efect creşterea vitezei de transfer a datelor; stă la baza implementării sistemelor multi-procesor.

[7] Digital Radio Frequency Memory – componentă a unui sistem de atac electronic în banda radar, care permite înregistrarea semnalului radar ţintă, modificarea parametrilor acestuia, amplificarea şi reemiterea acestuia către radarul ţintă, în scopul dezinformării privind coordonatele reale ale platformelor proprii de luptă şi/sau generării de ţinte false.

TEHNOLOGII MODERNE DE ANALIZĂ A DATELOR GEOSPAȚIALE

Florin ȚENEA
Aurel MIHAI
Mihai BĂJINARU*

Abstract

*This article offers a brief insight into the GEOINT organizations (**GEO**spatial**INT**elligence), in order to highlight the modern technologies and methods used widely to create intelligence products. These products provide geospatial support for national troops acting at all operational levels. Additionally, GEOINT products are used across national borders for monitoring and assessing the situation on specific military/civilian areas of interest.*

*Firstly, the paper takes into consideration the actual state-of-the-art regarding the GEOINT domain. It covers topics such as GIS (**G**eographical **I**nformation **S**ystem) technology which, practically, has changed everything in the last two decades by easing the process of making GEOINT products. Another topic approachedby this article refers to the work of image analysts, which have a remote sensing background and are trained to distinguish critical elements on the images.*

Further, the article covers the topics concerning different types of data used in the GEOINT production, offering a compendious insight of them from a technical point of view.

The main subject consists of the actual development of methods and algorithms that solve difficult and time consuming problems such as multi-temporal change detection and ship detection. Another topic covered is the rapidly expansive artificial intelligence (AI) field of study. As concluded, this domain will become more and more useful in the GEOINT organizations because of its specific algorithms which could solve the problem of lacking specialized personnel and speeding up GEOINT workflows.

***Keywords**: GEOINT, intelligence, GIS, image analysis, geospatial support, Big Data, Artificial Intelligence.*

În societatea contemporană, aflată în continuă schimbare, informațiile îşi pierd rapid valoarea, se alterează şi pot genera decizii greşite. În acest context este obligatorie existența unor metode rapide de procesare, interpretare şi analiză a informațiilor sensibile, care să conducă către evaluări corecte ale situațiilor de criză şi la alegerea cursurilor de acțiune corespunzătoare.

Din perspectiva GEOspatialINTelligence/ GEOINT, informațiile trebuie să conțină referințe geografice precise, să fie însoțite de meta-date („date despre date”), să poată fi analizate facilşi să permită corelarea spațială şi atributivă cu alte informații specifice altor subramuri de INTelligence.

Datele utilizate în domeniul GEOINT poartă denumirea de date geospațiale.Având în vedere fenomenul globalizării, analiştii din domeniul GEOINT au nevoie de soluții GIS care să furnizeze date în timp real, cu mare capacitate de procesare şi care să permită partajarea şi gestionarea facilă a produselor geospațiale.

Soluțiile web GIS au luat amploare în ultimii ani, ajungând acum la pachete complete,

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

portabile, cu o gamă foarte largă de servicii de date şi hartă. În prezent, datele au un grad mai mare de accesibilitate, făcând trecerea de la era lipsei de date în era *"big data"*.În acest context, abundența de date din surse variate poate deveni o problemă,iar validarea acestui volum mare de date s-a transformat în una dintre principalele activități ale specialiştilor ce integrează datele geospațiale în diferite sisteme.

Culegerea de informații presupune monitorizarea unui set complex de amenințări globale, de la atacuri cibernetice până la revolte politice şi sociale. O platformă GEOINT adresată acestui domeniu trebuie să gestioneze toate sursele de informații (*Multi-INT*) şi să producă în timp util informații precise necesarepentru luarea deciziilor.

În cazul specific al domeniului de intelligence,GIS urmăreşte**:**

- proiectarea modelelor de date specifice poligoanelor de antrenament;
- crearea unei baze de date geospațiale pentru zonele de interes, pornind de la conceptele de modelare specifice;
- pregătirea tragerii cu echipamente militare într-un timp redus (prin eliminarea etapelor intermediare privind studiul hărților şi culegerea datelor de pe acestea);
- portabilitate (aplicația poate fi implementată pe mai multe calculatoare);
- posibilitatea imprimării produselor geografice realizate;
- reducerea timpului necesar întreținerii bazei de date;
- creşterea vitezei de reacție privind descoperirea şi nimicirea țintelor inamicului;
- generarea rapoartelor cu privire la modificările survenite în timp asupra obiectivelor monitorizate.

O platformă GEOINT trebuie să ofere soluții pentru a gestiona, analiza şi vizualiza datele din surse Multi-INT şi a le integra într-o imagine geografică uşor de înțeles şi utilizat. Date aparent fără legătură, din imagini satelitare, videoclipuri, senzori, inteligență umană, social media şi din alte surse, sunt transformate pentru a ajuta la stabilirea opțiunilor, la setarea priorităților şi la luarea deciziilor.

Pentru a ajunge la informații (date cu un înțeles clar delimitat) este necesară analiza tipurilor de date geospațiale utilizate în cadrul GEOINT şi înțelegerea particularităților acestora. Platformele aeriene şi satelitare sunt echipate cu senzori electro-optici (*EO*), SAR (***S****ynthetic****A****perture****R****adar*), LIDAR (***LI****ght****D****etection****A****nd****R****anging*) etc., care baleiază suprafața terestră colectând imagini la diferite rezoluții. Printre cele mai performante platforme se regăsesc: constelația SENTINEL (SAR – Sentinel-1, EO – Sentinel-2), constelația PLÉIADES (imagini EO cu rezoluție spațială sub-metrică), constelația WORLDVIEW (imagini EO cu rezoluție sub-metrică sub 50 cm), TanDEM-X şi TerraSAR-X (SAR) etc.

Imaginileelectro-optice (EO)

Înregistrările electro-optice (*EO*) sunt cele mai utilizate datorită nivelului de detalii oferit şi uşurinței interpretării elementelor din teren. O limitare pentru acest tip de înregistrare o constituiefaptul că este dependentă de iluminarea solară, condiții atmosferice, nebulozitate, unghiul de incidență etc.

Datele brute (*raw data*) primite de la platformele de înregistrare sunt recepționate de către stațiile terestre (*ground-segment*) care efectuează procesarea acestora, iar apoi sunt furnizate beneficiarilor de servicii de imagini.

Întrucâtatmosfera acționează ca o lentilă complexă formată din mai multe straturi având coeficienți de refracție diferiți, imaginile preluate de platforma satelitară sunt distorsionate şi nu reflectă realitatea din teren. Astfel, este necesară procesarea acestor imagini prin aplicarea unor corecții radiometrice în vederea eliminării influenței factorilor atmosferici. Prelucrarea radiometrică include calibrarea senzorului utilizat, eliminarea efectelor unghiului de iluminare solară şi a celui de incidență, completarea liniilor lipsă din imagine, eliminarea efectelor radiometrice provocate de relief (iluminare neuniformă, reflectanțădiferențială în funcție de pante şi elemente de teren), corectarea reflectanțeiToA (***T****op* ***of*** ***A****tmosphere*).

După eliminarea efectelor datorate factorilor atmosferici, înregistrările sunt încadrate într-un sistem de coordonate care le conferă referință geografică. Acest lucru este realizat prin utilizarea poziției platformei la momentul preluării imaginii (efemeride precise) în cadrul procesului de proiectare punctuală a pixelilor în sistemul de coordonate din teren. Ultima etapă de parcurs înainte de livrarea imaginii către beneficiar este legată de prelucrarea geometrică a înregistrării. Scopul acesteia constă în eliminareadistorsiunilorprovocate de influența reliefului asupra imaginii. Prelucrarea geometrică presupune utilizarea unui model digital al terenului ce conține, pe lângă coordonatele în plan orizontal, și valorile altimetrice ale terenului. Practic, înregistrarea satelitară se va suprapune, utilizând o metodă de interpolare (NearestNeighbour, biliniară, cubică, Kriging, Spline etc.) peste suprafața 3D a terenului, rezultând o reprezentare precisă a realității din teren.

Principala utilizare a imaginilor optice are loc la nivelul procesului de interpretare a elementelor din teren, aflate la suprafață, nemascate.Pe baza acestora, se pot realiza evaluări ale situației de la sol, pot fi concepute planuri de acțiune, având un important aport în procesul decizional al comandanților structurilor de forțe.

Imaginile SAR

Imaginile SARsunt invariante la condițiile atmosferice și independente de ciclul zi-noapte deoarece utilizează propria sursă de iluminare. Înregistrările SAR parcurg un flux de procesare, de la datele brute (*raw data*) până la produsul livrabil, mult mai lung comparativ cu cele electro-optice. Semnalul se procesează inițial pe distanță și apoi pe azimut, utilizând tehnica de *zero-padding* și transformata Fourier rapidă (*FFT*). După introducerea corecțiilor (puls calibrare, reconstrucție semnal, mișcare pe orbită, zgomot termal etc.), aplicarea algoritmilor Doppler și extragerea informațiilor referitoare la fază se aplică inversa transformatei Fourier rapide (*IFFT*), din care rezultă un produs SLC (***S**ingle **L**ook **C**omplex*) care poate fi distribuit către beneficiari. Acest produs satisface majoritatea cerințelor utilizatorilor, conținând și informații referitoare la fază, șipoate fi folosit, spre exemplu, la detectarea schimbărilor temporale dintr-o zonă de interes pe baza coerenței (*Coherence Change Detection*).

Pentru beneficiarii care nu posedă mijloace de procesare performante este livrat un produs derivat, **GRD** (***G**round **R**ange **D**etected*), care nu conține informații despre fază, are o dimensiune virtuală mai redusă și a fost corectat radiometric și geometric, deci poate fi utilizat imediat.

Pentru a evalua elemente terestre mascate, semi-îngropate sau țintel false, se utilizează produse SAR în analiza GEOINT preluate cu diverse benzi RADAR ce au caracteristica de a penetra parțial solul.

Pe de altă parte, imaginile SAR sunt potrivite pentru detecția schimbărilor dintr-o zonă, utilizându-secoerențadintrebenzileadouăimagini temporale (*CoherenceChangeDetection*), metodă care va fi prezentată mai departe în acest articol. O derivată a procesului de detecție pe baza produselor SAReste reprezentată de posibilitatea de a monitoriza navele aflate pe mare/ocean.

Datele LIDAR

Pentru analize tridimensionale este utilizată tehnologia LIDAR prin care se produc modele digitale ale terenului (*MDT*) cu precizie ridicată.

Datele sunt colectate sub formă de nor de puncte care conțin informații referitoare la poziția spațială (*X, Y*), altimetrie (*Z*), dar și clasificarea pe categorii (pământ, apă, vegetație, construcții, asfalt etc.). Acestea sunt preluate în mare parte cu platforme aeriene, pe zone restrânse, fiind o tehnologie caracterizată prin costuri ridicate de utilizare.

Pentru a avea rezultate cât mai precise, platforma aeriană este obligată să zboare la o altitudine redusă (sub 5.000 m) și din acest motiv tehnologia LIDARnu poate fi utilizată în zone caracterizatedeunnivelridicatdepericol.Produsele derivate din aceste date se constituie din modele digitale ale terenului care pot fifolositeîn cadrul unor lucrări specifice, precum: studiul vizibilității dintr-o zonă, analiza culoarului de trecere a unui convoi, selecția punctelor optime de amplasare a

forţelor speciale/lunetişti, alegerea zonelor optime aterizării (*helicopter landingzones*), profile 3D ale clădirilor, aplicaţii tactice etc.

În continuare, sunt prezentate o parte din metodele utilizate la nivelul domeniului GEOINT pentru a satisface nevoile şi cerinţele naţionale, respectiv internaţionale:

❖ **Detecţia navelor pe mare/ocean**

Supravegherea maritimă poate fi realizată utilizând mai multe opţiuni, dintre care amintim: *Automatic Identification System* (AIS), *Long Range Identification and Tracking* (LRIT) şi *Vessel Monitoring System* (VMS). O altă modalitate o reprezintă mijloacele indirecte care nu implică vreun sistem aflat la bordul navelor.

În cadrul GEOINT, detecţia navelor se poate realiza utilizând imagini satelitare SAR, fiind o metodă indirectă prin care se pot monitoriza inclusiv navele care nu sunt dotate cu sisteme de urmărire sau care au emiţătoarele oprite, tactică specifică navelor care efectuează activităţi ilegale (pescuit ilegal, piraterie, cercetare radio-electronică etc.). Monitorizarea se poate realiza continuu, inclusiv pe timpul nopţii, datorită specificului imaginilor SAR de a nu fi dependente de lumina solară.

Fluxul de lucru urmăreşte mai întâi separarea zonei maritime de zona de uscat prin crearea unei măşti vectoriale. După o calibrare radiometrică a imaginii, se aplică un algoritm de detecţie cunoscut în literatura de specialitate drept *Two-Parameter Constant False Alarm Rate* (CFAR). Acesta parcurge imaginea pixel cu pixel şi compară valoarea pixelului central cu o valoare prag pe baza căreia realizează clasificarea obiectelor. În imaginea SAR, apa are cel mai mic răspuns RADAR şi e reprezentată prin culori închise, iar navele, fiind construite din metal (răspuns RADAR ridicat), apar drept ţinte luminoase. Astfel, detecţia se realizează facil, clasificând pixelii vecini cu răspuns RADAR puternic drept nave. Rezultatele pot fi îmbunătăţite prin introducerea unui prag de discriminare a obiectelor bazat pe setarea unei limite inferioare, respectiv superioare, cu scopul de a filtra ţintele false.

Rezultatele pot fi exportate astfel încât se poate crea o bază de date cronologică a navelor detectate, care poate fi verificată cu datele înregistrate de sistemele comune de monitorizare enunţate anterior. Astfel, se pot determina navele suspecte, cu emiţătorul de poziţionare oprit

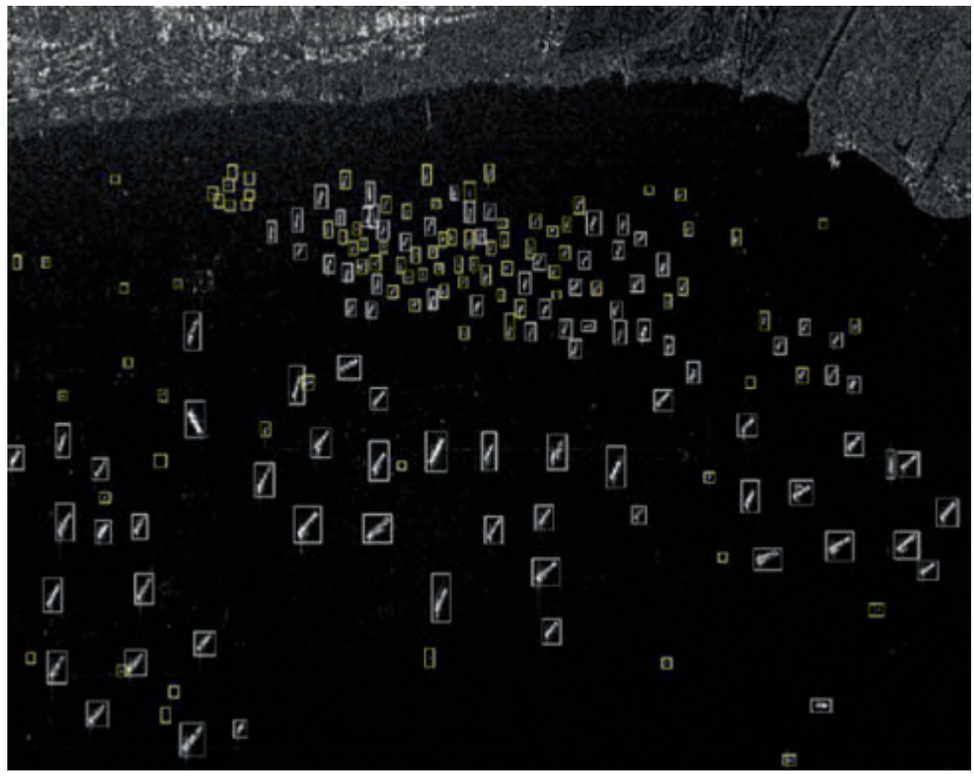


Fig. 1: Rezultatul detecţiei navelor pe mare[1]

sau fără emițător, iar rezultatele evaluării sunt transmise către structurilecompetente (Pază de Coastă, Forțe Navale etc.).

❖ **Detecția schimbărilor temporale**

Schimbările elementelor din teren survin foarte des în zona obiectivelor militare datorită mişcărilor de trupe sau tehnică, precum şi în urma instalării rapide a unor infrastructuri temporare. Prin urmare, analiştilor de imagine le revine sarcina de a baleia suprafețe vaste la un nivel de detaliu foarte ridicat pentru a monitoriza aceste schimbări şi a evalua situația eficient şi corect. Pentru o monitorizare rapidăa unor suprafețe maride teren, în cadrul GEOINT se utilizează algoritmi de detecție automată a schimbărilor temporale aplicați pe imagini SAR.

Fluxul de lucru utilizează două sau mai multe produse SAR, de tip SLC (*Single Look Complex*), având aceeaşi polarizare, traiect şi tip de preluare (*IW – Interferometric Wave*). Imaginile sunt procesate radiometric prin efectuarea unei calibrări a senzorului, eliminarea zgomotului impuls şi aplicarea unui algoritm de tip *Multilooking*. În continuare, imaginile sunt prelucrate geometric pentru a elimina efectele datorate reliefului (basculare, scurtare distanțe, umbrire etc.) şi înscrise într-un sistem de coordonate.

Sunt cunoscute mai multe metodologii utilizate în detecția schimbărilor temporale, dar cea mai utilizată este cea bazată pe calcularea coerenței dintre benzile imaginilor. Se mai parcurge o etapă, cunoscută în literatura de specialitate ca algebra benzilor, în care se generează*suma* şi diferența benzilor spectrale ale imaginilor. Produsul coerenței, alături de banda sumă şi banda diferență, formează un produs cu trei benzi de tip RGB, în care se disting trei categorii de forme: elemente care nu au suferit schimbări între momentele temporale ce caracterizează imaginile; elemente care au cunoscut schimbări

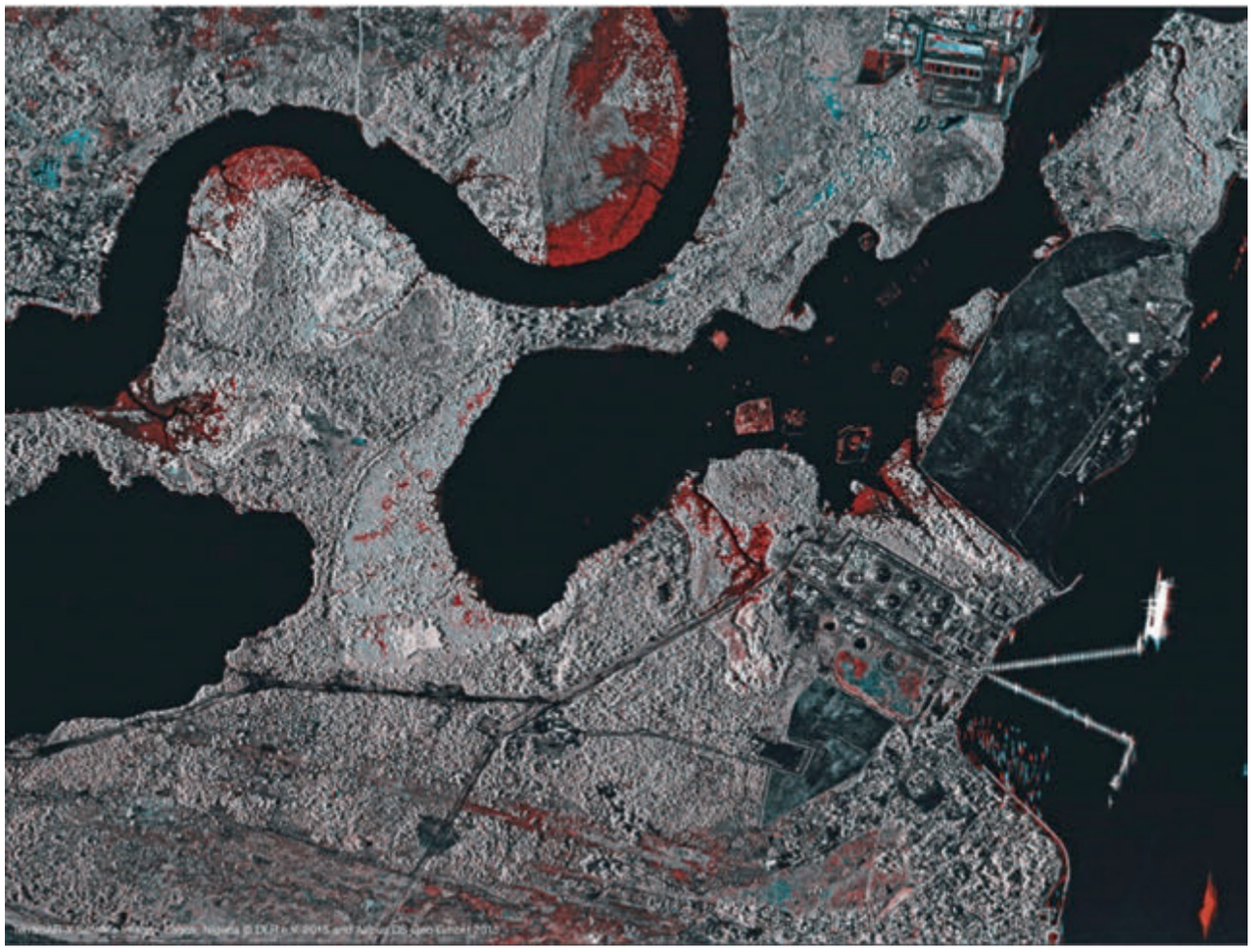
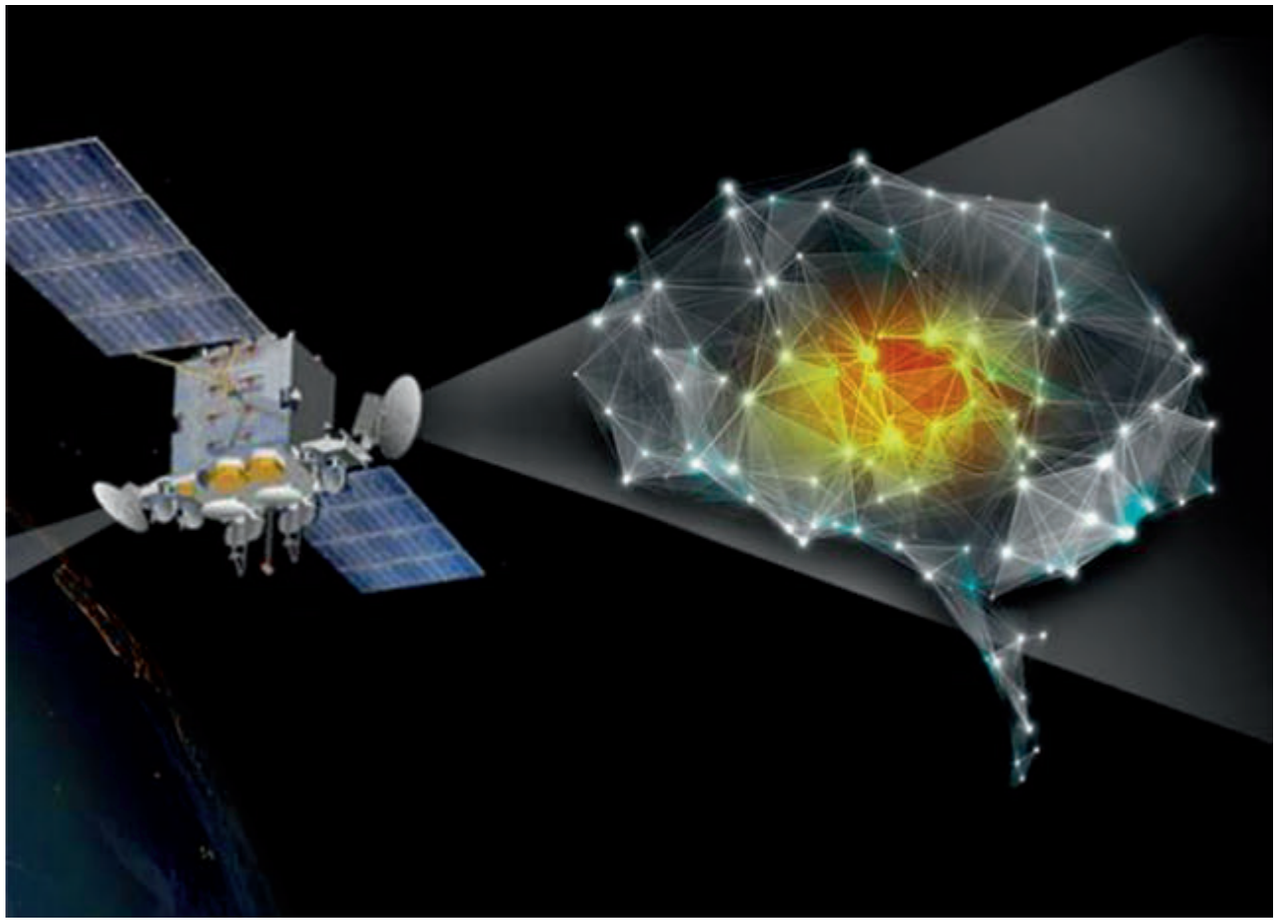


Fig. 2: Produs obținut prin metoda coerentă de detecție a schimbărilor temporale[2]



de natură artificială (construcția unor noi bretele de acces pe pistă, căi de comunicații noi, tehnică ce şi-a schimbat poziția etc.);elemente modificate natural (zonă inundată sau decopertată). Un produs de acest tip poate ajuta extrem de mult analiştii de imagine în monitorizarea unui obiectiv, reducând timpul necesar evaluării.

Domeniile în care aceste tehnici îşi găsesc utilitatea sunt:

- monitorizarea evoluției vegetației;
- mişcări fine ale terenului/construcțiilor (alunecări, ridicări, scufundări);
- evaluarea activităților de contrabandă;
- identificarea punctelor de plecare/tranzit folosite în imigrarea ilegală;
- monitorizarea activităților de la granițe pe zone mari şi foarte mari;
- detectarea urmelor de activități umane (căi de acces utilizate, activități desfăşurate pe timp de noapte);
- monitorizarea activităților legate de proliferarea armelor de distrugere în masă;
- analiza în timp a infrastructurilor critice.

În timp ce inovațiile în domeniul informațiilor pentru apărare se bazează deseori pe apariția unor noi sisteme de culegere, un factor determinant pentru viitorul GEOINT îl reprezintă datele din mai multe surse generate şi prelucrate de maşini inteligente.

În SUA, directorul NGA (National Geospatial-Intelligence Agency), Robert Cardillo, a numit recent inteligența artificială (AI) drept o prioritate majoră pentru comunitatea GEOINT: „Dacă am încerca să exploatăm manual toate imaginile pe care le vom colecta în următorii 20 de ani, am avea nevoie de 8 milioane de analişti de imagini.”

AI are şi va avea un rol din ce în ce mai important în:

- geo-referențierea automată a imaginilor;
- detectarea automată a schimbărilor şi extragerea, clasificarea şi identificarea acestora;
- evaluarea preciziei de cunoaştere a datelor;
- actualizarea bazei de date şi vizualizarea datelor.

În momentul de față, în domeniul GEOINT utilizarea AI se bazează, în principal, pe dezvoltarea de noi algoritmi şi îmbunătățirea acurateței acestora. În ultimii ani au fost lansate mai multe competiții pentru realizarea de aplicații geospațiale:

- IARPA's Multi-View Stereo 3D Mapping;
- The SpaceNetChallenge, CosmiQ Works, Digital Globe şi NVIDIA;
- The Defence Scienceand Technology Lab's Semantic Segmentation;
- IARPA's Functional Map of the World Challe;
- Planet's Forest Recognition;
- USSOCOM's Urban 3D.

În concluzie, domeniul GEOINT se remarcă printr-o fluiditate ridicată şi o continuă dezvoltare, dictată în mare parte de cerințele de informații tot mai complexe. Datorită datelor de mari dimensiuni cu care se lucrează şi abundenței informațiilor, organizațiile GEOINT au o tendință de orientare către utilizarea tehnicilor de prelucrare *Big Data,* pentru a valorifica eficient datele, dar şi a algoritmilor de inteligență artificială pentru a clasifica obiecte şi a descoperi regresiv tendințe ale datelor.

Viitorul GEOINT va depinde, în mare parte, de dezvoltarea şi integrarea algoritmilor de inteligență artificială în cadrul fluxului de lucru, având în vedere că personalul din acest domeniu are nevoie de o perioadă lungă de specializare, pe fondul nivelului înalt de expertiză profesională cerut.

Bibliografie:

1. PREISS, Mark, Nicholas Stacy (2006), *Coherent ChangeDetection: Theoretical Description and Experimental Results,* Defence Science and Technology Organisation, Australia;
2. NIȚU I., *Ghidul analistului de intelligence*, Editura Academiei Naționale de Informații, Bucureşti, 2011;
3. *The state andfuture of GEOINT* 2018, USGIF, USA;
4. STANAG 2251 AgeoP-17, *Scope and presentation of military geographic information and documentation*, NATO, 2015;
5. *National Geospatial-IntelligenceAgency*- Analysis 2020 Technology Plan;
6. https://www.satcen.europa.eu/page/military_capabilities;
7. https://nga.maps.arcGIS.com/home/index.html;
8. http://www.esri.com/library;
9. http://gisdevelopment.net;
10. https://rus-copernicus.eu/portal/wp-content/uploads/library/education/training/
11. OCEA01_ShipDetection_Trieste_Tutorial.pdf

[1] https://rus-copernicus.eu/portal/wp-content/uploads/library/education/training/OCEA01_ShipDetection_Trieste_Tutorial.pdf

[2] https://www.semanticscholar.org/paper/Ship-Detection-in-SAR-Imagery-via-Variational-Song-Xu/79fe589d6d5b05ad3bb3ba87e93dad88ef11ffdf/figure/0

CONCEPTUL I2 – IDENTITY INTELLIGENCE ÎN CADRUL NATO

Teodor NEICULESCU
Rareş ROŞU[*]

Abstract

"Who?" represents a fundamental question in the process of understanding the operational environment. The answer to this question offers the basic information about the subject who is acting or who is affected directly or indirectly by a certain action. The question "Who?" highlights a person/entity from a social group offering the individual's or the group's identity as an answer.

In the field of intelligence or security, the answer to the question "Who" indicates an individual/ organization which is in one of the following statesin relation with our forces: person/organization that belongs to our own forces, allied forces, neutral forces or hostile forces.

Identity intelligence answers in a complex and systemic manner to the questions related to people identity, their activities, locations, how they operate and the motivation that stands behind their behavior and actions. All of these parameters are analyzedin all three moments of time: past, present and future.

Key words*: identity, anonymity, biometrics, human network analysis, challenges.*

Ce este identitatea?

În literatura de specialitate există diferite accepțiuni privind definirea identității. Conform psihologului Erik Erikson, identitatea reprezintă un sentiment subiectiv şi tonic al unei unități personale şi al unei continuități temporale[1], iar în cazul perturbării acestui sentiment se instalează criza de identitate[2].

În abordarea psihologiei genetice, potrivit lui JeanPiaget, se insistă asupra noțiunii de socializare. Construirea identității prin transmiterea comportamentelor sociale şi prin organizarea reprezentărilor mintale este un proces atât cognitiv, cât şi unul afectiv şi expresiv. Prin intermediul limbajului, individul asimilează şi îşi însuşeşte simbolistica, regulile şi valorile care să îi permită comunicarea cu semenii, să se identifice sau să se diferențieze şi să îşi marcheze apartenența la unele grupuri sau să le respingă pe altele[3].

Identitatea etnică reprezintă sentimentul unui individ de apartenență la un grup etnic. Grupurile etnice constituie indivizi legați de un simț împărtăşit reciproc de apartenență la o structură culturală comună. Elementele centrale care definesc trăsăturile unui grup etnic pot fi de natură religioasă, geopolitică, lingvistică, tradițională, tribală sau unele combinații ale oricăror dintre aceste caracteristici[4]. Un grup etnic poate reprezenta atât majoritatea, cât şi minoritatea unei populații, putând fi dominant sau lipsit de putere în cadrul societății.

Identitatea unui individ nu este o caracteristică fixă, prestabilită, ci este fluidă şi mereu schimbătoare. Aceasta derivă din capacitatea indivizilor şi, implicit, a grupurilor de a se transforma în mod constant pentru a se adapta situațiilor nou întâlnite. Astfel, confruntarea cu spețe multiple conduce la achiziționarea de noi

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

identități, care le permit să evolueze pentru a depăși crizele.

Dat fiind faptul că oamenii sunt ființe sociale, este necesar ca indivizii să se afilieze diferitelor grupuri pentru a satisface nevoia de socializare, putând delimita două tipuri de identități: identitatea socială – sinele definit în termenii calității de membru al grupului, și identitatea personală – sinele definit în termenii relației personale și a atributelor personale[5]. Astfel, pentru a putea determina identitatea (ca întreg) unui individ, este necesară analizarea atât a individului, cât și a rolului și relațiilor pe care acesta le deține în cadrul grupurilor la care este afiliat. Grupurile la care aderă indivizii prezintă morfologii, structuri și interese multiple și diverse, având ca efect multiplicitatea identităților membrilor, ceea ce conduce la dificultăți în procesul de identificare a acestora, a rolului și legăturilor dintre aceștia.

Anonimatul vectorilor umani de amenințare

În domeniul sociologiei, anonimatul reprezintă condiția în care identitatea unui individ nu este cunoscută de ceilalți.

Unul dintre tipurile de influență socială care poate determina un individ normal să se angajeze în fapte dominate de cruzime sau alte comportamente antisociale este reprezentat de integrarea acestuia într-o mulțime. Astfel, identitatea individului devine subjugată grupului, realizându-se procesul de dezindividualizare. Anonimatul este considerat unul dintre factorii contribuitori la comportamentul antisocial manifestat de persoanele normale în cadrul mulțimilor, alături de un nivel ridicat de excitare comportamentală și o comutare a atenției dinspre sine către evenimentele externe[6]. Totodată, anonimatul este reprezentativ și în cadrul societății de masă[7].

În vederea eliminării sau reducerii anonimatului vectorilor de amenințare, NATO dezvoltă capabilitatea de *date biometrice*. Această capabilitate contribuie la procesul generat de activitățile de stabilire a identității.

Primul obiectiv al reducerii sau eliminării anonimatului este reprezentat de determinarea legăturii dintre entități. În cadrul acestui obiectiv se vizează prelevarea și compararea datelor biometrice în vederea identificării și stabilirii legăturii dintre un insurgent/terorist și o rețea, un loc, un obiect sau un eveniment.

Al doilea obiectiv este determinat de identificarea pozitivă, cu acuratețe ridicată, a unei ținte în cadrul unei operații.

Al treilea obiectiv este reprezentat de modul în care forțele NATO percep sau se comportă față de indivizi care prezintă interes, întâlniți pe timpul operațiilor.

Necesitatea dezvoltării domeniului *„Identity Intelligence”/I2*

Domeniul informațiilor derivate din identitate (*Identity intelligence*) a înregistrat o evoluție accelerată în ultimele decenii, deoarece conflictele armate au cunoscut o extindere spațio-temporală. Extinderea este cauzată de forțele de opoziție care nu își mai limitează acțiunile doar la teatrele de operații[8], ci le exteriorizează și în zonele din afara teatrului, în „zonele de interes strategic” ale acestora.

Identity Intelligence (I2) reprezintă produsul de informații rezultat în urma procesării atributelor de identificare ale indivizilor, grupurilor, rețelelor umane sau populației de interes[9].

În cadrul conceptului strategic al NATO și cu prilejul summit-urilor Alianței, de la Lisabona, Chicago și din Țara Galilor, s-a stabilit faptul că actori statali sau non-statali care au prezentat o amenințare reală la adresa securității și siguranței statelor membre NATO acționează în umbra anonimatului. Vectorii de amenințare sunt reprezentați de[10]:

- persoane care fac parte din grupări teroriste;
- grupări insurgente care execută atacuri împotriva trupelor NATO, retrăgându-se după atac în rândul populației locale;
- grupuri de persoane aparținând serviciilor de informații ostile care desfășoară activități de culegere de date și informații despre capabilitățile și misiunile NATO;

- *hackerii* care, sub protecţia anonimatului, accesează neautorizat sisteme informatice NATO pentru a produce prejudicii organizaţiei;
- grupările transnaţionalede criminalitate organizată care operează în ariile de operaţii ale NATO şi pe teritoriile statelor membre NATO;
- piraţii care se deplasează în apele internaţionale folosind identităţi false sau pretinzând că sunt lucrători în cadrul companiilor maritime.

Identificându-se nevoia operaţională a Alianţei, în sens general, şi a statelor membre sau partenere, în particular, NATO a lansat o serie de concepte şi documente programatice care vin în sprijinul doctrinar şi decizional al armatelor statelor membre, agenţiilor de informaţii şi securitate şi organismelor de impunere a legii.

Considerente operaţionale

În cadrul unei operaţii militare, I2 se regăseşte în cadrul tuturor fazelor acesteia. Tranziţia activităţilor de stabilire a identităţii între faze reprezintă de fapt o orientare a efortului informaţional, având în vedere obiectivele comandantului operaţiei. Principala provocare rezidă din adaptarea corectă a efortului de culegere într-o dimensiune temporală de lungă durată şi un mediu caracterizat de un nivel scăzut de informaţii culese, exploatate şi analizate.

Scopul I2 este de a crea puntea dintre domeniul datelor biometrice şi cel al analizei reţelelor sociale şi a reţelelor umane (SNA – Social Network Analysis/HNA- Human Network Analysis). Aceasta presupune analiza tipurilor de legături între diverse entităţi (reprezentate prin noduri)[11].

I2 este parte a ciclului operaţional al activităţilor de stabilire a identităţii. Activităţile

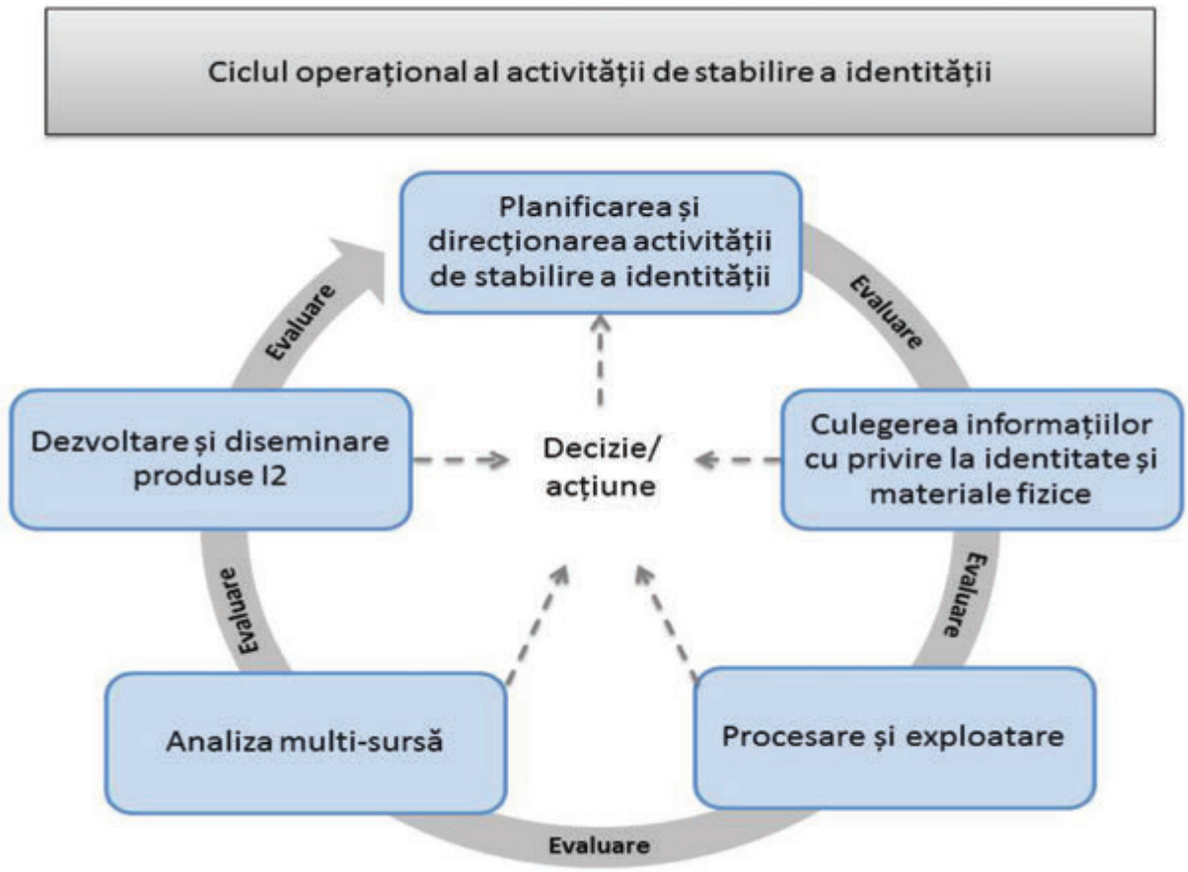


Fig. 1: Ciclul operaţional al activităţii de stabilire a identităţii[14]

de stabilire a identității/identificarea reprezintă un ansamblu de funcțiuni şi acțiuni care au ca scop recunoaşterea şi diferențierea entităților în vederea sprijinului decizional (vezi Fig. 1).

Din perspectiva domeniului militar, informațiile obținute din I2 reprezintă o componentă a activităților de stabilire a identității/ identificării factorilor umani, contribuind semnificativ la cunoaşterea şi înțelegerea situațională prin aducerea de aport informațional la imaginea recunoscută. Identitatea primară este exprimată din punct de vedere național, rasial şi religios (exemple specifice pot fi afilierea de trib şi de clan). Identitățile secundare includ preferințele personale. Indivizii aparțin mai multor grupuri sociale care determină identitatea lor culturală. Mai mult, oamenii tind să ordoneze aceste identități în funcție de importanța pe care o acordă fiecărui grup. În consecință, identitatea culturală a unui individ poate intra în conflict cu a celorlalți, cum ar fi cazul în care loialitatea de trib poate intra în conflict cu afilierea politică.

În acelaşi timp, identitatea socială reprezintă un bun indicator asupra intereselor unui actor din mediul operațional. Aşadar, referindu-se la motivațiile bazale, determinante de comportamente, identitatea socială face parte şi ea din cadrul motivațiilor de bază alături de securitatea fizică, necesitățile primare, bunăstarea economică şi participarea politică.

Abordarea activității de identificare se realizează într-o manieră sistemică, vizându-se înțelegerea aprofundată a capabilităților adversarului, rețelelor de infrastructură şi sprijin logistic, persoanelor cheie şi a altor actori relevanți, contribuind la creşterea nivelului de conştientizare al mediului operațional[12].

I2 generează produsul de intelligence rezultat în urma activității de procesare a atributelor de identitate cu privire la indivizi, grupuri, rețele sau populații de interes[13].

Identificarea şi caracterizarea actorilor relevanți dintr-un spațiu, realizată prin intermediul informațiilor derivate din *identity intelligence*, furnizează o înțelegere îmbunătățită asupra modului în care actorii şi rețelele din care aceştia fac parte şi influențează mediul operațional[15].

Atributele de identificare reprezintă caracteristicile biografice, biometrice şi contextuale prin care un individ, sistem sau grup poate fi recunoscut în mod unic.

În abordarea NATO s-a realizat o definire cuprinzătoare a identității. Aceasta este descrisă în Manualul de combatere a amenințării anonime – AIntP-15 *Countering Threat Anonymity: Biometrics in Support of NATO Operationsand Intelligence.* Potrivit acestuia, identitatea reprezintă un set de atribute sau caracteristici care pot fi utilizate să descrie, să distingă sau să recunoască o persoană.

Atributele biometrice ale unei persoane furnizează un set de caracteristici distincte, irefutabile, care pot fi folosite pentru identificarea acesteia. Acestea sunt suficiente pentru a diferenția un individ dintr-o mulțime. Identitatea, în mediul militar, pe lângă faptul că determină cine este o persoană, furnizează informații cu privire la contactele dintre individ şi forțele NATO[16].

Atributele identității sunt cele de natură biometrică, biografică sau situațională aparținând unui individ. Sunt două tipuri de atribute ale identității:

- atributele biometrice reprezintă caracteristicile biometrice şi comportamentale ale unui individ din care se disting trăsături biometrice repetabile, care pot fi extrase în scopul recunoaşterii biometrice;
- atributele biografice reprezintă atributele fizice şi non-fizice ale unui individ. În această categorie se regăsesc numele, vârsta, adresa, numărul de telefon, locul naşterii, naționalitatea, nivelul educațional, nivelul de acces la informații clasificate şi istoricul financiar.

I2 fuzionează atributele de identitate (informații biografice, biologice, biometrice, comportamentale sau legate de reputație) cu alte informații şi date asociate atributelor, pentru a identifica şi evalua nivelul amenințării reprezentate de actorii sau rețelele din care aceştia fac parte, capabilitățile, centrele de greutate, obiectivele, intențiile şi cursurile de acțiune potențiale în vederea sprijinirii procesului decizional. Atributele situaționale reprezintă

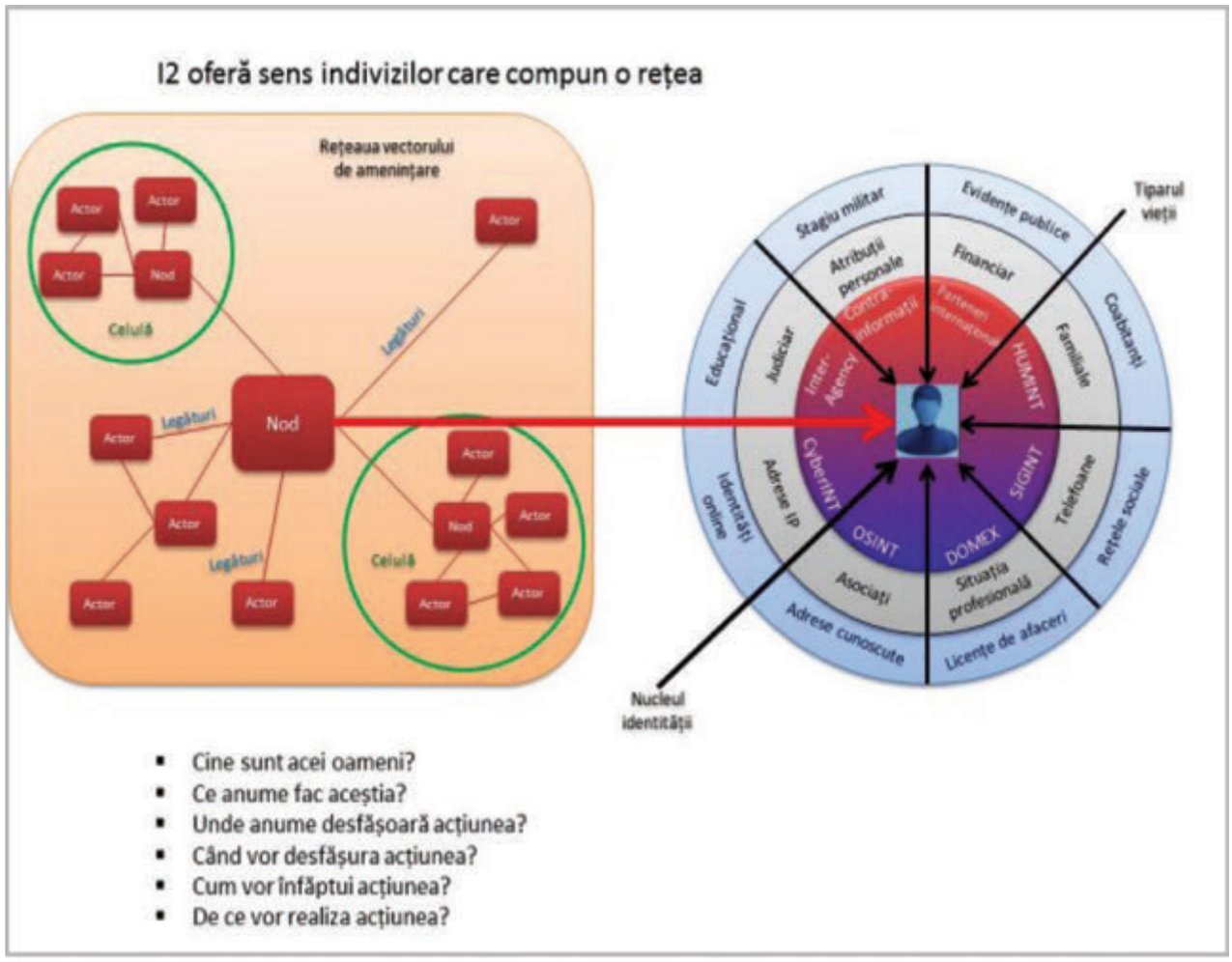


Fig. 2 Relația dintre indivizi şi rețelele umane[19]

rolul unui individ în cadrul unei activități sau a unui eveniment.

Produsele informative obținute în urma activității de I2 în domeniul militar se regăsesc în pachetele de informații care însoțesc țintele în procesul de management al țintelor/*targeting*. Prima instituție care a dezvăluit oficial că folosește capabilitatea I2 a fost Comandamentul Forțelor pentru Operații Speciale al Armatei SUA (US SOCCOM) în anul 2012[17].

Provocări

Domeniul I2 se confruntă cu o serie de provocări care se regăsesc atât în domeniul militar, cât şi în cel civil.

Un exemplu în acest sens este oferit de faptul că I2 este întrebuințat atât în domeniul militar/intelligence, cât şi în cel al securității. În domeniul securității, I2 are ca scop furnizarea de servicii de securitate în care persoanele care beneficiază de acces în complexele vizate posedă identități credibile. Verificarea credibilității identității acestora presupune o acuratețe foarte ridicată în ceea ce privește identificarea biometrică, deoarece arhitectura de securitate se bazează pe modelul de tip „încredere zero”[18].

În domeniul securității, analiza pornește de la evaluarea stării de securitate proprii. Astfel, abordarea domeniului I2 poate fi rezumată la a cunoaşte totul cu privire la o identitate din toate perspectivele – biometrică, biografică, tiparul comportamental şi sarcinile asociate identității respective, scopul analizei I2 fiind detectarea anomaliilor şi prevenirea desfăşurării „unor acțiuni care pot avea efecte negative asupra indivizilor sau organizației”. De exemplu, există indicatori care confirmă faptul că individul X va desfăşura o acțiune în momentul t1 din viitor, la locul Z1.

Pentru a putea fi complet operabile, sistemele I2 trebuie să depăşească diverse provocări (juridice, de securitate, de dezvoltare a infrastructurii IT&C, de interoperabilitate etc.). O provocare cu un impact extrem de mare pentru aceste sisteme este reprezentat de implementarea noilor tehnologii I2 şi integrarea acestora cu cele vechi, pentru ca acestea să poată funcționa concomitent.Un exemplu în acest sens este reprezentat de situația din Angola, în care Guvernul a înregistrat în baza de date națională aproximativ 7,5 milioane de cetățeni. Existând deja o bază de date biometrice a cetățenilor şi un sistem funcțional de analiză a datelor, integrarea noilor tehnologii care ar permite o capacitate mai bună de analiză prin găsirea de noi algoritmi de identificare trebuie realizată într-o manieră care să nu afecteze datele şi să fie în continuare operabilă utilizând vechile sisteme informatice.[20]

În planul interoperabilității, problemele sunt cauzate de diversitatea producătorilor de echipamente de procesare a datelor biometrice care se regăsesc pe piața liberă. Chiar dacă aplică acelaşi standard ISO de producție, fiecare producător utilizează modele diferite de tehnologii, care se concretizează în aplicații de diferite formate. În acest caz, autoritățile australiene oferă un bun exemplu deoarece au introdus *modelul invizibil* de identitate, care posedă elemente comune de încărcare a datelor, permițând astfel introducerea în baza de date națională a oricărui format de date. Totodată, Australia a introdus şi un sistem de identificare multi-modal care permite realizarea potrivirii cu o acuratețe ridicată, deoarece utilizează în comparare recunoaşterea facială, scanarea irisului şi analiza ADN.

În sfera analitică, principala provocare este reprezentată nu de modul în care se face analiza, ci de dezvoltarea de algoritmi de identificare în cazulapariției unor situații anormale[21]. Un exemplu privind utilizarea unor astfel de algoritmi este oferit de sistemul de supraveghere al persoanelor din aeroporturile din Australia. Capabilitatea care poartă numele de monitorizarea fluxurilor de persoane în cadrul unui context (Context-sensitive Workflows) realizează potrivirea între datele biometrice şi cele biografice pentru a determina identitatea unui individ, apoi determină contextul în care acesta se află şi realizează recomandări cu privire la măsurile şi acțiunile ce trebuie luate în ceea ce priveşte individul. Capabilitatea utilizează analiza avansată a datelor, alături de inteligență artificială în procesul analitic de I2.[22]

La nivelul NATO s-a concluzionat faptul că în procesele de analiză a sistemului de sisteme (System of SystemsAnalysis - SOSA) sau a sistemelor de ținte (Target SystemsAnalysis - TSA) au apărut probleme referitoare la standardizarea şi interoperabilitatea necesară NATO cu privire la înțelegerea, influențarea şi producerea de efecte asupra rețelelor umane, de-a lungul întregului spectru de amenințări şi la toate nivelurile de conflict.

Concluzii

Analiza I2 poate fi utilizată în rezolvarea oricărei cerințe de informații care implică actori precum lideri militari, constructori de dispozitive explozive improvizate, cercetători, oameni de ştiință, proliferatori, piraţi, traficanţi de armament, hackeri, terorişti, insurgenţi etc.[23]

Prin fuzionarea proceselor de analiză din cadrul NATO, Alianța va fi pregătită să:

- reducă sau înlăture gradul de anonimat al amenințărilor;
- furnizeze forțelor NATO identificări pozitive, rezoluții şi capacitatea de a rezolva conflictele de date legate de identitate;
- sprijine protecția forței prin identificarea încercărilor adversarilor de a utiliza identități false pentru a obține accesul în bazele şi unitățile NATO.

În scopul dezvoltării capabilităților de fuzionare a informațiilor şi partajare a acestora în rândul organizațiilor militare de informații şi securitate, este necesară înglobarea acestora într-un concept unic integrator. Instituțiile şi organismele militare şi civile care pot duce capabilitatea I2 la nivelul la care să deservească nevoile comune de securitate şi siguranță sunt: Organizația Internațională de Poliție Criminală -

International Criminal Police Organization (INTERPOL), NATO, Organizaţia pentru Securitate şi Cooperare în Europa (OSCE) şi Agenţia Europeană pentru Poliţia de Frontieră şi Garda de Coastă - FRONTEX. De asemenea, Comandamentul Armatei SUA pentru Europa (*United StatesArmy European Command* - EUCOM) are principalul rol în acordarea de asistenţă în vederea dezvoltării capabilităţii pe linia informaţiilor militare. Actualmente, la nivelul statelor membre ale NATO, agenţii precum *The National Ground Intelligence Center* (NGIC), *DefenseForensicsandBiometrics Agency*(DFBA) şi *FBI'sNextGenerationIden tification* (NGI) ale SUA deţin cea mai vastă cunoaştere în domeniul I2[24].

La momentul actual, conceptul I2 se află încă într-o fază incipientă. Din cauza sensibilităţii domeniului şi a diversităţii accepţiunilor şi limitărilor operaţionale ale statelor membre, demersurile în vederea implementării şi angajării acestuia în operaţii este încetinit de limitări legale şi dificultăţi care vizează interoperabilitatea sistemelor. Analiza I2 este utilizată pentru a combate vectorii de ameninţare anonimă prin identificarea potenţialilor agresori la adresa forţelor NATO (prin componenta de identificare biometrică) şi prin relevarea rolurilor acestora în cadrul organizaţiilor şi legăturilor existente între aceştia (prin componenta de analiză a reţelelor umane). Astfel, I2 oferă Alianţei mijloacele necesare atât pentru a evalua şi recomanda ţinte, cât şi pentru a identifica potenţiale cursuri de acţiune pentru abordarea corectă a acestora, în funcţie de statutul lor, pentru a obţine un grad maxim de eficienţă.

La nivelul României, domeniul I2 se află în faza de dezvoltare a capabilităţilor. Prin intermediul dialogului dintre instituţiile cu atribuţii în domeniul apărării naţionale, securităţii şi siguranţei naţionale (Ministerul Apărării Naţionale, Serviciul de Informaţii Externe, Serviciul Român de Informaţii, Ministerul Afacerilor Interne), România face paşi în direcţia punerii în practică a deciziilor asumate în cadrul Summit-ului NATO de la Bruxelles (11-12 iulie 2018), în care statele membre au agreat politica privind datele biometrice, care, în concordanţă cu legile naţionale şi normele internaţionale aplicabile şi sub rezerva cerinţelor şi restricţiilor naţionale, va susţine în continuare abilitatea aliaţilor de identificare a luptătorilor teroriştişi a altor vectori de ameninţare, precum şi de a respecta Rezoluţia nr.2396 a Consiliului de Securitate al ONU. Un aspect de interes care presupune ca instituţiile române să accelereze dezvoltarea capabilităţii I2 este reprezentat de iniţiativa de politică externă pe care România a lansat-o în anul 2015 referitoare la înfiinţarea Curţii Internaţionale împotriva Terorismului[25], o iniţiativă care, pentru a fi pusă în practică şi a avea rezultate, are nevoie de dezvoltarea capabilităţilor de reducere a gradului anonimităţii a vectorilor umani de ameninţare.

Aşadar, răspunsul la întrebarea „Cine?" este unul complex, care presupune, aşa cum ne arată dezvoltarea domeniului, nu doar identitatea, ci şi acţiunile individului, în mod individual sau în cadrul unui grup, necesitând o cunoaştere aprofundată a domeniilor sociologiei şi psihologiei sociale. Totodată, din perspectivă organizaţională, dezvoltarea domeniului I2 presupune o cooperare strânsăîntre organizaţiile militare, de securitate, siguranţă şi informaţii, pe bază de acorduri şi programe de cooperare, concretizate în acţiuni comune, baze de date şi platforme de schimb de date şi informaţii.

Bibliografie:

1. STRICKLAND B., *The Gale Encyclopedia of Psychology,* ediţia a 2-a. Ed. Gale Group, Farmington Hills, 2001;
2. ZAMFIR C., Vlăsceanu L., *Dicţionar de sociologie*, Ed. Babei, Bucureşti, 1998;
3. ERIKSON Erik, *Adolescence et crise. La quete de i'dentite*, trad. fr. Paris, Flamarion, 1972, preluat de Gilles Ferreol, Cauche P., Duprez N.G., Simon M., *Dicţionar de sociologie*, editura Polirom, Iaşi, 1998;
4. HOGG, M., *Social IdentityandtheSovereignty of theGoup: A Psychology of Belonging*, în Sedikides, C., Brewer M. [eds.], 154 Individual Self, Relational Self and Collective Self, Ed. Psychology Press, Philadelphia, 2001;

5. SCÂRNECI F., *Introducere în sociologia identității*, Ed. Universității Transilvania din Braşov, 2009;
6. ANDREI,Elena Adelina, *Secrete interconectate. Analiza rețelelor sociale*, 22 decembrie 2016, online la https://intelligence.sri.ro/legaturi-periculoase/ accesat la 10.04.2019
7. LAKSHMI, Ashok, *Move Over Sci-Fi, Identity Intelligence Is Going Mainstream*, 24.04.2018, online la http://blogs.unisys.com/onpoint/move-over-sci-fi-identity-intelligence-is-going-mainstream/, accesat la 12.04.2019;
8. LAKSHMI,Ashok, interviu realizat de Tom Temin la data de 28.01.2019, online la https://federalnewsnetwork.com/voices-of-government-it/2019/01/turn-biometrics-into-full-identity-intelligence/ accesat la data de 10.04.2019;
9. MORRIS, Victor R., *Identity and Biometrics Enabled Intelligence (BEI) Sharing for TransnationalThreatActors*, online la https://smallwarsjournal.com/jrnl/art/identity-and-biometrics-enabled-intelligence-bei-sharing-for-transnational-threat-actors accesat la 14.04.2019;
10. *Manualulde planificare a operațiilor în Armata României*, Statul Major General, Bucureşti 2011;
11. *Manualul de combatere a amenințării* anonime – AIntP-15,Ed. A, versiunea 1, 2015;
12. JointPublication 2-01.3 *Joint Intelligence Preparation of theOperationalEnvironment*, US Chefs of Staff, Washington, 2014;
13. Joint Doctrine Note 2-16, *IdentityActivities*, US JointChiefs of Staff, august 2016;
14. *NATO Concept for Identity Intelligence (I2)*, IMSWM-0272-2017, 26 May 17;
15. *SeriousAndOrganized Crime ThreatAssessment 2017*, online la www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017;
16. *Europol Analysis Projects*, online la www.europol.europa.eu/crime-areas-trends/europol-analysis-projects;
17. Kimery Anthony, USSOCOM, *Army Look toBiometrics Industry For New Techologies for SOF oftheFuture,* online la www.biometricupdate.com/201811/ussocom-army-look-to-biometrics-industry-for-new-techologies-for-sof-of-the-future;
18. *Dosare de actualitate pentru Ministerul Afacerilor Externe* online la www.mae.ro/taxonomy/term/491/1.

[1] Zamfir C., Vlăsceanu L., *Dicționar de sociologie*, Ed. Babei, Bucureşti, 1998, p.550.
[2] Erikson Erik, *Adolescence et crise. La queted'identite*, trad. fr. Paris, Flamarion, 1972, preluat de Gilles Ferreol, Cauche P., Duprez N.G., Simon M., *Dicționar de sociologie*, editura Polirom, Iaşi, 1998, p.85.
[3] Ibidem.
[4] Strickland B., *The Gale Encyclopedia of Psychology*, ediția a 2-a. Ed. Gale Group, Farmington Hills 2001, p. 229.
[5] Hogg, M., 2001, *Social Identity and the Sovereignty of the Goup: A Psychology of Belonging*, în Sedikides, C., Brewer M., 154 *Individual Self, Relational Self and Collective Self*, Psychology Press, Philadelphia, preluat de Scârneci F., *Introducere în sociologia identității*, Ed. Universității Transilvania din Braşov, 2009, p. 34.
[6] Strickland B., *The Gale Encyclopedia of Psychology*, ediția a 2-a. Ed. Gale Group, Farmington Hills 2001, p. 605;
[7] Zamfir C., Vlăsceanu L., *Dicționar de sociologie*, Ed. Babei, Bucureşti, 1998, p. 550.
[8] Potrivit *Manualului de planificare a operațiilor*, Statul Major General, Bucureşti 2011, p. 115, teatrul de operații - TO reprezintă un spațiu, definit la nivel politico-militar, în care se desfăşoară/sprijină acțiuni militare/operații, care poate fi împărțit într-una sau mai multe Zone de operații întrunite. TO au în general o suprafață apreciabilă, permițând desfăşurarea operațiilor în adâncime, la contact şi în spate, pe parcursul unei perioade extinse de timp.
[9] *NATO Concept for Identity Intelligence (I2),*IMSWM-0272-2017, 26 May 17, p. 2.
[10] *Manualul de combatere a amenințării anonime* – AIntP-15 Ediția A, versiunea 1, 2015, p. 15.
[11] Andrei Elena Adelina, *Secrete interconectate. Analiza rețelelor sociale*, 22 decembrie 2016, online la https://intelligence.sri.ro/legaturi-periculoase/ accesat la 10.04.2019.
[12] *Joint Doctrine Note 2-16*,*IdentityActivities*, US JointChiefs of Staff, august 2016, p.11;
[13] Ibidem 16, p.129;
[14] Ibidem 12, p. 31.

[15] Joint Publication 2-01.3 *Joint Intelligence Preparation of the Operational Environment*, US Chiefs of Staff, Washington, 2014, p. 41.
[16] *Manualul de combatere a ameninţării anonime – AIntP-15*, 2015, p. 77.
[17] Kimery Anthony, USSOCCOM, *Army Look toBiometrics Industry For New Techologiesfor SOF of The Future* online la www.biometricupdate.com/201811/ussocom-army-look-to-biometrics-industry-for-new-techologies-for-sof-of-the-future.
[18] LakshmiAshok, interviu realizat de Tom Temin la data de 28.01.2019, online la https://federalnewsnetwork.com/voices-of-government-it/2019/01/turn-biometrics-into-full-identity-intelligence/ accesat la data de 10.04.2019.
[19] *NATO Concept for Identity Intelligence (I2),* IMSWM-0272-2017, 26 May 17, p. 10.
[20] Ibidem 21.
[21] Ibidem 21.
[22] LakshmiAshok, *Move Over Sci-Fi, Identity Intelligence IsGoingMainstream*, 24.04.2018, online la http://blogs.unisys.com/onpoint/move-over-sci-fi-identity-intelligence-is-going-mainstream/ accesat la 12.04.2019.
[23] *NATO Concept for Identity Intelligence (I2)*, IMSWM-0272-2017, 26 May 17, p. 10.
[24] Morris, Victor R.,*IdentityandBiometricsEnabled Intelligence (BEI) Sharing for TransnationalThreatActors*, online la https://smallwarsjournal.com/jrnl/art/identity-and-biometrics-enabled-intelligence-bei-sharing-for-transnational-threat-actors accesat la 14.04.2019.
[25] *Dosare de actualitate pentru Ministerul Afacerilor Externe* online la www.mae.ro/taxonomy/term/491/1, accesat în 10.04.2019.