Anul X nr. 3/2018

# INFOSFERA

## Revistă de studii de securitate şi informaţii pentru apărare

**Revistă cu prestigiu ştiinţific
recunoscut de Consiliul Naţional de Atestare a Titlurilor, Diplomelor
şi Certificatelor Universitare (CNATDCU), indexată în bazele de date
internaţionale EBSCO şi CEEOL**

**Direcţia Generală de Informaţii a Apărării**

# CUPRINS

# MESAJUL ŞEFULUI STATULUI MAJOR AL APĂRĂRII CU OCAZIA ANIVERSĂRII A 159 DE ANI DE INFORMAȚII MILITARE

***General Nicolae-Ionel CIUCĂ,***
***Şeful Statului Major al Apărării***

*Pe 12 noiembrie 2018 sărbătorim 159 de ani de la semnarea, de către domnitorul Alexandru Ioan Cuza, a actului de constituire a Corpului de Stat Major al Armatei Principatelor Unite, în cadrul căruia un rol important îl avea Serviciul de informații militare.*

*De la înființarea sa, Serviciul de informații militare s-a transformat, adaptat şi modernizat, odată cu Armata României, pentru a răspunde deziderateloor naționale de securitate şi dezvoltare, îndeplinindu-şi întotdeauna sarcinile cu responsabilitate şi profesionalism.*

*Misiunea sa principală, de furnizare a informației relevante şi oportune pentru fundamentarea deciziilor politico-militare şi militare în domeniul securității naționale şi pentru evitarea surprinderii strategice, a fost întotdeauna îndeplinită cu succes. În spatele acestui succes, stau militari şi civili pentru care excelența în activitate reprezintă un fapt profesional cotidian.*

*Pentru a susține afirmația de mai sus, am să mă refer, pe scurt, la istoria recentă, marcată de transformări esențiale ale Armatei României.*

*Accederea în NATO şi UE a fost posibilă şi datorită muncii asidue, pe tărâmul diplomației militare, a ataşaților apărării care, cu abnegație şi determinare, au promovat aspirațiile României de a fi parte a unor alianțe cu care împărtăşeam acelaşi sistem de valori. Ulterior, după primirea în structurile amintite, efortul ataşaților apărării a continuat, pentru a furniza informațiile necesare transformării rapide a Armatei României şi ridicarea la standardele de profesionalism ale NATO, pentru realizarea interoperabilității cu noii parteneri şi promovarea intereselor naționale.*

*Prin numărul, amploarea şi calitatea misiunilor desfăşurate, Direcția informații militare (DIM) a contribuit, alături de camarazii din celelalte categorii de forțe ale Armatei, la consolidarea statutului României de partener serios, competent şi credibil în cadrul Alianței Nord-Atlantice şi al Uniunii Europene, cu un aport remarcabil la buna îndeplinire a misiunilor de menținere a păcii şi de luptă împotriva terorismului.*

*Istoria recentă a consemnat şi o serie de crize care au avut un impact major asupra securității regionale şi globale, situații care au însemnat tot atâtea provocări pentru Direcția informații militare. Războaiele din Balcani şi secesiunile violente din spațiul fostei Uniuni*

*Sovietice ar fi putut altera semnificativ securitatea României, fără aportul informativ esențial al DIM. Activitatea personalului acestei unități de elită, atât în perioadele pre-conflict, conflict, şi, apoi, de menținere a păcii, s-a ridicat la exigențele impuse de conducerea Ministerului Apărării Naționale, stabilitatea României fiind rezultatul firesc al acestor eforturi.*

*Un alt domeniu în care personalul DIM îşi demonstrează calitățile deosebite îl constituie executarea unor misiuni cu un grad de risc ridicat, de culegere şi prelucrare de date şi informații în sprijinul asigurării cu informații a contingentelor naționale şi multinaționale participante la acțiuni militare.*

*Rezultatele muncii, priceperii şi dăruirii militarilor din cadrul Direcției informații militare se regăsesc în aprecierile aliaților şi partenerilor noştri, primite pentru curajul, dăruirea şi profesionalismul desăvârşit cu care au fost şi sunt îndeplinite misiunile de luptă specifice acestor structuri în teatrele de operații.*

*Am convingerea că provocările actuale ale mediului de securitate, care includ atât crize clasice, prelungite, în proximitatea de est a României, regiunea Balcanilor, Orientul Mijlociu şi Nordul Africii, dar şi amenințări asimetrice precum terorismul, migrația ilegală şi atacurile cibernetice, vor fi întâmpinate şi contracarate eficient de către DIM, continuând astfel cu succes misiunea de apărare a României.*

*Cu prilejul aniversării a 159 de ani de existență, vă adresez felicitări şi mulțumiri pentru sacrificiile şi eforturile depuse în activitatea de mare răspundere şi importanță pe care o desfăşurați.*

*La mulți ani!*

*Cu deosebită considerație,*
***Şeful Statului Major al Apărării***
***General Nicolae-Ionel CIUCĂ***

# MESAJUL DIRECTORULUI GENERAL AL DGIA, CU PRILEJUL SĂRBĂTORIRII A 159 DE ANI DE LA ÎNFIINȚAREA PRIMEI STRUCTURI DE INFORMAȚII MILITARE

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

*În anul sărbătoririi Centenarului Marii Uniri, împlinirea a 159 de ani de informații militare se înscrie ca un eveniment important al devenirii Armatei Române şi Statului Român.*

*Reformele inițiate de domnitorul Alexandru Ioan Cuza după constituirea statului român modern, rezultat al Unirii Principatelor Române din 24 ianuarie 1859, au cuprins şi înființarea Secției a II-a, în cadrul Statului Major al Armatei Principatelor. Misiunile acestei noi secții, stabilite prin „Înalt Ordin de zi nr. 83", emis în data de 12 noiembrie 1859, includeau „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".*

*În continuare, structurile de informații militare, alături de întreaga armată, s-au remarcat printr-o contribuție semnificativă în momentele esențiale din trecutul României – Războiul de Independență, cele două războaie mondiale, aderarea la Alianța Nord-Atlantică şi la Uniunea Europeană, participarea la coaliții multinaționale în teatre de operații din Balcani, Orientul Mijlociu, Asia de Sud-Vest sau Africa.*

*Direcția informații militare a parcurs multiple transformări adaptative, în concordanță cu modificările mediului de securitate, regional şi global, şi, implicit, cu diversificarea şi amplificarea riscurilor şi amenințărilor la adresa securității naționale. Misiunea fundamentală, a direcției, aceea de a furniza informații de nivel strategic liderilor politico-militari, în scopul asigurării superiorității decizionale, a fost îndeplinită cu succes, contribuind la consolidarea imaginii de structură de elită a Direcției generale de informații a apărării şi a Armatei României.*

*Provocările mediului operațional au fost depăşite prin profesionalism şi dăruire, atât în domeniul diplomatic al ataşaturii apărării, cât şi în teatrele de operații din Kosovo, Bosnia, Irak sau Afganistan. Participarea cu experți în comandamentele NATO sau UE este unanim apreciată, aportul ofițerilor de informații români fiind recunoscut şi valorizat la nivelul partenerilor şi aliaților. Experiența acumulată în diverse domenii subsumate informațiilor militare a permis înființarea Centrului de excelență NATO în domeniul HUMINT în România, precum şi organizarea unor cursuri, pe diferite specialități, pentru parteneri din afara NATO şi UE.*

*Aflată permanent în căutarea şi identificarea celor mai eficiente mijloace care să-i permită obținerea informațiilor credibile şi oportune, Direcția informații militare continuă*

*să îşi perfecţioneze resursa umană şi să îşi modernizeze capabilităţile, în acord cu exigenţele NATO şi UE, cu progresul tehnologic global şi creşterea complexităţii ameninţărilor. Astfel, domeniile SIGINT, IMINT şi GEOINT, în mod deosebit, sunt în plină dezvoltare, obiectivul final fiind creşterea capacităţii de a furniza avertizări timpurii privind producerea unor evenimente cu impact major asupra securităţii României sau a aliaţilor, în proximitatea ţării noastre sau în zonele unde Armata României îşi desfăşoară activitatea.*

*Apreciez că pentru mine este un privilegiu să coordonez activitatea acestei structuri cu o înaltă ţinută morală şi profesională, fiind onorat să le adresez membrilor Direcţiei informaţii militare cele mai sincere mulţumiri şi succes în îndeplinirea misiunilor ce le revin!*

*Cu deosebită consideraţie,*

***Directorul General al Direcţiei generale de informaţii a apărării,***
***General Marian HĂPĂU***

# DIRECȚIA INFORMAȚII MILITARE – 159 DE ANI DE EXCELENȚĂ ÎN INFORMAȚII MILITARE

***General-maior Marian SIMA, Şeful Direcției informații militare***

*Direcția Informații Militare (DIM) este o unitate a Armatei care însoțeşte istoria acesteia încă din secolul XIX, în forme diferite, dar având mereu acelaşi scop: furnizarea informațiilor militare şi politico-militare relevante şi oportune pentru îndeplinirea tuturor misiunilor subscrise apărării naționale şi angajamentelor asumate la nivel internațional.*

*Înființarea, la 12 noiembrie 1859, prin „Înalt Ordin de Zi nr. 83", a Secției a II-a din cadrul Statului Major al Armatei Principatelor Unite, de către domnitorul Alexandru Ioan Cuza, rămâne actul major de voință prin care Direcția informații militare şi-a început activitatea.*

*Anul 2018 are multiple semnificații pentru structura pe care o reprezint, astfel: ne alăturăm tuturor românilor care aniversează Centenarul Marii Uniri, sărbătorim 159 de ani de la înființarea primei structuri de informații militare din Armata României şi 14 ani de informații militare în cadrul NATO.*

*Experiența dobândită de Direcția informații militare de-a lungul existenței sale este reflectată astăzi prin maturitatea acestei instituții şi responsabilitatea sa în misiunile pe care le îndeplineşte, contribuind la afirmarea României drept un partener serios, competent şi credibil în cadrul Alianței Nord-Atlantice şi Uniunii Europene, cu o contribuție recunoscută la îndeplinirea cu succes a misiunilor de menținere a păcii şi de luptă împotriva terorismului.*

*Evoluțiile politice şi de securitate din istoria recentă, din proximitatea strategică a României, subliniază postura statului român de pol de stabilitate regională şi de furnizor de securitate. Lărgirea spectrului de riscuri neconvenționale, cu caracter transnațional şi terorist, precum şi diversificarea tipologiei crizelor şi a conflictelor generează provocări multiple, care necesită reacții multidirecționale, bazate pe mobilitate, oportunitate, diversitate, coerență şi complementaritate.*

*Astfel, aportul serviciului de informații militare devine o necesitate obiectivă în cadrul Ministerului Apărării Naționale şi a sistemului național de securitate, sprijinind totalitatea demersurilor militare şi politico-militare la nivel strategic.*

*În actualul context internațional de securitate, compex şi impredictibil, Direcției informații militare îi revine rolul de a reprezenta una dintre instituțiile cheie, responsabile de asigurarea prevenirii surprinderii strategice militare la nivelul sistemului securității naționale.*

*Direcția informații militare, prin structurile sale şi prin unitățile subordonate operațional, adaptate standardelor euroatlantice, a devenit o instituție care asigură, prin intermediul dispozitivului ataşaturii apărării, reprezentarea diplomatică militară a structurilor Ministerului Apărării Naționale în relația cu alte state. De asemenea, aceasta este autoritate națională în ceea ce priveşte capabilitățile SIGINT şi de război electronic şi administrează*

*sistemul NATO privind culegerea şi exploatarea câmpului de luptă (Battlefield Intelligence Collection and Exploitation System – BICES).*

*Efortul Direcţiei informaţii militare, în cadrul misiunilor şi activităţilor curente ale Alianţei, se concretizează în contribuţia cu experţi la nivelul comandamentelor NATO, în cadrul cărora ofiţeri ai Direcţiei ocupă funcţii de mare responsabilitate. De asemenea, printr-un flux continuu cu produse de informaţii, conform priorităţilor şi cerinţelor informative aliate, România se află între primele patru naţiuni care, prin informaţiile oferite, au contribuit la fundamentarea deciziilor la nivelul Alianţei, având în atenţie evoluţia situaţiilor regionale (inclusiv din Orientul Mijlociu) şi a evenimentelor care influenţează nemijlocit mediul de securitate al ţării noastre.*

*Prezenţa, pe linia informaţiilor militare, în majoritatea comandamentelor NATO şi în Direcţia informaţii a Statului Major Militar Internaţional al UE (unde DIM se află între primele trei structuri contributoare cu produse de informaţii), ne permite să rămânem conectaţi şi să avem un comportament pro-activ, în acest domeniu, în relaţia cu ambele organizaţii internaţionale. Această prezenţă ne asigură nu numai vizibilitate şi recunoaştere în cadrul NATO şi UE, dar şi relevanţă ca suport decizional la nivel politico-militar.*

*În aceeaşi notă, sunt obligat să subliniez efortul constant şi rezultatele deosebite obţinute în urma participării cu forţe şi capabilităţi de informaţii la operaţii în afara teritoriului statului român, desfăşurate sub egida NATO, UE, forţe de coaliţie şi iniţiative regionale. Beneficiind de expertiza acumulată, am reuşit să încadrăm poziţii din ce în ce mai importante în cadrul comandamentelor acestor misiuni internaţionale. În acelaşi timp, Direcţia informaţii militare şi-a îndeplinit obiectivele prin furnizarea de informaţii relevante şi acţionabile în vederea realizării protecţiei forţei pentru structurile din teatrele de operaţii din Balcani şi Afganistan.*

*Prin activităţi specifice pentru conducerea şi coordonarea personalului şi structurilor de informaţii, serviciul de informaţii militare operează permanent modificările care se impun în arhitectura sa de informaţii, în funcţie de evoluţia mediului de securitate.*

*În prezent, Direcţia informaţii militare reprezintă expresia schimbărilor succesive survenite în cadrul procesului de reformă al Armatei României, imaginea unui sistem modern, în continuă evoluţie, care, prin întreaga activitate, răspunde cerinţelor de securitate şi apărare naţională.*

*Este de datoria mea şi a celor care, în viitor, vor fi liderii acestei structuri, să demonstreze faptul că Direcţia informaţii militare, în amplul proces de transformare şi modernizare a Armatei României, va continua să coordoneze eficient activitatea de informaţii, supraveghere şi cercetare, ca structură de tip ISR, şi va integra structurile de informaţii militare, unităţile şi subunităţile de cercetare într-un sistem unitar, coerent şi profesionist, care să asigure comandanţilor un suport viabil şi realist pentru fundamentarea deciziilor la toate nivelurile.*

*În încheiere, aş dori să adresez mulţumirile mele liderilor Ministerului Apărării Naţionale, Direcţiei generale de informaţii a apărării şi Statului Major al Apărării pentru sprijinul competent şi continuu în desfăşurarea activităţilor DIM, precum şi profesioniştilor acestei structuri de elită care îşi îndeplinesc misiunile în condiţii complexe, dedicându-şi viaţa unui scop mai presus de interesele personale – securitatea României şi a cetăţenilor ei.*

*La mulţi ani!*

***Şeful Direcţiei informaţii militare,***
***General-maior Marian SIMA***

Direcția generală de informații a apărării

# INFOSFERA, anul X, nr. 3, 2018

## Revistă de studii de securitate şi informații pentru apărare

# CONSIDERAȚII GENERALE PRIVIND EVOLUȚIA PE TERMEN LUNG A MEDIULUI DE SECURITATE GLOBAL

***Gabriel ANGHEL***
***Ciprian ANTONESCU*** *

***Abstract***

*The main goal of characterizing the future global and regional security environment is to support political and military decision-makers in developing defense policies and establishing capability acquisition plans as well as force structure design. The analytical method used to predict the main characteristics of the future security environment is Predictive Analysis. In principle, the method consists in identifying the core trends of the domains that influence most the security environment – political, technological, economical, and social – and developing specific scenarios.*

*On the political domain, the on-going process of power transfer from the Euro-Atlantic sphere to the Asian emerging economies as well as the increasingly importance of non-state actors in state's governments have been identified as the main trends. Regarding the technological domain, the extraordinary development of disruptive technologies such as Artificial Intelligence, additive manufacturing, robotics, nanotechnology and biotechnology will have a critical impact on the security environment over the next decades. On the economical domain, the current tendencies of advancing commercial protectionist measures together with the emergence of new manufacturing technologies will pose a serious challenge to the globalization process. Also, the current social trends – urbanization, irregular migration, ageing population in developed countries – will continue to pose a significant challenges to the security environment on medium and long term.*

***Keywords****: global security environment, social systems, predictive analysis, methodology, enthropy, energy, geopolitics, technology, economies, social.*

În ultimii ani, caracteristica determinantă a mediului de securitate la nivel global a fost reprezentată de **accentuarea instabilității, incertitudinii şi complexității**, tendință care, probabil, se va menține şi pentru următorii 15-20 de ani. Procesele care determină mediul de securitate la nivel global se manifestă în domenii multiple - geopolitic, tehnologic, economic şi social - şi sunt puternic interconectate. Principalele direcții de evoluție în domeniile menționate, care vor influența mediul de securitate pe termen lung, sunt: transferul parțial al puterii de la spațiul euroatlantic la cel asiatic, încheierea epocii industriale şi trecerea către era digitală, intensificarea măsurilor protecționiste şi erodarea/transformarea procesului de globalizare, respectiv factorul demografic caracterizat de distribuția spațială asimetrică a populației.

Este un truism faptul că într-o lume caracterizată de competitivitate, conectivitate şi complexitate, important este nu numai să răspundem provocărilor de securitate actuale, ci, mai ales, să anticipăm ceea ce viitorul ne poate aduce. Analiza mediului de securitate pe termen lung, instrument care vine în sprijinul decidenților politici şi militari cu responsabilități

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

în dezvoltarea politicilor de apărare, proiecția capabilităților şi a structurii de forțe, presupune două aspecte: (1) prezentarea descriptivă a unui context strategic care, ulterior, va contribui la caracterizarea mediului operațional al viitorului şi (2) identificarea amenințărilor şi oportunităților posibile, rezultat al unei analize riguroase a direcțiilor principale de evoluție în domeniile cu impact major asupra securității.

**Analiza prospectivă – considerații generale**

Descrierea caracteristicilor esențiale ale mediului de securitate pe termen lung se realizează prin utilizarea unor metodologii specifice analizei prospective. Spre deosebire de analiza de informații pe termen scurt şi mediu, care estimează starea viitoare a unui sistem luând în considerare o evoluție inerțială a acestuia, exprimată cu ajutorul unui vocabular probabilistic specific, **analiza prospectivă îşi propune caracterizarea posibilelor stări finale** ale unui sistem, prin identificarea actualelor şi potențialelor direcții de evoluție în domenii critice.

În general, estimarea pe termen scurt a stării viitoare a unui sistem se face prin extrapolare, definită în acest context ca procesul prin care analiza se realizează pe baza **observațiilor stărilor anterioare** (analiza evenimentelor din trecut, Fig. 1.a), **fără a se modifica forțele care acționează asupra sistemului**[1]. Prin comparație, analiza prospectivă este un proces mult mai complex, metodologiile specifice luând în calcul problematica abordărilor teoretice analitice pentru perioada de tranziție a sistemului de la starea inițială A la starea finală B. Din cauza

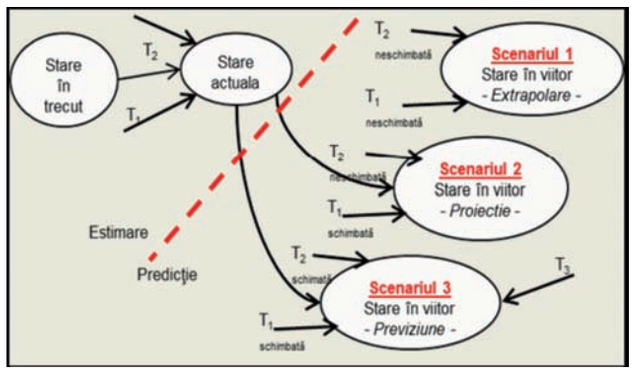



***Fig. 1.a – Prezentarea schematică a metodei de analiză prospectivă***

intervalului de timp mare, precum şi a numărului semnificativ al variabilelor care influențează evoluția sistemului, **evoluția de tip inerțial nu mai corespunde realității**.

Din această perspectivă, mulți cercetători în domeniul analizei de informații au teoretizat analiza prospectivă pornind de la echivalența sistemelor fizice şi a celor sociale, în ceea ce priveşte evoluția acestora. Astfel, se consideră că determinarea stării unui sistem social poate fi estimată prin analiza comportamentelor părților componente, aplicându-se în acelaşi timp conceptele extinse de *energie* şi *entropie*, ca măsură a gradului de ordine/dezordine a sistemului[2]. Pe cale de consecință, aplicarea legii a II-a a termodinamicii[3] în analiza prospectivă conduce la concluzia existenței, în timp, a unor **puncte de inflexiune** în care comportamentul sistemului social este puternic instabil şi impredictibil (fig. 1.b).

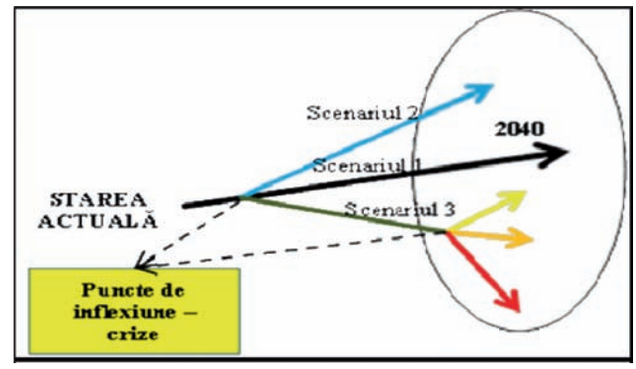



***Fig. 1.b – Existența punctelor de inflexiune care corespund potențialelor situații de criză***

În aceste puncte, entropia sistemului poate fi, teoretic, redusă prin modificarea tendințelor actuale şi/sau prin manifestarea unor noi tendințe. Din acest motiv, analiştii trebuie să aibă capacitatea unei înțelegeri multisciplinare (geopolitică, tehnică, economică, socială) a problematicii studiate[4].

Un alt aspect extrem de important al analizei prospective îl reprezintă identificarea fenomenelor convergente, teoretic posibil predictibile, şi a celor divergente. În acest sens, fenomenele convergente sunt consecințe ale relației de cauzalitate, care exprimă, de asemenea, unul dintre principiile de bază ale fizicii clasice[5]. Prin contrast, fenomenele divergente, asupra cărora este aproape imposibilă

formularea unei predicții comportamentale, nu sunt guvernate de legea cauzalității, ci de cea a probabilității. În general, fenomenele asociate fizicii cuantice sunt divergente. Un exemplu de fenomen/ eveniment divergent este „lovitura de stat".

Metoda de analiză prospectivă, utilizată pentru caracterizarea mediului de securitate pe termen lung, presupune următoarele etape[6]:

- **determinarea stării curente a sistemului**, prin analiza datelor şi informațiilor deținute;
- **identificarea şi evaluarea tendințelor actuale** de dezvoltare în patru domenii critice (geopolitic, tehnologic, economic şi social) pentru mediul de securitate;
- **evaluarea modificărilor probabile,** în timp, a tendințelor identificate;
- **considerarea tendințelor noi**, probabil a se manifesta la un anumit moment în viitor;
- **elaborarea scenariilor** utilizând metoda extrapolării, proiecției şi previziunii.

În continuare, vom analiza principalele direcții de evoluție pentru patru domenii considerate a avea o influență majoră asupra mediului de securitate.

**Direcții de evoluție geopolitică la nivel global**

Din punct de vedere geopolitic, actuala arhitectură instituțională a sistemului de securitate la nivel global, implementată după cel de-Al Doilea Război Mondial, este supusă unor transformări profunde şi permanente, generate de procese care au loc atât în relațiile interstatale - *transferul parțial al puterii la nivel global de la spațiul euroatlantic la cel euroasiatic*, cât şi în interiorul statelor - *difuzia actului de guvernare de la autorități către actori nonstatali*[7].

Procesul de redistribuire a puterii politice, economice şi militare este inițiat şi condus de puteri emergente (în principal China şi India) sau resurgente (F.Rusă) şi impune revenirea la un **sistem de relații internaționale caracterizat de competiția între marile puteri.**

Deşi instituțiile care formează arhitectura de securitate globală continuă să asigure un cadru formal pentru exprimarea politică la nivel internațional, **există încercări de diminuare a relevanței acestora atât din partea puterilor emergente, cât şi de către organizațiile politice sau de securitate alternative**, care se consideră marginalizate sau excluse din cadrul procesului de decizie la nivel global[8]. Acțiunea organizațiilor alternative este facilitată şi de inabilitatea instituțiilor la nivel global de a se adapta schimbărilor în curs, în special în ceea ce priveşte creşterea numărului actorilor internaționali relevanți şi a modului de interacțiune dintre aceştia.

Cel mai probabil, modelul actual de instituire a ordinii mondiale, bazat pe promovarea valorilor democrațiilor occidentale, îşi va diminua relevanța. În schimb, interesele geopolitice, economice şi militare ale **statelor** vor determina natura relațiilor internaționale. Această nouă realitate geopolitică va conduce la **regionalizarea problemelor de securitate**, respectiv identificarea unor arhitecturi de securitate regionale, garantate prin acorduri formale sau informale între marile puteri. De asemenea, revenirea la un sistem de relații internaționale caracterizat de **„Realpolitik"** va reduce relevanța principiului multilateralismului în favoarea relațiilor bilaterale sau în format multilateral restrâns, cu efecte directe asupra capacității statelor mici şi mijlocii de a-şi promova interesele naționale.

În ceea ce priveşte **creşterea rolului actorilor non-statali**, deşi pentru următorii 15-20 ani statul va rămâne actorul principal în relațiile internaționale, companiile private şi organizațiile neguvernamentale vor prelua asigurarea unor servicii de securitate aflate, în mod tradițional, în responsabillitatea autorităților guvernamentale (ex.: securitatea cibernetică). Transferul puterii interstatale de la structurile guvernamentale la actori non-statali benigni va avea efecte benefice, în principal prin creşterea transparenței actului de guvernare şi implicarea activă a societății civile în procesul decizional. Pe de altă parte, creşterea rolului actorilor non-statali maligni (organizații teroriste sau de crimă organizată) va genera consecințe negative asupra mediului de securitate.

**Direcții de evoluție geopolitică la nivel european**

Într-o viitoare ordine globală caracterizată de construcția triunghiulară SUA-China-F.Rusă, **UE ar putea reprezenta factorul decisiv al echilibrului sistemic**, dacă va reuşi să dezvolte suficient de articulat ambele dimensiuni (transatlantică şi eurasiatică), simultan cu gestionarea amenințărilor dimensiunii sudice.

Proiectul european este supus unor provocări geopolitice, economice, sociale şi de securitate generate atât de dinamica internă a Uniunii, cât şi de procesele la nivel global. Cele mai importante provocări de securitate sunt: resurgența politică şi militară a F.Ruse, terorismul, migrația ilegală, promovarea ideilor protecționiste şi a curentului iliberal, precum şi inegalitățile sociale şi economice. Atât transferul puterii la nivel global, cât şi posibila reversibilitate a globalizării vor influența, de asemenea, mediul de securitate din spațiul european. Efectele secundare ale proceselor menționate (creşterea naționalismului pe fondul delegitimării partidelor tradiționale fiind cel mai evident) pot genera schimbări importante în percepția statelor europene referitoare la amenințări şi riscuri de securitate. Pe fondul dezangajării selective a SUA, UE, cu sprijinul altor actori cu interese similare, precum şi al unor resurse financiare adecvate, s-ar putea angaja suplimentar în proiecte geopolitice şi economice globale – reimpulsionarea multilateralismului, ca principiu de guvernare la nivel global, reformarea şi revigorarea globalizării etc.

În plan regional, UE nu mai reprezintă singurul pol de atracție, alternativele fiind generate de resurgența forțelor iliberale în state precum F.Rusă şi Turcia. În acest context, pentru următorii 15-20 ani, stabilirea unor relații funcționale cu F.Rusă şi Turcia va deveni un obiectiv central al politicii externe a UE. În plan intern, prioritățile la nivelul Uniunii vor fi proiectele majore privind reforma structurilor de guvernare, gestionarea Brexit, migrația ilegală, creşterea relevanței în plan militar (planurile de creştere a cheltuielilor generate de asumarea unor responsabilități sporite în plan securitar, inclusiv în cadrul NATO).

În domeniul apărării, cadrul general al evoluțiilor anticipate vizează concentrarea eforturilor pe două direcții: (1) consolidarea conectivității industriei europene de apărare la evoluțiile dimensiunii de apărare, respectiv maturizarea profilului ambițios al Cooperării Structurate Permanente/PESCO, şi (2) consolidarea capacității operaționale a UE, centrată pe ideea posibilității de susținere a unui angajament militar într-o regiune de criză. Opțiunea pe care motorul franco-german a indicat că intenționează să orienteze PESCO vizează dezvoltarea de proiecte cu impact profund în definirea unui profil robust al apărării europene, respectiv dezvoltarea într-o matrice permanentă – teritorială a apărării europene, în spiritul scenariului avansat în cadrul procesului de reflecție.

Zona Balcanilor de Vest va continua să reprezinte o provocare de securitate pentru UE

***Analiză alternativă***

- Transferul puterii politice de la spațiul Euroatlantic la cel Eurasiatic poate fi stopat de evoluțiile din domeniile tehnologic şi economic, în special de progresele realizate în ceea ce priveşte Inteligența Artificială şi 3D printing, respectiv consolidarea tendințelor de reversibilitate a globalizării.
- Interesele comune în ceea ce priveşte continuarea procesului de globalizare pot determina convergența pe plan internațional a acțiunilor politice ale Chinei şi UE pentru menținerea sistemului economic liberal.

atât din cauza tensiunilor inter-etnice şi inter-confesionale remanente, a instabilităţii politice, a corupţiei în instituţiile guvernamentale, a proliferării reţelelor de crimă organizată, cât şi din cauza creşterii influenţei politice, economice şi militare a altor actori globali.

Ameninţările neconvenţionale din zona Orientului Mijlociu şi Nordul Africii (OMNA) vor continua să reprezinte o prioritate pentru securitatea spaţiului european. Deşi nu va deveni actorul principal în OMNA, foarte probabil UE se va implica alături de puterile regionale, SUA şi F.Rusă în scopul avansării proceselor politice de reglementare a crizelor.

**Direcţii de evoluţie în tehnologie**

Tehnologia va continua să modeleze structura societăţii umane atât din punct de vedere cultural, cât şi economic, la toate nivelurile acesteia. Direcţiile actuale de evoluţie în domeniul tehnologic constituie, în ansamblu, o revoluţie, în măsura în care acestea deschid perspective complet noi în ceea ce priveşte tiparele comportamentale la nivel individual şi colectiv, cu impact asupra mediului de securitate. Din această perspectivă, tehnologiile noi sau emergente oferă oportunităţi deosebite, dar, în acelaşi timp, prezintă noi vulnerabilităţi şi riscuri determinate de realităţile erei digitale spre care lumea se îndreaptă[9]. Într-un viitor previzibil, majoritatea inovaţiilor tehnologice actuale vor fi integrate în domeniul apărării, independent de gradul ameninţării. Pentru ca acest fapt să se materializeze vor fi necesare investiţii importante, cu consecinţe deloc neglijabile asupra bugetelor militare.

La ora actuală, schimbările majore care au loc în domeniul tehnologiei, în special în ceea ce priveşte viteza procesoarelor, inteligenţa artificială (IA)[10], imprimarea 3D, robotica, autonomia sistemelor, energia direcţionată, cyber, biotehnologia şi nanotehnologia, vor determina, pe termen lung, nivelul de competitivitate economică al statelor. Diferenţa cu care statele avansează în dezvoltarea/integrarea noilor tehnologii va determina **adâncirea decalajelor dintre statele dezvoltate şi cele în curs de dezvoltare**, cu repercusiuni asupra interoperabilităţii la nivel instituţional, inclusiv în domeniul securităţii. În acelaşi timp, producţia sistemelor relaţionate noilor tehnologii necesită o mare cantitate de materiale rare, ceea ce va determina apariţia unei competiţii reale pentru controlul acestor resurse. În plus, funcţionarea acestor sisteme necesită o cantitate mare de energie, cu implicaţii importante şi costisitoare asupra dezvoltării infrastructurii energetice[11].

***Fig. 2 – Operaţii în mediul urban (Sursa: Internet)***

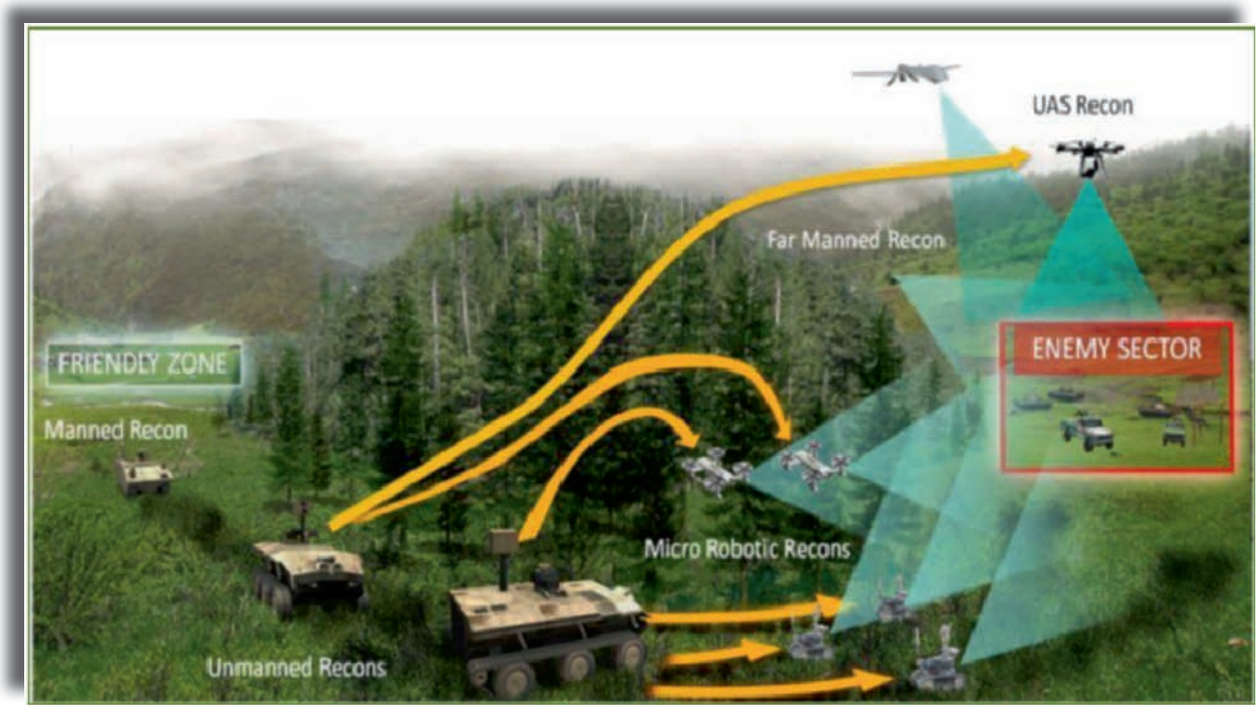



***Fig. 3 – Operaţii ISR (Sursa: Internet)***

De asemenea, modificarea formală a cadrului juridic şi adoptarea unor noi norme etice, care să ia în considerare influenţa noilor tehnologii digitale asupra vieţii sociale, vor deveni priorităţi imediate. Astfel, utilizarea de către structurile de forţă ale unui stat a sistemelor de armament letale sau neletale care încorporează IA va impune modificarea valorilor morale şi a principiilor etice larg acceptate de către societate, precum şi dezvoltarea politicilor, doctrinelor, regulamentelor şi procedurilor de angajare a respectivelor sisteme de armament.

Dintre toate domeniile noi sau emergente ale tehnologiei, foarte probabil impactul major asupra mediului de securitate îl vor avea IA şi cyber. Principiul fundamental al dezvoltării IA constă în capacitatea sistemelor/maşinilor de a identifica modele de acţiune/comportament, conform unor criterii şi algoritmi bine definiţi, prin analiza unui volum foarte mare de date. Acest proces necesită dezvoltarea bazelor de date, a infrastructurii necesare accesării şi evaluării informaţiilor stocate, precum şi a părţii mecanice corespunzătoare – robotica.

Dezvoltarea IA va influenţa semnificativ şi domeniul militar. Se estimează că noile generaţii de echipamente militare şi sisteme de armament vor încorpora IA, ceea ce va determina modificări importante în actualele doctrine şi concepte operaţionale de ducere a acţiunilor de luptă, în special în ceea ce priveşte funcţiunile C2 (comanda şi controlul), operaţiile ISR (fig. 3) şi cele de sprijin logistic (fig. 2)[12]. Aplicaţiile tehnologiei digitale în domeniul militar se vor concretiza, în principal, în dezvoltarea vehiculelor/sistemelor militare autonome[13] şi a roboţilor. Sistemele militare autonome cu IA încorporată vor îmbunătăţi abilitatea acestora de a opera independent în câmpul de luptă, vor eficientiza procesul de luare a deciziei de către comandanţi, prin analizarea unui volum foarte mare de date furnizate de senzorii din câmpul de luptă şi realizarea unei imagini integrate a acestuia, şi vor contribui la procesul de sincronizare a acţiunilor diferitelor sisteme de armament angajate. În acest context, obţinerea, evaluarea, utilizarea şi stocarea informaţiei în mediul operaţional devine o activitate esenţială a comandanţilor. Pe de altă parte, interconectarea echipamentelor militare şi a sistemelor de armament în mediul operaţional va genera vulnerabilităţi ale reţelelor digitale, care vor impune adoptarea de măsuri adecvate pentru protejarea acestora împotriva acţiunilor disruptive ale adversarului.

O caracteristică esenţială a dezvoltărilor în domeniul tehnologic o reprezintă interconectarea

***Analiză alternativă***

- În situația în care implementarea noilor tehnologii digitale în industria manufacturieră şi servicii nu va avea ca rezultat creşterea susținută a productivității muncii în statele dezvoltate, este posibilă declanşarea unei noi crize economice, cu efecte negative asupra mediului de securitate global.
- Tendințele de reversibilitate ale globalizării pot amplifica unele probleme sistemice ale economiei chineze (inexistența unei clase de mijloc puternice, dezvoltare insuficientă a zonelor rurale), ceea ce poate conduce la încetinirea semnificativă a ritmului de creştere economică a acestui stat, cu repercusiuni asupra creşterii economice globale.

globală a dispozitivelor digitale[14], ceea ce impune definirea unui nou domeniu operațional – domeniul cibernetic. Apariția noului tip de realitate virtuală, ca element intrinsec al vieții la nivel individual şi social, a avut o influență majoră în schimbarea caracteristicilor puterii. Acest spațiu virtual este relativ uşor de accesat de o gamă largă de actori, atât statali, cât şi nonstatali.

De asemenea, apariția mediului cyber a modificat paradigma arhitecturii de securitate constituită după cel de-al Doilea Război Mondial, în care cei mai importanți actori din sistem au preferat să mențină conflictul militar în afara granițelor naționale. În cazul mediului cibernetic, situația a suferit o schimbare majoră, întrucât realitatea ultimilor ani demonstrează că inclusiv statele puternice din punct de vedere militar pot fi lovite major pe teritoriul național de capabilitățile cibernetice ale adversarului. Din această perspectivă, în domeniul cibernetic capacitățile ofensive şi cele defensive trebuie dezvoltate simultan pentru a putea constitui elemente de descurajare eficiente. În acelaşi timp, operațiile cibernetice împotriva infrastructurii critice naționale sau internaționale pot determina răspunsuri de natură militară.

Caracterul descentralizat şi natura dispersată a punctelor de intrare/ieşire ale mediului cibernetic se vor menține şi în viitor, ceea ce va defini vulnerabilitățile acestuia. Deşi infrastructura mediului cibernetic este, de obicei, localizată pe teritoriile unor state suverane, în special infrastructura de stocare a informațiilor, controlul asupra acesteia este dificil de realizat. Dominația locală asupra infrastructurii cibernetice poate fi realizată temporar, însă dominația globală a acestui mediu nu poate fi realizată. În următorii 15 ani, provocările la adresa securității informațiilor şi a infrastructurii cibernetice vor creşte exponențial.

Din punct de vedere militar, **operațiile cibernetice şi cele de informații vor fi principalele activități în mediul operațional al viitorului**. Acestea nu vor fi executate independent, ci vor fi incluse în abordarea integrată, unitară, hibridă a campaniei militare. Integrarea capabilităților cibernetice în procesul de targeting va contribui, de asemenea, la postura generală de descurajare. Protecția şi reziliența la operații cibernetice vor fi esențiale, în condițiile în care sistemele militare vor deveni din ce în ce mai dependente de rețelele de informații, în special prin integrarea senzorilor, sistemelor de armament şi a sistemelor de comandă-control.

**Direcții de evoluție în domeniul economic**

Principala direcție de dezvoltare în domeniul economic, la nivel global, este transferul centrului de greutate din spațiul euroatlantic către cel asiatic. Estimările actuale poziționează China ca cea mai mare economie la nivel mondial în jurul anului 2026, devansând astfel SUA[15]. Foarte probabil, economia globală va avea pentru următorii 15-20 ani o rată de creştere anuală de aproximativ 3%,

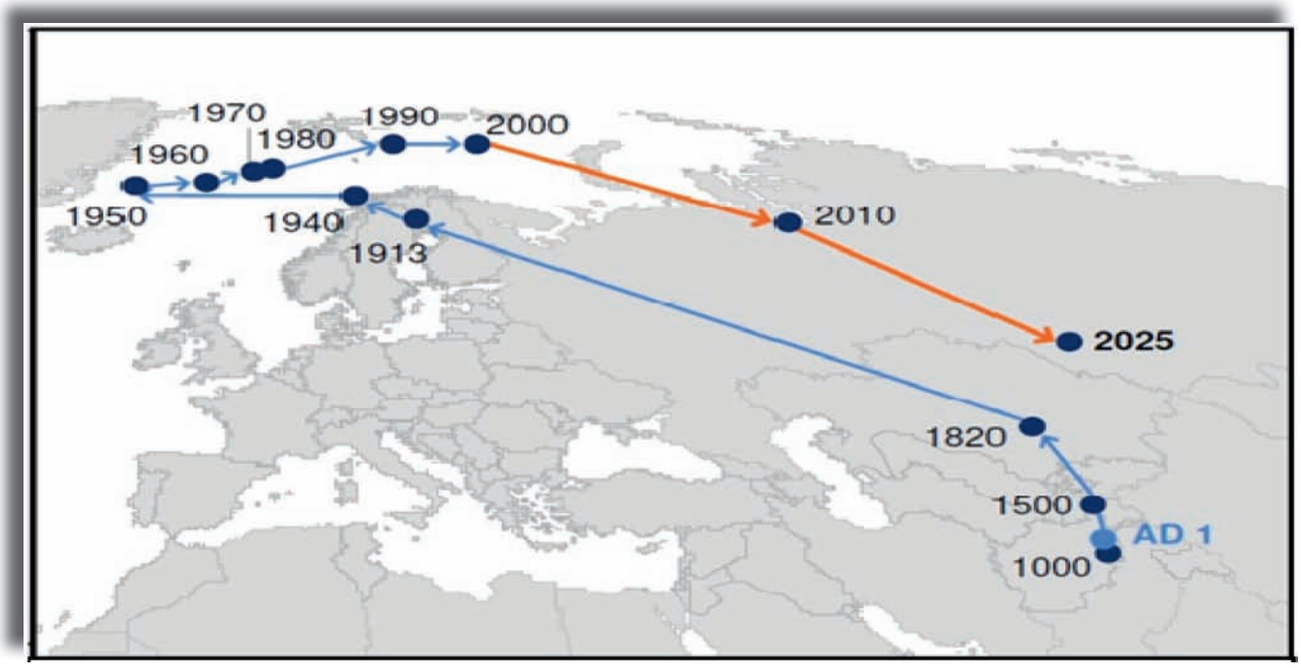



*Fig. 4 – Evoluția în timp a centrului de greutate al economiei globale*
*(Sursa: McKinsey Global Institute)*

cu o încetinire semnificativă în 2020 determinată de o reducere a creşterii economice în principalele economii emergente asiatice.

Din punct de vedere economic, procesul de globalizare a influențat decisiv mediul de securitate actual, prin deschiderea pieţelor, intensificarea integrării economice şi transferul industriilor manufacturiere din statele dezvoltate către regiuni cu productivitate mare a forței de muncă. La ora actuală, automatizarea proceselor de fabricaţie şi dezvoltarea curentului comercial protecționist determină o încetinire a globalizării. Automatizarea proceselor de producție va determina **revenirea industriilor manufacturiere în statele de origine** şi localizarea producției în apropierea pieţelor de desfacere, cu impact potențial negativ asupra dezvoltării statelor emergente. Impactul asupra statelor a căror creştere economică se bazează pe existența forței de muncă ieftine va fi direct; **forța de muncă ieftină nu va mai reprezenta un avantaj în competiția economică globală**. De asemenea, în noua paradigmă geopolitică a competiției între marile puteri, **accesul şi controlul resurselor naturale vor juca un rol important** în definirea mediului de securitate.

Un factor economic cu potențial impact negativ asupra mediului de securitate îl reprezintă creşterea la un nivel fără precedent a datoriei globale în toate sectoarele (guvernamental, corporatist şi privat), exprimată în procente din produsul intern brut (PIB)[16]. Conform Fondului Monetar Internațional, nivelul datoriei globale era în 2015 de 152 trilioane USD, superior celui înregistrat la începutul celei mai recente crize financiare (2007-2009). În plus, în ultimii 10 ani economiile majore nu au reuşit să reducă procentul datoriei raportat la PIB. Dacă tendința se va menține pe o perioadă îndelungată, este probabilă crearea unui efect de domino în pieţele financiare şi declanşarea unei crize financiare mult mai puternice comparativ cu cea din 2007-2008.

Creşterea interconectivităților sistemelor financiare la nivel mondial, deşi benefică sub aspect economic, va determina vulnerabilizarea acestora la atacuri cyber atât din partea actorilor statali, cât şi a celor non-statali. Pe de altă parte, interconexiunile economice şi financiare la nivel global reduc riscul declanşării unui conflict armat major între state. Deşi acest lucru este pozitiv în esență, el favorizează apariția acțiunilor de tip hibrid.

**Direcții de evoluție în domeniul social**

Principalele direcții de dezvoltare în domeniul social, care vor influența major mediul de securitate în urmatoarele decenii, sunt: evoluția demografică asimetrică, urbanizarea rapidă, polarizarea societăților, accentuarea fenomenului de îmbătrânire a populației, migrația.

Rata de creştere a populației în țările în curs de dezvoltare, în special pe continentul african şi în America Latină, va fi de peste 7 ori mai mare comparativ cu cea din țările dezvoltate[17]. Creşterea populației va determina intesificarea procesului de urbanizare, dar şi a migrației din motive economice. Astfel, se estimează că populația globului va fi de 8,5 miliarde în 2030 şi de 9,7 miliarde în 2050[18]. Pentru țările în curs de dezvoltare, existența unui segment important al societății format din populația tânără, cu oportunități reduse privind accesul la educație sau pe piața muncii, va cataliza nemulțumirile generale, facilitând apariția mişcărilor sociale.

În acelaşi timp, procesul de îmbătrânire a populației se va manifesta cu precădere în regiuni precum Europa, America de Nord, F.Rusă, Japonia şi China. Deşi, la ora actuală, cel mai mare procent al populației cu vârstă peste 60 ani, respectiv 25%, este în Europa, se estimează că, până în 2050, situația se va generaliza la nivel global, cu excepția Africii. În statele cu populație îmbătrânită cererea de resurse pentru sectorul medical şi al asigurărilor sociale va creşte, ceea ce va limita abilitatea autorităților de a aloca fonduri pentru sectoarele responsabile cu securitatea internă şi apărarea națională.

Polarizarea societăților pe motive ideologice, economice sau religioase va continua să reprezinte o sursă majoră de conflict. Cu toate că fenomenul se manifestă la scară globală, societățile vestice sunt în mod deosebit vulnerabile din cauza culturii şi sistemului politic specific democrațiilor de tip occidental, care recunosc individul şi drepturile acestuia ca valori fundamentale în organizarea socială. Indiferent de aria în care se manifestă polarizarea, numitorul comun îl reprezintă interesele diferite şi divergente ale indivizilor din societatea respectivă. În timp, polarizarea poate conduce la pierderea coeziunii sociale, cu efecte importante asupra mediului de securitate intern. De asemenea, trebuie menționat că polarizarea se poate manifesta şi între state, regiuni sau culturi diferite.

Procesul social care va avea însă cel mai mare impact asupra mediului de securitate în următoarele decenii îl reprezintă **urbanizarea accelerată**. Acesta se manifestă în toate regiunile globului, cu viteze şi la scară diferită. Astfel, regiunile cu rată mare de creştere a populației (Africa, America Latină) vor cunoaşte un proces de urbanizare accelerată. De asemenea, în statele cu economii emergente din Asia (în special China) urbanizarea se va desfăşura la o scară şi cu o viteză deosebită[19]. La ora actuală, la nivel global, numărul oraşelor cu populație de cel puțin 1 milion de locuitori este de 512, estimându-se că numărul acestora va creşte la 662 până în 2030, în timp ce numărul oraşelor cu populație de peste 10 milioane de locuitori va creşte de la 31 la 41 în acelaşi interval de timp.

Ocupând o suprafață totală de numai 3% din suprafața terestră, oraşele consumă aproximativ 75% din totalul resurselor naturale[20]. La ora actuală, capacitățile autorităților locale privind asigurarea nevoilor de subzistență cu apă şi alimente, în cazul multor mega-oraşe (mega-cities), sunt depăşite de rata accelerată a urbanizării, cu implicații directe asupra asigurării unui standard minim al calității vieții[21]. Degradarea calității vieții creează vulnerabilități sociale care pot fi exploatate de organizațiile teroriste sau de crimă organizată.

Din punct de vedere militar, pe termen lung, oraşele vor deveni mediul operațional predilect al desfăşurării conflictelor armate. Provocările unui astfel de mediu operațional la adresa forțelor angajate în operații sunt multiple. Domeniile în care operațiile militare vor fi executate, de multe ori concomitent, sunt: terestru, aerian, maritim, cyber şi spațial. De asemenea, oraşele au atât o dimensiune verticală, inclusiv spațiul subteran, cât şi una orizontală de desfăşurare a operațiilor militare.

Menținerea inegalităților economice şi sociale, lipsa oportunităților în educație şi cele de pe piața forței de muncă, influența schimbărilor climatice asupra mediului înconjurător, precum şi conflictele armate vor determina existența unui important potențial migraționist pentru

***Analiză alternativă***

- Urbanizarea rapidă în regiuni precum Africa poate reprezenta o oportunitate prin concetrarea unei forțe de muncă relativ ieftine, care poate determina dezvoltarea rapidă a unor sectoare economice.
- Tehnologiile noi şi cele emergente au potențialul de a creşte, prin automatizare şi AI, productivitatea industriilor manufacturiere din statele dezvoltate, atenuând astfel efectul îmbătrânirii populației asupra forței de muncă active şi a bugetelor naționale.
- Polarizarea poate avea un rezultat benefic prin creşterea implicării civice a populației în viața politică şi culturală a societății, funcționând astfel ca un mecanism de autoreglare socială.

următoarele decade de timp. Factori potențatori ai acestui fenomen, respectiv globalizarea, structura de vârstă a societății diferită între statele dezvoltate şi cele în curs de dezvoltare, prezența rețelelor de traficanți, vor contribui, de asemenea, la persistența fenomenului migraționist. La ora actuală, la nivel mondial, mai mult de jumătate din fluxul migraționist este preluat de state aparținând G-8, în special din cauza lipsei forței de muncă tinere în statele respective. În Germania şi Japonia, de exemplu, procentul populației tinere, cu vârste cuprinse între 15 – 24 ani, va scădea sub 25% până în 2035[22]. Pe de altă parte, inabilitatea statelor țintă de a gestiona şi integra social numărul relativ mare de migranți va determina intensificarea radicalizării împotriva acestora şi creşterea importanței curentelor politice naționaliste şi iliberale.

**Concluzii**

Pentru următoarele două decenii, puterea geopolitică şi cea economică vor cunoaşte un transfer între principalii actori statali pe plan internațional. Astfel, după aproape un secol de dominație economică, Statele Unite vor fi devansate de China, ca putere economică globală predominantă. Cu un nivel al comerțului internațional previzionat a fi dublu comparativ cu cel al SUA, China va deveni principala putere economică mondială. De asemenea, India va deveni una din cele mai importante economii mondiale, ceea ce va determina creşterea corespunzătoare a profilului geopolitic al acesteia.

Cu toate acestea, SUA vor continua să fie statul cu cea mai mare influență la nivel internațional, dominația militară americană rămânând un factor de necontestat. SUA vor opera într-o lume multipolară (post-occidentală) în care puterea economică globală va fi deținută de state al căror produs intern brut pe cap de locuitor va fi mult mai mic decât cel existent la ora actuală în statele dezvoltate. Consecința acestei realități va fi o implicare mai mică a Chinei, Indiei sau Braziliei în soluționarea problemelor de securitate la nivel global, comparativ cu implicarea actuală a SUA şi UE, şi o concentrare a autorităților acestor state către dezvoltare internă. Pe cale de consecință, este probabil ca mediul de securitate să fie caracterizat de creşterea instabilității şi incertitudinii.

Analizând tendințele de dezvoltare în domeniile geopolitic, tehnologic, economic şi social, prezentate anterior, se pot construi cel puțin trei scenarii privind mediul de securitate la nivelul anului 2040:

1. **Multipolaritatea sistemului internațional**. În cadrul acestui scenariu, guvernarea la nivel mondial va fi asigurată de un grup de state (puteri globale), niciunul dintre acestea neavând suficientă putere politică, economică sau militară pentru a cataliza comunitatea internațională către acțiuni comune. În esență, sistemul internațional va fi caracterizat de un vacuum al puterii, SUA neavând puterea sau voința politică de a-şi asuma rolul de lider mondial. Interesele

naționale ale puterilor globale vor prevala în fața oricărori valori general acceptate, ceea ceea ce va conduce la inabilitatea acestora de a rezolva prin cooperare problemele de securitate globale. Din punct de vedere economic, globalizarea va cunoaşte un proces de reversibilitate, majoritatea statelor adoptând măsuri comerciale protecționiste.

2. **Unipolaritatea occidentală**. Scenariul presupune existența unei lumi multipolare, caracterizate însă de predominanța puterii politice, economice şi militare a democrațiilor de tip occidental (SUA, UE, Australia, Canada etc.) organizate în alianțe formale sau informale. Divergențele privind soluțiile la problemele de securitate globale sau regionale manifestate între Occident şi puterile emergente (China, India, F.Rusă) vor bloca activitatea instituțiilor internaționale şi vor conduce la abordări unilaterale pentru soluționarea majorității acestora. Riscul apariției conflictelor armate va creşte.
3. **Multipolaritate regională**. Transferul puterii politice şi economice de la spațiul euroatlantic către cel asiatic va determina apariția unei lumi multipolare caracterizate de existența a două blocuri economice majore. SUA vor menține sistemul economic liberal pentru asigurarea funcționării alianței cu UE. Pe de altă parte, puterile emergente eurasiatice îşi vor asuma responsabilități sporite în ceea ce priveşte securitatea globală, ceea ce va conduce la dezvoltarea şi implementarea unui set de norme şi reguli de guvernare globală. Mediul de securitate va fi caracterizat de o relativă stabilitate.

**Bibliografie:**


1. BRUNE, Nancy, *Global Trends 2030*, 2018, disponibil online la http://gt2030.com/category/gt2030.
2. CLARK, Robert M, *Intelligence analysis – A targeted – centric approach*, 2006, Library of Congres, SUA.
3. COMMINS, Stephen, *Global Trends 2030*, 2018, disponibil online la http://gt2030.com/category/gt2030.
4. LANGMUIR, Irvin citat în Clark, Robert M., *Intelligence analysis – A targeted–centric approach*, 2006, Library of Congres, SUA.
5. LAZAR, Arthur, *Puterea cibernetică, un pilon esențial al puterilor viitorului*, 2017, disponibil online la https://cybersecuritytrends.ro/puterea-cibernetica-un-pilon-esential-al-puterilor-viitorului.
6. MAVROFIDES, Thomas; KAMEAS, Achilleas; PAPAGEORGIOU, Dimitris; LOS, Antonios, *On the Entropy of Social Systems: A Revision of the Concepts of Entropy and Energy in the Social Context*, 2011, John Wiley & Sons, Ltd.
7. *Multi Domain Battle: Evolution of Combined Arms for the 21st Century*, 2107, US Army Training and Doctrine Command.
8. PENDLETON, Gordon, *Joint Urban Operations and the NATO Urbanisation Project*, 2015, ACT/NATO.
9. RYTE, Marc-André, *A patra revoluție industrială şi impactul său asupra forțelor armate*, 2017, disponibil online la https://cybersecuritytrends.ro/a-patra-revolutie-industriala-si-impactul-sau-asupra-fortelor-armate.
10. *Strategic Foresight Analysis*, 2017 Report, Allied Command Transformation/NATO.


[1] Prin forțe care acționează asupra sistemului se înțeleg acțiuni, tendințe, direcții de dezvoltare a domeniilor principale.
[2] Thomas Mavrofides, Achilleas Kameas, Dimitris Papageorgiou, Antonios Los, *On theEntropy of Social Systems: A revision of the Concepts of Entropy and Energy in the Social Context*, 2011, John Wiley&Sons, Ltd.
[3] În timp, entropia unui sistem creşte, în absența intervenției unor forțe externe asupra acestuia.
[4] Robert M. Clark, *Intelligence analysis. A targeted – centric approoch*, 2006, Library of Congres, SUA.
[5] Langmuir, Irvin citat în Clark, Robert M, *Intelligence analysis. A targeted – centric approach*, 2006, Library of Congres, SUA.
[6] Idem 4.

[7] Conform National Intelligence Council/SUA, actorii nestatali sunt definiți ca „entități ne-suverane care exercită o influență semnificativă la nivel național și internațional”.

[8] Exemple în acest sens sunt grupul BRICS - format din Brazilia, F.Rusă, India, China și Africa de Sud - și organizația regională Asociația Statelor din Asia de Sud-Est - formată din 10 state sud-est asiatice care își propun ca obiectiv principal integrarea economică, politică, militară, culturală și educațională a statelor semnatare.

[9] *Strategic Foresight Analysis*, 2017 Report, Allied Command Transformation/NATO.

[10] Inteligența Artificială reprezintă capacitatea sistemelor computerizate de a executa operații care, în mod normal, necesită inteligență umană, respectiv percepție și decizie.

[11] Marc-André Ryte, *A patra revoluție industrială și impactul său asupra forțelor armate*, 2017, disponibil online la https://cybersecuritytrends.ro/a-patra-revolutie-industriala-si-impactul-sau-asupra-fortelor-armate (accesat la 20.08.2018).

[12] *Multi Domain Battle: Evolution of Combined Arms for the 21st Century*, 2107, US Army Training and Doctrine Command.

[13] Autonomia este definită ca nivelul de independență pe care oamenii îl acordă sistemelor pentru executarea unei anumite sarcini, într-un mediu determinat. Ea se bazează pe o combinație de senzori și de calcul pentru a se deplasa în interiorul mediului definit, precum și capabilități sofware necesare procesului de decizie.

[14] Arthur Lazar, *Puterea cibernetică, un pilon esențial al puterilor viitorului*, 2017, disponibil online la https://cybersecuritytrends.ro/puterea-cibernetica-un-pilon-esential-al-puterilor-viitorului, (accesat la 19.08.2018).

[15] *Strategic Foresight Analysis*, 2017 Report, Allied Command Transformation/NATO.

[16] Ibidem.

[17] Ibidem.

[18] Nancy Brune, *Global Trends*, 2030, 2018, disponibil online la http://gt2030.com/category/gt2030, (accesat la 25.08.2018).

[19] Conform raportului *Urban World: Cities and the rise of the consuming class*, întocmit de McKinsey Global Institute, în China procesul de urbanizare se desfășoară la o scară de 100 de ori mai mare și cu o viteză de 10 ori mai mare comparativ cu procesul similar care a avut loc în Marea Britanie în secolul 18, determinat de revoluția industrială.

[20] Stephen Commins, *Global Trends 2030*, 2018, disponibil online la http://gt2030.com/category/gt2030 (accesat la 24.08.2018).

[21] Pendleton, Gordon, *Joint Urban Operations and the NATO Urbanisation Project*, 2015, ACT/NATO.

[22] *Strategic Foresight Analysis*, 2017 Report, Allied Command Transformation/NATO.

# INFORMAȚIILE MmilitARE ÎN CADRUL UNIUNII EUROPENE

***Robert CĂLINOIU****

***Abstract***

*As a member state of the European Union, Romania is represented from all its central structures. Within the EUMS (European Union Military Staff) Romania participates with military personnel, including experts from the Military Intelligence Directorate. This provides a number of advantages, as follows: the expertise provided by partners on fields/ areas less covered by information at a national level but with possible impact on national security (for example: illegal migration, organized crime or terrorism), the opportunity to know a different perspective than the national one in order to build cooperation policies according to common interests, increasing the credibility of Romania at the level of the central structures of the EU, but also at the level of the bilateral relations due to the quality work.*

***Keywords****: Union European, EU Common Security and Defence Policy – CSDP, European Union Military Staff - EUMS, intelligence structures, sharing intelligence,*

**Crearea Statului Major Militar al Uniunii Europene (European Union Military Staff – EUMS)**

EUMS este parte a structurilor de securitate şi apărare ale UE (din cadrul EU Common Security and Defence Policy – CSDP), care la rândul lor sunt incluse în cadrul arhitecturii de securitate şi politică externă a UE (EU's Common Foreign and Security Policy – CFSP), şi este coordonat, începând cu 2011, de Serviciul European de Acțiune Externă (European External Action Service – EEAS).

Inițiativele de cooperare europeană în domeniul politic şi economic îşi au originea la sfârşitul anilor 1940. După discuții în formate bi şi multilaterale, în 1948 a fost înființată Uniunea Europei Occidentale (Western European Union – WEU), de către Marea Britanie, Franța, Belgia, Germania de Vest, Italia, Luxemburg şi Olanda. Ulterior, WEU a furnizat cadrul necesar consultărilor şi discuțiilor pe diverse teme, preponderent politice şi economice, dar care au inclus deseori şi securitatea şi apărarea europeană.

Conceptul de politică externă comună şi de securitate (CFSP) a fost introdus începând cu anul 1993, odată cu Tratatul de la Maastricht, devenind unul dintre pilonii cooperării în cadrul UE. În cadrul Tratatului, se stabilea că CFSP include „toate aspectele legate de securitatea Uniunii, constituind cadrul necesar dezvoltării unei politici de apărare comune care, în timp, ar putea conduce la o apărare comună[1]". Ulterior, pe timpul Summit-ului bilateral franco-britanic de la Saint-Malo (04–05.12.1998), prim-ministrul britanic şi preşedintele francez au semnat o declarație comună care statua că Uniunea Europeană „trebuie să aibă capacitatea de a acționa autonom, sprijinită de forțe militare credibile şi mecanisme care ar putea decide folosirea lor, pentru a fi în măsură să răspundă crizelor internaționale[2]". Declarația a marcat o schimbare semnificativă a poziției Marii Britanii,

*Autorul este expert în cadrul Ministerului Apărării Naționale.*

care până la acel moment blocase orice intenție de a crea capabilități militare în interiorul Uniunii Europene, în timp ce Franța, retrasă din structurile militare ale NATO în 1966 (unde a revenit în 2009), căuta mijloace de a-şi consolida securitatea prin crearea unor mecanisme în cadrul UE.

Declarația a permis conducerilor statelor UE să lanseze, cu ocazia Summitului Consiliului European de la Koln, din iunie 1999, conceptul de „politică de securitate şi apărare europeană (European Security and 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 europene comune de securitate şi apărare (Common Security and Defence Policy – CSDP). La crearea şi dezvoltarea structurilor formale care să aibă ca atribuții 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, marcat de 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 apariția ca structuri formale a Comitetului Politic şi de Securitate (Political and Security Committee – PSC), a Comitetului Militar al UE (EU Military Committee – EUMC) şi a Statului Major Militar al UE (EU Military Staff – EUMS) – în cadrul Secretariatului General al Consiliului UE.

**Structura şi atribuțiile EUMS**

Decizia Consiliului UE de înființare a EUMS a prevăzut ca misiuni ale acestei structuri avertizarea timpurie, evaluări ale situațiilor de criză şi planificare strategică pentru operațiile de management al crizelor pe care UE le poate derula (operațiuni umanitare şi de salvare, menținere a păcii[3]).

Odată cu semnarea, în 2009, a Tratatului de la Lisabona şi înființarea Serviciului European de Acțiune Externă, s-a decis ca toate structurile CSDP, inclusiv EUMS, să treacă din compunerea Secretariatului General al Consiliului la EEAS. Pentru a sublinia importanța EUMS ca singur furnizor de expertiză militară în cadrul instituțiilor Uniunii Europene, acesta a fost subordonat nemijlocit Înaltului Reprezentant şi Vicepreşedinte al Comisiei Europene (HR/VP).

Având o structură de aproximativ 200 de persoane, militari şi civili, EUMS, condus de un director general – trei stele şi un director adjunct/şef de stat major – două stele, este organizat pe cinci direcții şi patru birouri, conform figurii nr. 1.

**Informațiile militare[5] în cadrul UE/EUMS**

Una dintre cele cinci direcții ale EUMS este Direcția informații (EUMS Intelligence Directorate – DINT), ale cărei misiuni sunt: furnizarea contribuțiilor specifice în procesul de avertizare timpurie, întocmirea evaluărilor privind situațiile de criză, contribuția cu informații la planificarea misiunilor, furnizarea de informații în procesul de planificare a răspunsului la crize şi de produse specifice pentru operații şi aplicații.

Direcția este condusă de un general de brigadă (echivalent), funcție ocupată de un reprezentant provenind din unul din statele membre şi organizată pe trei secții: politici în domeniul informațiilor, sprijin şi analiză (producție). Este important de observat că una din cele trei funcții de şef de secție este ocupată în prezent de un expert național detaşat din cadrul Direcției generale de informații a apărării. Personalul DINT provine din statele membre UE, fiind detaşat (National Seconded Expert – SNE) pe o perioadă de la doi la patru ani, o parte din acesta constituind şi punct de contact cu structurile de informații din statele de proveniență şi asigurând legătura bidirecțională de comunicații şi transfer de produse informative, de la DINT la serviciul de informații militare (SIM) național. DINT nu are structuri de culegere, informațiile clasificate utilizate provenind de la serviciile de informații militare

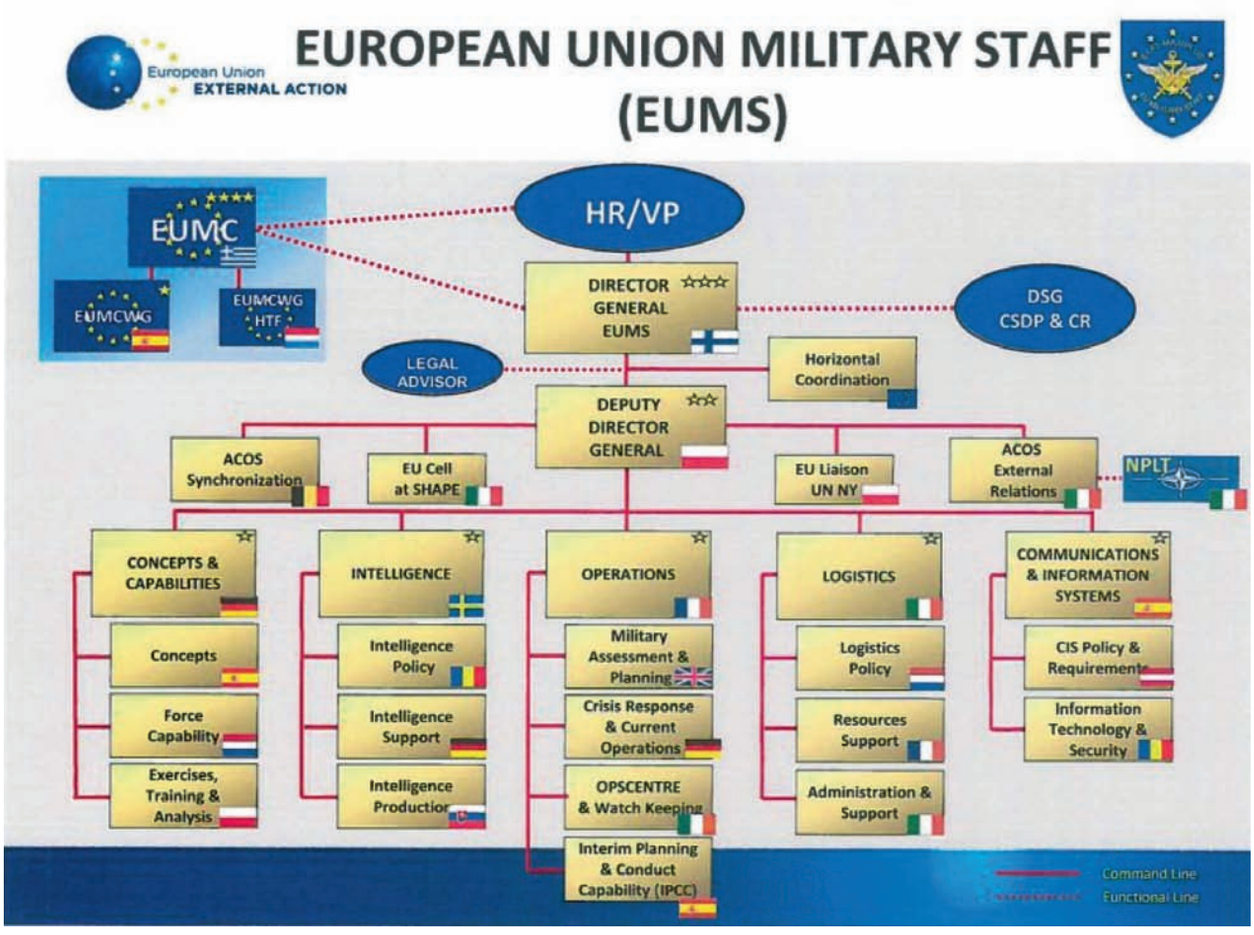



*Fig. nr. 1*

şi civile (cele civile primite prin intermediul Centrului de Informații – Intelligence Center – INTCEN, structură civilă de informații aflată de asemenea în EEAS şi cu care DINT cooperează strâns în cadrul formatului Single Intelligence Analysis Capacity – SIAC), precum şi de la Centrul Satelitar european (EU Satellite Center – SATCEN). De asemenea, sunt analizate şi informații neclasificate, obținute fie de la Delegațiile UE în diverse state, pe timpul misiunilor specifice în state terțe (Fact Finding Missions – FFM), de la think-tank-uri sau pe timpul participării la conferințe şi prelegeri. Contribuțiile cu informații ale serviciilor statelor membre sunt voluntare, subiectele acestora având, de obicei, legătură cu zonele sau fenomenele de interes imediat ale fiecărui stat (zone de criză, migrație, terorism etc.).

Secția analiză este organizată atât pe birouri geografice, cât şi pe subiecte de interes (amenințări transnaționale şi amenințări hibride). Produsele acesteia sunt atât în format hârtie, cât şi sub formă de briefinguri, furnizate periodic sau la cererea conducerii UE. Printre documentele elaborate se numără analize punctuale (Intelligence Briefing Notes), analize privind amenințările la adresa securității UE (Threat Assessments), analize de intelligence (Intelligence Assessments). Dintre materialele periodice ar putea fi enumerate Analiza anuală privind amenințările globale (Annual Global Threat Review – AGTR) şi Evaluările săptămânale (SIAC Weekly – în cooperare cu INTCEN).

Managementul activității de informații este realizat, din perspectiva statelor membre, de către Comitetul Director (Director's Board), format din directorii serviciilor de informații militare din statele membre UE. Acesta se întâlneşte o dată pe an sau ori de câte ori este nevoie. Pentru pregătirea deciziilor acestuia sunt organizate alte două întâlniri ale reprezentanților SIM UE, la nivelul directorilor pentru analiză şi la nivelul

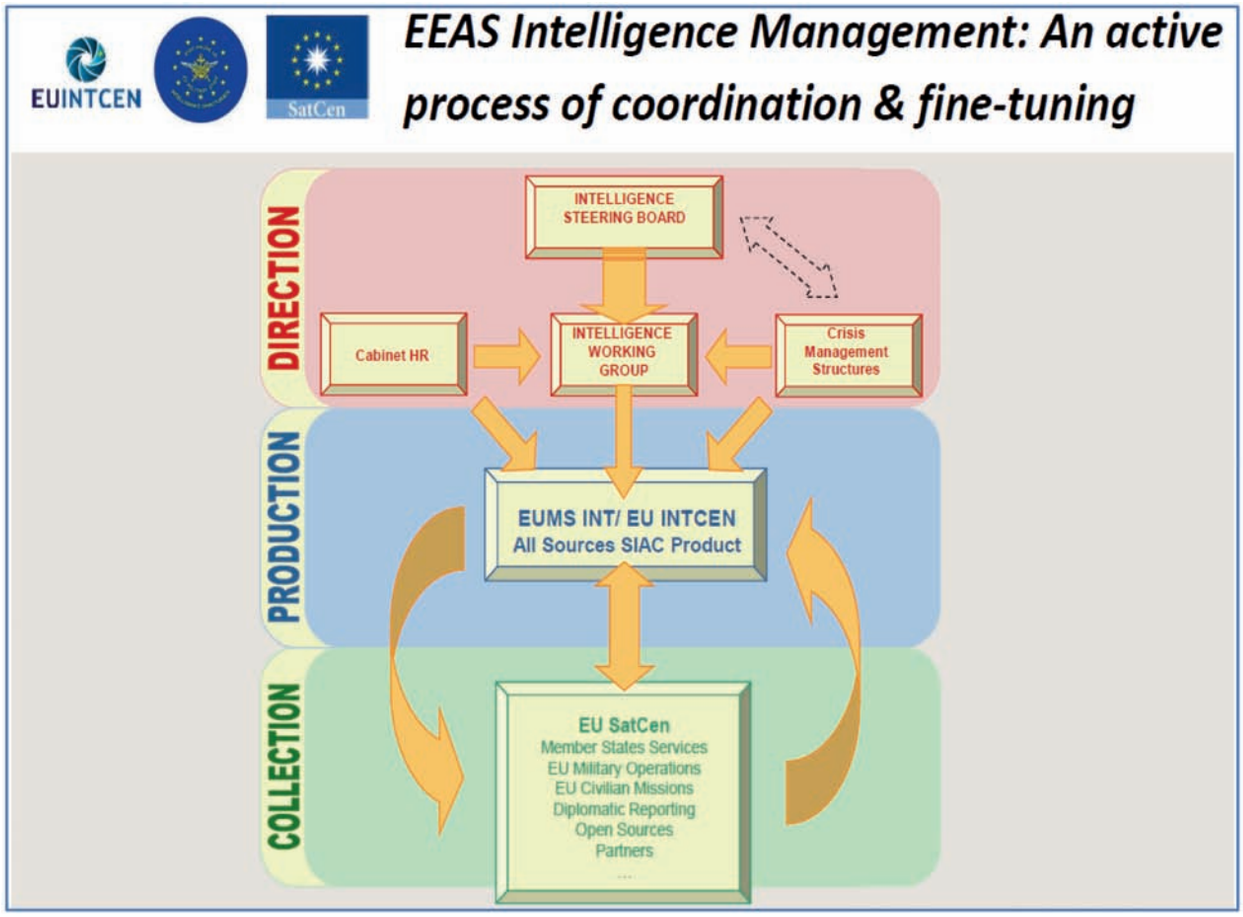



***Fig. nr. 2***

şefilor structurilor politicilor de planificare a activităților de informații.

Din perspectiva UE, activitatea de informații este condusă de un Comitet de informații (Intelligence Steering Board – ISB) din care face parte și directorul Direcției informații a EUMS, ale cărui decizii sunt coordonate cu cabinetul HR/VP și structurile de management al crizelor din EEAS, fiind transmise spre execuție DINT, INTCEN și SATCEN. O schemă generală a acestui proces este redată în figura nr. 2.

Printre preocupările curente de adaptare la mediul de securitate actual al structurilor de informații ale UE se află și înființarea unei celule de analiză a amenințărilor hibride – EU Hybrid Fusion Cell. Aceasta este formată din personal aparținând DINT și INTCEN și analizează activități precum cele de propagandă/ dezinformare, atacuri cibernetice, operațiuni psihologice, acțiuni subversive, terorism/ sabotaj, exploatarea diferențelor culturale, de limbă sau religioase, activitățile economice folosite în scopul obținerii de avantaje politice („pipeline politics"), sprijinirea mișcărilor secesioniste, migrația și exploatarea migranților, folosirea grupurilor de presiune, mercenarilor și terților în diverse acțiuni.

**Avantajele participării naționale active în cadrul DINT EUMS**

În calitate de stat membru al Uniunii Europene, România, prin reprezentanți din instituții naționale diverse, este prezentă în toate structurile centrale ale UE. Astfel, prezența în cadrul EUMS cu personal aparținând MApN este firească, inclusiv în cadrul DINT. Mai departe, participarea Direcției informații militare și a DGIA cu experți în cadrul DINT conferă o serie de obligații, dar și avantaje. Dacă la capitolul obligații am menționat deja participarea cu produse informative la efortul global, în ceea ce privește avantajele, pot fi enumerate, printre altele, beneficierea de expertiza celorlalte servicii, pe arii și domenii de interes mai puțin acoperite la nivel național, dar care

influențează și securitatea României (exemplu: migrația ilegală și fenomenele asociate, precum crima organizată și terorismul), oportunitatea de a prezenta și susține un punct de vedere național pe un subiect de securitate de interes major (și care, ulterior, după realizarea unui produs de informații integrat în cadrul SIAC va fi prezentat conducerii UE), oportunitatea de a lua la cunoștință despre o perspectivă diferită de cea națională și de a înțelege și formula politici de cooperare în funcție de interesele comune sau divergente ale unui stat partener, creșterea nivelului de încredere la nivelul structurii profesionale a UE, dar și în plan bilateral, prin derularea unei activități de calitate de către reprezentanții din cadrul DINT, dar și prin contribuții apreciate de materiale specifice transmise, precum și beneficierea de produsele finite realizate în cadrul DINT (SIAC), chiar dacă nu s-au transmis contribuții naționale. În cele din urmă, dar nu mai puțin importantă, putem sublinia creșterea prestigiului informațiilor militare din România în cadrul comunității de informații europene, precum și adoptarea sau transferul bunelor practici europene în sistemul național pentru creșterea eficienței activității în domeniul informațiilor.

**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 *Moondial Nieuws* 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 și Apărare cu sprijinul Universității Naționale de Apărare la București, în perioada 05 – 09.02.2018;
5. Broșura de prezentare a EUMS;
6. https://www.cvce.eu/en/obj/information_brochure_on_the_european_union_military_staff_eums-en-1bcbd497-c5e3-4b7a-ab54-9e392e0c1483.html;
7. LASSCHE, Deborah, articol în revista *Militaire Spectator*, https://www.militairespectator.nl/thema/internationale-samenwerking/artikel/eu-military-staff-frog-boiling-water;
8. Site-ul oficial al EEAS; https://eeas.europa.eu/headquarters/headquarters-homepage_en/3602/Organizationchart.


[1] ”(…) all questions related to the security of the Union, including the eventual framing of a common defence policy, which might in time lead to a common defence”; sursa: Tratatul de la Maastricht, Titlul V – Provisions on a common Foreign and Security policy, Articolul J.4, p. 126;

[2] „The European Union must have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so, in order to respond to international crises”; sursa: Declarația de la Saint-Malo, articolul 2, p. 2.

[3] The Petersberg tasks – humanitarian and rescue tasks, peacekeeping tasks, and tasks of combat forces in crisis management, including peace-making.

[4] Sursa: https://eeas.europa.eu/headquarters/headquarters-homepage_en/3602/Organizationchart

[5] Pentru prima dată în cadrul UE, crearea unei capabilități în domeniul informațiilor a fost prevăzută tot în declarația comună franco-britanică de la Saint-Malo, 4 decembrie 1998: “In order for the European Union to take decisions and approve military action where the Alliance as a whole is not engaged, the Union must be given appropriate structures and a capacity for analysis of situations, sources of intelligence, and a capability for relevant strategic planning, without unnecessary duplication, taking account of the existing assets of the WEU and the evolution of its relations with the EU.” (articolul 2 al documentului).

[6] Sursa: Prezentare a lt. col. Francisco Rodriguez Berbel-Lopez la cursul CSDP organizat de Colegiul European pentru Securitate și Apărare cu sprijinul Universității Naționale de Apărare la București, în perioada 05 – 09.02.2018.

# ATAŞATURA APĂRĂRII – VECTOR AL DIPLOMAȚIEI MILITARE ROMÂNE

***Dr. Florin-Ion MARINESCU***
***Drd. Petru DIMA*** *

***Abstract***

*The defense attaché, as a military diplomat, has important responsibilities in diplomatic representation in the states where he is accredited and in the development and conduct of bilateral military co-operation. From the perspective of national security, the military attaché's main missions are to: promote military cooperation (bilateral and multilateral), increase the contribution of the Romanian Armed Forces to regional and global stability, identify and report timely events and international developments that could affect national interests, achieving the interoperability of the Romanian Armed Forces with the armies of the NATO and EU member states and, last but not least, developing forms of cooperation with the armies of the partner states.*

***Keywords:*** *defense attaché, military cooperation, national interests, interoperability.*

**Aspecte generale**

Începutul secolului XXI este marcat de transformări profunde ale mediului de securitate. Lumea a devenit tot mai complexă, dinamică şi interdependentă, iar ireversibilitatea fenomenului globalizării a devenit certitudine. Evoluția securității globale din ultimul deceniu, în general pozitivă, a confirmat faptul că succesul acțiunilor diplomatice şi stabilitatea sunt rezultatul colaborărilor multidimensionale, în care domeniile politic, economic şi militar asigură consistență şi sinergie.

Caracteristicile riscurilor şi amenințărilor actuale, impredictibile şi cu caracter profund perturbator, coroborate cu poziționarea României pe flancul estic al Alianței Nord-Atlantice şi al Uniunii Europene, la interfața unor zone cu risc de securitate ridicat, au determinat adaptarea rolului şi misiunilor Atașaturii apărării, structură care prin misiunile sale trebuie să fie în măsură să identifice şi să evalueze, în mod oportun, riscurile şi amenințările la adresa României, să contribuie la promovarea intereselor naționale şi să participe în mod activ la crearea unei imagini favorabile a României în plan internațional.

**Scurt istoric**

Funcția de atașat al apărării a apărut în secolul al XVII-lea, pe timpul Războiului de 30 de ani, când Ducele de Richelieu a trimis în străinătate cei mai competenți ofițeri, pentru a stabili legături cu forțele aliate, a supraveghea

*Autorii sunt experți în cadrul Ministerului Apărării Naționale.*

„dezvoltările militare” ale adversarilor şi pentru a culege informaţii. Abia în secolul al XVIII-lea se generalizează practica trimiterii ataşaţilor apărării pe lângă misiunile diplomatice externe, iar în secolul al XIX-lea un număr din ce în ce mai mare de state definesc instituţia ataşaţilor apărării. Acest demers a fost accelerat atât de emergenţa structurilor naţionale de forţă, cât şi de constituirea imperiilor coloniale.

Secolul al XX-lea a adus schimbări majore în ceea ce priveşte numărul, misiunile şi importanţa acordată ataşaţilor apărării. În această perioadă, necesitatea de a recurge cât mai des la serviciile ataşaţilor apărării a fost determinată de creşterea numărului statelor, complexitatea ridicată a sistemelor de armament, intensificarea relaţiilor internaţionale şi creşterea importanţei culegerii şi schimbului de informaţii.

În anul 1961 drepturile, obligaţiile şi responsabilităţile diplomaţilor au fost transpuse în Convenţia de la Viena, moment în care ataşaţilor apărării li s-au acordat drepturi şi imunităţi conform statutului diplomatic.

În România, diplomaţia militară s-a afirmat în timp ca o componentă permanentă, activă şi rezultativă a diplomaţiei publice, care a contribuit la promovarea cu succes a obiectivelor politicilor externe şi de securitate ale României.

Momentele care jalonează evoluţia instituţiei Ataşaturii apărării au ca punct de plecare înfiinţarea, în anul 1859, prin „Înalt Ordin nr. 83“ al domnitorului Alexandru Ioan Cuza, a „Secţiei a II-a Statistică şi Studiul Armatelor Străine” – prima structură română de informaţii militare.

În anul 1860, domnitorul Cuza trimite la Paris primul „reprezentant militar”, formula oficială fiind astfel adoptată, deoarece România nu putea acredita, în acea perioadă, ataşaţi militari. Acest moment, când primul diplomat militar român şi-a început mandatul la Paris, poate fi considerat ca punct de referinţă în istoria ataşaturii apărării române. Este vorba de căpitanul Ioan (Iancu) Alecsandri, fratele poetului Vasile Alecsandri, care şi-a adus o contribuţie importantă atât pentru recunoaşterea internaţională a Actului Unirii, în care Franţa


a avut un rol deosebit, cât şi la dezvoltarea relaţiilor militare româno-franceze.

În anul 1878 au fost trimişi la posturi permanente primii ataşaţi militari ai României, la Constantinopol şi Paris.

Ulterior, dispozitivul ataşaţilor apărării a cunoscut diferite etape de dezvoltare, dar şi de reducere, fenomenul fiind în directă dependenţă cu evoluţiile din situaţia politico-militară internă şi internaţională. Astfel, în anul 1918 România avea la post ataşaţi militari în 14 state, acest dispozitiv fiind *redus la zero în anul 1945*. Numărul birourilor externe a revenit la 14 posturi până în anul 1948. A urmat o perioadă relativ constantă până în anii ’80, când numărul ataşaţilor militari a fost din nou redus semnificativ. După 1990, dispozitivul şi misiunile ataşaturii apărării au fost fundamental regândite şi dezvoltate după principii moderne, într-o manieră corelată şi perfect compatibilă cu instituţiile similare din statele membre NATO.

În anul 2018, România are acreditaţi ataşaţi ai apărării în 64 de state: 34 de birouri ale ataşaţilor apărării cu reşedinţă permanentă în ţările de acreditare, respectiv 30 de state acoperite prin extinderi de acreditare.

Din punct de vedere cantitativ şi calitativ, actualul dispozitiv al birourilor ataşaţilor apărării a atins dimensiuni fără precedent în istoria de 159 de ani de existență a Direcției informații militare, acesta fiind supus unui proces permanent de adaptare şi modernizare.

**Misiunile Ataşaturii apărării**

Ataşaţii apărării, în calitatea lor de diplomați militari, realizează reprezentarea diplomatică permanentă a ministrului apărării naționale, secretarilor de stat, a şefului Statului Major al Apărării şi a şefilor categoriilor de forțe armate în statele de acreditare. Aceştia au responsabilități importante în problematica dezvoltării şi derulării cooperării militare bilaterale, precum şi în cea a reprezentării în statele de acreditare.

Misiunile fundamentale ale diplomației militare pe linia asigurării securității naționale se concretizează în acțiuni de promovare şi dezvoltare a colaborării militare bilaterale şi multilaterale, sporirea contribuției Armatei României la stabilitatea regională şi globală, identificarea şi semnalarea oportună a evenimentelor şi evoluțiilor internaționale care ar putea afecta interesele naționale, participarea la realizarea interoperabilității Forțelor Armate române cu armatele statelor membre NATO şi UE, precum şi inițierea şi dezvoltarea unor forme de cooperare bilaterală cu armatele statelor partenere.

În acelaşi timp, în conformitate cu prevederile Convenției de la Viena, ataşații apărării desfăşoară o activitate intensă pentru a se informa despre condițiile şi evoluția evenimentelor din statul acreditar, care să permită identificarea în timp oportun a factorilor de risc şi amenințare la adresa României, pentru evitarea surprinderii strategice, precum şi pentru sprijinul cu informații relevante a decidenților politico-militari şi militari, în scopul formulării şi adoptării celor mai corecte decizii la nivel strategic.

Totodată, rolul ataşaților apărării în cadrul misiunilor diplomatice ale României este deosebit de important, axat pe reprezentarea Ministerului Apărării Naționale, consilierea şefului de misiune în probleme de apărare şi securitate, participarea împreună cu alți diplomați la acțiuni oficiale conexe afacerilor politico-militare şi de reprezentare externă.

**Adaptarea permanentă a Ataşaturii apărării**

În prezent, structura Ataşaturii apărării este rezultatul schimbărilor succesive survenite în cadrul Armatei României şi al procesului de readaptare permanentă a misiunilor birourilor ataşaților apărării, în funcție de țara de acreditare, prin lărgirea spectrului competențelor şi introducerea unei noi abordări a relațiilor militare cu autoritățile statelor de acreditare. Astfel, misiunile birourilor ataşaților apărării care funcționează pe lângă misiunile diplomatice ale României au devenit din ce în ce mai diversificate şi complexe, pentru a face față, pe de o parte, solicitărilor naționale şi, pe de altă parte, de a reprezenta cu onoare şi demnitate Armata României.

Nu trebuie omis faptul că toate aceste obiective s-au înfăptuit cu oameni, cu ataşații apărării, dar şi cu cei care le îndrumă activitatea de acasă, iar de competențele şi de calitățile lor morale şi profesionale au depins şi depind, în mare măsură, respectul şi aprecierile de care Armata Română se bucură în relațiile cu aliații şi cu partenerii.

Generațiile actuale nu trebuie să-i uite pe cei câteva sute de oameni aleşi, care timp de un secol şi jumătate, prin iscusința vorbei, ascuțimea minții, prestanță şi dragoste de țară au adus Armatei prețuire din partea aliaților şi partenerilor şi respect din partea inamicului. Aceşti oameni, care de-a lungul timpului au îndeplinit nobila misiune diplomatică de ataşat român al apărării, fie că au fost prinți, mareşali, scriitori sau „doar” ofițeri, trebuie să iasă din anonimat şi să rămână în memoria colectivă a Armatei Române, deoarece doar peste generații urmaşii lor vor putea şti cu adevărat cât de mult au făcut ei pentru neam şi țară.

**Concluzie**

Instituția Ataşaturii apărării este şi va rămâne principalul instrument de promovare a diplomației militare la nivelul Ministerului Apărării Naționale, centrul focal al relațiilor militare externe şi un factor activ de transpunere în practică a obiectivelor politicii externe române.

**Bibliografie:**

1. Colectiv de autori, *Direcția Informații Militare între ficțiune si adevăr*, București 1994;
2. Colectiv de autori, *Dicționar de termeni diplomatici*, Universitatea Națională de Apărare, SUA;
3. MALIȚA, Mircea, *Diplomația*, Editura Didactică şi Pedagogică, Bucureşti, 1968;
4. CLOŞCA, Ionel şi Ion SUCEAVA, *Tratat de drept Internațional umanitar*, Editura V.I.S. Print, Bucureşti, 2000.

# CENTRUL DE EXCELENȚĂ NATO ÎN DOMENIUL HUMINT LA SCHIMBUL DE GENERAȚII

***Florin-Vasile TOMIUC***
***Alexandru KIS*** *

***Abstract***

*The NATO HUMINT Centre of Excellence (HCOE) from Oradea/Romania is at the time of generation change, with new leadership and adjusted working formula.*

*At the same time, the widely recognized performance of the Centre in the areas of standards custodianship, concept development and experimentation, education and training, and lessons learned and analysis, faces a particular challenge - not only for reconfirming and consolidating the commitment to further support NATO in these transformational areas, but also to align itself to the strategic thinking driving the Alliance's Intelligence capability reform.*

*In this respect, the Centre's exploratory features have to be properly exploited, with regard to the flexibility offered by COE's status in engaging both NATO and non-NATO expertise, and connections with Industry and Academia.*

***Keywords:*** *NATO, NATO HUMINT Centre of Excellence, Intelligence, transformation*

**Centrele de excelență NATO şi reforma în domeniul informațiilor militare în cadrul Alianței Nord-Atlantice**

Summitul NATO de la Varşovia, din 2016, a inițiat o schimbare revoluționară în ceea ce privește abordarea de către NATO a subiectului informațiilor militare, pe fondul unor disfuncționalități legate de managementul informației şi de îndeplinire a rolului fundamental de anticipare şi avertizare timpurie a acestei capabilități în relația cu forurile decizionale ale Alianței, în condițiile unui mediu de securitate tot mai complex. Acțiunile hibride şi măsurile active ale Rusiei, orientate către slăbirea coeziunii şi coerenței strategice a statelor NATO[1], alături de pericolul reprezentat de răspândirea armamentului de distrugere în masă, atacurile cibernetice, terorism, influxurile masive de migranți, competiția pentru resurse, crima organizată[2], sunt toate amenințări ce reclamă un răspuns articulat în interesul salvgardării valorilor noastre comune.

În acest sens, în cadrul adaptării structurii de comandă a NATO, un element cheie este reprezentat de înființarea unei divizii comune pentru informații (compusă din structurile reunite de informații militare şi civile) şi securitate (Biroul NATO pentru securitate), cu capacități de colectare şi analiză îmbunătățite – JISD/ Joint Intelligence and Security Division. Dar, după cum arăta chiar directorul acestei structuri, Arndt Freytag von Loringhoven, capabilitatea Intelligence în NATO înseamnă mult mai mult decât JISD, fiind necesară cuprinderea ca resursă a tuturor specialiştilor din structurile de comandă şi forțe NATO, comunitățile de informații militare şi civile ale statelor membre, precum şi organizații afiliate NATO, cum e cazul

**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.*

Centrului NATO pentru fuziunea informațiilor (NATO Intelligence Fusion Centre/NIFC) din Molesworth (Marea Britanie) sau a centrelor de excelență NATO active în domenii conexe securității şi informațiilor militare[3].

*Atlantic Voices* publica la începutul anului un articol dedicat contribuției centrelor de excelență NATO la ceea ce se dorește o „imunitate strategică" a Alianței, cu accent pe transformarea capabilităților de securitate şi informații militare ale NATO. Dr. Victor Madeira, autorul articolului, vede ca repere fundamentale în procesul de consolidare a capabilității „Intelligence" în NATO acreditarea centrelor de excelență NATO pentru HUMINT (Human Intelligence – informații din surse umane[4]) şi pentru contrainformații (CI) în 2010, respectiv 2017, ca vectori ai transformării efective a modului în care informațiile militare pot să evolueze funcțional către o nouă dimensiune[5], în virtutea conceptului şi caracteristicilor de lucru specifice ale acestor organizații. De aici, o serie de provocări pentru înțelegerea corectă a aşteptărilor sistemice şi viziunea strategică de dezvoltare a celor două instituții.

Pentru a contura în mod elocvent ce înseamnă Centrul de excelență NATO în domeniul HUMINT pentru transformarea capabilității „Intelligence" în cadrul Alianței Nord-Atlantice, voi face un scurt recurs la istoria devenirii acestuia, cu accent pe evoluția serviciilor/produselor pe care Centrul le pune la dispoziția structurilor şi națiunilor aliate.

**Centrul de Excelență NATO în domeniul HUMINT - o instituție matură în serviciul Alianței Nord-Atlantice**

La puțin timp de la aderarea României la NATO, țara noastră a valorificat, în 2005, o oportunitate de nişă în cadrul oferit de dezvoltarea Rețelei de Transformare a Alianței, inițiind înființarea Centrului de Excelență NATO[6] în domeniul HUMINT la Oradea. Oferta României a fost acceptată de către Alianță ca apreciere a contribuției de până atunci a militarilor români în teatrele de operații, şi, în special, datorită valorii dovedite în domeniul HUMINT în cadrul misiunilor externe.

Odată demarat proiectul, acesta s-a bucurat de sprijinul susținut din partea Direcției informații militare din cadrul Direcției generale de informații a apărării (DGIA) şi a presupus un proces complex de negocieri şi ateliere de lucru internaționale, fundamentare conceptuală, construire şi acreditare a instituției, un rol decisiv jucându-l echipa de proiect condusă de către viitorul director al Centrului, colonelul (la acea vreme) Eduard Simion.

Astfel, la data inaugurării oficiale a Centrului de excelență NATO din Oradea – 16 martie 2010 – acesta beneficia, pe lângă un consistent aport național, de contribuția de excepție a celorlalte națiuni sponsor: Grecia, Slovenia, Turcia şi Ungaria, cărora li s-au adăugat ulterior Slovacia, Polonia, Republica Cehă şi Statele Unite ale Americii, instituția fiind în continuare deschisă aderării altor state NATO.

Înființarea rețelei Centrelor de excelență are multiple semnificații atât pentru NATO, cât şi pentru națiunile participante. Pe de o parte, Centrele gestionează proiecte şi programe în sprijinul dezvoltării capabilităților existente, în ceea ce privește managementul lecțiilor învățate/bunelor practici, activitatea de analiză, dezvoltarea de concepte, experimentare şi standardizare, asigurând totodată oportunități deosebite pentru procesul de educare şi instruire în NATO; pe de altă parte, participarea națiunilor la Centrele de excelență, dincolo de contribuția asumată, are rațiuni şi interese bine justificate, avantajele imediate incluzând: asigurarea implementării viziunii şi reprezentării intereselor naționale în produsele specifice, asigurarea accesului nemijlocit la dezvoltările de ultimă oră în domeniul de interes şi la produsele specifice ale centrului, în condiții preferențiale. În plus, pe lângă vizibilitatea internațională şi la nivelul Alianței, relația cu partenerii din cadrul Centrului permite dezvoltarea de proiecte comune, facilitând interacțiunile bilaterale şi multilaterale între națiunile participante.

Centrul de excelență NATO din Oradea are ca obiectiv principal satisfacerea cererilor de sprijin ale Alianței în domeniul dezvoltării doctrinare şi conceptuale, al experimentării, gestionării procesului de lecții învățate, asigurării managementului activităților de educație şi instruire,


***Fig. nr. 1 – Punctul de informare NATO organizat de către***
***Centrul de Excelență NATO în domeniul HUMINT la Universitatea din Oradea***

precum şi furnizarea de soluții educaționale şi de instruire individuală şi colectivă în domeniul HUMINT în conformitate cu standardele NATO şi prin relaționare cu o multitudine de entități din cadrul structurilor de comandă şi de forțe ale Alianței, dar şi în afara acestora.

În timp scurt de la acreditarea sa, Centrul de excelență NATO din Oradea a reuşit să atingă o serie de obiective strategice, fundamentale pentru proiecția pe termen lung a sprijinului său pentru transformarea şi dezvoltarea capabilității HUMINT în NATO.

Atingerea acestor obiective a fost o performanță în sine în cadrul rețelei centrelor de excelență NATO, venind ca un corolar al proactivității Centrului, manifestată prin implicarea în toate proiectele, procesele şi evenimentele importante din domeniul HUMINT sau legate de aspecte concrete ale conectării sale la pulsul Alianței[7].

În plus, baza de relaționare largă pe care instituția a construit-o şi consolidat-o în timp, printr-o politică dinamică şi continuă, prin disponibilitatea de angajament şi prioritizarea judicioasă a resurselor, a fost un alt reper important în construirea rețetei succesului. Astfel, pe lângă structurile de coordonare din cadrul comandamentelor strategice ale Alianței şi participarea în variate grupuri de lucru NATO, au fost stabilite relații de lucru în primul rând cu națiunile aliate, cu structuri din cadrul comandamentelor operaționale sau de armă, cu centre de instruire NATO şi cu alte centre de excelență a căror activitate se interconectează la diferite niveluri de interes, dar şi cu instituții din zona academică şi industria de securitate.

Având în vedere faptul că procesele de reformă şi transformare reclamă viziune, performanță şi deschidere, accesul la medii care promovează confruntările de idei, facilitează înțelegerea procesualității fenomenelor şi permit aprofundări multidimensionale ale problematicilor de interes este o permanentă preocupare pentru comanda Centrului. Deschiderea şi inter-relaționarea cu mediul academic, dezvoltarea de parteneriate cu universități, institute de cercetare, ONG-uri, în cadrul unor proiecte specifice, asigură premisele necesare unor astfel de „achiziții” în materie de cunoaştere, permițând, totodată, promovarea culturii de securitate NATO.

În acest sens, relevantă este relația specială de colaborare cu Universitatea din Oradea unde, din 2014, prin contribuția Centrului, în cadrul bibliotecii universitare funcționează un punct de informare NATO menit să asigure bibliografia specifică studenților şi cadrelor didactice[8] (Fig. nr. 1).

În plus, dezvoltarea Centrului ca organizație bazată pe cunoaştere, prin integrarea viziunii, politicii şi cerințelor NATO în materie de management al cunoaşterii informației, adoptate şi adaptate ca fundament al propriilor necesități de schimb de informații, reprezintă un element de maximă importanță pentru eficiența organizațională.

Şi, poate mai presus de toate, ținând cont de faptul că resursa umană este cea care dă sens şi valoare organizațiilor şi proceselor din cadrul acestora (importanța capitalului uman fiind recunoscută şi promovată ca una dintre cele şase priorități majore la nivelul Comandamentului Aliat pentru Transformare), trebuie subliniat aportul excepțional al corpului multinațional de cadre din Centrul HCOE la performanțele şi prestigiul acestuia. De la acesta se aşteaptă contribuția decisivă în orientarea efortului instituției către cele mai bune soluții care să servească procesul de transformare a disciplinei Intelligence în NATO.

**Centrul de Excelență NATO în domeniul HUMINT la schimbul de generații**

Anul 2018 este menit să contureze reperele de „rebranding" pentru Centrul de excelență din Oradea, proces inițiat în 2017, odată cu predarea ştafetei comenzii şi adaptarea structurală a organizației la noile cerințe funcționale, realocările de personal şi definirea direcțiilor strategice de orientare a activității Centrului.

Relansarea activităților de culegere activă de observații şi identificare a bunelor practici în teatrele de operații, întărirea capacităților de analiză, demararea de noi proiecte de dezvoltare conceptuală, restructurarea sistemului de management al calității, manifestarea proactivă ca responsabil departamental pentru educația şi instruirea HUMINT în NATO (concretizată prin înființarea comunității de interes a furnizorilor de soluții educaționale, rafinarea cerințelor de instruire în paralel cu elaborarea unei viziuni strategice a dezvoltării spectrului educațional, incluzând prezența în mediul online şi stimularea folosirii de soluții avansate, moderne, în actul didactic), lărgirea ofertei educaționale prin cursuri ce acoperă cerințele de instruire pentru toate funcțiunile specialității, revizuirea într-un cadru actualizat a standardelor HUMINT – sunt doar câteva direcții prin care fiecare dintre ariile funcționale urmăreşte să contribuie, într-o viziune integrată, la un răspuns optimizat față de cerințele actuale de evoluție a capabilității HUMINT în NATO.

Chiar dacă rolul şi responsabilitățile Centrului au cunoscut o permanentă dezvoltare (în oglindă cu accentul pus de NATO pe dezvoltarea capabilității Intelligence), se manifestă nevoia unei reconectări proactive la forurile ce promovează **gândirea strategică,** în vederea identificării corecte şi oportune a instanțelor transformării în domeniu, raportat la mediul şi cerințele specifice. Se aşteaptă ca Centrul să nu se rezume la a răspunde cerințelor, ci şi la a contribui la formularea acestora, într-o abordare inovatoare, deschisă, sensibilă la provocările prezente şi viitoare, într-o societate holistic conectată la fenomenul securitar.

Dr. V. Madeira vede Centrul de Excelență NATO în domeniul HUMINT ca fiind perfect echipat pentru a promova astfel de dezbateri de idei, orientate către cerințele dobândirii unui nivel dezirabil pentru „imunitatea strategică" a Alianței, în primul rând prin statutul său, care îi oferă un caracter de „punte" între NATO şi orice altă contribuție externă Alianței, cu flexibilitatea şi agilitatea acțională aferentă, dar şi prin experiența dobândită în aproape o decadă de activitate în sprijinul acesteia[9]. Această temă trebuie dezvoltată şi operaționalizată în coordonare cu forurile strategice ale Alianței, atât în cadrul comunităților de interes reprezentate de Grupurile de lucru NATO pentru HUMINT (NATO HUMINT Working Group – NHWG) şi pentru tehnologie HUMINT (NATO HUMINT Technology Working Group – NHTWG),

cu sprijinul comunităților conexe pe linie de lecții învățate şi analiză, dar şi educaţie şi instruire, cât şi în cadrul larg de dezbateri oferit de mediul academic, unde Centrul urmăreşte să iniţieze astfel de dezbateri. În plus, proiectele de cercetare finanțate de către NATO în cadrul diferitelor programe şi inițiative trebuie să reflecte în mod corespunzător nivelul de prioritate acordat capabilității Intelligence în NATO, stimulând cercetarea şi inovația în domeniu.

Rămâne ca toate aceste atribute să fie judicios rafinate în resursă a transformării capabilității Intelligence în NATO, astfel încât Centrul de excelență din Oradea să îşi consolideze statutul de contributor de excepție la eforturile Alianței de a se reforma **şi adapta** provocărilor mediului de securitate actual şi viitor.

**Bibliografie:**


1. GALEOTTI, Mark, „Russian intelligence is at (political) war“, *NATO Review Magazine* 12/05/2017, https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/EN/index.htm;
2. MADEIRA, Victor, „NATO COEs: Transforming Security and Intelligence to Boost Strategic Immunity“, *Atlantic Voices*, Vol. 8, Issue 01, January 2018, https://www.slideshare.net/Atlantictreatyassociation/atlantic-voices-nato-counterintelligence;
3. SIMION, Eduard; KIS, Alexandru, *New features of the NATO Centres of Excellence in support of the North-Atlantic Alliance Transformation*, pp. 125-131, în volumul celei de a 22-a Conferințe Internaționale – “The Knowledge-Based Organization”, Editura Academiei Forțelor Terestre ”Nicolae Bălcescu”, Sibiu, 2016;
4. von LORINGHOVEN, Arndt Freytag, „Adapting NATO intelligence in support of One NATO“, *NATO Review Magazine*, 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;
5. https://media.uoradea.ro/article353-Lansarea-c%C4%83r%C5%A3ii-colonelului-dr-Eduard-Simion-%C5%9Fi-a-Punctului-de-Informare-NATO.


---

[1] Mark Galeotti, „Russian intelligence is at (political) war“, *NATO Review Magazine*, 12/05/2017, https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/EN/index.htm;

[2] https://www.nato.int/wearenato/security-challenges.html.

[3] Arndt Freytag von Loringhoven, „Adapting NATO intelligence in support of One NATO“, *NATO Review Magazine*, 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;

[4] În angrenajul informațiilor pentru apărare, domeniul informațiilor din surse umane reprezintă un element aparte, specificul său fiind dat de accesul la aspecte pe care senzorii tehnici nu le pot atinge: intenția adversarului, starea sa fizică, psihică şi morală, vulnerabilitățile individuale, rețelele umane etc., acestea fiind extrem de importante în confruntarea cu un inamic neconvențional, cu o identitate înşelătoare şi impredictibil în planificarea acțiunilor. Din jocul actorilor şi implicațiile multiple ale acestei activități rezidă complexitatea şi sensibilitatea acestui domeniu;

[5] Victor Madeira, „NATO COEs: Transforming Security and Intelligence to Boost Strategic Immunity”, *Atlantic Voices*, Vol.8, Issue 01, January 2018, https://www.slideshare.net/Atlantictreatyassociation/atlantic-voices-nato-counterintelligence;

[6] Existența Centrelor de excelență NATO îşi are originile în reorganizarea structurii de comandă militară a Alianței şi a lansării procesului de transformare sub egida Comandamentului Aliat pentru Transformare (Allied Command Transformation – ACT), în urma Summit-ului de la Praga din 2002. Odată cu conştientizarea necesității alocării unor resurse suplimentare care să sprijine eforturile ACT în domeniul transformării, Comitetul Militar al NATO a mandatat națiunile aliate, prin Conceptul său privind Centrele de excelență - MCM 236-03 (2003), să înființeze, într-un cadru stabilit şi în anumite condiții, centre de excelență menite să promoveze transformarea în cadrul Alianței, acestea fiind înțelese ca „*entități naționale sau multinaționale capabile să ofere expertiză şi experiență recunoscută în sprijinul Alianței, în special în sprijinul transformării*”. Centrele de excelență se bucură de statutul de *organizație militară internațională*, sub auspiciile Protocolului de la Paris, fiind structuri afiliate ACT, dar fără a face parte din structura de comandă a NATO;

[7] Eduard Simion, Alexandru Kis, *New features of the NATO Centres of Excellence in support of the North-Atlantic Alliance Transformation*, pp. 125-131, în volumul celei de-a 22-a Conferințe Internaționale – „The Knowledge-Based Organization”, Editura Academiei Forțelor Terestre ”Nicolae Bălcescu”, Sibiu, 2016;

[8] https://media.uoradea.ro/article353-Lansarea-c%C4%83r%C5%A3ii-colonelului-dr-Eduard-Simion-%C5%9Fi-a-Punctului-de-Informare-NATO.

[9] Victor Madeira, *Op. Cit.*

# SPAȚIUL CIBERNETIC – UN NOU MEDIU OPERAȚIONAL –

***Cornel Vasile ARGINT-ZAHARIOAEI****

***Abstract***

*The unprecedented development of technology creates opportunities in all areas of society but at the same time brings challenges and vulnerabilities. At all times, the latest technological innovations have been adapted to the military field, being generally turned into war instruments. Thus, the expansion of IT&C applications in all areas of life so far has inevitably led to the use of cyberspace in all areas of a military nature. This has led to the shaping and development of a new operational environment - the cyberspace. The interdependence of risks and threats in the cyberspace, coupled with the transformations and the unpredictability of the security environment, are major challenges to national security. States will need to equip themselves with a new set of capabilities for cyber, defensive and offensive actions at all levels (strategic, tactical, and operational).*

***Keywords:*** *technology, cyberspace, risks and threats, cyber-defense, Internet of Things.*

**Introducere**

Evoluția tehnologică, axată în prezent în jurul domeniului IT&C, va continua să aibă un impact major asupra dezvoltării statelor şi societății civile. Dezvoltarea exponențială a tehnologiei creează tot mai multe oportunități în toate domeniile societății, conducând la creșterea eficienței şi rapidității proceselor. Cu toate acestea, orice nouă tehnologie atrage după sine şi apariția unor provocări şi vulnerabilități, la care statele vor fi obligate să se adapteze.

Se poate observa cu uşurință modul în care implementarea tehnologiei informației a produs intensificarea informațională a majorității aspectelor, elementelor şi instituțiilor fundamentale ale societății. Accentuarea dependenței de informație a determinat extinderea la nivel global a rețelelor şi a serviciilor bazate pe tehnologia informațiilor.

Aşa cum s-a întâmplat de-a lungul istoriei, cele mai noi tehnologii au fost dezvoltate şi adaptate întotdeauna domeniului militar, fiind transformate în instrumente ale războiului. Extinderea generalizată a aplicațiilor IT&C în toate domeniile a condus inevitabil la folosirea spațiului cibernetic în aproape toate zonele cu specific militar, creând deopotrivă oportunități şi vulnerabilități. În acest mod, a apărut firesc un nou mediu operațional – spațiul cibernetic.

Scopul acțiunilor militare întreprinse în acest nou mediu operațional este similar celui din celelalte medii operaționale (terestru, maritim, aerian, cosmic şi electromagnetic), respectiv cunoaşterea situației şi obținerea de efecte ofensive şi defensive. Diferența este reprezentată de instrumentele folosite pentru desfăşurarea acțiunilor, în spațiul cibernetic folosindu-se cu predilecție instrumente virtuale.

La nivel politico-strategic, apariția spațiului cibernetic a generat o nouă formă de manifestare a puterii în relațiile internaționale – *puterea cibernetică*. Aceasta depinde direct proporțional de infrastructura digitală, de resursele hardware şi software, precum şi de potențialul de modelare

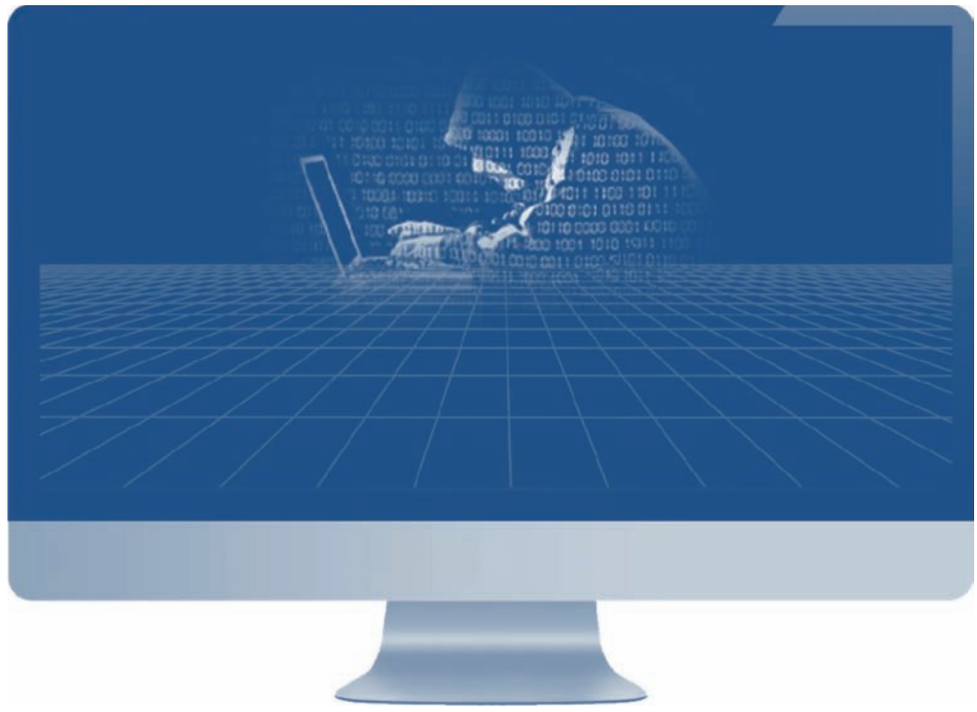
*Autorul este expert în cadrul Ministerului Apărării Naționale.*

a informațiilor transmise prin mediul cibernetic. În ultimul timp, ca urmare a facilitării accesului la spațiul cibernetic, factorul determinant al puterii cibernetice este reprezentat de resursa umană.

Una dintre cele mai complete definiții ale puterii cibernetice, general acceptată în literatura de specialitate, este cea oferită de Daniel Kuehl, potrivit căruia *puterea cibernetică este abilitatea de a utiliza spațiul cibernetic pentru a crea avantaje şi a influența elementele în toate mediile operaționale şi peste toate celelalte instrumente ale puterii.*

şi servicii s-au dovedit a fi extrem de propice pentru proliferarea „armelor" utilizate în spațiul cibernetic. Opțiunile de contracarare sunt reduse, cu atât mai mult cu cât actorii implicați pot include, pe lângă regimuri statale permisive, şi entități non-statale.

Spre deosebire de formele clasice de derulare a războiului în care amplitudinea forței fizice era determinantă, în confruntările moderne o pondere importantă au avut-o acțiunile în plan informațional. După anii '80, dezvoltarea impresionantă a mijloacelor de informare, de



**Specificitatea operațiilor cibernetice**

Se poate aprecia că, în viitorul apropiat, mediul internațional de securitate va fi marcat de un grad mare de incertitudine şi impredictibilitate, determinat de numeroşi factori, unii dintre aceştia înregistrând o manifestare lineară şi previzibilă (fiind consecințe obiective ale mediului de securitate sau rezultate ale unor strategii şi programe pe termen mediu şi lung), iar alții, printre care şi cei specifici spațiului cibernetic, având un caracter neaşteptat şi profund perturbator, reprezentând elemente de discontinuitate strategică.

Contextul tehnologic şi facilitatea accesului la tehnologiile moderne, creşterea libertății de mişcare şi liberalizarea schimburilor de mărfuri la Internet la noile tehnologii de informare şi comunicare, au declanşat procesul de revizuire a ideii de „proiecție a puterii".

Schimbarea raportului dintre forța fizică şi inteligența beligeranților, de la sfârşitul secolului XX şi începutul secolului XXI, este rezultatul progresului tehnologic al „erei nucleare". Aceasta a modificat profund natura războiului, rezumată de Raymond Aron prin formula „război improbabil, pace imposibilă". Practic, pacea era imposibilă din cauza rivalităților prea puternice dintre cele două blocuri politico-militare, iar războiul era improbabil deoarece efectele utilizării armelor atomice ar fi condus la un rezultat aleatoriu sau catastrofal pentru ambii adversari.

În prezent, această schimbare este reflectată cel mai bine în spațiul cibernetic, unde acțiunile desfășurate sunt mai ușor acceptate de societate, datorită numărului redus de victime, dar și de entitățile beligerante, prin prisma rezultatelor acestor acțiuni care le permit îndeplinirea obiectivelor.

Principalele trăsături ale operațiilor cibernetice, care le recomandă a fi utilizate înaintea altor operații clasice, sunt:

a) gradul ridicat de anonimizare – identificarea atacatorilor este aproape imposibilă;
b) impredictibilitatea „armelor" cibernetice, în special în cazul amenințărilor de tip „0 day";
c) absența unor frontiere de natură geografică;
d) efectul aproape instantaneu la țintă;
e) multitudinea de ținte care pot fi lovite simultan – atacul mai multor sisteme informatice cu o singură aplicație malițioasă (*malware*);
f) lipsa unor soluții rapide de remediere a consecințelor pe care le generează;
g) utilizarea unor tehnologii relativ simple, ieftine și larg răspândite pentru obținerea unor efecte de amploare;
h) ștergerea diferențelor dintre nivelurile de comandă, de la tactic la strategic.

Cerințele informaționale specifice spațiului cibernetic pot fi sintetizate prin parafrazarea învățăturilor strategului chinez Sun Tzu, astfel: (1) cunoașterea și actualizarea în permanență a situației din spațiul cibernetic; (2) împiedicarea adversarului de a penetra sistemele informatice proprii pentru a intra în posesia de informații reale; (3) dezinformarea adversarului prin lansarea de informații eronate în spațiul cibernetic sau prin furnizarea directă a acestora.

Spațiul cibernetic poate fi modelat prin trei niveluri – fizic, logic și social (Figura nr. 1).

Nivelul fizic include componenta geografică și componenta de rețea fizică (infrastructura terestră, maritimă, aeriană, spațială și electromagnetică). Componenta geografică reprezintă locația fizică a elementelor ce aparțin rețelei. Componenta de rețea fizică include tot ce înseamnă hardware și infrastructură (cabluri, fibre optice, unde electromagnetice) ce reprezintă suportul pentru rețea și conectorii fizici (conectori, emițătoare/receptoare radio, rutere, servere și calculatoare). La acest nivel pot

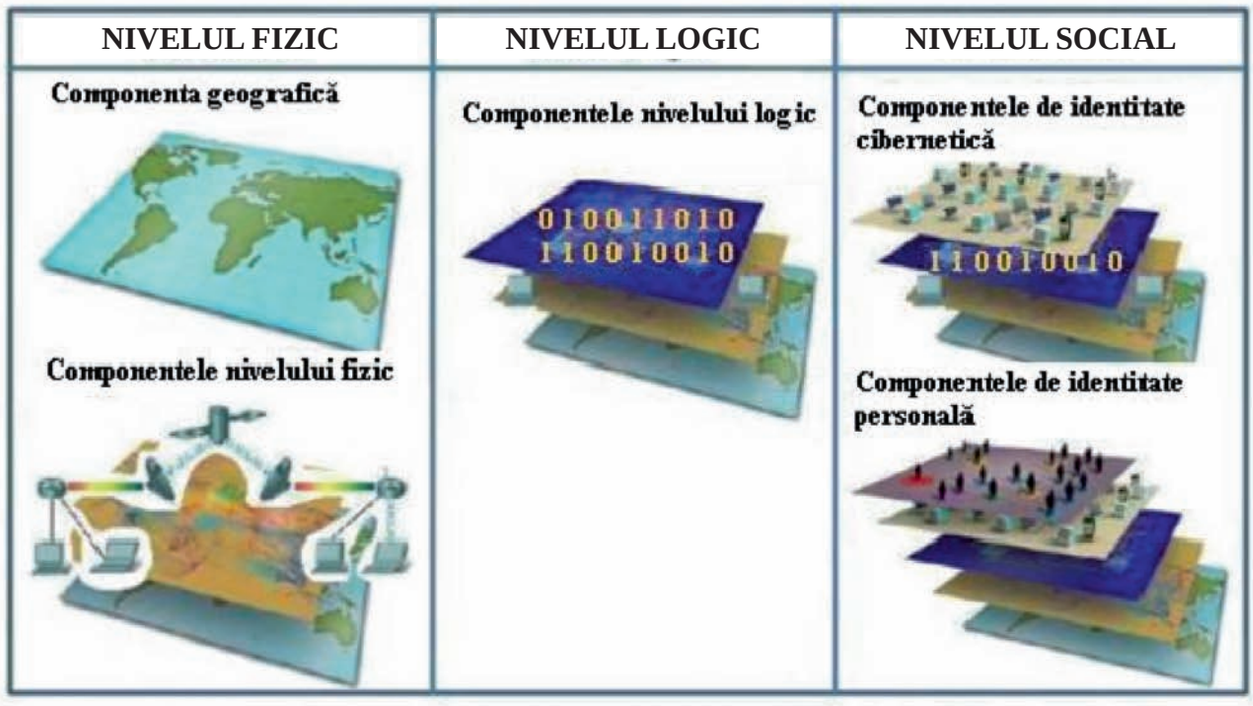



***Fig. nr. 1***

fi anticipate atacuri împotriva infrastructurilor, echipamentelor, armamentelor sau rețelelor. În acest strat, legătura între spațiul cibernetic şi alte spații este evidentă. Un raid aerian poate distruge, de exemplu, clădiri care adăpostesc servere şi astfel să blocheze capacități sau funcții din spațiul cibernetic. În acest mod, izolarea spațiului cibernetic ca un câmp de luptă distinct nu mai este posibilă.

Nivelul logic este constituit din conexiunile logice dintre nodurile rețelei. Nodurile reprezintă orice echipament conectat într-o rețea de calculatoare. Într-o rețea bazată pe protocolul internet (IP), nodul este reprezentat de orice echipament cu o adresă IP. La acest nivel, atacurile survin cel mai adesea prin utilizarea de softuri malițioase care permit distrugerea sistemelor informatice şi programelor adverse, indisponibilizarea lor sau preluarea controlului asupra lor.

Nivelul social este compus din componentele umane şi cognitive, şi include identitatea cibernetică şi identitatea personală. Identitatea cibernetică reprezintă elementele tehnice de identificare a unei persoane sau a unei entități (instituție, grup etc.) în rețea: adresa de mail, adresa de IP, număr de telefon etc. Identitatea personală reprezintă indivizii care sunt în spatele elementelor tehnice. Un individ poate avea mai multe identități cibernetice (exemplu: diferite adrese de mail pe diferite stații de lucru) şi, invers, în spatele unei identități cibernetice pot fi mai mulți utilizatori. La acest nivel, un adversar va urmări obținerea neautorizată de informații sau modificarea datelor stocate sau transmise, pentru a determina adversarul să ia decizii greşite. Se observă aici foarte clar diversitatea acțiunilor posibile împotriva forțelor armate în spațiul cibernetic şi numeroasele vulnerabilități care trebuie controlate.

Prioritizarea activităților între cele trei niveluri devine foarte dificilă, din moment ce consecințele în toate cele trei straturi se pot dovedi fatale pentru sistemul informatic în ansamblul său. Aproape toate acțiunile posibile sunt relevante pentru securitatea militară.

Infrastructurile informatice, tot mai importante în societatea modernă, devin în acelaşi timp ținte şi vectori ai atacurilor cibernetice. Similar unui atac convențional, securitatea populației este pusă în pericol. Un război în spațiul cibernetic poate aduce victoria prin atacarea infrastructurilor civile critice din domeniul aprovizionării energetice (apă, gaz, electricitate), sănătății, traficului rutier, feroviar sau aerian, aprovizionării generale etc.

**Evoluția viitoare a spațiului cibernetic**

Datorită dezvoltării exponențiale a echipamentelor hardware şi a aplicațiilor software, este extrem de greu să se realizeze o evaluare precisă a modului în care vor evolua acțiunile specifice în mediul cibernetic. Totuşi, există câteva elemente care oferă indicii asupra caracteristicilor unor posibile activități care se vor desfăşura în acest nou mediu operațional:

a) anumite state vor răspunde atacurilor cibernetice prin acțiuni militare convenționale, după cum deja este precizat în anumite doctrine militare;
b) armele cibernetice vor fi folosite în cazul conflictelor deschise pentru culegerea de informații, perturbarea sau influențarea senzorilor şi a comunicațiilor, influențarea deciziilor şi chiar distrugerea fizică a anumitor echipamente;
c) avantajul principal al unui agresor care foloseşte spațiul cibernetic va fi oferit de dificultatea adversarului de a conştientiza că este atacat şi de a identifica autorul atacului;
d) agresorul nu va fi neapărat un stat sau o grupare organizată, ci poate fi o entitate izolată, un grup terorist cu mijloace limitate sau grupuri infracționale motivate doar de câştiguri financiare;
e) agresorul va putea acționa oriunde şi instantaneu; flexibilitatea spațiului cibernetic permite fiecărui actor sau fiecărui utilizator să-şi construiască propriul spațiu în funcție de utilizarea sa, de reprezentările sau de interesele sale;

f) generalizarea acțiunilor în spațiul cibernetic prin dezvoltarea dispozitivelor aparținând „Internetului Obiectelor" (Internet of Things – IoT). Conceptul IoT presupune că, în viitor, majoritatea obiectelor care ne înconjoară vor fi conectate la Internet, fiecare având un IP propriu. În prezent, acest concept este deja vizibil într-o gamă largă de aplicații: camere de supraveghere, sisteme de avertizare, sisteme de semaforizare, electrocasnice etc. În viitor, se estimează generalizarea conectării obiectelor la Internet: autovehicule inteligente, clădiri inteligente, orașe inteligente etc. În general, echipamentele din categoria IoT sunt limitate din punct de vedere al resurselor (energie, capacitate de transfer, memorie, spațiu de stocare etc.), ceea ce se concretizează într-un nivel scăzut de securitate, care, implicit, reprezintă o oportunitate de exploatare a acestora de către potențiali atacatori;

g) forțele armate moderne vor deține capabilități militare avansate bazate pe tehnologia informațiilor, inclusiv „arme cibernetice". Aceste noi capabilități pot fi utilizate într-o manieră nedistructivă, asigurând supravegherea și culegerea de informații din spațiul cibernetic, sau într-o manieră distructivă, făcând posibilă alterarea sau distrugerea informațiilor rezidente pe mediile de stocare, precum și distrugerea fizică a sistemelor informatice conectate și controlate prin spațiul cibernetic;

h) sub umbrela unei anonimități plauzibile, statele vor utiliza capacitățile cibernetice proprii pentru spionaj militar și industrial, pentru supravegherea și interceptarea comunicațiilor, precum și pentru manipularea informațiilor și comunicațiilor destinate unor actori țintă.

**Concluzii**

Evoluția tehnologică a condus la apariția unui nou mediu operațional de confruntare care aduce cu sine modificarea paradigmei desfășurării operațiilor militare.

Interdependența riscurilor și amenințărilor din spațiul cibernetic, dublată de mutațiile și impredictibilitatea accentuată a mediului de securitate, reprezintă provocări cu impact major la adresa abordărilor naționale în domeniul securității și apărării. În acest context, statele vor fi nevoite să se doteze cu un set nou de capabilități pentru conducerea operațiunilor cibernetice defensive și ofensive la nivel strategic, tactic și operațional. Acestea vor conține un arsenal complet pentru desfășurarea de operații: culegerea de informații, protejarea infrastructurii proprii și desfășurarea de acțiuni ofensive.

De asemenea, în vederea optimizării exploatării unor astfel de capabilități, statele vor trebui să integreze apărarea cibernetică în concepții, doctrine, planificări operaționale și programe pentru pregătirea specialiștilor, astfel încât să se asigure flexibilitatea efectelor. Acest proces include integrarea capabilităților specifice operațiunilor din spațiul cibernetic cu cele cinetice, dar și cu alte forme de război informațional, precum STRATCOM și PSYOPS.

**Bibliografie:**


1. RYTE, Marc-Andre, „A patra revoluție industrială și impactul său asupra forțelor armate", octombrie, 2017, online la adresa https://cybersecuritytrends.ro;
2. KEPE, M.; BLACK J.; MELLING J. și PLUMRIDGE Jess, *Exploring Europe's capability requirements for 2035 and beyond*, European Defence Agency, RAND Europe, iunie 2018;
3. LAZĂR, Arthur, „Puterea cibernetică, un pilon esențial al puterilor viitorului", iulie, 2017, online la adresa https://cybersecuritytrends.ro;
4. DAN-ȘUTEU, Ștefan-Antonio, „Rolul apărării cibernetice în cadrul sistemelor de comandă și control", *Buletinul UNAp „Carol I"*, martie, 2017.

# GEOINT – INTEGRATOR ŞI PLATFORMĂ SUPORT PENTRU ANALIZA MULTI-SURSĂ

***Alexandru ZAMFIR****

***Abstract***

*In the current security environment, where intelligence services are facing a context of information overload and distortion, every day, the GEOINT capability provides fast and reliable analysis that supports the decision making process.*

*The term GEOINT stands for GEOspatial INTelligence, which is a discipline that comprises the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on Earth. The information from collateral sources, collected by other intelligence capabilities, could be fused into an integrated intelligence product, as added value.*

*Taking into consideration the modern intelligence paradigm, the GEOINT domain is considered to be a complementary discipline, but in the same time it enables the integration of other intelligence domains – HUMINT, SIGINT, OSINT – on a geospatial support.*

***Keywords****: GEOINT, geospatial support, imagery, intelligence.*

În contextul actual de securitate, în care serviciile de informaţii se confruntă cu un aflux masiv de date şi informaţii al căror nivel de veridicitate este dificil de stabilit, analiza GEOspatial INTelligence (GEOINT) oferă într-un interval de timp redus produse informative cu un grad ridicat de credibilitate.

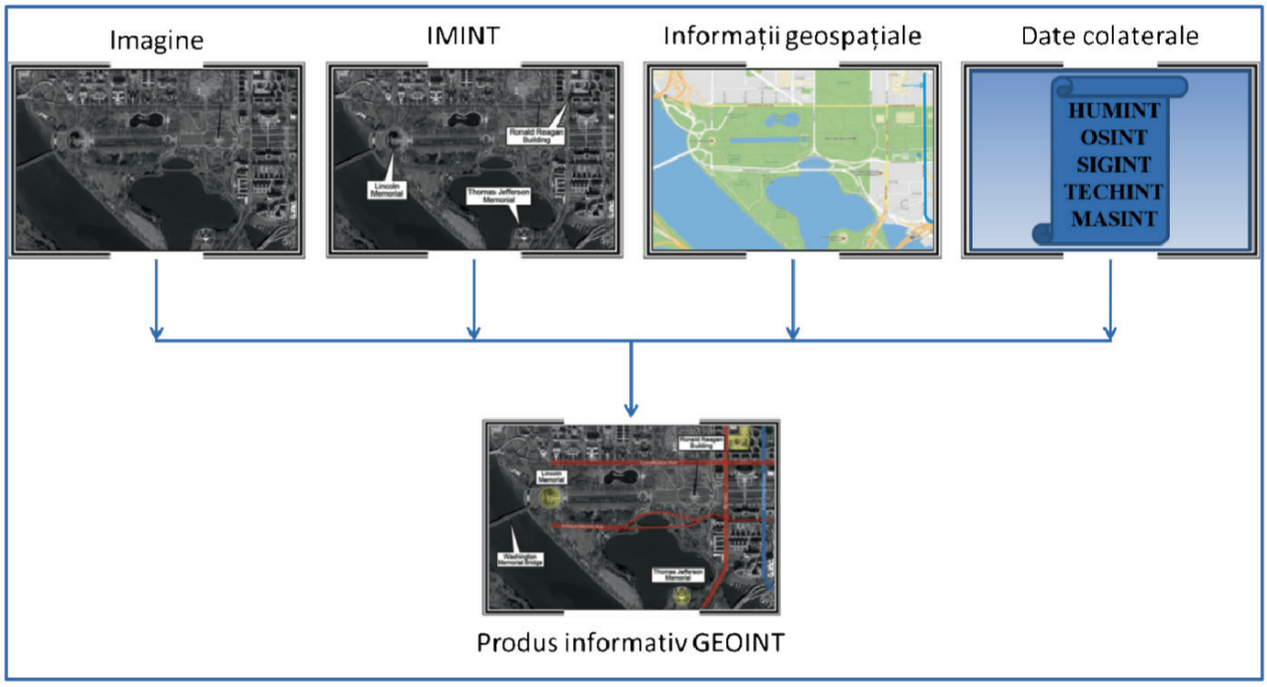
Preocuparea unui serviciu de informaţii de a dezvolta domeniul GEOINT denotă atât interesul de a asigura capacitatea de promovare şi protejare a intereselor naţionale şi de îndeplinire a angajamentelor euroatlantice asumate în planul securităţii şi apărării, dar şi nivelul de ambiţie al acestei structuri de informaţii[1].

Potrivit Agenţiei Naţionale pentru Informaţii Geospaţiale SUA (National Geospatial Intelligence Agency – NGA), GEOINT constă în analiza şi exploatarea imaginilor şi informaţiilor geospaţiale pentru a descrie, evalua şi a evidenţia vizual detaliile fizice şi activităţile referenţiate geografic de pe suprafaţa Pământului[2].

GEOINT este o disciplină care a evoluat prin integrarea imaginilor, a IMagery INTelligence (IMINT), a datelor şi informaţiilor geospaţiale într-un cadru multi-funcţional, capabil să sprijine misiunile desfăşurate la nivel naţional şi internaţional, dar şi misiunile executate în teatrele de operaţii.

GEOINT este o capabilitate de intelligence de natură tehnică, din aceeaşi categorie cu SIGnal INTelligence (SIGINT) sau IMINT, spre deosebire de clasicul HUMan INTelligence (HUMINT) sau modernul Open Source INTelligence (OSINT). Principiul de bază al GEOINT este organizarea şi combinarea tuturor datelor disponibile în jurul locaţiilor geografice, urmată de exploatarea acestora, pentru a crea produse informative care să fie uşor de utilizat de către decidenţii politico-militari[3].

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




Imaginea de mai sus oferă un exemplu privind fiecare dintre cele patru elemente componente ale GEOINT şi rezultatul valorificării acestora în cadrul unui produs informativ integrat[4].

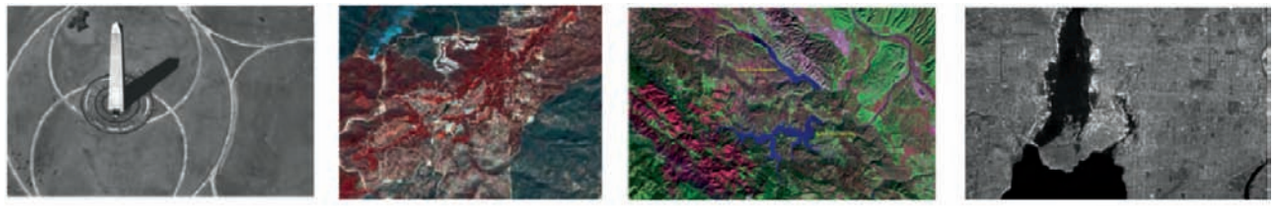
**Fluxul de culegere a informațiilor**

Imaginile sunt colectate de un sistem format din senzori şi platforme. Soluția sistemului utilizat pentru colectarea datelor depinde de tipul de date necesare, de condițiile în care sunt colectate datele şi de scopul pentru care sunt utilizate.

Principalele **platforme de colectare** a datelor sunt împărțite în următoarele categorii[5]:

- **Sateliți guvernamentali sau comerciali**. Aceştia orbitează la o altitudine mai ridicată decât celelalte platforme aeriene, fiind capabili să colecteze informații de pe întreaga suprafață terestră, inclusiv din teritorii ostile sau zone unde alte platforme aeriene nu au acces.
- **Platforme aeriene cu pilot sau fără pilot uman** (*manned or unmanned aerial vehicles – UAV*). Spre deosebire de platformele satelitare, platformele aeriene sunt capabile să ofere monitorizarea permanentă a unei locații sau ținte. De asemenea, platformele aeriene aparținând forțelor armate pot primi misiuni în timp real, fiind mult mai flexibile din punct de vedere operațional. Totuşi, eficacitatea platformelor aeriene poate fi limitată de către spațiul aerian de zbor interzis sau de către condițiile meteorologice[6].
- **Platforme terestre.** Orice obiect de pe suprafața Pământului, aflat în mişcare sau static, care are montat o cameră sau un senzor.
- **Platforme maritime cu pilot sau fără pilot uman.** În această categorie sunt incluse navele, submarinele, navele subacvatice de supraveghere sau geamandurile.

Principala sursă de informații pentru analiza GEOINT este reprezentată de imagini, existente în orice format, culese de către senzori de-a lungul întregului spectru electromagnetic. **Categoriile principale de senzori**[7] sunt electro-optici (EO) şi RADAR (radio detecting and ranging), fiecare având multiple alte subtipuri. Avantajul imaginilor RADAR față de imaginile optice este dat de senzor, care permite iluminarea mediului şi a obiectelor, utilizând impulsurile electromagnetice, fiind un senzor activ. Imaginile culese de către senzorii SAR (Synthetic Aperture Radar) nu sunt dependente de condițiile atmosferice, cum ar fi acoperirea cu nori sau furtunile de nisip, şi pot prelua imagini atât ziua, cât şi noaptea. Imaginile SAR sunt similare unei radiografii X-ray a unei zone sau a unui obiect.




Particularitatea unui produs informativ GEOINT este faptul că exploatează şi integrează informaţii geospaţiale, caracteristice domeniului cartografiei. **Informaţiile geospaţiale**[8] sunt derivate din datele provenite de la diferite surse, care includ platforme şi senzori utilizaţi pentru colectarea de imagini, senzori subacvatici de tip sonar şi senzori tereştri. Informaţiile geospaţiale pot fi grupate în următoarele categorii principale:

- **Aeronautice:** obstacole aeriene, zone de interdicţie aeriană, rute de zbor şi hărţi aeronautice etc.;
- **Maritime:** rute maritime, obstacole subacvatice, restricţii de navigare, infrastructura portuară, hărţi nautice etc.;
- **Topografice:** informaţii legate de infrastructură (drumuri, reţele electrice etc.), forme de relief naturale şi artificiale, date despre populaţie, vegetaţie şi hidrografie, toponime etc.;
- **Date de elevaţie:** informaţii privind înălţimea unor obiecte de pe suprafaţa Pământului (clădiri şi forme de relief), înălţimi de pe suprafaţa Pământului sau de pe fundul mărilor şi oceanelor (batimetrie, facilităţi subacvatice);
- **Geodezice:** date magnetice sau gravimetrice, dar şi sisteme de coordonate geografice.

**Particularităţi ale analizei GEOINT**

Domeniul GEOINT consolidează capabilităţile în domeniul informaţiilor militare, prin integrarea teledetecţiei în cadrul analizei militare moderne. Astfel, analiza facilităţilor militare şi a forţelor armate dislocate într-o zonă de interes beneficiază de următoarele avantaje operaţionale:

- **Accesul la informaţia brută**. Avantajul faţă de sursele clasice de intelligence este reprezentat de accesul la date şi informaţii neprelucrate. În prezent, din ce în ce mai multe companii comerciale oferă imagini satelitare de înaltă şi foarte înaltă rezoluţie (< 1m), iar concurenţa din acest domeniu conferă GEOINT o gamă vastă de surse de date;
- **Acoperire globală**[9]. Prin intermediul unei proceduri de tasking ale platformelor satelitare, imagini din zonele de interes pot fi obţinute aproximativ în timp real, asigurând un timp de răspuns mult mai redus decât în cazul colectării informaţiilor din alte surse de informaţii;
- **O altă perspectivă de analiză a informaţiilor**. Prin proiectarea pe un suport geospaţial a informaţiilor din alte surse, analistul vizualizează informaţiile disponibile dintr-un alt unghi. De exemplu, în teatrul de operaţii Afganistan, acest concept este utilizat în cadrul analizei predictive, atunci când se doreşte studierea modului de operare al insurgenţilor, cu ajutorul conceptelor TTP (*Tactics, Techniques and Procedures*) legate de amplasarea dispozitivelor explozive improvizate sau în cadrul procesului de targeting, pentru stabilirea ritmului de viaţă cotidian (pattern of life) pentru o persoană de interes;
- **Precizie şi acurateţe**. Prin activităţi specifice se determină coordonatele geografice precise ale unei ţinte de interes, dar şi dimensiunile obiectelor şi alte caracteristici, deseori aflate în medii nepermisive din punct de vedere operativ.
- **Dovezi conforme cu realitatea din teren**. Gradul de veridicitate al analizelor GEOINT realizate folosind imaginile obţinute prin teledetecţie este dificil de infirmat, comparativ cu situaţiile în care validarea este efectuată cu alte surse convenţionale de informaţii.

- **Utilizarea unor surse multiple**. Disciplina GEOINT foloseşte senzori diferiți pentru a îmbunătăți eficacitatea procesului de analiză a obiectivelor de interes. Pe lângă imaginile culese cu senzori electro-optici, GEOINT utilizează imagini SAR, IR (infra-red) sau obținute prin tehnologia LIDAR (LIght Detection And Ranging). În funcție de particularitățile fiecărei analize, se pot culege imagini prin metode diferite, pentru a satisface nevoile beneficiarilor. De exemplu, în cazul în care un anumit obiectiv se dorește a fi analizat pe timpul nopții, se vor folosi imagini SAR, care nu sunt dependente de iluminarea solară[10].
- **Modalitate neintruzivă.** GEOINT oferă posibilitatea de colectare a informațiilor din medii nepermisive sau ermetice, prin intermediul platformelor satelitare care nu sunt constrânse de reglementări specifice spațiilor aeriene suverane ale altor state.

**Limitări ale analizei GEOINT**

Analiza din surse GEOINT prezintă însă şi o serie de limitări, în pofida suitei de avantaje operaționale descrise mai sus. Unele dintre aceste limitări pot fi depăşite printr-o planificare oportună a misiunilor de culegere a datelor. De asemenea, progresul tehnologic înregistrat de către noile tehnologii de preluare a datelor imagistice oferă posibilități de teledetecție care pot, în parte, satisface nevoile operaționale.

- **Potențialele ținte pot fi ascunse.** Prin utilizarea metodelor clasice de mascare sau dispunerea tehnicii militare în hangare, detectarea şi identificarea țintelor devine dificilă.
- **Proces consumator de timp.** Multe dintre imaginile utilizate în analiza GEOINT necesită un proces de prelucrare şi analiză, consumator de timp, deşi timpul de procesare a fost redus substanțial datorită dezvoltării tehnologiei în domeniu.
- **Condiții meteo şi iluminare**. Influența parametrilor de mediu poate fi covârşitoare atunci când este necesară culegerea unei imagini satelitare la un anumit moment, deoarece o mare parte din acoperirea globală satelitară este realizată cu senzori electro-optici, dependenți de condițiile meteo, cum ar fi acoperirea cu nori şi iluminarea solară.
- **Necesitatea coroborării informației cu alte surse**. Pentru a interpreta şi identifica corespunzător elementele de interes, este necesară colaționarea şi coroborarea informațiilor din alte surse cu datele GEOINT avute la dispoziție.

**GEOINT – integrator şi platformă suport pentru analiza multi-sursă**

Având în vedere paradigma actuală de intelligence, domeniul GEOINT este considerat ca fiind o disciplină complementară, dar şi integrator al domeniilor clasice de intelligence – HUMINT, SIGINT, OSINT[11]. GEOINT oferă, de asemenea, posibilitatea de a funcționa ca suport în procesul de luare a deciziilor pe toate cele trei paliere, tactic, operativ şi strategic, tehnologiile GIS (*Geographic Information System*) având capabilitatea de a integra informații culese cu ajutorul surselor umane sau din surse deschise şi orice alte date din surse tehnice[12].

GEOINT schimbă percepția generală referitoare la unul dintre produsele de bază, hărțile georeferențiate, conform căreia acestea sunt doar o reprezentare statică a mediului operațional. Progresele tehnologice înregistrate în ultima perioadă de către aplicațiile software GIS dedicate au creat abilitatea de a integra capabilitățile celorlalte discipline de intelligence pentru vizualizarea, analiza şi diseminarea informațiilor fuzionate din zonele de interes.

Utilitatea GEOINT este dată, în principal, de integrarea comprehensivă pe un suport geospațial a tuturor informațiilor furnizate de către celelalte surse, oferind astfel utilizatorului o altă perspectivă de vizualizare şi înțelegere a informațiilor, prin intermediul unei hărți electronice interactive şi dinamice. Astfel, analiştii şi decidenții militari pot vizualiza spațiile de interes operativ şi informativ prin intermediul unor aplicații web intuitive, în care informațiile sunt convertite şi structurate sub forma unor straturi tematice (layere)[13].

Principiul de funcționare al acestei platforme colaborative este bazat pe asocierea de componente spațiale datelor în cadrul fluxului de procesare, pentru a permite analizarea datelor, utilizând o tehnologie GIS. Diseminarea este posibilă sub forma unor produse informative GEOINT, care includ hărți simple, sau sub forma unor hărți dinamice şi accesibile prin intermediul portalului intern, din cadrul organizației, atât beneficiarilor, cât şi celorlalți analişti care lucrează pe acelaşi spațiu de interes.

Aplicațiile software GIS sunt, de asemenea, compatibile cu aplicații software pentru analizarea datelor, ceea ce înseamnă că analiştii au la dispoziție un instrument puternic care le permite să efectueze asocieri, analize temporale şi geospațiale.

**GEOINT folosit pentru validarea informațiilor**

În activitatea de intelligence, informațiile provenite dintr-o singură sursă nu pot fi suficiente pentru a evalua o informație ca fiind sigură sau certă. În marea majoritate a cazurilor, informația este catalogată ca posibilă sau probabilă, având în vedere criteriile specifice fiecărui tip de intelligence (de exemplu, în cazul HUMINT, se ține cont de veridicitatea informației şi de credibilitatea sursei)[14].

GEOINT-ul oferă posibilitatea de a certifica veridicitatea informației şi, după caz, de a completa informația. Spre exemplu, sursele deschise pot oferi informații interesante despre dislocări de tehnică de aviație pe o bază aeriană. Prin analiza imagistică a obiectivului militar se poate confirma informația conform căreia a fost dislocată tehnică de aviație şi, în acelaşi timp, se poate completa această informație prin identificarea tipurilor de aeronave şi a numărului acestora.

Există o serie de elemente care pot afecta corectitudinea rezultatelor obținute prin validarea multi-sursă. În primul rând, termenul de predare a produsului informativ poate crea o presiune a timpului asupra analistului, care alege să răspundă în timp util solicitării din partea beneficiarului, fără a încerca o validare a informației prin acumularea de mai multe date GEOINT. În al doilea rând, procesul de coroborare a surselor poate fi dificil, doar din simplul fapt că nu toate informațiile din alte surse conțin şi atributul spațial, atât de necesar atunci când se ia în calcul convergența cu domeniul GEOINT[15].

**Concluzii**

În cele mai multe cazuri, produsele informative sunt realizate sub forma unor documente pe suport hârtie, electronic sau prezentări expuse direct beneficiarului. GEOINT oferă posibilitatea de a menține consumatorii de intelligence conectați în timp real la evoluțiile din zonele de interes, cu scopul de a sprijini procesul de luare a deciziilor, prin intermediul unei analize integrate a spațiului de luptă. Integrarea informațiilor provenite din sursele clasice de intelligence şi proiectarea acestora pe un suport geospațial, utilizând aplicații software de tip GIS, reprezintă un instrument puternic pentru monitorizarea contextului de securitate sau operațional.

GEOINT poate reprezenta cel mai mare numitor comun al „INT”-urilor, locul unde celelalte surse/categorii de informații se pot intersecta[16].

Cu toate că acest articol abordează doar aspecte privind exploatarea şi analiza imaginilor şi informațiilor geospațiale şi crearea produselor informative, domeniul este mult mai complex şi include instruirea personalului, tehnologia de colectare a datelor, cercetare şi dezvoltare, stocarea şi diseminarea produselor informative GEOINT. Volumul foarte mare de date diversificate care necesită procesare implică întrebuințarea unor tehnologii complexe în cadrul analizei GEOINT, dar şi abilități tehnologice deosebite ale analiştilor specializați pe acest domeniu de nişă.

Serviciile de informații îşi consolidează capabilitățile de răspuns la situații de criză, conflict şi avertizare timpurie prin continuarea dezvoltării domeniului GEOINT, pentru colectarea de informații din medii nepermisive şi pentru integrarea pe un suport geospațial a informațiilor provenite din celelalte surse de informații, având ca scop final adoptarea deciziilor de către factorii decidenți politico-militari.

**Bibliografie:**


1. FOCA, Marcel; BĂLOI, Aurel-Mihai, *GEOINT Analysis – suport decizional care poate face diferența*, în *ARS ANALYTICA – Provocări şi tendințe în analiza de intelligence*, Editura Rao, Bucureşti, 2013;
2. Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0, 2018, p. 4, disponibil on-line la https://www.nga.mil/ProductsServices/Pages/GEOINT-Basic-Doctrine-Publication.aspx;
3. GRĂDINARU, Cătălin, „GEOINT – capabilitate specifică secolului XXI", în *Infosfera*, nr. 2/2010, DGIA, Bucureşti;
4. COSTEA, Cătălina, *Analiza multisursă*, în *ARS ANALYTICA – Provocări şi tendințe în analiza de intelligence*, Editura Rao, Bucureşti, 2013, p. 197;
5. CALOTĂ, Edward; CĂLIN, Vasile, „Păsări de fier – O perspectivă modernă asupra spațiului de luptă informațional", în *Infosfera*, nr. 2/2010, DGIA, Bucureşti, p. 66;
6. https://en.wikipedia.org/wiki/Geospatial_intelligence;
7. https://www.esri.com/en-us/arcgis/products/arcgis-enterprise/what-you-get;
8. https://gisgeography.com/passive-active-sensors-remote-sensing/;
9. https://www.nga.mil/ProductsServices/Pages/default.aspx;
10. https://en.wikipedia.org/wiki/Geospatial_intelligence.


[1] Marcel Foca, Aurel-Mihai Băloi, *GEOINT Analysis – suport decizional care poate face diferența*, în *ARS ANALYTICA – Provocări şi tendințe în analiza de intelligence*, Editura Rao, Bucureşti, 2013, p. 185.
[2] https://www.nga.mil/ProductsServices/Pages/default.aspx.
[3] https://en.wikipedia.org/wiki/Geospatial_intelligence.
[4] Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0, 2018, p. 4, disponibil on-line la https://www.nga.mil/ProductsServices/Pages/GEOINT-Basic-Doctrine-Publication.aspx.
[5] Geospatial Intelligence (GEOINT) Basic Doctrine (2018), op. cit., p. 7.
[6] Edward Calotă, Vasile Călin, „Păsări de fier – O perspectivă modernă asupra spațiului de luptă informațional", în *Infosfera nr. 2/2010*, DGIA, Bucureşti, p. 66.
[7] Geospatial Intelligence (GEOINT) Basic Doctrine (2018), op. cit., p. 10.
[8] Geospatial Intelligence (GEOINT) Basic Doctrine (2018), op. cit., p. 13.
[9] Cătălin Grădinaru, „GEOINT – capabilitate specifică secolului XXI", în *Infosfera nr. 2/2010*, DGIA, Bucureşti, p. 75.
[10] https://gisgeography.com/passive-active-sensors-remote-sensing/.
[11] Cătălin Grădinaru, op. cit., p. 70.
[12] Marcel Foca, Aurel-Mihai, Băloi, op. cit., p. 189.
[13] https://www.esri.com/en-us/arcgis/products/arcgis-enterprise/what-you-get.
[14] Cătălina Costea, „Analiza multisursă", în *ARS ANALYTICA – Provocări şi tendințe în analiza de intelligence*, Editura Rao, Bucureşti, 2013, p. 197.
[15] Cătălina Costea, op. cit., p. 199.
[16] Marcel Foca, Aurel-Mihai, Băloi, op. cit., p 191.

# IMPLICAȚIILE UTILIZĂRII INTELIGENȚEI ARTIFICIALE ÎN DOMENIUL MILITAR

***Georgian NEDELCU****

***Abstract***

*Both military and commercial robots will in the future incorporate artificial intelligence that could make them capable of undertaking tasks and missions on their own. In the military context, this gives rise to an examination as to whether such robots should be allowed to execute such missions, especially if there are the situations that involve the use of lethal force against human beings.*

*To better understand the issues at stake, this paper presents a framework explaining the current state of the art for AI in the military field, the strengths and weaknesses of the technology, and what the future likely holds. The paper demonstrates that while computers and AI can be superior to humans in some skills and rule based tasks, under situations in the presence of significant uncertainty that require judgment and knowledge humans are superior to that.*

***Keywords****: military robots; unmanned systems; holistic scenarios; self-navigation; collective behavior; self-recovery, armament program, defense industry, military hardware.*

**Date generale**

În perspectivă, roboții autonomi, atât cei cu specific militar, cât şi cei civili, vor avea încorporată inteligență artificială (IA), care le va asigura capacitatea de a înțelege ordinele (sarcinile, misiunile), de a percepe mediul în care se află și de a lua decizii în vederea executării misiunilor încredințate.


*Autorul este expert în cadrul Ministerului Apărării Naționale.*

În general, ciclul de procesare a informațiilor specific inteligenței umane urmează secvența percepție – gândire – acțiune. Pe baza anumitor percepții din mediul înconjurător este derulat un proces de analiză (*gândire*), iar după ce sunt analizate opțiunile disponibile, se ia decizia şi se acționează. IA este programată să urmeze etape similare procesului uman. Astfel, computerul simte ceea ce este în jurul acestuia, iar apoi procesează şi ia decizii. Din această perspectivă, deşi computerele şi sistemele dotate cu IA sunt superioare ființelor vii în executarea unor sarcini de rutină care necesită unele îndemânări şi procese repetitive, în situații care necesită judecată şi luarea unor decizii într-un mediu caracterizat de incertitudine, ființele umane sunt net superioare IA.

Roboții militari sunt utilizați în cadrul unor sisteme integrate (care includ sisteme de culegere a datelor, sisteme de analiză şi de luare a deciziilor), au diferite configurații şi mărimi în funcție de misiunile de îndeplinit[1] şi pot opera cu un anumit nivel de autonomie sau sunt controlați de la distanță. Roboții militari sunt utilizați în toate mediile de luptă: terestru, aerian şi naval. Deşi majoritatea acestora execută misiunile în mod automat, în prezent aproape toate sistemele fără pilot implică intervenția umană pentru fiecare aspect practic al operării acestora.

Viitorul IA în realizarea şi operarea roboților militari este direct legat de capacitatea de proiectare de sisteme autonome independente, capabile să ia decizii pe baza cunoştințelor şi a experienței acumulate. Spre exemplu, unele dintre sistemele aeriene fără pilot (*Unmanned Aerial Vehicle – UAV*) vor putea patrula deasupra unei zone şi vor aştepta apariția țintei. Un exemplu în acest sens este reprezentat de către sistemul UAV Harop[2], dezvoltat în cadrul industriei de apărare israeliene.

Sistemele UAV autonome de înălțime mare vor putea fi utilizate ca legături de date de rezervă în situația distrugerii sateliților de comunicații sau ca platforme pe care să fie instalate lasere pentru combaterea rachetelor balistice.

Sistemele de luptă sub apă vor deveni şi mai importante în viitor, în condițiile în care, de pe mare, forța va fi proiectată în interiorul zonelor Anti-Access/Area Denial (A2/AD). Sistemele de luptă sub apă fără pilot (*Unmanned Underwater Vehicle – UUV*) vor putea executa o serie de misiuni cu un grad ridicat de periculozitate, cum ar fi:

- operații de deminare sau minare în proximitatea zonei de coastă a inamicului;
- culegerea de informații de la rețeaua de senzori de sub apă în zone maritime disputate;
- patrulare cu sonar activ;
- reîncărcarea submarinelor cu rachete.

**Evoluții în domeniul inteligenței artificiale. Implicații în plan militar**

În ultimii cinci ani, cercetătorii au atins unele obiective[3] în domeniul tehnologiei IA, mult mai devreme decât estimările inițiale ale experților.

Progresul rapid din domeniul IA este favorizat de patru factori principali:

- creşterea exponențială a performanțelor sistemelor informatice;
- disponibilitatea unor baze de date care facilitează sistemul de învățare al roboților (ceea ce le va permite roboților militari să ia decizii bazate pe datele furnizate de senzori);
- performanțele în implementarea tehnicilor de învățare a roboților;
- investiții financiare semnificative în dezvoltarea domeniului roboticii.

Dezvoltările din ultimii ani în domeniul IA vor avea implicații şi în domeniul securității naționale, aducând schimbări cel puțin în două domenii: superioritatea militară şi superioritatea informațiilor. În ceea ce priveşte superioritatea militară, progresul înregistrat în IA şi, implicit, în domeniul roboților militari, va face să fie disponibile noi capabilități, iar cele existente vor deveni accesibile unui număr tot mai mare de actori (statali şi non-statali). În ceea ce priveşte domeniul cibernetic, activitățile care în prezent necesită personal înalt calificat, cum ar fi de exemplu operațiile de tip Amenințare Persistentă Avansată (*Advanced Persistent Threat*), vor fi, în viitor, în mare parte, automatizate. Din punct de vedere al superiorității informațiilor, IA va

îmbunătăți capabilitățile de culegere şi de analiză a datelor, dar şi pe cele de generare a metadatelor.

Inițial, progresul tehnologic va asigura cel mai mare avantaj forțelor armate (FA) din state dezvoltate şi avansate din punct de vedere tehnic şi tehnologic, la fel cum s-a întâmplat cu sistemele UAV şi UGV (*Unmanned Ground Vehicle*). Odată ce costurile tehnologiei vor scădea, statele cu limitări bugetare şi cu forțe armate mai puțin avansate din punct de vedere tehnic vor adopta aceste tehnologii, fapt ce va fi urmat şi de către actorii non-statali. Acest model se observă şi în prezent: Statul Islamic (SI) a utilizat UAV-uri comandate de la distanță în sprijinirea derulării propriilor operații militare, exemplu fiind cel al atacării bazei ruse Hmeymim din Siria, prin utilizarea de sisteme aeriene fără pilot, realizate din componente comerciale[4]. De asemenea, în viitor, organizațiile teroriste vor înregistra o creştere a utilizării vehiculelor autonome pe timpul executării de atacuri.

Pe lângă o serie de beneficii, utilizarea IA în domeniul militar prezintă şi o serie de riscuri, astfel:

- posibilitatea ca un subiect (care poate fi un stat, actor non-statal sau organizație teroristă sau de crimă organizată) să utilizeze IA într-un scop ilegal, cum ar fi executarea unui atac terorist (o mașină autonomă transformată în VBIED[5] fără prezența şoferului sinucigaş);
- posibilitatea ca IA însăşi să scape de sub control şi să înceapă să ia propriile decizii.

În prezent, în cadrul Departamentului Apărării al SUA sunt în derulare demersuri pentru dezvoltarea de noi capabilități militare pe baza IA. Un exemplu în acest sens este reprezentat de proiectul Maven, cunoscut şi sub denumirea de Algorithmic Warfare Cross-Functional Team (AWCFT), care are ca scop integrarea IA, alături de metadate şi maşini de învățare, în dezvoltarea capabilităților militare americane. Cu toate că zona inițială de interes a AWCFT este dezvoltarea de algoritmi pentru descoperirea şi clasificarea obiectelor, în acelaşi timp, vor fi consolidate toate inițiativele tehnologice, bazate pe algoritmi, asociate domeniului informațiilor pentru apărare, pentru consolidarea procesului decizional militar.

În 2017, Laboratorul de Tehnologie şi de Ştiință în Domeniul Apărării din Marea Britanie a lansat o inițiativă care vizează dezvoltarea unui sistem automat de identificare şi clasificare a vehiculelor pe baza imaginilor satelitare.

**Din punct de vedere al aspectului legal**, este în derulare o inițiativă internațională de creare a unui acord care să prevadă interzicerea utilizării sistemelor de armament autonome ce înglobează IA.

Obiectivul acestor demersuri îl reprezintă semnarea unui tratat internațional de interzicere totală a unor asemenea sisteme de armament. În acest sens, inițiatorii acestui demers promovează modelul Tratatului de neproliferare nucleară, al Tratatului interzicerii minelor antipersonal sau pe cel al interzicerii armelor chimice şi bacteriologice.

Lansată în aprilie 2013, Campania de stopare a Roboților Ucigaşi reprezintă un grup de organizații non-guvernamentale care are ca obiectiv interzicerea preventivă a sistemelor de armament letale autonome. Membrii organizației au solicitat guvernelor şi ONU elaborarea de politici care să vizeze dezvoltarea sistemelor de armament letale autonome. Ulterior, în iulie 2015, peste o mie de experți în domeniul IA au semnat un document comun (prezentat pe timpul celei de-a 24-a Conferințe Internaționale în domeniul IA, de la Buenos Aires), prin care avertizează asupra amenințării declanşării unei curse a înarmării în domeniul IA şi solicită interzicerea sistemelor de armament autonome.

În mai 2018, în Franța, Organizația pentru Tehnologie şi Ştiință din cadrul NATO a derulat o activitate cu tema „IA în procesul decizional militar". În aceeaşi linie de preocupări, ONU a anunțat deschiderea unui nou birou la Haga, care va avea ca obiect de activitate monitorizarea dezvoltărilor în domeniul IA şi al roboticii.

**Din punct de vedere etic**, este vizată modalitatea de interacțiune dintre om şi maşină. Astfel, în ceea ce priveşte sistemele de armament autonome letale (*Lethal Autonomous Weapons Systems* – LAWS), interacțiunea om-maşină este împărțită în trei categorii:

1. factorul uman în lanțul decizional al utilizării forței letale (*Man in the Loop*);
2. factorul uman monitorizează lanțul decizional şi are posibilitatea de intervenție în orice moment asupra deciziei de utilizare a forței letale (*Man on the Loop*);
3. factorul uman în afara lanțului decizional, fără control asupra deciziei de utilizare a forței letale *(Man out of the Loop*).

În pofida intensificării în 2017 a demersurilor care vizează conştientizarea riscurilor utilizării LAWS, unele state continuă eforturile de dezvoltare ale unor astfel de sisteme de armament. Referitor la această problematică, vicepreşedintele Comitetului Întrunit al Şefilor de State Majore (SUA), generalul Paul Selva, a precizat că factorul uman trebuie menținut în lanțul decizional al utilizării forței letale. În schimb, în 2015, Ministerul Afacerilor Externe britanic nu a sprijinit în mod explicit interzicerea utilizării LAWS, motivând că dreptul umanitar internațional asigură o reglementare suficientă în acest sens. Totuşi, forțele armate britanice operează doar sisteme

de armament care fac obiectul monitorizării şi controlului de către factorul uman.

În iulie 2017, China a prezentat *Planul de dezvoltare a inteligenței artificiale de generație următoare*, în care IA este desemnată ca o tehnologie transformațională care va sprijini puterea militară şi economică viitoare. Potrivit acestui document, până în anul 2030 China trebuie să devină forța preeminentă în domeniul IA, pe baza unei strategii de fuziune militar-civilă. Demersul Beijingului vizează intensificarea integrării sectorului militar cu cel civil, reflectând faptul că IA reprezintă o tehnologie cu dublă utilizare, aspect ce va conduce atât la constrângeri în ceea ce priveşte dezvoltarea tehnologiilor care încorporează IA, cât şi la reglementări în domeniul neproliferării.

Preşedintele F.Ruse, Vladimir Putin, declara (în septembrie 2017) că „inteligența artificială este viitorul, nu numai pentru F.Rusă, ci pentru întreaga omenire, iar cine va deveni lider în acest domeniu va controla lumea".

Comandantul Comandamentului Cibernetic şi pentru Spațiul Informațional din Germania, generalul-locotenent Ludwig Leinhos, a declarat (15.02.2017, în marja Conferinței pe probleme de securitate de la München) că Germania are o poziție clară şi că nu va intenționa să achiziționeze sisteme de armament autonome. În schimb, forțele armate germane vor trebui să fie pregătite să se apere împotriva unor astfel de arme, în situația în care vor fi utilizate de către alte state. Pe timpul aceleiaşi activități, fostul secretar general al NATO, Anders Fogh Rasmussen, a declarat că trebuie prevenită producerea şi utilizarea unor sisteme de armament autonome, care ar putea să creeze şi mai multă instabilitate, iar utilizarea IA şi a roboților în domeniul militar va amplifica viteza de ducere a acțiunilor de luptă.

În replică, coordonatorul campaniei de Stopare a Roboților Ucigaşi, Mary Wareham, a declarat că 22 de state au fost deja de acord să sprijine interzicerea sistemelor de armament autonome (exemplu UAV-urile). Mai mult, M.Wareham a adăugat că este importantă asigurarea controlului uman al sistemelor de armament, iar în acest sens este nevoie urgentă de încheierea de acorduri, având în vedere ritmul alert de evoluție a acestei tehnologii.

**Provocări legate de operaționalizarea roboților militari**

În prezent, este în derulare o „cursă a înarmării" în domeniul civil care vizează dezvoltarea de roboți autonomi în mai multe domenii (cele mai avansate fiind domeniile industriei auto şi aerospațiale), expertiză care va migra şi către domeniul militar. Din această perspectivă, cel mai probabil, va avea loc o creştere a autonomiei roboților militari, atât din punct de vedere al diversității, cât şi al calităților acestora. Un aspect critic al acestei evoluții va fi reprezentat de capacitatea companiilor din cadrul industriilor de apărare de dezvoltare şi testare a roboților autonomi, în special a celor destinați utilizării forței letale.

Deoarece sistemele operaționale actuale sunt mai mult automate decât autonome, în prezent se depun eforturi în domeniul cercetării şi dezvoltării pentru trecerea de la stadiul de dezvoltare la cel de implementare. Maturizarea acestor tehnologii întâmpină o serie de obstacole, legate de costuri şi apariția unor probleme tehnice neprevăzute, dar la fel de problematice sunt şi barierele organizaționale şi culturale.

Forțele armate americane au implementat dispoziții care restricționează dezvoltarea şi utilizarea sistemelor cu anumite capacități autonome. Cea mai importantă dintre acestea face referire la necesitatea existenței unui decident uman în lanțul de comandă al sistemelor de atac care au în organică roboți militari şi în cel decizional, pentru toate situațiile care implică utilizarea forței letale.

Cel mai probabil, cea mai mare schimbare în modul în care vor fi duse acțiunile de luptă în viitor va fi reprezentată de dislocarea simultană a mai multor roboți, în conceptul denumit „roi". Roiurile de roboți vor asigura o mai mare unitate de efort, o mai bună coordonare, informații mai bune şi o mai mare viteză de acțiune[6].

Combinația factorilor menționați va continua să producă progrese rapide în domeniul tehnologiei IA pe termen scurt, mediu şi lung. Pe termen scurt, cel mai probabil, progresul înregistrat în domeniul IA va conduce la un grad mai mare de utilizare a roboților autonomi în sprijinul personalului militar, precum şi la o creştere a numărului de misiuni de luptă executate de către roboții militari. Creşterea utilizării roboților

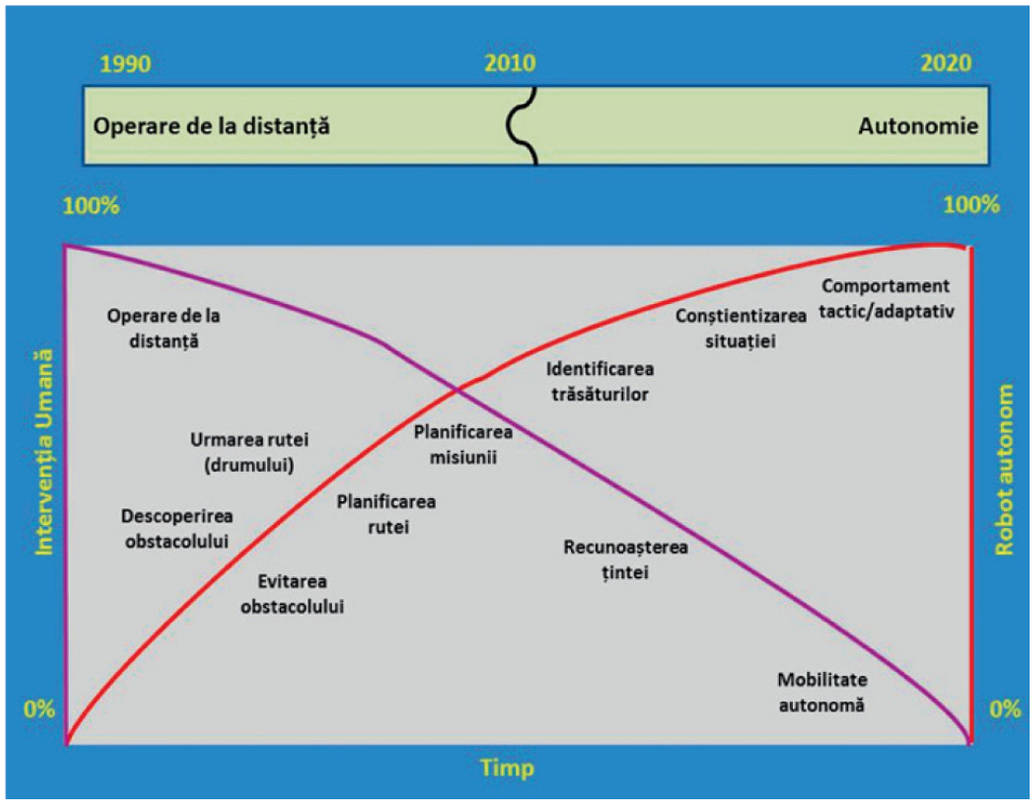



*Fig. nr. 1 Estimarea forțelor armate americane de dezvoltare a roboților militari*

militari (Fig. nr.1) şi a sistemelor autonome va conduce şi la o creştere a puterii actorilor statali şi non-statali.

**Cerințe generale pentru roboții militari:**

- distributivitatea – capacitatea de operare în spații fizice largi, în pofida diferențelor de gabarit, formă şi orientare;
- pe timpul operării, care include navigație, deplasare, observare, culegere de date, transport de materiale (inclusiv sisteme de armament şi muniții), trebuie avut în vedere şi impactul asupra celorlalte sisteme cu şi fără pilot, precum şi impactul asupra mediului;
- integrarea şi operarea cu factorul uman în cadrul aceluiaşi sistem de comandă-control;
- siguranță în operare pentru personalul uman al unităților dotate cu sisteme de roboți;
- acțiunile/comportamentul sistemelor dotate cu roboți militari ar trebui să respecte normele etice şi prevederile legislației internaționale, în special în situațiile care prezintă pericol la adresa integrității şi a vieții umane.

**Tendințe de dezvoltare a roboților militari în cadrul Forțelor Terestre (FT) ale SUA**

În prezent, forțele armate americane investesc în proiecte de cercetare şi dezvoltare pentru testarea şi operaționalizarea roboților militari. Un exemplu în acest sens este decizia FT ca reducerea personalului militar de la 540.000 de militari la 420.000 de militari, până în 2019, să fie compensată prin folosirea roboților militari, pentru menținerea capacității de luptă la acelaşi nivel. Această tendință are loc şi în contextul în care costul cu resursa umană are cea mai mare pondere din buget (instruire, hrănire, sprijin pe timpul dislocării în teatre de operații, asistență medicală asigurată atât în timpul serviciului militar, cât şi după trecerea în rezervă).

Dezvoltarea roboților militari în cadrul forțelor terestre americane se face respectând următoarele cerințe:

1. modularitatea: arhitectura modulară va permite schimbarea rapidă a tehnologiei, inserarea de kit-uri pentru misiune şi modernizări (sunt vizate autonomia, software-ul şi calculatorul de bord);

2. în 2018, FT vor lansa câteva studii concept pentru definirea caracteristicilor tehnico-tactice ale viitoarei flote de UGV-uri, în vederea creşterii interoperabilităţii şi flexibilităţii pe timpul executării misiunilor; cerinţele principale vizează realizarea unui şasiu comun pentru fiecare categorie de UGV (mici, mijlocii şi mari);
3. autonomie (grad mai mare de independenţă);
4. comunicaţii: sistem de comunicaţii cu bandă de lucru mai mare, sporirea interoperabilităţii, a securităţii cibernetice şi a criptării; modernizarea sistemului de comunicaţii prin încorporarea următoarelor tehnologii: MIMO (multiple input, multiple output) şi Mobile Ad-hoc Network (MANET);
5. mobilitate/anduranţă: sporirea eficienţei energetice pe termen lung prin diversificarea sistemelor de propulsie – motoare alimentate cu gaz lichefiat, motoare hibride etc.; UGV vor fi destinate executării de operaţii în teren fragmentat – necesitatea acoperirii unor zone mai întinse şi îndeplinirea de roluri diferite; convertirea ATV-urilor (All Terrain Vehicle) în vehicule autonome (odată cu maturizarea acestei tehnologii în domeniul comercial).

Calendarul dezvoltării roboţilor militari şi a sistemelor autonome în cadrul FT americane se prezintă astfel:

| | |
|---|---|
| **Pe termen scurt (2017 - 2020):** | - creşterea nivelului de conştientizare a situaţiei pentru trupele debarcate la eşaloane mici: datele culese să fie organizate şi prioritizate pentru sprijinirea procesului decizional şi scăderea timpului de reacţie;<br>- reducerea încărcăturii fizice a trupelor debarcate: programul Grupei de Transport Echipament Multirol (*Squad Multipurpose Equipment Transport – SMET*), cu următoarele cerinţe: un vehicul care să urmeze militarii şi care să transporte echipamentul unei grupe de infanterie (cu masa maximă de 454 kg), cu viteza de deplasare de 3 km/h, autonomia de 72 de ore (fără realimentare) pentru o distanţă de 97 km; trei moduri de operare: autonom, semiautonom şi cu comandă de la distanţă; de asemenea, platforma trebuie să fie capabilă să furnizeze energie cu puterea de 3 kW pe timpul staţionării şi 1 kW pe timpul deplasării; în acest sens, au fost selecţionate patru platforme şi au fost semnate contracte pentru producerea a 20 de vehicule pentru fiecare sistem;<br>- îmbunătăţirea sprijinului logistic prin utilizarea unor sisteme terestre automate – utilizarea de sisteme fără pilot;<br>- facilitarea deplasării prin deminarea căilor de comunicaţii – programul Route Clearance Interogation System (RCIS). |
| **Pe termen mediu (2021 – 2030)** | - creşterea nivelului de conştientizare a situaţiei prin integrarea unor sisteme autonome avansate;<br>- creşterea autonomiei pentru UGV de dimensiuni medii şi mari, în vederea sporirii sprijinului logistic;<br>- îmbunătăţirea sprijinului logistic prin operaţionalizarea de convoaie autonome – vehiculele vor deveni mai autonome în detrimentul urmăririi unui vehicul cu operator;<br>- îmbunătăţirea capacităţii de manevră şi a masei transportate – tehnologia autonomă off-road va ajunge la maturitate, ceea ce le va face capabile să opereze inclusiv în teren accidentat în condiţii de luptă. |
| **Pe termen lung (2031-2040)** | - creşterea conştientizării situaţiei prin recunoaştere permanentă realizată de sisteme tip „roi” (*swarming system*); recunoaşterea terenului, în special în mediul urban;<br>- creşterea sprijinului logistic prin utilizarea sistemului aerian automat de livrare cargo – executarea de misiuni autonome în zone izolate sau cu grad de periculozitate ridicat;<br>- facilitarea manevrei, concomitent cu dezvoltările către sisteme de luptă fără pilot, sisteme care vor avea o amprentă mai redusă şi o anduranţă mai mare pentru neutralizarea ţintelor cu valoare ridicată dislocate în adâncimea teritoriului inamic. |

**Concluzii şi evaluări**

Introducerea inteligenței artificiale în domeniul militar de către state precum SUA, Federația Rusă, China şi Marea Britanie, corelată cu folosirea sistemelor de armament de precizie, va conduce la creşterea avantajului tactic al platformelor autonome controlate de la distanță, în particular UAV/UGV.

Pe termen mediu şi lung, IA va avea implicații asupra potențialului militar al unui stat, aspect care deja a determinat creşterea substanțială a investițiilor în domeniul IA şi, în particular, dezvoltarea şi diversificarea aplicațiilor militare care vor îngloba IA.

Dotarea forțelor armate cu roboți autonomi va depinde de modul şi nivelul conceptual şi organizațional de integrare al acestora cu platformele sistemelor actuale de comandă-control.

Utilizarea IA în domeniul militar va conduce la revizuirea strategiilor şi doctrinelor militare, precum şi la dezvoltarea de noi sisteme de armament şi, implicit, la adaptarea modului de planificare şi ducere a acțiunilor de luptă. Procesul de automatizare a luării deciziei va avea un rol din ce în ce mai important la fiecare nivel de comandă şi control.

Competiția în asigurarea dominației în domeniul IA alimentează o cursă a înarmării care, în perspectivă, va reprezenta un factor de insecuritate, care ar putea avea un efect destabilizator, întrucât caracteristicile sistemelor de armament robotizate nu vor fi cunoscute total decât în momentul în care vor fi angajate efectiv în acțiuni militare.

În vederea reducerii riscurilor rezultate din utilizarea IA şi a sistemelor de armament autonome, este necesară prezența factorului uman în lanțul decizional al angajării forței letale. Până la agrearea şi implementarea unor reguli internaționale care să impună acest principiu, utilizarea sistemelor de armament autohtone va crea instabilitate strategică, având în vedere că descurajarea nucleară reprezintă unul dintre primele domenii care ar putea fi afectat de operaționalizarea unor astfel de capacități.

**Bibliografie:**


1. Chatham House, The Royal Institute of International Affairs, *Artificial Intelligence and the Future of Warfare*, M. L. Cummings International Security Department and US and the Americas Program, January 2017;
2. *International Journal of Advanced Research in Artificial Intelligence*, no. 4/2015, Military Robotics: Latest Trends and Spatial Grasp Solutions, Peter Simon Sapaty;
3. *The Economist*, „Getting to grasp with military robotics", 25 January 2018, online www.economist/special.report/2018/01/25;
4. *International Journal of Advanced Research in Artificial Intelligence*, no. 4/2015, Military Robotics, Latest Trends and Spatial Grasp Solutions, Peter Simon Sapaty;
5. Harvard Kennedy School, Belfer Center for Science and International Affairs, *Artificial Intelligence and National Security*, Greg Allen and Taniel Chan, July 2017;
6. Meir Amit Intelligence and Terrorism Information Center, *A series of attacks against the Russian bases in Hmeymim and Tartus*, 10 January 2018.
7. Stockholm International Peace Research Institute, Dealing with the challenges posed by emerging technologies, Vincet Boulain and Maaike Verbruggen, December 2017;
8. Defense Group Inc., Center for Intelligence Research and Analysis, *China's Industrial and Military Robotics Development*, October 2016.
9. Seminar, The Force Awakes: AI and the Modern Warfare, 15/02/2018, München Security Conference, www.securityconference.de/en;
10. Chatham House, The Royal Institute of International Affairs, *Artificial Intelligence and the Future of Warfare*, M. L. Cummings International Security Department and US and the Americas Program, January 2017;
11. UGVs for the modern battlefield, The evolution of unmanned ground operations support, 18 January 2018, www.ihsmarket.com/research-analyst/UGVs-for-the-modern-battlefield;
12. UGVs for the modern battlefield, The evolution of unmanned ground operations support, 18 January 2018, www.ihsmarket.com/research-analyst/UGVs-for-the-modern-battlefield.

[1] Misiuni de transport, căutare-salvare şi utilizare a forţei letale şi neletale.

[2] Sistemul UAV Harop, dezvoltat de compania Israel Aerospace Industries (IAI) este o dronă antiradiolocaţie care se poate dirija în mod autonom către un emiţător radioelectronic. Harop execută misiuni de patrulare într-un anumit sector al câmpului de luptă şi combate ţintele angajate prin autodistrugere la impactul cu ţinta, fiind dotat cu o încărcătură de luptă de 23 kg.

[3] Sunt de menţionat progresele în domeniul IA: capacitatea de recunoaştere a imaginilor superioară performanţelor umane, capacitatea de recunoaştere vocală şi, cel mai semnificativ din punct de vedere militar, înfrângerea unui fost pilot de luptă al forţelor aeriene americane într-un simulator de luptă aeriană.

[4] În noaptea de 05/06.01.2018, 10 UAV-uri au atacat Baza Aeriană rusă din Hmeymim, iar alte trei au vizat Baza de asigurare tehnico-materială (Bz.Asg.Th.Mat.) rusă de la Tartus.

[5] Vehicle Borne Improvised Explosive Device.

[6] Roiurile de roboţi vor putea fi dislocate în diferite forme şi mărimi, fiecare destinat pentru executarea unei misiuni specifice, cum ar fi: misiune de recunoaştere pentru o zonă extinsă, apărarea unei grupări de nave sau a unei grupări de forţe terestre. Mai mult, roiurile vor fi capabile să lucreze în mod individual, pentru a îndeplini diferite misiuni, odată ce vor fi dislocate, sau vor putea lucra în comun, într-un singur roi.

# CONSIDERAȚII PRIVIND ACTIVITĂȚILE DE INFORMAȚII, SUPRAVEGHERE ŞI CERCETARE (ISR)

*Teodor NEICULESCU*
*Rareş ROŞU* *

***Abstract***

*ISR is a wide variety of systems for acquiring and processing information in order to provide actionable information needed by national security decision makers and military commanders. ISR consists into a set of capabilities that integrates in a synchronized way the collection capabilities with those specific to the intelligence cycle: processing, exploitation, and dissemination of end products to provide direct support for planning, preparedness and conduct of operations. Through ISR, the collection of information is accomplished by assigning tasks specific to each field. This is a complex process involving five steps: burden sharing, collection, processing, exploitation and dissemination. If the surveillance activity is passive, the Reconnaissance is an active one, fast and targeted in order to obtain specific target information.*

***Keywords:*** *Intelligence Surveillance Reconnaissance, Target Acquisition, JISR, ISTAR*

**Introducere**

ISR este un acronim din limba engleză, care înseamnă *Intelligence, Surveillance* şi *Reconnaisance*. Relația dintre procesul ISR şi ciclul informațional constă în faptul că procesul ISR reprezintă mijlocul prin care cerințele de culegere sunt îndeplinite prin repartizarea de sarcini mijloacelor ISR. Din punct de vedere structural, procesul ISR se desfăşoară în cinci etape, astfel: repartizarea sarcinii, culegerea, procesarea, exploatarea şi diseminarea.

ISR este definit ca un set de capabilități de informații şi operații care sincronizează şi integrează planificarea şi operațiile tuturor capabilităților de culegere cu procesarea, exploatarea şi diseminarea informațiilor rezultate, în sprijinul direct al planificării, pregătirii şi executării operațiilor[1]. Acronimul ISR reprezintă:

- ***I – Intelligence*** sau informațiile reprezintă toate disciplinele de culegere a informațiilor sau capabilitățile/mijloacele de culegere, precum şi rezultatul pe care aceste discipline/capabilități/ mijloace îl pot asigura comandantului şi/sau elementelor statului major[2];
- ***S – Surveillance*** sau supravegherea reprezintă observarea sistematică a spațiului aerian, zonelor de suprafață, subterane/subacvatice, locurilor, persoanelor sau obiectelor, prin mijloace vizuale, acustice, electronice (comunicații şi non-comunicații), optoelectronice şi în infraroşu, fotografice sau de altă natură[3];
- ***R – Reconnaissance*** sau cercetarea reprezintă o misiune executată pentru a obține, prin observare vizuală sau prin alte metode de detecție, informații despre activitățile şi resursele unui adversar sau potențial adversar sau pentru a procura date referitoare la caracteristicile meteorologice, hidrologice sau geografice ale unei anumite zone[4].

În timp ce supravegherea este o activitate pasivă care se desfăşoară pe o durată lungă de timp, misiunile de cercetare sunt în general active, rapide şi orientate spre a obține o informație specifică despre un obiectiv.

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

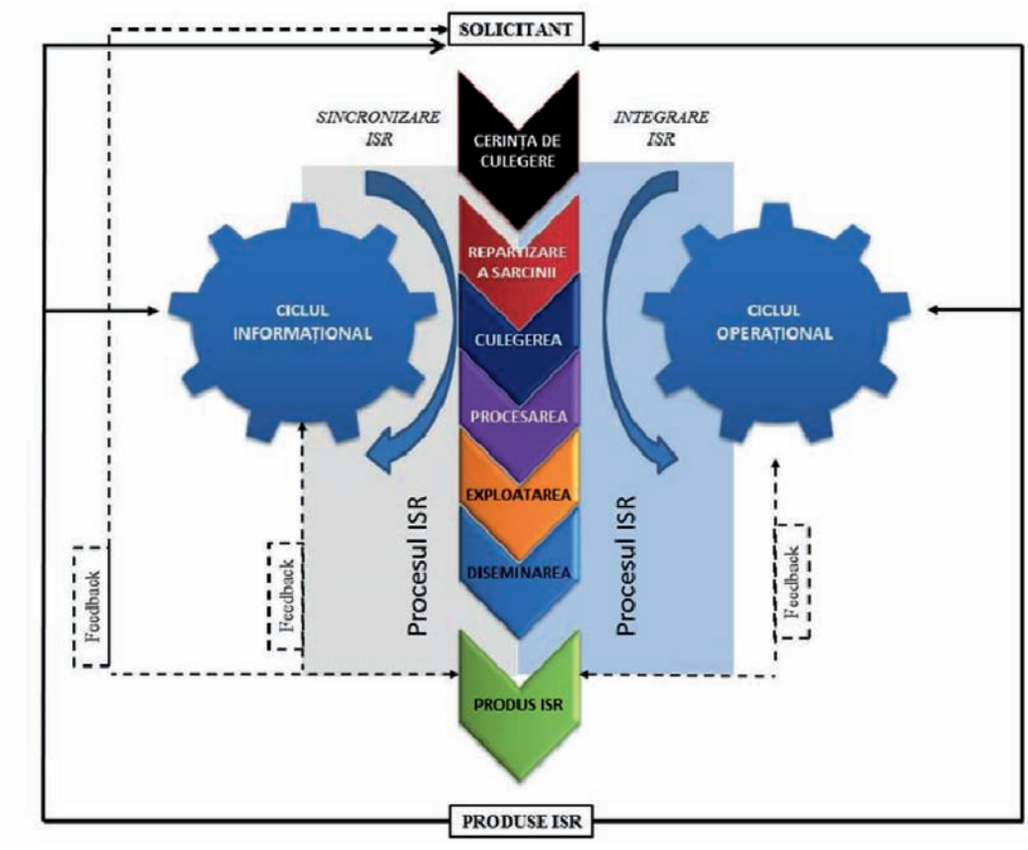



***Fig. nr. 1 – Procesul ISR (Sursa I.A. – I.5, Doctrina întrunită pentru informații, supraveghere şi cercetare)***

Domeniul ISR este cunoscut şi sub denumirile de JISR sau ISTAR, în funcție de eşalonul care planifică, execută şi evaluează operația (tactic, operativ sau strategic). JISR desemnează ISR la nivelul operativ, în care se utilizează elemente întrunite („J" reprezintă nivelul întrunit „*joint*"). La nivel tactic, se mai utilizează conceptul de ISTAR, unde acronimul TA (*Target Acquisition*) reprezintă detectarea, identificarea şi localizarea țintei[5], fiind utilizat de structuri implicate direct în procesul de *targeting*. Procesul de *targeting* realizează legătura direcționărilor şi precizărilor de la nivel strategic cu acțiunile specifice de la nivel tactic, prin ciclul de management întrunit al țintelor de la nivel operativ, concentrat şi abordat sistematic pentru crearea efectelor specifice, necesare îndeplinirii obiectivelor militare şi pentru obținerea stării finale dorite[6].

**Arhitectura unui sistem ISR**

Arhitectura ISR cuprinde toate organizațiile, procesele şi relațiile dintre sistemele care conectează elementele de culegere, bazele de date, serviciile, aplicațiile, structurile de analiză şi beneficiarii informațiilor dintr-un mediu operațional. Arhitectura ISR trebuie să fie concepută astfel încât să faciliteze managementul produselor ISR, asigurând funcțiunile ISR şi sprijinul structurilor de informații şi operații la toate nivelurile (tactic, operativ şi strategic).

Sistemul ISR este compus, în principiu, din subsistemul de planificare, coordonare/conducere şi analiză a informațiilor, subsistemul de culegere şi subsistemul de comunicații şi informatică. Domeniile misiunilor sistemelor ISR, în principal, sunt aceleaşi pentru nivelurile strategic, operativ şi tactic; sarcinile se stabilesc în funcție de nivel, obiective, cerințe şi capabilități disponibile.

**ISR în NATO**

După perioada Războiului Rece, la nivelul NATO a fost semnalată apariția unor noi tipuri de amenințări şi vulnerabilități, pentru care au fost adoptate măsuri de contracarare sau de reducere a probabilității sau impactului. Una dintre aceste

măsuri o reprezintă asigurarea unui sprijin de informații adecvat la toate nivelurile NATO, atât la nivel politic şi politico-militar, cât şi la nivelul structurilor de forțe (cu compoziție în general multinațională).

În acest sens, au fost întreprinse o serie de măsuri concrete, care au urmărit realizarea următoarelor obiective:

- elaborarea unui cadru normativ prin care să se asigure interoperabilitatea între sistemele ISTAR ale diferitelor state membre;
- elaborarea unui cadru normativ referitor la capabilitățile ISR minim necesare la fiecare nivel al comandamentelor NATO (atât de nivel operativ, cât şi tactic) sau puse la dispoziția NATO de către statele membre, dar şi la nivelul unităților şi formațiunilor puse la dispoziția NATO, indiferent dacă acestea au caracter național sau multinațional;
- promovarea cooperării între statele membre de a realiza şi utiliza împreună capabilități ISR performante, cu costuri reduse (prin conceptul *smart-defence*).

Primul obiectiv mai sus-menționat a fost realizat prin elaborarea, în 2005, a Arhitecturii NATO de interoperabilitate ISR (NATO Intelligence, Surveillance and Reconnaissance Interoperability Architecture – NIIA), prin care s-au pus bazele aspectelor tehnice prin care se realizează interoperabilitatea între sistemele ISR/ISTAR ale statelor membre.

Al doilea obiectiv a fost realizat prin instrumentele NATO de planificare a apărării, stabilind, începând cu 2002, în Catalogul de capabilități şi prin Obiectivele Forței (devenite, ulterior, Ținte de capabilități) cerințe explicite referitoare la capabilitățile necesare fiecărei structuri luptătoare. Astfel, s-a încercat o uniformizare a nivelului minim de realizare a sprijinului de informații prin elemente organice la nivel brigadă, divizie şi corp de armată, prin enumerarea capabilităților de informații necesare pentru culegere (inclusiv coordonarea culegerii), integrare şi procesare la fiecare dintre nivelurile menționate. Aceste capabilități au fost grupate sub denumirea generică de capabilități ISTAR.

Cel de-al treilea obiectiv, respectiv cooperarea între statele membre pentru realizarea unor capabilități ISR/ISTAR comune, a fost enunțat la Summit-ul NATO de la Chicago din 2012. Astfel, pe fondul crizei economico-financiare a fost constatată tendința de diminuare a cheltuielilor de apărare în majoritatea statelor membre NATO. Totuşi, riscurile şi amenințările la adresa Alianței şi a fiecărui stat membru în parte au rămas aceleaşi, eventual s-au înmulțit, fapt care generează crearea şi/sau menținerea unor capabilități apte să răspundă corespunzător. În acest context, a apărut soluția cooperării inter-state pentru realizarea şi folosirea unor echipamente sau tehnologii, care ar fi aproape inaccesibile fiecărui stat membru separat. În domeniul ISR se evidențiază două proiecte, şi anume, Allied Ground Surveillance (AGS), respectiv Multi-intelligence All-source Joint ISR Interoperability Coalition (MAJIIC).

De asemenea, în cadrul Summit-ului NATO de la Chicago s-au stabilit obiectivele de întărire ale nivelului de cooperare şi de realizare a conexiunii între forțele aliate. Astfel, s-a convenit ca statele să furnizeze Alianței capabilități proprii ISR pentru realizarea misiunilor conduse de NATO. Doi ani mai târziu, în cadrul Summit-ului din Țara Galilor, din 2014, statele membre NATO au reconfirmat faptul că domeniul JISR reprezintă în continuare o prioritate de nivel înalt pentru NATO. Astfel, la nivelul NATO s-a organizat un sistem JISR care furnizează date şi informații oportune şi în timp real sau aproape real factorilor de decizie.

Sistemul NATO JISR este constituit din sistemul de supraveghere terestră al NATO (*Aliance Ground Surveillance* – AGS), sistemul aeropurtat de avertizare şi control (*Airborne Warning and Control System* – AWACS), mijloacele ISR aparținând statelor membre, precum şi datele şi informațiile puse la dispoziția NATO de statele membre.

Experiența pe care NATO a dobândit-o în urma operațiilor din Afganistan şi Libia s-a concretizat în dezvoltarea mijloacelor de culegere, care au devenit mult mai accesibile; schimbarea s-a produs datorită faptului că statele membre NATO dețin un număr semnificativ de senzori,

capabili să culeagă informații din mediile terestru, aerian, maritim, electromagnetic şi cibernetic, iar evoluția tehnologiilor de comunicații permite diseminarea respectivelor informații către toți beneficiarii care posedă acces la rețelele de comunicații şi informatică[7].

Unul dintre instrumentele folosite la nivel NATO pentru dezvoltarea capabilităților ISR îl reprezintă exercițiul UNIFIED VISION (UV). Acest exercițiu, de tip *trial*[8], se desfăşoară din doi în doi ani şi are rolul de a integra şi armoniza progresele tehnice şi doctrinare din cadrul domeniului ISR.

În contextul creşterii amenințării anonime la adresa securității forțelor NATO şi a securității naționale a statelor membre sau partenere ale Alianței, la nivelul NATO s-a dezvoltat conceptul de „Identity Intelligence" – I2. Acesta furnizează informațiile cu privire la legăturile dintre datele biometrice[9] şi informațiile procesate în Analiza Rețelelor Umane şi Sprijinul Managementului Țintelor (*Human Network Analysis and Support to Targeting* – HNAT).

**ISR în Armata României**

În Armata României, conceptul ISR a fost adaptat în conformitate cu necesitățile şi resursele avute la dispoziție. Luând modelul doctrinar al NATO, Armata Română şi-a însuşit elementele care definesc acest concept şi le-a inclus, în 2015, în *Concepția privind dezvoltarea sistemelor şi capabilităților de informații, supraveghere şi cercetare în Armata României*, document cadru atât din perspectiva definirii conceptului, cât şi din cea a dezvoltării capabilităților ISR. Un element important în cadrul acestei concepții îl constituie enunțarea cerințelor operaționale de îndeplinit de către fiecare tip de capabilitate ISR, abordarea organizațională a arhitecturii ISR, în sensul determinării elementelor structurale necesare la fiecare eşalon, precum şi direcționări referitoare la dezvoltarea capabilităților ISR, abordate în manieră integrată: aspectele doctrinare, organizatorice, pregătirea, echipamentele, comanda, personalul, infrastructura şi interoperabilitatea (DOTMLPFI – *Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Interoperability*).

În anul 2017, la nivelul Armatei României s-a adoptat *Doctrina întrunită pentru informații, supraveghere şi cercetare*. Acest document defineşte conceptele specifice domeniului ISR, principiile de integrare şi sincronizare a capabilităților ISR, atât la fiecare nivel de comandă, cât şi între eşaloane diferite, prin care disciplinele şi capabilitățile de culegere şi activitățile de exploatare asigură suportul necesar pentru a răspunde unei cereri de informații, în sprijinul planificării şi executării operațiilor[10].

**ISR – analiză critică sumară**

Mediul operațional reprezintă un complex de condiții, circumstanțe şi factori care influențează angajarea capabilităților şi deciziile comandantului, iar cunoaşterea şi înțelegerea acestuia sunt fundamentale pentru succesul acțiunii militare şi obținerea stării finale dorite.

Domeniile misiunilor sistemelor ISR includ: asigurarea indiciilor şi avertizării, pregătirea întrunită de informații a mediului operațional, identificarea organizării pentru luptă şi dispunerea forțelor adversarului, estimarea situației, monitorizarea situației, sprijinul pentru protecția forței şi sprijinul procesului de management al țintelor.

Un sistem ISR eficient contribuie la creşterea capacității de luptă sau de adaptare la un context non-linear de securitate al forțelor proprii, fapt care poate reprezenta un obstacol în calea obiectivelor forțelor ostile. Sistemul ISR oferă entităților luptătoare un nivel superior de cunoaştere pentru a acționa, eficientizându-le acțiunile. Fiind compus din elemente de planificare şi direcționare, culegere, analiză şi diseminare, care interacționează între ele în cadrul ciclului informațional, sistemele ISR oferă sprijin pentru luarea deciziilor, în vederea angajării forțelor în operații.

În viitor, ținând cont de necesitățile operaționale şi de angajamentele asumate la nivelul Alianței, Armata României va achiziționa

sisteme ISR pentru a răspunde necesităților forțelor terestre, aeriene, navale şi a celor pentru operații speciale.

Apartenența la NATO şi la UE reprezintă oportunități deosebite în sensul dezvoltării sistemului ISR. Într-o abordare realistă, este foarte costisitor şi greu de exploatat un sistem de tip HALE (High Altitude Long Endurance)[11] sau AWACS. Cu toate acestea, adoptând o strategie de tip *one-to-many* se poate utiliza o capabilitate foarte costisitoare şi cu un grad ridicat de acoperire de nivel strategic de toți membrii Alianței. În acest sens, la nivelul NATO există inițiativa NATO *Smart Defence*, iar la nivelul Uniunii Europene conceptul *Pooling and Sharing*. Aceste inițiative se concretizează în proiecte multinaționale, cu scopul de a dezvolta capabilități în comun. Un bun exemplu de cooperare în cadrul mecanismelor enumerate mai sus este reprezentat de capabilitatea NAEW&C (NATO Airborne Early Warning and Control Force) şi sistemul Allied Ground Surveillance (AGS).

**ISR în viitor**

În viitorul apropiat principalele provocări la care sistemele ISR trebuie să răspundă sunt reprezentate[12] de creşterea volumului de date obținute cu mijloacele ISR, cerințe de capabilități de comunicații şi tehnologia informației tot mai ridicate.

În vederea realizării evoluției sistemului ISR, atât în planul NATO cât şi în cel intern al statelor membre, trebuie avute în vedere următoarele elemente direcționale:

- extinderea protocoalelor de schimb de informații în baza principiului nevoii de diseminare, astfel încât orice utilizator să aibă posibilitatea de a accesa informațiile pe o platformă *on-line*, nu doar beneficiarii direcți;
- optimizarea noilor tehnologii într-o manieră care să permită integrarea acestora în arhitectura ISR.

Domeniul ISR este un domeniu evolutiv, supus în primul rând evoluției tehnologiei. În acest context, în cadrul Summit-ului de la Varşovia din 2016, NATO a lansat inițiativa cu privire la viitorul controlului şi supravegherii – *Alliance Future Surveillance and Control (AFSC)*. Potrivit acesteia, flota de avioane care asigură capabilitatea AWACS urmează să fie scoasă din uz, după 50 de ani de exploatare, în anul 2035[13].

La nivel național, în documentele programatice pentru Armata României s-a stabilit că domeniul ISR reprezintă una dintre direcțiile prioritare de acțiune. Principalele sisteme care vor fi supuse transformării şi integrării într-o structură de tip C4ISR sunt sistemele integrate de comunicații şi informatică, punctele de comandă de nivel divizie şi brigadă, echipamentele specifice pentru echipe de control aerian tactic, sistemul de comunicații prin satelit, echipamentele pentru securizarea rețelelor, stocurile strategice de echipamente IT, programele informatice etc. Integrarea capabilităților ISR într-un sistem de tip C4ISR reprezintă, în cele din urmă, realizarea unui deziderat în materie de comunicare de tip *sensor to shooter*.

**Bibliografie:**


1. I.A. – 1.5 Doctrina întrunită pentru informații, supraveghere şi cercetare, București, 2017;
2. AJP - 2.7 Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance, Edition A 01.07.2016;
3. AJP - 3.9 Allied Joint Doctrine for Joint Targeting ed. A, Ver. 1, aprilie 2016;
4. *Field Army ISTAR Handbook*, Marea Britanie, ed. 2007;
5. *Joint Intelligence, Surveillance and Reconnaissance* din 18.06.2018, online la https://www.nato.int/cps/en/natohq/topics_111830.htm?selectedLocale=en, accesat la 29.08.2018;
6. *Unified Vision 2018 Tests Interoperability and New Technologies* online la https://www.nato.int/cps/en/natohq/news_156098.htm?selectedLocale=en accesat la 29.08.2018;
7. LUNAN, Mark, „Biometrics New Doctrinal Concepts", *The Three Swords Magazine*, nr. 33/2018, online la http://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf, accesat la 27.08.2018;

8. NATO & Int'l Military Staff, Concept for Identity Intelligence (I2) (2017);
9. Manualul Comandamentului NATO al Componentei pentru operații speciale, (SOCC), 2014;
10. VEUM, Kurt, Architecture & Applications Group Head, NATO Communications and Information A-gency, *Joint Intelligence, Surveillance & Reconnaissance (JISR) in NATO* din 09.09.2016, online la https://fmv.se/Global/Dokument/Nyheter%20och%20Press/2016/Sensorsymposium%202016/2_Veum_NVIA_JISR%20Initiative%20-%20Overview%20for%20SWE%20Sensors%20Conf%20(7%20Sep%202016)%20N-U.pdf, accesat la 28.09.2018;
11. CAPELLEN, G.D., *NSPA Industry Day - NATO Alliance Future Surveillance and Control (AFSC)* – 10.04.2018 - online la https://www.nspa.nato.int/en/organization/logistics/LogServ/afsc.htm accesat la 05.09.2018;
12. MURRAY B., *Beyond AWACS: The Need for political ownership and engagement*, Adunarea Parlamentară a NATO online la https://www.nspa.nato.int/en/organization/logistics/LogServ/afsc.htm accesat la 05.09.2018.

---

[1] I.A. – 1.5 *Doctrina întrunită pentru informații, supraveghere şi cercetare*, Bucureşti, 2017, p. 8;
[2] Idem, p. 15;
[3] Idem 1, p.16;
[4] Idem 1, p.17;
[5] *Field Army ISTAR Handbook*, Marea Britanie, ed. 2007, p. 5;
[6] AJP 3.9 *Allied Joint Doctrine for Joint Targeting* ed. A Ver. 1, aprilie 2016, p. 15;
[7] *Joint Intelligence, Surveillance and Reconnaissance* din 18.06.2018, online la https://www.nato.int/cps/en/natohq/topics_111830.htm?selectedLocale=en;
[8] *Trial* vizează în principal îndeplinirea unor obiective de interoperabilitate tehnică şi procedurală între diferite sisteme, fără a se concentra, în mod special, pe problematica operațională;
[9] Mark Lunan, „Biometrics New Doctrinal Concepts", revista *The Three Swords Magazine*, nr. 33/2018, online la http://www.jwc.nato.int/images/stories/threeswords/Biometrics_2018.pdf;
[10] I.A. – 1.5 *Doctrina întrunită pentru informații, supraveghere şi cercetare*, Bucureşti, 2017, p. 3;
[11] NATO a achiziționat sistemul AGS Northop Grumman RQ-4 (NATO AirGroundSurveillance UAV);
[12] Kurt Veum, „Architecture & Applications Group Head, NATO Communications and Information Agency", *Joint Intelligence, Surveillance & Reconnaissance (JISR) in NATO* din 09.09.2016, online la https://fmv.se/Global/Dokument/Nyheter%20och%20Press/2016/Sensorsymposium%202016/2_Veum_NVIA_JISR%20Initiative%20-%20Overview%20for%20SWE%20Sensors%20Conf%20(7%20Sep%202016)%20N-U.pdf;
[13] G.D. Capellen, *NSPA Industry Day - NATO Alliance Future Surveillance and Control (AFSC)* – 10.04.2018.

# ASOCIAȚIA DIPLOMAȚILOR MILITARI ÎN REZERVĂ ŞI ÎN RETRAGERE „ALEXANDRU IOAN CUZA” - TRECUT ŞI PREZENT

***General de brigadă (r) Dan NICULESCU*** *

***Abstract***

*The Association of Reserve and Retired Military Diplomats „Alexandru Ioan Cuza” (ARRMD) represents a voluntary association of the officers in reserve or retirement that have deployed or supported directly or through related actions the military diplomatic activity of knowing the armed forces of other states and promoting and developing the relations of the Romanian Armed Forces with them. The purpose of ARRMD is to promote the traditions of the military diplomacy activity and the history of the military intelligence service of the Romanian Armed Forces in the spirit of the assumed foreign exchange, the cultivation of the civic values specific to the rule of law, the promotion of the fundamental values of democracy, of the national interests and of the Romanian Armed Forces, the development of relations with civil society for the benefits of its members. The ARRMD members participate in educational, cultural, commemorative activities organized by central and local authorities. Also, the members of ARRMD support various projects and actions of the structures of the Ministry of National Defense. The activity of ARRMD is carried out under the slogan „Homeland-Honor-Tradition”.*

***Keywords**: Association of Reserve and Retired Military Diplomats „Alexandru Ioan Cuza” (ARRMD), military, diplomacy, promoting traditions, democracy, supporting Ministry of National Defense.*

În anul 1990, la scurt timp după schimbarea de regim, un grup de ofițeri în rezervă, având în frunte pe generalul-maior Stelian Popescu, s-a hotărât să formeze o organizație democratică a cadrelor militare în rezervă şi retragere, dând naştere astfel Ligii Naționale a Ofițerilor în Rezervă şi în Retragere (LNORR), devenită ulterior Uniunea Națională a Cadrelor Militare în Rezervă şi în Retragere (UNCMRR), şi în prezent Asociația Națională a Cadrelor Militare în Rezervă şi în Retragere „Alexandru Ioan Cuza” (ANCMRR).

Inițiativa grupului s-a bucurat de un succes remarcabil în rândurile foştilor militari de profesie, ieşiți din activitate şi dornici de a contribui la eforturile generale ale poporului român de a reforma statul şi de a-l reaşeza pe structuri democratice.

În acest context, colonelul (r) ing. Mitică Detot, care făcea parte din grupul membrilor fondatori ai LNORR, a primit sarcina de a se ocupa de relațiile internaționale ale Ligii. Aşa cum era firesc, acesta s-a orientat către foştii săi colegi, care beneficiau de experiență în domeniul relațiilor externe, fiind familiarizați cu evoluțiile politico-militare internaționale şi cunoscători ai mai multor limbi străine, dar şi ai armatelor altor state.

La primele întâlniri au participat circa 20-30 de invitați şi apoi din ce în ce mai mulți.

În cadrul unei astfel de reuniuni, la 12 decembrie 1991, colonelul în rezervă Marin Sorescu a făcut propunerea să se constituie şi

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

o asociație a ofițerilor de informații militare aflați în rezervă sau în retragere, separată de LNORR. Scopul era acela de a se valorifica şi promova experiența şi tradițiile din domeniul informațiilor militare, de a studia documentele de arhivă şi, nu în ultimul rând, de a continua să contribuie la nevoile conducerii Armatei României. Propunerea colonelului Sorescu a fost primită cu interes, viitoarea asociație urmând să fie denumită „Asociația Ofițerilor de Informații Militare în Rezervă şi în Retragere" (AOIMRR). La scurt timp după luarea acestei hotărâri a fost înființat Grupul de inițiativă, a cărui menire era aceea de a întocmi documentele necesare pentru legalizarea noii asociații.

În anul 1993, la conducerea Direcției informații militare (DIM) a fost numit generalul-locotenent Decebal Ilina, care s-a ataşat imediat demersurilor organizatorice şi de legalizare a noii asociații, încurajând inițiatorii şi implicându-se în înlăturarea dificultăților inerente acelei perioade.

Anticipând rolul şi locul AOIMRR în ansamblul formelor asociative ale ofițerilor în rezervă şi în retragere, un grup de foşti ataşați militari români, format din coloneii în rezervă Victor Paraschiv, Dumitru Apostol, Emil Burghelea, Mitică Detot şi Gheorghe Nicoară, au început să se întrunească pentru elaborarea unor lucrări privind evoluția situației politico-militare internaționale şi implicațiile acesteia asupra securității şi apărării României, beneficiar principal fiind Ministerul Apărării Naționale.

Şeful DIM, generalul-locotenent Decebal Ilina, încurajat de experiența şi capacitățile intelectuale ale membrilor viitoarei organizații, a solicitat sprijinul acestora pentru întocmirea unei istorii a serviciului militar de informații care să fie oferită publicului cu ocazia aniversării, la 12 noiembrie 1994, a 135 de ani de la emiterea de către domnitorul Alexandru Ioan Cuza a Înaltului Ordin de Zi nr. 83, pentru înființarea Secției a 2-a, prima structură de informații a Armatei României şi precursoarea actualei Direcții informații militare. În acest sens, s-a constituit un colectiv care a reuşit să elaboreze în termenul stabilit lucrarea ***Direcția Informații Militare – între ficțiune şi adevăr.*** A fost o noutate editorială absolută, primită cu surprindere şi interes de societatea civilă.

În paralel cu aceste preocupări, Grupul de inițiativă a întocmit proiectul de statut al AOIMRR, precum şi celelalte documente necesare demersului de legalizare.

La data de 2 iunie 1995, coloneii în rezervă Mitică Detot şi Laurențiu Sbera s-au prezentat la şedința publică a Judecătoriei Sectorului 2 Bucureşti unde completul de judecată a respins inițial dosarul pe motiv că ar contrazice reglementările în vigoare la acea dată. Decizia completului a fost influențată de campania negativă din mass-media la adresa serviciilor de informații româneşti, apreciindu-se constituirea organizației ofițerilor rezervişti proveniți din DIM ca fiind neoportună în acele momente.

La insistențele reprezentanților Grupului de inițiativă şi pentru a se da posibilitatea identificării unei soluții viabile, completul de judecată a amânat decizia pentru data de 8 iunie 1995. Şi de această dată completul şi-a menținut poziția inițială şi a recomandat obținerea avizului

Consiliului Suprem de Apărare a Țării (CSAT). Solicitarea făcută CSAT de către Grupul de inițiativă a fost respinsă cu argumente similare celor ale judecătorilor.

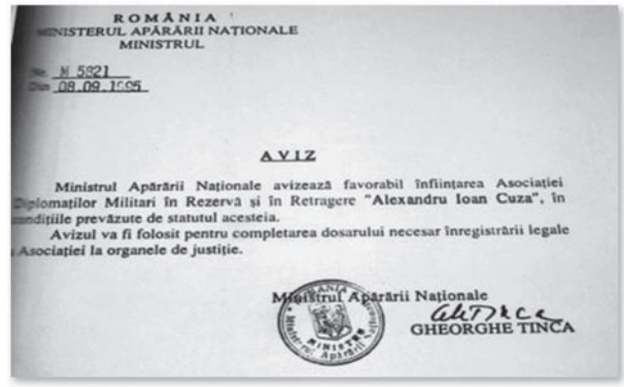
La data de 20 iunie 1995, Grupul de inițiativă, consultându-se cu şeful DIM asupra dificultăților întâmpinate pentru obținerea legalizării AOIMRR, a conturat trei opțiuni:

1. luarea în considerare a observațiilor CSAT şi refacerea dosarului de legalizare conform acestor observații;
2. continuarea întrunirilor periodice ale foştilor atașați militari, fără a se constitui deocamdată într-o formă asociativă;
3. întreruperea oricărei acțiuni şi aşteptarea unui moment favorabil pentru astfel de demersuri.

În cele din urmă, s-a optat pentru prima cale. S-a hotărât astfel refacerea şi completarea Statutului, solicitarea avizului ministrului apărării naționale, scoaterea de pe rol a vechiului dosar şi prezentarea la judecătorie a unuia nou. Astfel, ținându-se cont şi de observațiile instanței de judecată, s-a hotărât, în primul rând, schimbarea denumirii AOIMRR în Asociația Diplomaților Militari în Rezervă şi în Retragere „Alexandru Ioan Cuza”, iar noul dosar a fost luat în dezbateri de către instanță la 28 noiembrie 1995. De data aceasta instanța a aprobat înființarea ADMRR, hotărârea fiind publicată în Monitorul Oficial din 25 ianuarie 1996.

Nu putem să nu menționăm sprijinul primit din partea Ministerului Apărării Naționale, personal al ministrului apărării din acea vreme, domnul Gheorghe Tinca, cel care a avizat favorabil înființarea noii asociații.

Primul Consiliu de Conducere a fost format din şapte membri titulari şi trei membri supleanți, iar preşedintele asociației a fost ales colonelul în rezervă inginer Mitică Detot. La propunerea membrilor Consiliului, prima Adunare Generală a asociației a aprobat acordarea titlului de Preşedinte de Onoare al ADMRR domnului general-locotenent Decebal Ilina, locțiitor al şefului Statului Major General şi şef al Direcției informații militare, ca o recunoaştere a sprijinului acordat pentru constituirea şi legalizarea ADMRR.



ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
MINISTRUL

Nr. N 5921
Data 08.09.1995

AVIZ

Ministrul Apărării Naționale avizează favorabil înființarea Asociației Diplomaților Militari în Rezervă şi în Retragere "Alexandru Ioan Cuza", în condițiile prevăzute de statutul acesteia.

Avizul va fi folosit pentru completarea dosarului necesar înregistrării legale a Asociației la organele de justiție.

Ministrul Apărării Naționale
GHEORGHE TINCA

În luna mai 2008, Adunarea Generală a ADMRR a acordat titlul de „Preşedinte Fondator” domnului general de brigadă în rezervă inginer Mitică Detot.

Astfel, a fost înființată o organizație a foştilor diplomați militari, bazată pe principii democratice, în concordanță cu modificările sistemului politico-social din România. Era evident că înființarea ADMRR constituia o noutate atât pentru societatea civilă, cât şi pentru instituția militară.

Încă de la început, conducerea ADMRR a căutat să stimuleze membrii Asociației să scrie şi să publice lucrări memorialistice, studii geopolitice, relatări inedite din viața de ataşat militar, mărturii despre evenimente politico-militare notabile la care au participat, probleme specifice muncii de informații, cât şi analize, comentarii, propuneri privind apărarea şi securitatea României. Scopul principal era şi este acela de a sublinia continuitatea tradiției şcolii româneşti de informații militare, prestigiul acesteia, capacitatea sistemului informativ militar de a se adapta imperativelor istorice şi caracterul său deschis în sensul că acceptă experiența altora şi contribuie cu propria experiență la îmbogățirea culturii generale de intelligence.

Membrii asociației noastre transmit mai departe experiența dobândită în anii mulți de serviciu în slujba țării.

Perioada ce a urmat după înființare a fost marcată de o efervescență creatoare a membrilor Asociației, excelând mai ales lucrările de memorialistică şi cele privind activitatea specifică ataşaturii militare. În acest context, în Enciclopedia Armatei Române, apărută în anul 2009, au putut fi menționate 53 de titluri de lucrări


având ca autori membri ai ADMRR. De atunci până în prezent, numărul scrierilor membrilor noştri s-a dublat.

Începând din anul 2015, ADMRR editează o revistă bianuală de geopolitică intitulată ***Dincolo de orizonturi***, publicație care s-a bucurat încă de la început de popularitate şi interes atât în țară, cât şi în străinătate.

De asemenea, pentru a uşura comunicarea cu membrii noştri, Asociația şi-a creat propriul website (*www.admrr.com*), în care sunt postate atât activitățile curente, specifice fiecărei asociații de rezerviști militari, dar şi o parte din scrierile membrilor noştri, de la poezii până la lucrări valoroase de analiză politică şi militară.

Un alt obiectiv de bază care stă în atenția Asociației, poate cel mai important, este acela de a dezvolta simțămintele de prietenie, solidaritate şi camaraderie între membrii noştri, şi de a menține permanent legătura cu aceştia, în scopul identificării aşteptărilor şi speranțelor lor. În paralel, conducerea ADMRR este preocupată şi promovează permanent stabilirea şi întreținerea unor relații de cooperare cu celelalte structuri asociative ale rezerviştilor militari, precum Asociația Națională a Cadrelor Militare în Rezervă şi în Retragere „Alexandru Ioan Cuza", Asociația Națională a Veteranilor de Război, Asociația

Națională Cultul Eroilor „Regina Maria”, Asociația Cercetaşilor Militari în Rezervă şi în Retragere, Asociația Militarilor în Rezervă şi în Retragere din Domeniul Radioelectronic „Radul Negru” etc. Dorim ca această colaborare să capete aspecte cât mai concrete şi militäm pentru unificarea, într-o formă acceptabilă, a structurilor asociative ale rezerviştilor militari, fapt pentru care acordăm atenție contactelor cu asociațiile cu care am semnat acorduri de cooperare, dar nu excludem pe nimeni, toți, indiferent de denumirea asociației, fiindu-ne camarazi.

O activitate în care ADMRR se implică asiduu este aceea de a distribui cărți donate de membrii noştri la bibliotecile şcolare din țară. Am mers chiar mai departe şi, în ultimi trei ani, am dus cărți şi calculatoare în Republica Moldova, la Muzeul Militar din Chişinău şi la biblioteci şi şcoli din Cimişlia. În funcție de numărul cărților strânse de la membrii noştri, intenționăm să extindem această activitate şi în Bucovina de Nord şi, eventual, în Voivodina.

După 23 de ani de existență a ADMRR, putem concluziona că bilanțul este pozitiv, ceea ce nu înseamnă că nu se poate face mai mult.

Este reconfortant să vedem că într-o societate dominată de interese personale, neliniști şi frici, membrii ADMRR au înțeles că „NOI” este mai important decât „EU”.