UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Conferinţa Ştiinţifică Internaţională

STRATEGII XXI

Cu tema:

„COMPLEXITATEA ŞI DINAMISMUL MEDIULUI DE SECURITATE”

Centrul de Studii Strategice de Apărare şi Securitate
Bucureşti, 11 - 12 iunie 2015

VOL. 2

Coordonatori
Stan ANTON
Iuliana Simona ȚUȚUIANU

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
București, 2015

ISSN 2285-9462
ISSN-L 1844-3087

CUPRINS

GEOGRAFIA MILITARĂ – PRECURSOARE A GEOSTRATEGIEI

Dr. Silviu NEGUŢ
Profesor universitar, Academia de Studii Economice Bucureşti
silviu.negut@gmail.com

Rezumat: *Geostrategia, ca şi concept, deşi mai vechi decât cel de geopolitică, a fost foarte rar utilizat din cauza unor confuzii terminologice şi, mai mult decât atât, datorită existenţei Strategiei şi a Geografiei militare ca discipline bine individualizate. Studiul demonstrează că Geografia militară, o disciplină mult mai complexă decât se crede de obicei, este adevărata precursoare a Geostrategiei.*

Cuvinte cheie: *Geostrategie, Geografie, Geografie militară, Strategie, Geopolitică*

Introducere sau începuturile *Geostrategiei*

La fel ca şi în *Geopolitică*, şi în cazul *Geostrategiei*, fenomenele care o caracterizează sunt mult mai vechi decât momentul concretizării acesteia în cunoscutul, acum, concept. Dintotdeauna a existat o miză teritorială, o configuraţie anume a teatrului de operaţiuni, valorificată de actorul care a cunoscut-o cel mai bine. Aceasta (miza teritorială) este, aşa cum subliniază un foarte bun cunoscător în domeniu, „o constantă pe care o regăsim în toate epocile istorice şi care continuă să-şi facă simţite efectele în ciuda evoluţiei prodigioase a mijloacelor de comunicaţie”[1].

După cum se va vedea, există o strânsă legătură între Geopolitică şi Geostrategie, uneori acestea chiar confundându-se. Dar dacă, în primul caz, anul menţionării conceptului, ca şi terminologie, a fost foarte clar (1899, politicianul suedez Rudolf Kjellén, într-o conferinţă), în cel de-al doilea caz, multă vreme a existat o nebuloasă, crezându-se că este destul de recent, abia nu cu mult timp în urmă stabilindu-se că, de fapt, este cu peste 50 de ani anterior, respectiv 1846, fiind folosit de italianul Giacomo Durando în lucrarea *Della nazionalita italiana*. Acesta face aprecieri surprinzătoare pentru acele timpuri, pe lângă conceptul de *geostrategie*, introducându-l şi pe cel de *geotactică*:

„M-am folosit de un cuvânt care nu cred că a fost utilizat până azi, cel de *geostrategie* (sublinierea noastră), de fiecare dată când a fost nevoie să apreciez terenul în abstract şi în afara folosirii forţelor organizate, dar, în mod firesc, mereu în relaţie cu ele. În consecinţă, eu vorbesc de *condiţiile geostrategice şi geotactice* (*sublinierea noastră*) ale Italiei şi Spaniei, când studiez în abstract structura şi caracteristicile terenului, dar eu vorbesc de mişcări sau axe de operaţiuni strategice sau tactice, când este vorba de operaţiuni militare executate asupra unor puncte determinate ale terenului. Ca urmare eu separ, prin raţionament şi pentru o mai mare claritate aceste două idei care, în fapte şi în aplicaţie, nu sunt niciodată disjuncte.”[2]

Din păcate, cei doi termeni nu au prins rădăcini: unul (*geotactica*) a dispărut în neant, iar celălalt (*geostrategia*) a revenit în atenţie mult mai târziu. În acest ultim caz nu au avut efect nici studiile unor analişti iberici, care şi ei, precum Durando, au inclus conceptul în titlul lucrărilor lor: *Estudo geoestratégico de Portugal* (1890, colonelul spaniol Manuel Castaños y Montijano) şi *Estudio geo-éstrategico dos teatros de operações nacionais* (1932, colonelul portughez Miranda Cabral). Explicaţia este dată de faptul că a prins mai bine în epocă, a fost mai spectaculoasă, *Geografia militară*.

[1] Hervé Coutau-Bégarie (2008), *Traité de Géostratégie*, 6eme edition, Editions Economica, Paris, p. 759.
[2] *Apud* Ferrnicio Botti (1995), *Le concept de géostratégie et son application la nation italienne dans les théories du géneral Durando*, în „Stratégique”, 58, 1995-2, p. 129.

Unii analişti apreciază că cel care a pus bazele geostrategiei moderne este geopoliticianul american de origine olandeză Nycholas Spykman care, în lucrarea *America's Strategy in World Politics* (1942), face o adevărată analiză geostrategică a emisferei vestice, iar în *The Geography of the Peace*, apărută postum (în 1944, la un an după moartea sa), defineşte exact esenţa geostrategiei: „În vremea războiului total (*global warfare*), strategia militară trebuie să considere întreaga lume ca o unitate şi să gândească toate fronturile în relaţiile lor mutuale"[3].

Dar el nu foloseşte termenul *geostrategie*, deşi referirile sunt implicite. De altfel nici alţi analişti care au merite similare, precum americanii Hans W. Weigert şi Vilhjalmur Stefansson (*Compas of the World*, 1944), amiralul francez Raoul Castex (*Théories stratégiques*, 1929-1939), cehii Fritz-Otto Miksche (*Les erreursstratégiques de Hitler,* 1945; *War Between Continents*, 1948) şi Emanuel Moravec (*La Stratégie nouvelle*, 1941) şi alţii.

Meritul „reinventării" termenului de *geostrategie*, la aproape 100 de ani de la menţionarea sa de către italianul Giacomo Durando, îi revine americanului George B. Cressey, într-o lucrare publicată în 1944, în care geostrategia este opusă geopoliticii militariste şi imperialiste: „Funcţia geostrategiei este aceea de a înţelege problemele şi potenţialul unei naţiuni şi de a sugera un program de dezvoltare internă şi de cooperare internaţională în interesul tuturor"[4]. Se adaugă spaniolul Kindelan (*Geobelica*, 1945), francezii Camille Rougeron (*La Prochaine guerre*, 1948) şi Pierre Célérier (*Géopolitique et géostratégie*, 1955), brazilianul Galbery do Cunto e Silva (*Geopolítica e geoestrategia,* 1959), americanul Saul B. Cohen (*Geography and Politics in a World Divided*, 1963), argentinianul Justo P. Briano (*Geopolítica et geostrategia americana*, 1966). Însă prea puţine lucrări pentru un interval de câteva decenii. Abia odată cu anii '70, numărul acestora se multiplică, impunându-se lucrări ale unor analişti precum Colin S. Gray (*The Geopolitis of Nuclear Era*, 1976), John G. Pappageorge (*Maintaining the Geostrategic Advantage*, 1977), Zbigniew Brzezinski (*Game Plan. Geostrategic Framework for the Conduct of the US-Soviet Contest*, 1986), Hervé Coutau-Bégarie (cu cele trei lucrări având în titlu termenul *Géostratégie*, închinate oceanelor Atlanticul de Sud, 1985, Pacific, 1987, şi Indian, 1993), André Vigarié (*Géostratégie des océans*, 1990, *La Mer et la géostratégie des nations,* 1995), amiralul René Besnault (*Géostratégie de l'Arctique,* 1992) ş.a.

1. Confuzii privind conceptul de *geostrategie*

Este de semnalat faptul că unii analişti o confundă cu *polemologia* (gr. *polemos* = război, *logos* = ştiinţă), ramură a ştiinţei politice având ca obiect studiul ştiinţific al războaielor, stabilirea tipologiei acestora ca fenomen sociologic, a cauzelor, efectelor, obiectivelor şi funcţiilor lor, având drept scop, înlăturarea acestora din viaţa societăţii. Termenul a fost introdus de sociologul francez Gaston Bouthoul (1896-1980), în 1945, inspirat fiind de omologul său francez Rudolf Steinmetz, fondator al unui institut de specialitate. Bouthoul va scrie apoi o lucrare (*Les guerres*, 1951), pe care o va transforma într-un adevărat tratat (*Traité de polémologie. Sociologie des guerres,* prima ediţie în 1970).

Se pot identifica şi alte confuzii: uni consideră că *Geostrategia* nu este altceva decât o altă denumire a *Geografiei militare*, iar alţii că este o ramură a *Geopoliticii* care studiază, în mod deosebit, problemele care ţin de securitate.

Sunt şi analişti care, pur şi simplu, o apreciază drept o noţiune similară *Geopoliticii*. De altfel, trebuie recunoscut că relaţia *Geostrategie-Geopolitică* este foarte dificilă, frontiera dintre ele fiind foarte permeabilă şi greu de identificat, mulţi autori/analişti fiind concomitent

[3]Nicholas Spykman (1994), *The Geography of the Peace*, Harcourt Brace, New York, p. 6.
[4]George B. Cressey (1944), *Asia's Lands and Peoples. A Geography of One Third of the Earth and Two-Thirds of its People*, McGraw-Hill, II, New York, p. 32.

revendicaţi de ambele domenii, cum remarcă, printre alţii, analistul moldovean Oleg Serebrian. Este suficient să ne gândim la americanul Alfred Thayer Mahan (1840-1914), autorul *teoriei puterii maritime* (*Sea Power*) şi britanicul Halford J.Mackinder (1861-1947), creatorul conceptului opus, respectiv *teoria puterii continentale* (*Land Power*), cunoscut mai ales sub numele de *teoria Heartland*-ului („inima Lumii")[5]. Dar mai sunt mulţi alţii, între care Julian Corbett (1854-1922), tot britanic, Virgilio Spigai (1907-1976), italian, ambii cu contribuţii însemnate în domeniul strategiei maritime.

Mulţi autori cu preocupări în domeniu, între care cunoscutul istoric britanic Arnold Toynbee (1889-1975), explică evoluţia strategiei doar, sau aproape exclusiv, prin evoluţia tehnicii de luptă: falanga – legiunea (romană) – arcul turcoman – praful de puşcă – puşca cu tragere rapidă – mitraliera – calea ferată – carul de luptă şi motorizarea – avionul – arma atomică etc., toate acestea marcând marile schimbări în domeniu. Numai că, aşa cum remarca generalul André Beaufre, în urmă cu peste 50 de ani, „este adevărat, perfecţionarea tehnicii constituie un factor esenţial al puterii. (…) Dar această avansare/perfecţionare se poate dovedi inutilă dacă ea este folosită de o strategie proastă. (…) Să ne amintim de recentele noastre experienţe în Algeria [se referă la francezi – *nota noastră*], de exemplu: ne-a permis, oare, nouă, armamentul modern de care am dispus să ne atingem scopul propus? De fapt nu există tactici optime în sine, orice tactică valorând doar în raport cu cea a adversarului. Noi am putut constata, de exemplu, că avionul şi carul de luptă sunt puse în dificultate de guerilă şi că arma nucleară nu i-a permis Statelor Unite să obţină un avantaj în Coreea, ci doar un armistiţiu de compromis. Aceasta vrea să spună că există ceva care trebuie să domine tactica: *alegerea tacticilor* (sublinierea noastră). *Iar alegerea tacticilor este strategie*. Tocmai strategia este aceea care va decide forma conflictului – ofensiv sau defensiv, insidios sau violent direct sau indirect –, dacă se va alege lupta în domeniul politic sau în domeniul militar, dacă se va utiliza sau nu arma atomică etc."[6].

În acest context este de amintit că, în perioada de după cel de-al Doilea Război Mondial, au prevalat, graţie mai ales confruntării Est-Vest, studiile strategice, pur militare, care le-au estompat pe cele geostrategice, deşi conţineau şi multe elemente ce ţin de geostrategie. Dintre cele dintâi, unele datorate unor reputaţi geopoliticieni, amintim câteva datorate unor analişti francezi (amiralul Raoul Castex, *Théories stratégiques*, 1929-1939; André Beaufre, *Stratégie de l'action,* 1966, *Stratégie pour domain. Les problèmes militaires de la guerre moderne,* 1972; Jean Paul-Charnay, *Essai général de stratégie,* 1973, *Métastratégie. Systèmes, formes et principes de la guerre féodale à la dissuasion nucléaire,* 1990, *Lastratégie,* 1995; Hervé Coutau-Bégarie, *Traité de Stratégie*, 1999; Philippe Moreau-Defarges, *Problèmes stratégiques contemporaines,* 1992; Lucien Poirier, *Stratégie théorique,* trei volume, primul în1982 cu titlul *Essais de stratégie théorique*), americani (Colin S. Gray, *Strategic Studies and Public Policy*, 1982, *War, Peace and Victory: Strategy and Statecraft for the Next Century*, 1990, *Explorations in Strategy,* 1998; Peter Paret, editor, *Makers of Modern Strategy*, 1985; John Baylis and Ken Booth, *Contemporary Strategy – I. Theories and Concepts*, 1987; Kenneth N. Brown, *Strategic. The Logistic – Strategy Link*, 1987; John M. Collins, *Grand Strategy. Principles and Practices*, 1973, *Military Strategy. Principles and Historical Perspectives*, 2002; Bernard Brodie, *Strategy as a Science*, 1949; Edward N. Luttwak, *Strategy and History,* 1985; Paul Kennedy, editor, *Grand Strategies in War and Peace*, 1991), britanici (Ken Booth, *Strategy and Ethnocentrism*, 1979; N.A.M. Rodger, *The Command of the Ocean. A Naval History of Britain* 1649-1815, trei volume, 2004; John

[5]Pentru detalii vezi:Aymeric Chauprade, François Thual (2004), *Dicţionar de geopolitică: state, concepte, autori*, Editura Corint, Bucureşti, pp. 506-510; Silviu Neguţ (2008), *Geopolitica. Universul puterii*, Editura Meteor Press, Bucureşti, pp. 32-38 ş.a.

[6]André Beaufre (1998), *Introduction à la stratégie*, Editura Hachette, Paris, pp. 69-70 (prima ediţie a fost publicată în 1963, la Editura Armand Colin).

Baylis şi John Garnett, editori, *Makers of Nuclear Strategy*, 1991), germani (Albert A. Stahel, *Klassiker der Strategie*. *Eine Bewertung*, 1996; Wilhelm Schaubourg-Lippe, *Schriften und Briefe. II Militärische Schriften*, 1977; se adaugă zecile de cărţi – fără a menţiona articolele –, închinate marelui strateg prusac Carl von Clausewitz), italieni (Carlo Jean, *Guerra, strategia e sicurezza,* 1997; Paulo Supino, *Strategia globale*, 1965), spanioli (Miguel Alonso Baquer, *En quié consiste la estrategia?,* 2000; Fernando de Bordejé y Morencos, *España, poder maritimo y estrategia naval*, 1982), portughezi (Virgílio de Carvalho, *Estratégia global e subsidios para una grande estratégia nacional*, 1986; Abel Cabral Couto, *Elementos de estratégia*: *Apontamentos para um corso*, două volume, 1988-1989), brazilieni (João Carlos Gonçalves Caminha, *Delineamentos de estratégia*, 1982).

2. Geografia militară – precursoare a geostrategiei

Nu ne putem imagina expansiunea oricărui stat din istoria omenirii şi, cu atât mai puţin, constituirea marilor imperii, toate realizate pe calea armelor, fără cunoaşterea cadrului natural şi, mai ales, a modului în care elementele acestuia puteau influenţa acţiunile militare în cauză. Toţi comandanţii militari au ţinut seamă de aceasta, de la cei din vechime (Sun Zi, Cyrus cel Mare, Alexandru cel Mare, Hannibal, Caesar, Traian ş.a.) la cei din Evul Mediu (Genghis Han, Solyman Magnificul, Petru cel Mare, Ştefan cel Mare ş.a.) şi din timpurile moderne (Napoleon Bonaparte şi toată pleiada de generali europeni, americani şi asiatici care a marcat ultimele două secole).

Multă vreme nu a avut un nume, de la o vreme i se zice *Geografie militară*, definită, pe scurt, *drept ştiinţa ce studiază impactul factorilor geografici, în special al reliefului, apelor şi climei, asupra acţiunilor militare*.

Astfel, generalul chinez Sun Zi/Sun-tzu (sec. VI-V î.Hr.), autorul primului tratat de strategie militară cunoscut până astăzi (*Arta militară*), afirma, în urmă cu două milenii şi jumătate: „Cel care nu cunoaşte configuraţia pădurilor şi munţilor, defileele şi mlaştinile, nu poate face ca armata sa să avanseze”. De asemenea, este arhicunoscut faptul că, în urmă cu peste o mie de ani, împăratul Constantin al VI-lea Porfirogenetul, atunci când pregătea o campanie, se informa asupra teatrului de operaţiuni (distanţe, resurse, starea drumurilor şi a capacităţilor de apărare), aşa cum reiese din lucrarea sa *De administrando imperio*.

Aşa cum bine sesizează analistul francez Hervé Coutau-Bégarie, legătura teoretică dintre *geografie* şi *război* este enunţată clar abia în secolul al XVIII-lea, în Franţa (Abatele Lenglet-Dufresnoy, *Méthode pour étudier la géographie*, 1716 şi *Introduction à la Géographie moderne* în „Encyclopédie méthodique. Géographie Moderne”, 1ere tom, 1782, mai cunoscută drept „Enciclopedia Panckoucke”, după numele editurii care a publicat-o), în cel următor fiind cu adevărat fundamentată, nu numai în Franţa, ci şi în Germania, Austria, Spania, Italia, Rusia şi alte ţări, formându-se adevărate şcoli. Este deosebit de semnificativă precizarea făcută în amintita enciclopedie: „Un general puţin instruit este timid; el va merge în operaţiuni tatonând, va vira, va consulta, va ezita… Un militar instruit, un general savant în geografie cunoaşte dinainte avantajele şi dezavantajele care pot rezulta din una sau altă poziţionare; el are deja triumful pe harta pregătită şi chiar înainte de a fi văzut inamicul, el a învins”.

Mai multe şcoli de geografie militară s-au individualizat în a doua jumătate a secolului al XIX-lea, între care se înscriu: franceză, germană, spaniolă, italiană, austriacă şi elveţiană, rusă, anglo-saxonă şi chiar şi una românească.

Concluzii

În urma studierii conceptelor de *geografie militară, geostrategie, geopolitică*, au rezultat următoarele concluzii:

- toate aceste concepte s-au fundamentat în a doua jumătate a secolului al XIX-lea, existând o puternică confuzie terminologică, uneori, chiar noţională, între ele;
- termenul de *geostrategie* (Giacomo Durando, 1846) îl precede pe cel de *geopolitică* (Rudolf Kjellén, 1899), alţii precum cel de *geotactică,* dispărând, datorită suprapunerii cu dezvoltarea deosebită a *Geografiei militare*, motiv pentru care şi cel de *geostrategie* a revenit în atenţie mut mai târziu (la aproape 100 de ani distanţă, respectiv George B. Cressey, 1944);
- iniţial s-a considerat că *Geostrategia* nu este altceva decât o altă denumire a *Geografiei militare*, iar alţii că este o ramură a *Geopoliticii* care studiază, în mod deosebit, problemele care ţin de securitate.

BIBLIOGRAFIE:

1. Beaufre, André (1998), *Introduction à la stratégie*, Editura Hachette, Paris.
2. Botti, Ferrnicio (1995), *Le concept de géostratégie et son application à la nation italienne dans les théories du géneral Durando*, în „Stratégique", 58, 1995-2.
3. Chauprade, Aymeric; Thual, François (2004), *Dicţionar de geopolitică: state, concepte, autori*, Editura Corint, Bucureşti.
4. Coutau-Bégarie, Hervé (2008), *Traité de Stratégie*, 6eme edition, Editions Economica, Paris.
5. Cressey, George B. (1944), *Asia's Lands and Peoples. A Geography of One Third of the Earth and Two-Thirds of its People*, McGraw-Hill, II, New York.
6. Neguţ, Silviu (2008), *Geopolitica. Universul puterii*, Editura Meteor Press, Bucureşti.
7. Spykman, Nicholas (1994), *The Geography of the Peace*, Harcourt Brace, New York.

MILITARIZAREA ARCTICII DE CĂTRE RUSIA

Cristina Simona BONDAR
Doctorand Academia Naţională de Informaţii „MIHAI VITEAZUL”
cristinabondar@gmail.com

Rezumat: *Creşterea luptei pentru influenţă şi resurse energetice a împins Federaţia Rusă spre o nouă cursă a înarmării în regiunea arctică. În acest scop, Moscova şi-a modificat cadrul legislativ, noile prevederi stipulând crearea unui Comandament Arctic, restaurarea impresionantelor capabilităţi militare din perioada sovietică, construirea unor noi baze militare şi furnizarea de echipament modern pentru acestea.*

Concomitent cu dezvoltarea acestor capabilităţi militare, Kremlinul desfăşoară aplicaţii pe scară largă, cu un rol demonstrativ la nivelul relaţiilor internaţionale.

Cuvinte cheie*:* militarizare, Federaţia Rusă, Regiunea Arctică

Introducere

După căderea Cortinei de Fier, regiunea arctică, teritoriu al confruntărilor tăcute între submarinele america şi ruseşti din timpul Războiului Rece, a intrat într-un con de umbră care a început să se ridice odată cu creşterea nevoilor energetice ale statelor lumii. Descoperirile din această zonă indică faptul că aici se află aproximativ 13% din rezervele neexploatate de petrol ale lumii şi 30% din volumul gazelor.

Ca urmare a creşterii divergenţelor dintre NATO şi Federaţia Rusă, tensiunile din această regiune vor înregistra o escaladare generată de vecinătatea dintre cei doi actori.

Politica Rusiei pentru Arctica are la bază mai multe documente strategice, printre care se regăsesc:

- Fundamentele Politicii de Stat a Federaţiei Ruse în Regiunea Arctică până în 2020, adoptată în 2008;
- Doctrina Militară a Federaţiei Ruse, din 2014;
- Strategia de securitate naţională a Federaţiei Ruse până în 2020;
- Concepţia Politicii Externe a Federaţie Ruse, publicată în 2013.

1. Interese ale Federaţiei Ruse în Oceanul Arctic

În ultima perioadă a fost observată o revitalizare a interesului Moscovei pentru această regiune, accentuându-se importanţa zonei pentru asigurarea obiectivelor economice şi de securitate ale Federaţiei Ruse. În acest sens, acţiunile Kremlinul în Arctica vizează mai multe elemente. Principala coordonată este reprezentată de dezvoltarea economică a teritoriilor ruse. În plus, statul vede această regiune drept o platformă de promovare a Rusiei ca mare putere mondială.

Potrivit estimărilor, până la mijlocul secolului 21, calota glaciară se va topi complet pe timpul verii, ceea ce va permite navigarea pe noi trasee, mai sigure şi mai ieftine, comparativ cu cele tranzitate în prezent, prin Cornul Africii, strâmtoarea Malacca sau Canalul Suez.

Concomitent cu interesele economice, un element deosebit de important al politicii ruse în zona arctică îl reprezintă şi perspectiva militară, o supremaţie în nordul extrem

oferindu-i Rusiei posibilitatea de a avea acces la oceane pentru submarinele sale, cu rol în politica de descurajare nucleară[1].

Pentru a atinge aceste scopuri, autorităţile acţionează inclusiv prin revendicări teritoriale.

2. Modalităţi de acţiune ale Moscovei în regiunea arctică

Moscova tratează orice interes străin faţă de această zonă, indiferent că este vorba de unul economic, comercial sau de mediu, drept o intenţie ostilă, ceea ce a condus la o retorică şi la un mod de acţiune menite să intimideze actorii interesaţi de această regiune.

Kremlinul a transmis numeroase mesaje, atât declarative, cât şi simbolice, pentru a susţine pretenţiile teritoriale din Arctica, prin multe dintre acestea încercând o impunere, uneori destul de agresivă, a suveranităţii asupra unor teritorii. În acest scop, una din principalele aserţiuni o reprezintă ideea potrivit căreia dorsalele Lomonosov şi Mendeleev fac parte din platforma continentală a Rusiei, ceea ce i-ar conferi dreptul, potrivit Convenţiei pentru Drepturile asupra Mărilor – *UNCLOS*, să revendice 200 de mile maritime de la ţărm şi să exploateze resurse la o distanţă de până la 350 de mile marine. Federaţia Rusă susţine că cele două forme de relief nu sunt dorsale, ci extensii ale platformei ei continentale. Pe de altă parte, şi Danemarca (prin suveranitatea pe care o are asupra Groenlandei) şi Canada, promovează teoria potrivit căreia Lomonosov face parte din platformele lor continentale. Acordarea drepturilor teritoriale pentru oricare din aceste state ar creşte considerabil zona în care ar ţările ar avea dreptul de a deschide exploatări minerale sau energetice.

1) Polul Nord
2) Dorsala Lomonosov
3) 200 de mile marine, limita zonei economice exclusive
4) Teritoriul revendicat de Federaţia

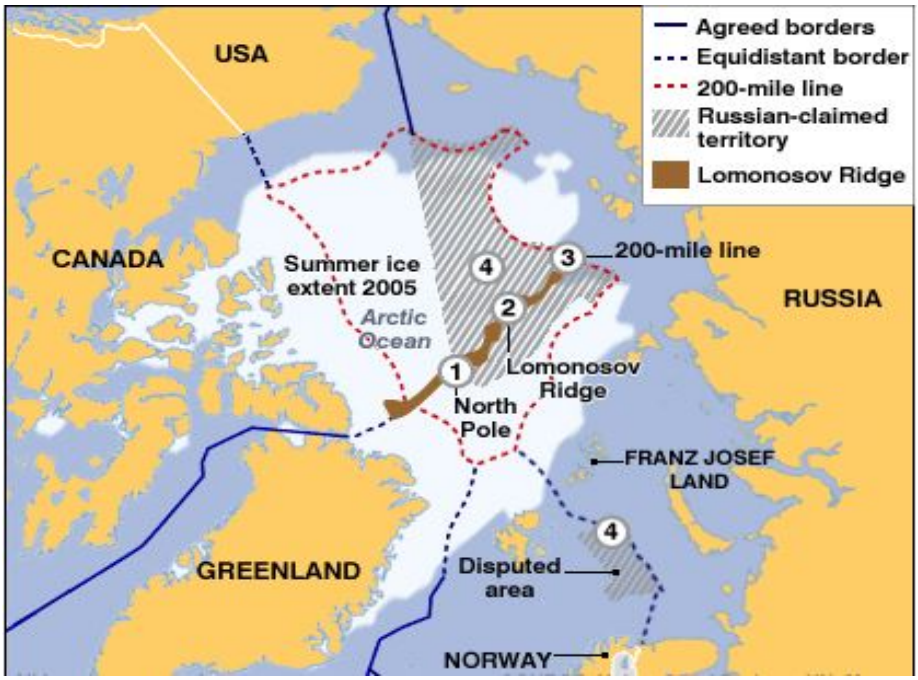


Figura 1, Revendicări teritoriale ale Federaţiei Ruse în Arctica
Sursa: „BBC”

[1] SMITH Mark, A.; KEIR; Giles, *Russia and the Arctic: The "Last Dash North"*, Defence Academy of the United Kingdom, 2007, available at http://www.academia.edu/929852/Russia_and_the_Arctic_the_Last_Dash_North_, consulted at 01 March 2015

Deşi Moscova a depus o solicitare către ONU pentru recunoaşterea dreptului asupra dorsalei Lomonosov în 2001, o soluţie în acest nu a fost adoptată până în prezent. Potrivit declaraţiilor oficialilor ruşi, această solicitare va fi reînnoită în 2015[2].

Pentru a întări aceste revendicări, Moscova a lansat misiuni exploratorii are au avut ca obiectiv colectarea unor date batimetrice şi aunor mostre de pe fundul oceanului. În plus, în 2007, două minisubmarine au plasat un steag din titan pe fundul mării, în apropiere de Polul Nord.

Acţiunea a generat critici la adresa Rusiei, fiind comparată de ministrul canadian de externe din acea perioadă, drept o colonizare specifică secolului al XV-lea[3]. Expediţia în cadrul căreia a fost făcut acest demers a avut ea însăşi un caracter demonstrativ, spărgătorul de gheaţă de pe care au fost lansate submarinele şi pe care s-a aflat inclusiv un deputat al Dumei de Stat, a fost prima navă care a reuşit să ajungă la Polul Nord, tăind calota glaciară[4].

Un alt punct fierbinte al regiunii îl reprezintă şi graniţa maritimă între SUA şi Federaţia Rusă, tratatul semnat în 1990 nefiind ratificat nici în prezent de Legislativul rus care îl percepe drept nedrept, fiind negociat într-o perioadă în care Uniunea Sovietică se afla în pragul prăbuşirii[5].

Un alt element asupra căruia cele două state nu au reuşit să ajungă la un acord îl reprezintă statutul Rutei Nordice. În timp ce Washingtonul militează pentru dreptul la liberă navigaţie, Moscova susţine că traseul trece prin apele ei teritoriale şi, prin urmare, este necesar ca navele care tranzitează zona trebuie să solicite permisiunea autorităţilor şi să plătească pentru furnizarea unor servicii ale spărgătoarelor ruse de gheaţă[6].

3. Componenta militară – element central al politicii Federaţiei Ruse în Arctica

În Fundamentele Politicii de Stat a Federaţiei Ruse în Regiunea Arctică până în 2020 se stipulează că modificarea balanţei de putere la graniţe se poate modifica în viitor, Rusia putând apăra interesele statului printr-o decizie de a utiliza forţa militară. Având în vedere că Federaţia Rusă este statul cu cea mai lungă graniţă către zona arctică, mai mult de 6.000 de kilometri, Moscova acţionează pentru securizarea acesteia în mai multe modalităţi.

Astfel:

- a reorganizat structura de conducere a operaţiunilor din Nord, unde a creat Comandamentul Strategic Comun;
- a redeschis baze militare din perioada sovietică şi a construit noi facilităţi militare în regiune;
- se află într-un proces de modernizare a capabilităţilor militare din regiune;
- intenţionează să crească numărul militarilor detaşaţi în Arctica.

Comandamentul Strategic Comun a devenit funcţional la 1 decembrie 2014. Are la bază Flota Nordică, la care au fost transferate şi unităţi, nave şi trupe din cadrul Districtelor de Vest, Central şi de Sud. Va cuprinde două brigăzi motorizate de infanterie, care au rolul de a

---

[2] Declaraţie a ministrului resurselor naturale, Serghey Donskoy, după o întrevedere cu preşedintele Vladimir Putin în aprilie 2015; disponibilă la http://barentsobserver.com/en/arctic/2014/04/putin-readies-arctic-territorial-claims-07-04

[3] *Russia plants flag under N Pole*; available at http://news.bbc.co.uk/2/hi/europe/6927395.stm; 2 august 2007, consulted at 20.02.2015

[4] PADRTOVA, Barbora, *Russian Approach Towards the Arctic Region*, 2012, available at http://cenaa.org/analysis/russian-approach-towards-the-arctic-region/, consulted at 15 february 2015

[5] KACZYNSKI, Vlad M., *US-Russian Bering Sea Marine Border Dispute: Conflict over Strategic Assets, Fisheries and Energy Resources*, Russian Analytical Digest, may 2007, available at http://www.css.ethz.ch/publications/pdfs/RAD-20-2-5.pdf , consulted at 21 march 2015

6ROSEN, Mark E.; ASFURA-HEIM Patricio, *Addresing the gaps in Arctic Governance*, octomber 2013, available at http://www.hoover.org/research/addressing-gaps-arctic-governance, consulted on 10 february 2015

susţine şi escorta navele care utilizează Ruta Nordică[7]. Prezenţa forţelor speciale a crescut cu 30% prin revitalizarea Celui de-al 61-lea Regimentul Independent de Infanterie Navală, care va staţiona alături de Cea de-a 200 Brigadă Independentă de Infanterie, la rândul ei reînfiinţată, la Baza Sputnik, din interiorul Cercului Polar, la o distanţă de 16 kilometri de graniţa cu Norvegia, şi 65 de kilometri de cea cu Finlanda.

Potrivit mass-media, în Comandamentul Strategic Comun vor funcţiona şi rachete de tip Panţir-1 şi sisteme de artilerie, elicoptere modificate pentru climat rece – Mi-8 Hip şi avioane MiG – 31 Foxhound[8].

Totodată, până la finalul anului 2015 a fost anunţată finalizarea modernizării şi redeschiderea bazelor militare construite în perioada sovietică, precum şi deschiderea unor noi facilităţi. Atrage atenţia inclusiv demararea procesului de construire a unei baze inclusiv într-o zonă clasificată de autorităţile ruse drept rezervaţie naturală, Insula Wrangel[9].

Figura 2, Baze militare ruse în Arctica
Sursa: http://www.globalsecurity.org/military/world/russia/vo-northern.htm

În plus, vor fi reactivate şi construite staţii radar, numărul acestora urmând să ajungă la şase[10]. Pentru a creşte capacitatea de supraveghere, Rusia intenţionează trimiterea în regiunea arctică inclusiv a unor drone de tip Orlan-10, cu o autonomie de 16 ore şi o arie operaţională de 600 de kilometri[11].

---

[7]*Russia to Form Arctic Military Command by 2017*; 1 October 2014, available at http://www.themoscowtimes.com/business/article/russia-to-form-arctic-military-command-by-2017/508199.html, consulted at 15 March 2015

[8]JENNINGS, Gareth, *Russia to build more Arctic airfields*, 12 January 2015, available at http://www.janes.com/article/47831/russia-to-build-more-arctic-airfields, consulted on 15 March 2015

[9]*Russia to Form Arctic Military Command by 2017*; 1 October 2014, available at http://www.themoscowtimes.com/business/article/russia-to-form-arctic-military-command-by-2017/508199.html, consulted at 15 March 2015

[10]*Joint Strategic Command*, available at http://www.globalsecurity.org/military/world/russia/vo-northern.htm, consulted on 14 March 2015

[11]*Russia plans Orlan-10 UAV Arctic deployment*, 7 January 2015, available at http://www.janes.com/article/

Regiunea arctică, spre deosebire de Marea Neagră sau Marea Baltică, oferă Rusiei posibilitatea de acces nemijlocit la oceanele lumii, semnificativă în acest sens fiind şi plasarea Cartierului General al celei mai puternice dintre flotele ei – Flota Nordică în zona. În componenţa structurii se regăsesc submarine nucleare, bombardiere strategice şi rachete intercontinentale.

Odată cu diminuarea capabilităţilor forţelor militare convenţionale ruse, importanţa politicii de descurajare nucleară a crescut în strategia Moscovei, sens în care statul încearcă o recâştigare a titlului de mare putere navală. În acest sens, s-a acordat o prioritate crescută modernizării arsenalului nuclear, inclusiv prin construirea unui nou submarin multirol din clasa Yassen şi plasarea de comenzi pentru alte tipuri de nave de acest fel, precum intenţiile de achiziţionare a mai multor submarine din clasa Borei, capabile să transporte rachete balistice[12].

Concomitent cu capabilităţile strict militare, Federaţia Rusă este singurul stat care dispune şi o flotă de spărgătoare de gheaţă cu propulsie nucleară, ultimul intrat în serviciu, şi cel mai puternic dintre acestea fiind „50 de ani de Victorie". Aceste nave au un rol decisiv în tranzitul oricărei vase civile sau militare de suprafaţă, facilitând atât trecerea prin banchiza compactă, cât şi traversarea unor ape periculoase a urmare a desprinderii unor gheţari.

Pentru a întări ideea de putere regională, Kremlinul desfăşoară periodic exerciţii militare în Arctica. Ultimele au avut loc în martie 2015, şi au implicat peste 80.000 de militari, 220 de aeronave, 41 de nave şi 15 submarine.

4. Dificultăţi de implementare a strategiei ruse pentru Arctica

Deşi a fost înregistrată o creştere a activităţii militare şi au fost implementaţi paşi concreţi pentru modernizarea forţelor din regiune, aceste evoluţii au avut loc pe fondul existenţei unei Armate slăbite. Ritmul de înnoire a fost unul lent, în pofida unor reforme radicale.

În pofida declaraţiilor belicoase, în mediul experţilor s-a atras atenţia că mijloacele de care dispune Federaţia Rusă nu reprezintă o ameninţare atât de mare. În acest sens, Alexandre Golts argumentează că discursul agresiv al Moscovei se întinde pe o perioadă lungă de timp dar, până în prezent din toate planurile măreţe ale acesteia, a fost pusă în practică doar detaşarea a două brigăzi care constau în câteva zeci de persoane. Chiar dacă numărul lor ar fi mai mare, tot le-ar fi imposibil să asigure o pază eficientă a coastelor arctice de la Murmansk la Vladivostok. Totodată, soldaţi nici măcar nu au un rol pur militar, personalul fiind folosit la construcţia unei noi baze militare. La acest aspect se adaugă şi elementele logistice, bazele aflate în perimetrul Cercului Polar fiind dificil de aprovizionat, în special cu combustibilul necesar misiunilor de patrulare.

În mediul experţilor s-a argumentat că şi impresionantele exerciţii militare au demonstrat lipsa de pregătire a forţelor din Arctica. Scenariul a fost unul similar tacticilor Războiului Rece şi a presupus identificarea şi distrugerea submarinelor şi a grupurilor de portavioane. Pentru această acţiune, au fost trimise o grupare de militari din centrul Rusiei. Pe de altă parte, brigăzile din Arctica au avut rolul de a neutraliza grupări subversive care au apărut exact în teritoriul controlat de acestea[13].

47732/russia-plans-orlan-10-uav-arctic-deployment;%20Russia%20plans%20Orlan-10%20UAV%20Arctic%20deployment;%207%20ianuarie%202015, consulted on 16 March 2015

[12]STAALESEN Atle, *New attack submarine ready before year's end*, Barents Observer, 20 August 2012, http://www.barentsobserver.com/en/security/new-attack-submarine-ready-years-end-20-08, consulted on 10 March 2015

[13]GOLTS, Alexander, *Why Russia's War Games Should Scare Nobody*, 23 March 2015, available at http://www.themoscowtimes.com/opinion/article/russia-s-war-games-should-scare-nobody/517898.html, consulted on 28 March 2015

Locaţia desfăşurării acestora, la mare distanţă de teritoriile aflate în dispută, induc ideea că scopul lor a fost demonstrativ pentru opinia publică, nu de a simula o situaţie reală, în care acestea ar putea fi implicate în acţiuni de luptă.

Un alt element care va afecta considerabil capabilităţile Moscovei în zonă îl reprezintă şi apropierea decomisionării spărgătoarelor de gheaţă atomice de care dispune. În lipsa unor planuri clare de construcţie a unor noi nave, este probabilă împlinirea predicţiei din 2012 a directorului Atomflot, Viacheslav Ruksha, oficialul afirmând că în perioada 2016 – 2017, Rusia va suferi un colaps în domeniu[14].

Concluzii

În pofida planurilor extrem de ambiţioase ale autorităţilor ruse pentru regiunea arctică, probabilitatea de materializare a lor este destul de scăzută. Acest aspect se datorează în principal unei lipse de resurse financiare care să fie directate în acest scop. Concomitent cu reducerea veniturilor Rusiei ca urmare a impunerii sancţiunilor Occidentale după anexarea Crimeii şi suportul acordat rebelilor din Doneţk şi Luhansk, măsurile au generat şi o reducere a accesului la noi tehnologii militare şi civile care să poată fi utilizate în zonă.

Acest aspect a condus, de pe o parte, la o încetinire a modernizării echipamentelor şi a construcţiei unora noi, Ucraina fiind unul din principalii furnizori de componente utilizate în această industrie. Pe de altă parte, sancţiunile au condus la o reticenţă a companiilor occidentale de a investi în exploatarea zăcămintelor de hidrocarburi, ceea e a devenit un impediment în evoluţia economică a regiunii. La acest aspect a contribuit şi diminuarea preţului petrolului, care a fost o nouă lovitură pentru economia deja şubrezită a Rusiei.

În plus, Ruta Nordică nu este momentan viabilă pentru utilizare curentă de către navele comerciale, costurilor crescute pentru infrastructură adăugându-li-se şi unele exorbitante ale companiilor de asigurări.

Cu toate acestea, deşi ritmul de implementare al reformelor va fi în continuare exclus, Kremlinul nu va renunţa la ambiţiile de impunere a Rusiei drept cel mai important actor în Arctica, atât din punct de vedere economic, cât şi militar.

BIBLIOGRAFIE:

1. FAITH, Ryan, *Russia's Massive Military Exercise in the Arctic Is Utterly Baffling*, 21 March 2015, available at https://news.vice.com/article/russias-massive-military-exercise-in-the-arctic-is-utterly-baffling, consulted on 28 March 2015.
2. GOLTS, Alexander, *Why Russia's War Games Should Scare Nobody*, 23 March 2015, available at http://www.themoscowtimes.com/opinion/article/russia-s-war-games-should-scare-nobody/517898.html, consulted on 28 March 2015.
3. JENNINGS, Gareth, *Russia to build more Arctic airfields*, 12 January 2015, available at http://www.janes.com/article/47831/russia-to-build-more-arctic-airfields, consulted on 15 March 2015.
   jfq-57/zysk.pdf, consulted on 20 February 2015.
4. Joint Strategic Command, available at http://www.globalsecurity.org/military/world/russia/vo-northern.htm, consulted on 14 March 2015.

[14]FAITH, Ryan, *Russia's Massive Military Exercise in the Arctic Is Utterly Baffling*, 21 March 2015, available at https://news.vice.com/article/russias-massive-military-exercise-in-the-arctic-is-utterly-baffling, consulted on 28 March 2015

5. KACZYNSKI, Vlad M., *US-Russian Bering Sea Marine Border Dispute: Conflict over Strategic Assets, Fisheries and Energy Resources*, Russian Analytical Digest, May 2007, available at http://www.css.ethz.ch/publications/pdfs/RAD-20-2-5.pdf , consulted at 21 March 2015.
6. PADRTOVA, Barbora, *Russian Approach Towards the Arctic Region*, 2012, available at http://cenaa.org/analysis/russian-approach-towards-the-arctic-region/, consulted at 15 February 2015.
7. ROSEN, Mark E.; ASFURA-HEIM Patricio, *Addresing the gaps in Arctic Governance*, October 2013, available at http://www.hoover.org/research/addressing-gaps-arctic-governance, consulted on 10 February 2015.
8. *Russia plans Orlan-10 UAV Arctic deployment*, 7 January 2015, available at http://www.janes.com/article/47732/russia-plans-orlan-10-uav-arctic-deployment;%20Russia%20plans%20Orlan10%20UAV%20Arctic%20deployment;%207%20ianuarie%202015, consulted on 16 March 2015.
9. *Russia plants flag under N Pole*; available at http://news.bbc.co.uk/2/hi/europe/6927395.stm; 2 August 2007, consulted at 20 February 2015.
10. *Russia to Form Arctic Military Command by 2017*; 1 October 2014, available at http://www.themoscowtimes.com/business/article/russia-to-form-arctic-military-command-by-2017/508199.html, consulted at 15 March 2015

Russia_and_the_Arctic_the_Last_Dash_North_, consulted at 01 March 2015.

11. *Russia's Arctic Strategy*, available at https://archive.org/stream/563663-russias-arctic-strategy/563663-russias-arctic-strategy_djvu.txt, consulted on 20 February 2015
12. SMITH Mark, A.; KEIR; Giles, Russia and the Arctic: The "Last Dash North", DefenceAcademy of the United Kingdom, 2007, available at http://www.academia.edu/929852/
13. STAALESEN Atle, New attack submarine ready before year's end, Barents Observer, 20 August 2012, http://www.barentsobserver.com/en/security/new-attack-submarine-ready-years-end-20-08, consulted on 10 March 2015.
14. STAALESEN, Atle, Putin readies Arctic territorial claims, 07 April 2012, available at http://barentsobserver.com/en/arctic/2014/04/putin-readies-arctic-territorial-claims-07-04, consulted at 05 March 2015.
15. ZYSK, Katarzyna, *Russia's Arctic Strategy, Ambitions and Constraints*, Norwegian Institute for Defence Studies, 2010, available at http://www.ndu.edu/press/lib/images/

ALOCAREA RESURSELOR ŞI GENERAREA CAPABILITĂŢILOR ÎN STUDIILE DE SECURITATE

Dr. Mihai ZODIAN
Asistent de cercetare la Centrul de Studii Strategice de Apărare şi Securitate din cadrul Universităţii Naţionale de Apărare „Carol I”
zodian@gmail.com

Rezumat: *Studiile de securitate s-au dezvoltat după sfârşitul Războiului Rece, în cadrul unei tentative de a imbogăţi agenda intelectuală şi publică dincolo de temele tradiţionale legate de recursul la forţă. Tendinţa respectivă corespundea unui interes social mai larg legat de fructificarea avantajelor păcii şi bunăstării, interes legat de o viziune optimistă a relaţiilor internaţionale şi a politicii, concepţie pusă sub semnul întrebării, însă, în situaţii de criză sau conflict. Comunicarea surprinde evoluţia studiilor de securitate şi relaţia lor cu puterea militară, argumentând că această problemă necesită să fie aprofundată, datorită importanţei sale teoretice şi politice*.

Cuvinte cheie: *securitate, capabilităţi, putere militară, realism, constructivism*

Această prezentare este dedicată investigării continuităţilor şi schimbărilor prin care a trecut domeniul studiilor strategice după sfârşitul Războiului Rece, din perspectiva alocării resurselor şi a generării capabilităţilor. Importanţa subiectului a sporit odată ce s-au resimţit consecinţele crizei economice începute în 2007-2008, îndeosebi în contextul conflictului din Ucraina. Tendinţele universitare pot reflecta realitatea socială, dar, concomitent, ele ne pot spune multe despre mentalităţile curenmte şi chiar să influenţeze politicile, în circumstanţe favorabile.

Mai precis, se pot observa tendinţe divergente în interiorul comunităţii transatlantice referitoare la definirea chestiunilor de securitate, sensul termenului şi politicile pe care actorii trebuie să le urmărească[1]. Acest pluralism al interpretărilor corespunde nuanţelor strategiilor şi comportamentelor care au caracterizat acest spaţiu după prăbuşirea Uniunii Sovietice în ceea ce priveşte reprezentarea ameninţărilor, alocarea resurselor, echilibrarea intereselor diferiţilor actori sociali şi dimensiunile investiţiilor. Printre problemele principale, menţionăm atitudinea referitoare la folosirea forţei, bugetare, dezvoltarea economică sau valoarea identităţii ca stimul al practicii politice.

Relaţia dintre cercetare şi acţiune este deseori discutată în cercurile academic, dar natura sa rămâne încă ambiguă. Diversele abordări oscilează între o viziune obiectivistă, unde studiile reproduc realitatea mediului de securitate şi una mai activistă sau critică, potrivit căreia ideile sunt o parte a lumii sociale pe care o definesc în parte[2]. Această lucrare nu-şi va propune să răspundă unei întrebări atât de complicate, ci se va mulţumi cu o descriere a principalelor tendinţe din domeniul studiilor strategice şi de securitate, privite prin lupa alocării resurselor pentru apărare.

[1] Robert Kagan, *Dincolo de paradis şi putere*, Antet, Bucureşti, 2005; Felix Ciută, „Mythologies of European Security”, conference at NSPSA, Bucharest, Romania, iulie 2014.

[2] Ole Waever, ”Figures of International Thought: Introducing persons instead of paradigms”, în Iver B. Neumann, Ole Waever, *The Future of International Relations*, *Masters in the Making*, Routledge, 1997, pp. 2-30.

Dincolo de paradigme

În termeni kuhnieni, stiinţele sociale ar fi puternic influeţate de modificările paradigmatice, mai precis, cele referitoare la asumpţiile de bază şi hărţile mentale care fundamentează cercetarea: ce este important, cum definim realitatea, cum identificăm problemele, ce concepte luăm în calcul şi prin ce metode le studiem[3]. Conceptul ne permite să legăm trăsăturile sociale şi tendinţele intelectuale într-un mod dinamic, evitând slăbiciunile atât ale abordărilor materialiste, cât şi ale celor idealiste. Cu toate acestea, în cazul ştiinţelor reale, conceptul este vulnerabil din cauza relativismului său implicit, iar referitor la domeniile sociale, ideea de paradigmă este inaplicabilă în mod riguros, ca urmare a pluralismului acestora, o situaţie constatată de creatorul său[4].

Eşecul nu a fost provocat de absenţa tentativelor. Guzzini a susţinut că realismul a jucat rolul de paradigmă, acea structură mentală ce-şi propune definirea unui întreg domeniu academic, îndeosebi în Statele Unite[5]. După Sfârşitul Războiului Rece, îndeosebi în cadrul Uniunii Europene, s-a pus accentul pe crearea unei paradigme alternative, care aprecia aspectele civile ale securităţii mai curând decât pe cele militare[6]. Aceste tendinţe au dus la un pluralism teoretic, chiar dacă realitatea studiată părea identică. În domeniul respectiv de studiu, modificările constau într-o subordonare a tematicii tradiţionale referitoare la folosirea forţei, faţă de subiecte precum noile ameninţări, chestiunile identitare, dezbaterile referitoare la reducerea rolului statului şi a distribuţiei de putere ca factori explicativi şi tendinţă de a include studiile strategice într-un domeniu mai extins al studiilor de securitate[7].

Explicaţia prin paradigme a devenit problematică, ca instrument de înţelegere a continuităţilor şi schimbărilor din ştiinţele sociale în general şi din cadrul studiilor de securitate în particular. În afara scepticismului exprimat de Kuhn, acest termen subestimează aspectul normativ şi politizat caracteristic domeniilor respective. Nicio viziune comună nu poate dura prea mult, deoarece opiniile şi interesele sunt divergentele, iar metodologia folosită oferă rezultate ambigue.

O alternativă este oferită de termenul regim de adevăr, elaborat de Michel Foucault, unul dintre cei mai influenţi filosofi postmoderni, promovate de autori precum Bradley Klein]n domeniul studiilor de securitate[8]. În linii mari, conceptul neagă existenţa unei unităţi esenţiale în interiorul unui domeniu de studiu, fiind mai aproape de o viziune pluralistă şi potenţial conflictuală, ceea ce este destul de asemănător cu felul în care arată studiile sociale, cel puţin pe termen lung. Puterea şi cunoaşterea sunt legate, prin comportamente şi practici, care sunt corelate şi capată sens tocmai prin aceste modele intelectuale, inspirate şi creatoare

---

[3] Thomas Kuhn, *Structura revoluţiilor ştiinţifice*, Humanitas, 2008.

[4] *Ibidem*, p. 58. Martin Curd, J. A. Cover, *Philosophy of Science. The Central* Issues, W.W. Norton and Company, 1998, pp. 210-251.

[5] Stephano Guzzini, *Realism şi relaţii internaţionale*, Institutul European, Iaşi, 2000. O discuşie interesantă despre conceptul de securitate se regăseşte în Radu-Sebastian Ungureanu, „Extinderea conceptului de securitate" şi „Conceptuyl de securitate" în Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), *Manual de relatii internationale*, Polirom, Iasi, 2008.

[6] Felix Ciută, *op. cit.*

[7] Exemplară pentru acest demers este lucrarea lui Barry Buzan, Popoarele, statele şi teama, Cartier, Chişinău, 2000. Vezi şi Radu-Sebastian Ungureanu, "Extinderea conceptului de securitate", în Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2008, pp. 187-198, Radu-Sebastian Ungureanu, "Conceptul de securitate", în Miroiu şi Ungureanu, *op. cit.,* p. 186.

[8] Michel Foucault, *Naşterea biopoliticii*, Idea, Cluj, 2007, p. 28; Bradley Klein, *Strategic Studies and World Order*, Cambridge University Press, 1994, pp. 3-12: Alan Collins, *Contemporary security* studies, Oxford University Press, 2013, pp. 78-81. O abordare apropiată, ce a securitizării, induce o diferenţă exagerată între securitate şi putere. Vezi Buzan, Barry, Waever, Ole, *Securitatea. Un nou cadru de analiză*, CA Publishing, Cluj 2001.

de realitate socială[9]. Discuţia nu se referă la capacitatea de explicare, ci la motivele pentru care aceste formule capată credibilitate, chiar dacă sunt ambigue şi potenţial contradictorii[10].

Vom vedea că statutul ontologic al studiilor strategice şi de securitate poate fi pus sub semnul întrebării, depinzând de contextul local şi de perspectivele cercetătorilor. Chiar şi în lucrarea de faţă, sunt discutate mai curând despre autori din spaţiul anglo-saxon, care domină dezbaterile, deşi dezvoltările disciplinare sunt mult mai plurale. De exemplu, în România, există, pe lângă primele domenii, suprapuneri cu relaţiile internaţionale, ştiinţele politice, sociologia, istoria şi îndeosebi cu geopolitica, în ciuda vulnerabilităţilor logice ale celei din urmă abordări, la fel cum, în Occident, practici realiste se pot întâlni alături de justificări liberale[11].

Deseori, pare că ceea ce contează mai curând este cum aceste demersuri unesc comportamente şi definesc identităţi. Consecinţa este că diferenţa dintre tradiţionalişti şi reformatorii studiilor de securitate sau între practicile americane şi europene, nu se poate reduce la opoziţia dintre putere şi slăbiciune, cum credea Kagan[12]. Mai curând, este vorba despre modalităţi diferite de a gândi şi a folosi puterea, una inspirată de liberalism şi realismul, în care elementul militar este distinct şi alta, mai globalizantă, care proiectează asupra întregii societăţi un proiect de reformă, dar în mod mai descentralizat[13].

Consecinţa regimurilor de adevăr este că trebuie să ne aşeptăm la relaţii apropiate între practicile, politicile de putere şi cunoaştere, fie ea academică sau cutumiară. Cum pot da sens unor relaţii ambigue şi potenţial conflictuale, ştiinţele sociale vor fi, la rândul lor, marcate de controverse şi de tentative eşuate de unificare. În acelaşi timp, trebuie să fom atenţi la riscul exagerării relaţiilor dintre cele două aspecte, deoarece, în ultimă instanţă, distincţiile rămân.

Obiectivul principal al lucrării de faţă este de a identifica avantajele şi dezavantajele respectivei tranziţii, fiind trecute în revistă patru lucrări de referinţă, selecţia lor bazându-se pe impactul avut şi pe gradul de reprezentativitate[14]. Majoritatea sunt lucrări colective şi vizează suprinderea întregului domeniu al studiilor strategice şi de securitate. Temele recursului la forţă şi ideile conexe vor defini structura acestei analize.

De la puterea militară la identitate şi înapoi

În această comunicare sunt discutate patru texte, considerate ca repere ale tendinţelor discutate anterior. Procesele şi pluralismul în creştere pot fi suprinse, dezvoltându-se în manieră incrementală, în paralele cu tensiuni teoretice uneori deosebit de intense. Principalele probleme dezbătute se referă la recursul la forţă, rolul statului, puterea explicativă a puterii versus cea a identităţii, noi perspective despre securitate şi ascensiunea programelor de cercetare care au pus realismul şi raţionalismul sub semnul întrebării, între care se numără constructivismul şi teoria critică.

Alocarea resurselor este un aspect fundamental al politicii, motiv pentru care conceptul de regim de adevăr se potriveşte subiectului[15]. În general, este de aşteptat ca formulele favorabile puterii militare să promoveze investiţii în acest domeniu, cu anumite

[9] *Ibidem*, p. 13; Columbia Peoples, Nick Vaughan-Williams, *Critical Security Studies: An Introduction,* Routledge, 2015, pp. 79-83.

[10] Foucault, *op. cit.,*pp. 13, 29.

[11] Sergiu Tămaş, *Geopolitica. O abordare prospectivă*, Noua Alternativă, Bucureşti, 1995; Hans Morgenthau, *Politica între naţiuni. Lupta pentru putere şi lupta pentru pace*, Polirom, iaşi, 2007, pp. 195-196.

[12] Kagan, *op. cit.*; Ciută, *op. cit*.

[13] Foucault, *op. cit*, pp. 15-17; Rita Floyd, „When Foucault met security studies: A critique of the Paris school of security studies", 2006 BISA annual conference.

[14] Kuhn, *op. cit.*

[15] Gøsta Esping-Andersen, *The Three World of Welfare Capitalism*, PrincetonUniversity Press, 1990.

limite, legate de prudenţă. Cele critice ar tinde spre o diversificare a obiectivelor distribuţiei. Dar amândouă sunt interesate de putere, de utilizarea sa şi de felul în care o gândim. Deci, chiar şi atunci când nu este abordată direct, tematica alocării resurselor este implicită în discuţia despre capabilităţi şi rolul statului.

Într-un volum colectiv publicat în 1997, Craig Snyder a argumentat pentru „lărgirea sferei de cuprindere a securităţii dinspre aspectele pur militare ale studiilor strategice pentru a include problemele non-militare”[16]. În viziunea sa, sfârşitul Războiului Rece a condus la un declin al importanţei teoriei realiste, care privilegia forţa şi statele, ca subiecte fundamentale, pentru a extinde atât evantaiul teoretic, cât şi noi tipuri de conflict[17]. Tradiţional, studiile strategice erau preocupate de utilizarea în mod eficient a forţei armate, mai ales de politici ca descurajarea nucleară sau războaiele limitate şi erau profund influenţate de mediul academic şi oficial american[18]. În Marea Britanice, potrivit autoruluii s-a dezvoltat o disciplină înrudită, a studiilor de securitate, care includea şi demersurile critice şi care căuta inclusiv alternative la regulile de joc ale competiţiei bipolare[19].

Sfârşitul Războiului Rece ar fi determinat o reducere a importanţei forţei militare în relaţiile internaţionale şi a fost însoţit, în acest domeniu, de ascensiunea interpretărilor culturale, care puneau accent pe structurile de idei si de interese, în dauna capabilităţilor şi a factorilor materiali[20]. În consecinţă, sensul securităţii trebuie extins „ceea ce pentru unii inseamnă a include efectul politicii interne asupra stabilirii agendei de securitate naţionale a statelor, iar pentru alţii, semnifică abordarea atât a ameninţărilor non militare la adresa bunăstării publice drept probleme de securitate”[21]. Cu toate acestea, Snyder şi ceilalţi autori au menţinut rolul statului ca principală instituţie responsabilă de gestionarea acestei problematici şi şi-au propus numai să „redefinească dezbaterea despre subiecte tradiţionale ca descurajarea, proliferarea şi revoluţia în afaceri militare folosind noi conceptualizări”[22].

Cele două tendinţe paralele, de extindere conceptuală dincolo de forţa armată şi de definire a unui nou domeniu sunt reflectate în lucrarea lui Barry Buzan şi Lene Hansen, *The Evolution of International Security Studies* din 2008[23]. Buzan a fost unul dintre iniţiatorii celor doua procese mai sus enunţate şi a făcut parte din „Şcoala de la Copenhaga”, unul dintre centrele de cercetare care au influenţat transformările domeniului studiilor de securitate după sfârşitul Războiului Rece. Noul domeniu s-ar creiona, în opinia autorilor, în jurul a patru probleme: rolul statului, relaţia dintre ameninţările interne şi externe, extinderea sferei conceptului de securitate şi caracterul conflictual implicit al acestui termen[24]. Ambiţia lor este de a corela mai multe demersuri intelectuale şi aplicate, cu ajutorul respectivei noţiuni, printre care au inclus studiile strategice, polemologia, ştiinţele politice şi relaţiile internaţionale[25].

Buzan şi Hansen argumentează că studiile strategice s-au dezvoltat în perioada postbelică, ca urmare a bipolarităţii şi problematicii nucleare, implicând un număr de cercetători civili ca Bernard Brodie sau Thomas Schelling în discutarea chestiunilor legate de

---

[16] Craig Snyder, “Introduction”, în Craig Snyder (coord.), *Contemporary Security and Strategy*, MacMillan, Ebbw Vale, 1999, p. ix.

[17] Craig Snyder, “Contemporary Security and Strategy”, în Craig Snyder (coord.), *Contemporary Security and Strategy*, MacMillan, Ebbw Vale, 1999, pp. 2-3.

[18] *Ibidem*, p. 4

[19] *Ibidem*, p. 4

[20] *Ibidem*, p.7

[21] *Ibidem*, pp. 7-8.

[22] *Ibidem*, p. 2

[23] Barry Buzan şi Lene Hansen, *The Evolution of International Security Studies*, Cambridge University Press, f.l., 2009.

[24] Buzan şi Lene Hansen, *op. cit*., Pp. 10-13.

[25] *Ibidem*, p. 14-15.

forţa militară[26]. Principalul produs intelectual a fost teoria descurajării sau distrugerea reciproc asigurată, care asigura menţinerea unei anumite stabilităţi, în condiţiile în care cele două superputeri deţineau forţe invulnerabile de ripostă[27]. Ca atare, era influenţat puternic de probleme practice şi de contextul american al originii sale şi a înlocuit demersuri mai vechi precum geopolitica, deşi nu au lipsit criticile[28].

Asemănător lui Snyder, Buzan şi Hansen consideră că sfârşitul Războiului Rece a marcat în mod fundamental evoluţia studiilor strategice. Cu toate acestea, ei nu adoptă o perspectivă liniară, ci pun în evidenţă fracturile şi tensiunile interioare acestor seturi înrudite de activităţi de cercetare: „o nouă diviziune între tradiţionalişti … şi cei care doresc să extindă şi să adâncească sensul securităţii”[29]. Primii adoptă o metodologie pozitivistă/raţionalistă, menţin accentul pus pe rolul forţei armate în definirea relaţiilor internaţionale şi sunt preocupaţi de teme ca rivalităţile potenţiale dintre marile puteri sau Revoluţia în Afacerile Militare[30]. Reformiştii au promovat concepţii non-militare despre securitate, dezbateri despre interdependenţă şi importanţa identităţii în politica mondială[31]. Cum admit până şi autorii parţial, acest bicefalism academic contemporan era deja prezent în celebra lucrare a lui Keohane şi Nye, *Putere şi independenţă*, publicată în 1977[32]. Buzan şi Hansen subliniază că transformările domeniului studiilor strategice/de securitate nu sunt pur şi simplu de origine intelectuală, ci provin din îmbinarea mai multor factori: relaţiile dintre actorii majori, schimbările tehnologice, evenimentele, dezbaterile interne şi considerentele instituţionale[33]. În cele din urmă, ei sunt de părere că discuţiile despre extinderea termenului de securitate vor rămâne în memoria colectivă a disciplinei[34].

Manualul coordonat de Paul D. Williams, *Security Studies*, poate fi considerat ca marcând apogeul curentului promotor al reformulării tematice şi disciplinare prezentate până acum[35]. Tematica reuneşte probleme clasice (războiul, terorismul) cu subiecte evidenţiate de reformişti (securitatea umană, sărăcia, migraţia, criminalitatea transnaţională) şi problematici „neutre” (dilema securităţii, conflicte etnice, alianţe). Editorul a argumentat că securitatea reprezintă un concept supus controverselor politice, o poziţie tipică teoriilor critice şi nu numai[36]. Subliniind dependenţa de context a termenului, Williams a considerat că domeniul trebuie să se emancipeze de legătura cu disciplina mai largă a relaţiilor internaţionale şi să devină autonom, invocând ca argumente reducerea rolului statului, americano-centrismul intelectual şi interdisciplinaritatea[37].

Ca şi Snyder, Buzan şi Hansen el identifică două mari curente, unul care privilegiază puterea, îndeosebi pe cea militară ca răspuns al problemelor de securitate şi altul care accentuează emanciparea, deşi acest termen rămâne destul de utopic[38]. El problematizează referenţii, publicul şi instrumentele utilizate în asigurarea securităţii[39]. Extinderea securităţii a pornit de la noi abordări despre problemele clasice ale folosirii forţei, a trecut printr-un

[26] *Ibidem*, p. 66.
[27] *Ibidem*, pp. 73-83.
[28] *Ibidem*, p. 1, pp. 101-104.
[29] *Ibidem*, p. 156.
[30] *Ibidem*, pp. 156-157, 165-170, 170-176.
[31] *Ibidem*, pp. 187-191.
[32] Robert O. Keohane, Joseph Nye jr., *Putere şi interdependenţă*, Polirom, Iaşi, 2009.
[33] Buzan şi Lene Hansen, *op. cit*., pp. 41-65.
[34] *Ibidem*, p. 272.
[35] Paul D. Williams, *Security Studies: An Introduction*, Routledge, f.l., 2008.
[36] Paul D. Williams, ”Security Studies”, în *Security Studies: An Introduction*, Routledge, f.l., 2008, p. 1.
[37] *Ibidem*, pp. 4-5.
[38] *Ibidem*, p. 6.
[39] *Ibidem*, pp. 6-10.

moment de extindere, atât a sensului, cât şi a obiectelor şi sectoarelor implicate, ajungând, în punctul culminant, să desemneze aproape tot spaţiul politicului, ceea ce poate fi o exagerare. Studiile referitoare la strategie şi la utilizarea forţei militare au trecut pe un plan relativ secundar, Rolul statului în definirea relaţiilor internaţionale a fost pus sub semnul întrebării, identitatea a luat locul puterii ca factor explicativ fundamental şi o pluralitate de actori a atras atenţia cercetătorilor.

Nu toţi specialiştii în domeniu s-au convins de argumentele reformatorii, considerând că extinderea sensului securităţii a fost fie exagerată, fie a reprezentat o modă tipică euforiei păcii. Tipic pentru abordarea tradiţionalistă este volumul *Strategy in the Contemporary World*, coordonat de John Baylis, James Wirtz, Colin S. Gray şi Eliot Cohen, un alt manual[40]. Pentru autori, „interesul exercitat de studiile strategice este ciclic şi reflectă evenimentele contemporane"[41]. Ascensiunea reformiştilor a fost, în consecinţă, un rezultat al speranţelor trezite de sfârşitul Războiului Rece şi nu neapărat un progres teoretic de durată[42].

Dimpotrivă, Baylis şi Wirtz au pus în centrul studierii securităţii noţiunea clasică de strategie, care uneşte mijloacele militare cu scopurile politice şi impactul socialului şi culturalului şi au subliniat apropierea dintre această concepţie şi teoriile realiste, pesimiste referitoare la progres, adepte ale unor politici de putere raţionale[43]. De asemenea, este important de subliniat că au respins criticile reformiştilor referitoare la apropierea de politic, deformare conservatoare a relaţiilor internaţionale şi etatism[44]. Prin urmare, Baylis şi Wirtz au limitat solicitările de integrare a studiilor strategice într-o disciplină securitară mai amplă, evidenţiind rolul forţei şi riscurile ambiguităţii conceptuale determinate de o extindere prea largă a conceptului[45]. În cele din urmă, ei adoptă soluţia opusă celei promovate de Snyder, probleme noi, dar explicaţii clasice[46].

În consecinţă, se pot observa divergenţe crescânde între perspective diferite referitoare la sensul securităţii. Raţionalismul şi recursul la forţa armată sunt mai accentuate de cealaltă parte a Atlanticului, iar identitatea şi aspectele civile tind să se bucure de influenţă în Europa. Tendinţele intelectuale merg în paralele cu deosebiri referitoare la definirea ameninţărilor, a strategiiilor şi a procedurilor de decizie.

Concluzii

Scopul acestei lucrări a fost de a trece în revistă literatura din domeniul studiilor strategice şi de securitate, subliniind pluralismul în creştere al acestuia. Contrar conceptului de paradigmă, considerăm că nicio viziune dominantă asupra lumii nu a apărut la Sfârşitul Războiului Rece. Deci, utilitatea acestui termen în disciplinele sociale sau conexe trebuie pusă sub semnul întrebării, pe lângă alte critici provenite din interiorul filosofiei ştiinţelor.

Conexiunea dintre cunoaştere şi putere devinde mai clară acum, pe fundalul acestei diversităţi. Cum nu a apărut un model dominant, rezultatul este asemănător unui haos conceptual. Uneori aceste discipline par identice, alteori diferite; uneori pot fi privite ca autonome, alteori par integrate; câteodată, se orientează spre forţa militară, câteodată adoptă o viziune mai extinsă...

---

[40] John Baylis, James Wirtz, Colin S. Gray, Eliot Cohen (coord.), *Strategy in the Contemporary World*, Oxford University Press,Bath, 2007.

[41] John Baylis, James Wirtz, "Introduction", în John Baylis, James Wirtz, Colin S. Gray, Eliot Cohen (coord.), *Strategy in the Contemporary World*, Oxford University Press,Bath, 2007, p. 2.

[42] *Ibidem*, p. 3.

[43] *Ibidem*, p. 4-9.

[44] *Ibidem*, pp 11-12.

[45] *Ibidem*, p. 13.

[46] *Ibidem*, p. 4.

Snyder şi colaboratorii săi au făcut un pas major spre tratatrea unor probleme vechi cu mijloace noi, inclusiv în ceea ce priveşte capacitatea de explicare a unor concepte precum distribuţia capabilităţilor. Aceste idei erau legate de valul în creştere de critici de care s-a lovit realismul, îndeosebi versiunea structuralistă. Totuşi, interacţiunea complexă dintre teorie şi fapte a împins mai aproape abordările studiilor strategice şi de securitate.

Buzan şi Hansen au oferit o perspectivă echilibrată asupra tendinţei de extindere a proceselor securitare, subliniind divergenţa în două tendinţe. Pe de-o parte, reformatorii au încercat să ofere o nouă perspectivă, definită prin creionarea mai multor sectoare şi actori, o concepţie civilă şi un accent special pus pe identitate. Pe de altă parte, tradiţionaliştii erau interesaţi de probleme de cercetare precum Revoluţia în Afacerile Militare.

Volumul coordonat de Paul Williams a marcat apogeul viziunii reformatorilor despre problemele de securitate. Numărul ameninţărilor este în creştere, în timp ce natura politică a acestora a fost abordată dintr-o perspectivă critică. Extinderea sensului şi a conţinutului risca să includă orice în termenul de securitate, cu potenţialul de confuzie şi de consum excesiv al resurselor.

În cele din urmă, Baylis şi colaboratorii au încercat să adapteze perspectivele clasice, îndeosebi realismul clasic, evoluţiilor mediului de securitate din perioada ulterioară Războiului Rece. Specificul studiilor strategice a fost căutat, îndeosebi, în multiplele utilizări pe care forţa militară le poate avea, de la descurajare la contraproliferare. Abordarea ce promova extinderea sensului securităţii era cel puţin extinsă.

Mulţumiri:

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului POSDRU/159/1.5/S/138822, cu titlul „Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile "Ştiinţe Militare", "Securitate şi Informaţii" şi "Ordine Publică şi Siguranţă Naţională" - Program de Formare Continuă a Cercetătorilor de Elită –" SmartSPODAS"."

BIBLIOGRAFIE:

1. Baylis, John, Wirtz, James, "Introduction", în Baylis, John, Wirtz, James, Gray, Colin S., Cohen, Eliot (coord.), Strategy in the Contemporary World, Oxford University Press,Bath, 2007.
2. Baylis, John, Wirtz, James, Gray, Colin S., Cohen, Eliot (coord.), Strategy in the Contemporary World, Oxford University Press,Bath, 2007.
3. Buzan, Barry, Popoarele, statele şi teama, Cartier, Chişinău, 2000.
4. Buzan, Barry, Hansen, Lene, The Evolution of International Security Studies, Cambridge University Press, f.l., 2009.
5. Ciută, Felix, "Mythologies of European Security", prezentare în cadrul SNSPA, 10 iulie 2014.
6. Collins, Alan, *Contemporary security studies*, Oxford University Press, 2013
7. Curd, Martin, Cover, J. A., Philosophy of Science. The Central Issues, W.W. Norton and Company, 1998.
8. Esping-Andersen, Gøsta, *The Three World of Welfare Capitalism*, PrincetonUniversity Press, 1990.

9. Floyd, Rita, „When Foucault met security studies: A critique of the Paris school of security studies", 2006 BISA annual conference.
10. Foucault, Michel, Naşterea biopoliticii, Idea, Cluj, 2007
11. Keohane, Robert O., Nye jr., Joseph, Putere şi interdependenţă, Polirom, Iaşi, 2009.
12. Klein, Bradley, *Strategic Studies and World Order*, Cambridge University Press, 1994.
13. Kuhn, Thomas, Structura revoluţiilor ştiinţifice, Humanitas, 2008.
14. Kagan, Robert, Dincolo de paradis şi putere, Antet, Bucureşti, 2005;
15. Miroiu, Andrei, Ungureanu, Radu-Sebastian, (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2006.
16. Morgenthau, Hans, Politica între naţiuni. Lupta pentru putere şi lupta pentru pace, Polirom, Iaşi, 2007
17. Peoples, Columbia, Vaughan-Williams, Nick, *Critical Security Studies: An Introduction,* Routledge, 2015.
18. Snyder, Craig, "Contemporary Security and Strategy", în Snyder, Craig, (coord.), Contemporary Security and Strategy, MacMillan, Ebbw Vale, 1999.
19. Snyder, Craig, "Introduction", în Snyder, Craig, (coord.), Contemporary Security and Strategy, MacMillan, Ebbw Vale, 1999.
20. Snyder, Craig, (coord.), Contemporary Security and Strategy, MacMillan, Ebbw Vale, 1999.
21. Tămaş, Sergiu, Geopolitica. O abordare prospectivă, Noua Alternativă, Bucureşti, 1995
22. Ungureanu, Radu-Sebastian, "Extinderea conceptului de securitate", în Miroiu, Andrei, Ungureanu, Radu-Sebastian, (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2008
23. Ungureanu, Radu-Sebastian, "Conceptul de securitate", în Miroiu, Andrei, Ungureanu, Radu-Sebastian, (coord.), Manual de relaţii internaţionale, Polirom, Iaşi, 2008.
24. Waever, Ole, "Figures of International Thought: Introducing persons instead of paradigms", în Neumann, Iver B., Waever, Ole, The Future of International Relations, Masters in the Making, Routledge, 1997
25. Williams, Paul D.,, "Security Studies", în Paul D. Williams, Security Studies: An Introduction, Routledge, f.l., 2008.
26. Williams, Paul D.,, Security Studies: An Introduction, Routledge, f.l., 2008.

COMPLEXITATEA ÎN MEDIUL DE SECURITATE

Florina Daniela GHEORGHE
Doctorand în „Informaţii şi Securitate Naţională", Academia Naţională de Informaţii „Mihai Viteazul", Bucureşti, România, ghe_florina@yahoo.com

Rezumat: *Mediul internaţional de securitate a cunoscut noi transformări, devenind extrem de volatil prin prisma amplificării rolului actorilor internaţionali nonstatali şi a manifestărilor de segregare, astfel încât vechile paradigme de explicare a cadrului internaţional au fost tot mai contestate sau insuficiente. Pe acest fond, în ultimii ani, teoreticieni ai Relaţiilor Internaţionale au avansat ideea de „haos" şi „noul anarhism din sistem", mediul de securitate fiind cunoscut sub abrevierea „VUCA" (volatil, incert, complex, ambiguu). Lucrarea de faţă îşi propune o nouă abordare oferită de teoria complexităţii: aceea de a evidenţia noi concepte pentru analiza sistemului internaţional, prin utilizarea unor modele de măsurare a comportamentului dinamic nonlinear al ordinii sistemelor complexe.*

Cuvinte cheie*:* mediu de securitate, haos, complexitate, comportament dinamic nonlinear.

Introducere

Trăim într-un secol marcat de incertitudine, evoluţii şi transformări rapide, manifestate atât la nivel de individ, cât mai ales la nivel societal/ organizaţional. Astfel, mediul de securitate nu face rabat de la aceste considerente. Amplificarea rolului actorilor non-statali, manifestările de segregare, precum şi ascensiunea fanatismului religios ne fac să asistăm, din ce în ce mai mult, la divizarea lumii. Aşa cum sublinia Robert Cooper[1], „astăzi avem, mai întâi, o lume premodernă caracterizată de prestatalitate şi haosul postimperial".

Devine tot mai evident că nu ne mai putem raporta la mediul de securitate prin prisma vechilor paradigme. Atentatele teroriste de la 11 septembrie, anexarea Crimeii de către Federaţia Rusă şi apariţia Statului Islamic (ca să oferim doar câteva exemple) nu mai au nimic în comun cu principiile echilibrului/ balanţei de putere care au guvernat Relaţiile Internaţionale până nu demult.

Mediul internaţional este un *sistem adaptiv complex*, în care mici schimbări ale condiţiilor iniţiale şi intervenţiile ulterioare de orice dimensiune, pot duce la efecte disproporţionat de mari, sau, aşa cum le numeşte Nassim Nicholas Taleb. „lebede negre", acestea având trei atribute majore: raritate, impact extrem şi predictibilitate retrospectivă[2].

Un sistem adaptiv complex apare în natură atunci când mediul este instabil, dar nu complet haotic. Mediile stabile conduc la sisteme în echilibru, care cel mai probabil nu se vor adapta la schimbări majore. În mediile haotice, sistemele nu pot găsi şabloane (pattern-uri) productive. La marginea haosului – o bună analogie cu transformările sociale curente – pot apare schimbări inovatoare şi dramatice în activitatea pattern-urilor, iar sistemele pot trece la

[1]Robert COOPER, *Destrămarea naţiunilor. Ordine şi haos în secolul 21*, Bucureşti: Editura Univers Enciclopedic, 2007, p. 42.
[2]Nassim Nicholas TALEB, *Lebăda neagră. Impactul foarte puţin probabilului*. Bucureşti: Editura Curtea Veche, 2010, p. 16.

nivele mai înalte de performanţă. Astfel de inovaţii, totuşi, depind de fluxurile de informaţie prin reţele interconectate[3].

1. Consideraţii despre securitate

De-a lungul timpului, teoreticieni ai Relaţiilor Internaţionale au formulat o multitudine de definiţii ale *conceptului de securitate*, neputând fi găsit un consens în privinţa acestui subiect.

În antichitate, termenul de „securitate" era înţeles în sensul de „libertate în faţa ameninţării". Această formulare este prezentă şi în definiţia oferită de Arnold Wolfers[4], potrivit căreia „securitatea, în sens obiectiv, măsoară absenţa ameninţărilor la adresa valorilor dobândite, iar într-un sens subiectiv, absenţa temerii că asemenea valori vor fi atacate". În acest concept pare să îşi găsească locul şi piramida lui Abraham Maslow, care situează securitatea pe cel de-al doilea nivel, după nevoile primare.

După cum am observat, Arnold Wolfers a conturat existenţa unor componente obiective şi subiective ale intereselor naţionale, precum şi ale ameninţărilor la care acestea sunt supuse. Astfel, politicile pe care le vor adopta statele în vederea asigurării securităţii vor fi definite în funcţie de interesele naţionale identificate şi a ameninţărilor la adresa acestora.

Pe de altă parte, curentul realist statuează că obiectivul fundamental al oricărui stat este propria sa supravieţuire. Conform teoriei lui Kenneth Waltz[5], „în anarhie, supravieţuirea este scopul cel mai înalt. Statele pot căuta să-şi îndeplinească alte obiective precum liniştea, beneficiul sau puterea doar dacă supravieţuirea este asigurată".

Securitatea unui stat se referă, generic, la lipsa ameninţărilor la adresa independenţei şi integrităţii teritoriale, precum şi la capacitatea sa de a le apăra.

În centrul dezbaterii privind securitatea se află statul, datorită caracterului său de suveran, însă trebuie să ţinem cont de faptul că traversăm un secol în care statul nu mai poate fi analizat ca subiect de sine stătător, ci prin prisma relaţiilor şi interdependenţelor cu alţi actori ai sistemului. Istoria a dovedit, nu o dată, că un stat nu-şi poate asigura în mod absolut securitatea acţionând de unul singur.

Barry Buzana introdus în literatura de specialitate termenul de c*omplex de securitate regională,* acesta reprezentând „un grup de state ale căror preocupări majore de securitate sunt interconectate în aşa măsură încât problemele lor naţionale de securitate nu pot fi tratate eficient în mod separat"[6]. Spre deosebire de subsistemul regional şi de sistemul subordonat, care sunt modalităţi de a trata împreună pe baza unui singur criteriu anumite state apropiate geografic, complexul de securitate aduce în prim-plan chestiunea existenţei unei interdependenţe semnificative între participanţi. În acelaşi context, este dezvoltată ideea că aceste interdependenţe nu sunt exclusiv militare, diplomatice sau politice, ele putându-se manifesta şi la nivel social, precum şi în domeniul economic sau în chestiuni de securitate a mediului[7].

---

[3]Judith E, INNER, David E. BOOHER, *Consensus Building and Complex Adaptive Systems: A framework for Evaluating Collaborative Planning*, Journal of the American Planning Association, toamna 1999, Vol. 65, No.4, p. 412.

[4]Arnold WOLFERS, *„National Security" as an Ambitious Symbol*, Political Science Quarterly, 1952, 67 <4>, p. 485

[5] Kenneth WALTZ, *Theory of International Politics*, McGraw-Hill, Boston, 1979

[6]Barry BUZAN, *Popoarele, statele şi teama: O agendă pentru studii de securitateInternaţională în epoca de după Războiul Rece,* Chişinău: Cartier, Cap.I, II, III, IV, 2000, p. 106

[7] BUZAN, *Popoarele, statele şi teama,* p. 106.

2. De la constructivism la complexitate

Constructivismul reprezintă unul dintre cele mai inovatoare curente de gândire în Relaţiile Internaţionale, numele cel mai frecvent asociat cu această teorie fiind cel al lui Alexander Wendt. Pentru constructivism, lumea interacţiunilor dintre actorii internaţionali este eminamente un spaţiu social. Sistemul internaţional este o creaţie socială în ansamblul său, la fel cum componentele sale definitorii – mai exact, procesele, actorii şi structurile internaţionale – sunt produse sociale. Una din premisele esenţiale ale constructivismului este că factorii materiali prezenţi în relaţiile internaţionale (teritorii, distanţe, capacităţi militare, resurse naturale) nu semnifică nimic în absenţa unor *procese sociale complexe* prin care li se atribuie un anumit sens[8].

Teoria complexităţii este predominant prezentă în ştiinţele sociale şi în informatică, Mark McElroy[9] apreciind că aceasta „este o soluţie de încredere în căutarea problemelor neortodoxe, furnizând o explicaţie pentru sensurile în care sistemele vii se angajează în învăţarea adaptivă". Pe de altă parte, Ortegon-Monroy[10]şi Smith şi Humphries[11] au concluzionat că Teoria complexităţii este dificil de tradus în practică.

Massimo Pigliucci[12] precizează că o figură cheie în dezvoltarea ştiinţei moderne a fost filosoful francez Rene Descartes, care a statuat că *ideea sistemelor complexe* poate fi înţeleasă analizând fiecare parte[13] pe rând, punând apoi toate piesele la un loc pentru a obţine o imagine comprehensivă (teoria reducţionismului). Pigliucci pune sub semnul întrebării această abordare, subliniind că există posibilitatea ca separarea componentelor să altereze proprietăţile atât de mult încât ceea ce am învăţat din studierea pieselor separate să ne inducă o idee diferită şi greşită asupra sistemului ca întreg: „Poate ştiinţa reducţionistă studia proprietăţile emergente care, prin definiţie, sunt rezultatul *interacţiunilor complexe*?" Acesta oferă drept exemplu interacţiunea dintre hidrogen şi oxigen care rezultă în apă. Pigliucci precizează că, ştiind absolut tot despre structura şi comportamentul atomilor care compun apa, ne permite prezicerea structurii nu şi a comportamentului apei. *Complexitatea produce noi proprietăţi specifice noului nivel al organizaţiei, care nu sunt rezultatul sumei părţilor, ci al interacţiunilor lor*.

De asemenea, acesta face legătura între cele două teorii, menţionând că Teoria complexităţii este derivată din Teoria haosului, de aici sintagma „haoplexitate" („chaoplexity", în engleză). Haosul se referă la un fenomen deterministic (nu întâmplător/ aleatoriu) caracterizat de proprietăţi speciale care fac ca predictibilitatea apariţiei lui să fie dificilă. Un comportament haotic este acela care deşi nu se produce aleatoriu, apare ca o serie de apariţii întâmplătoare. Dinamicile haotice sunt de obicei, dar nu întotdeauna, apanajul sistemelor nonlineare. Nu toate sistemele nonlineare generează comportamente haotice! Pornind de la „efectul fluture" al lui Edward Lorenz, Pigliucci precizează că termenul tehnic pentru acest fenomen este „sensibilitatea la condiţiile iniţiale" („SCI"), aceasta însemnând că o mică perturbaţie a sistemului poate cauza o serie de efecte care conduc, până la urmă, la consecinţe macroscopice.

---

[8]Alexander WENDT, *Contructing International Politics*, International Security, 20 (1), vara 1995

[9]Mark W. McELROY,*Integrating Complexity Theory, Knowledge Management and Organizational Learning*, Journal of Knowledge Management, Vol. 4 No. 3, 2000, pp. 195-203.

[10]Maria Carolina ORTEGON-MONROY,*Chaos and Complexity Theory in Management: An Exploration from a Critical Systems Thinking Perspective*, Systems Research and Behavioral Science,Vol. 20 No. 5, 2003, pp. 387-400.

[11]Aaron SMITH, Clare HUMPHRIES, *Complexity Theory as a Practical Management Tool: ACritical Evaluation*, Organization Management Journal, Vol. 1 No. 2, 2004, pp. 91-106.

[12]Massimo PIGLIUCCI,*Chaos & Complexity. Should We Be Skeptical?*, Skeptic Magazine, Altadena, California/ SUA, Vol. 8 No. 3, 2000, pp.62-70

[13]Pentru o viziune de ansamblu mai clară asupra demersului, citiţi pe mai departe cuvântul în sensul de „stat"

Piglicci mai subliniază că ne putem gândi la Teoria complexităţii ca la o încercare de a studia sistemele care îndeplinesc două condiţii: 1) sunt formate din multe părţi care interacţionează şi 2) interacţiunile rezultă în proprietăţi emergente care nu sunt imediat reductibile la o simplă sumă a proprietăţilor componentelor individuale.

Teoria complexităţii utilizează modele dinamice nonlineare pentru a măsura comportamentul sau ordinea sistemelor complexe.

Phil Anderson[14] apreciază că noile proprietăţi ajung să domine comportamentul unui sistem pe măsură ce creştem gradul de libertate sau introducem un parametru pentru a sparge simetria. Părţile componente ale unui sistem interacţionează. Creşterea numărului de interacţiuni sau accentuarea anumitor interacţiuni în detrimentul altora (de rupere a simetriei), declanşează bucle de feedback printre componente care conduc la un comportament colectiv. Componentele care sunt blocate într-un astfel de comportament pot fi tratate împreună ca o nouă unitate. În timp ce compoziţia unui sistem a rămas aceeaşi, frontierele sale interne – care sugerează cum se analizează un sistem în „piese" - au fost redesenate din interior. Sistemele complexe sunt de obicei organizaţii formate din multe părţi eterogene care interacţionează la nivel local, în absenţa unui filtru de ritm centralizat şi control.[15]

În sistemele nonlineare mici schimbări în elemente cauzale de-a lungul timpului nu produc în mod necesar mici modificări în alte aspecte particulare ale sistemului sau în caracteristicile sistemului ca întreg. Ambele pot modifica foarte mult, într-adevăr, şi, în plus, ele se pot schimba în moduri care nu implică doar un posibil rezultat.

Pavard şi Dugdale[16] au sintetizat următoarele proprietăţi ale complexităţii:

a) non-determinism şi nontractabilitate. Este imposibil de anticipat cu precizie comportamentul sistemelor complexe, chiar dacă cunoaştem cum funcţionează părţile sale. Comportamentul acestor sisteme nu este aleatoriu în sensul de haotic; ele operează prin efecte de feedback şi este improbabil să fie detectate prin măsurători standard sau prin asocierea dintre determinanţii asumaţi şi efectele presupuse.
b) descompunere funcţională limitată. Un sistem complex este o structură dinamică. Prin urmare, este dificil, dacă nu imposibil, să studiem proprietăţile sale prin descompunerea în părţi funcţionale stabile. Interacţiunea sa permanentă cu mediul şi proprietăţile sale de auto-organizare îi permit să se auto-restructureze.
c) natura distributivă a informaţiilor şi reprezentare. Un sistem complex posedă proprietăţi comparabile cu sistemele distributive (în sensul conexionist); ceea ce înseamnă că anumite funcţionalităţi nu pot fi localizate cu precizie. În plus, relaţiile care există între elementele unui sistem complex pot fi cu rază scurtă şi pot conţine bucle de feedback (atât pozitive cât şi negative).
d) emergenţă şi auto-organizare. Un sistem complex cuprinde proprietăţi emergente care nu sunt direct accesibile (identificabile sau anticipative) prin înţelegerea componentelor sale.

Astfel, în timp ce complexitatea ca o zonă de studiu distinctivă eludează definirea riguroasă, ceea ce putem spune la un nivel general, este că sistemele complexe sunt acele sisteme „al căror comportament global tinde către/ conduce la modele structurale şi dinamice

[14]Philip.W. ANDERSON, *More is Different*. Science, 177:393:396, 1972

[15]Walter FONTANA, Susan BALLATI, *Complexity; Introduction to Issues in and about „Complexity"*, în cadrul seminarului „Philanthropy and Social Change", Robert Wood Johnson Foundation, Princeton, New Jersey, 15 octombrie 1998

[16]Bernard PAVARD, Julie DUGDALE, *The Contribution of Complexity Theory to the Study of Sociotechnical Cooperative Systems*, disponibil la http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.70&rep=rep1&type=pdf, accesat la 15.03.2015

multi-scară”[17]. O proprietate importantă a sistemelor complexe este modul în care prezintă un comportament de auto-organizare, condus de interacţiuni coevoluţionare.

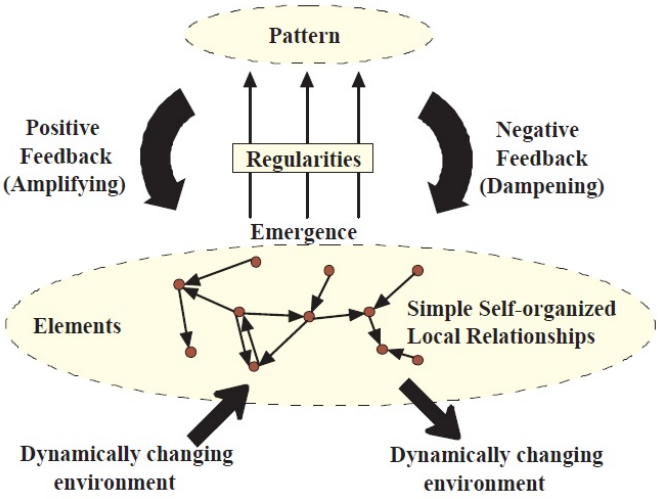


Figura nr. 1. Sistem adaptiv complex [Antoniou, Pitsillides 2007]

3. Complexitatea şi mediul de securitate

Neil E. Harrison, care a analizat relaţiile internaţionale prin prisma Teoriei complexităţii, a observat tendinţa actualelor teorii de a se baza pe modele sociale (realismul, spre exemplu, care consideră comportamentul politic ca fiind condus de caracteristici umane esenţiale din cadrul structurilor fixe). Teoria complexităţii vede politica mondială ca un sistem complex de auto-organizare în care macroproprietăţile se dezvoltă din microinteracţiuni. Harrison clasifică statul ca un sistem deschis către alte sisteme naturale şi sociale, întrucât are acces la sisteme tehnologice, culturale şi economice care influenţează alegerile politice. Statul este, de asemenea, influenţat de alte state şi de numeroase interacţiuni transfrontaliere dintre marile corporaţii, ONG-uri, grupuri teroriste, etc. În astfel de sisteme complexe este aproape imposibil de urmărit legăturile cauzale liniare[18].

În diferite contexte, aceeaşi cauză poate duce la rezultate diferite, iar acest lucru nu poate fi previzionat de modelele simpliste ale sistemelor internaţionale. Dat fiind faptul că interacţiunile se influenţează reciproc în cadrul sistemelor sociale, este necesar să ne uităm, mai degrabă, la evoluţia sistemului, decât la evenimente individuale atunci când cautăm cauzele efectelor observate. Teoria complexităţii se concentrează întocmai asupra proceselor şi relaţiilor dintre componente, şi nu pe componentele sistemului în sine.

Harrison a apreciat că aplicarea Teoriei complexităţii poate reprezenta un câştig pentru politica mondială: „această schimbare ontologică de la simplu la sisteme complexe deschide noi căi de cunoaştere şi înţelegere; validează metode de cercetare noi; iar teoriile nou fondate în această abordare vor genera soluţii radical diferite pentru probleme de politică”[19].

Complexitatea este prezentă şi atunci, sau mai bine spus, cu atât mai mult atunci, când ne referim la conflicte. Peter Coleman a observat un „paradox” în ceea ce le priveşte, conflictele fiind, „în esenţă, stabile în ciuda volatilităţii extraordinare şi a schimbării”.

---

[17]Lael PARROTT, Robert KOK,*Incorporating Complexity in Ecosystem Modelling*, Complexity International, vol. 7, 2000, p. 2

[18]Neil E. HARRISON, *Complex Systems and the Practice of World Politics*, în Neil E. HARRISON (ed.), *Complexity in World Politics, Concepts and Methods of a New Paradigm*, State University of New York, 2006, p. 8

[19]HARRISON, *Complex Systems and the Practice of World Politics*, p. 2

„Dacă avem în vedere conflictul din Orientul Mijlociu, de exemplu, ne pare, de cele mai multe ori, intransigent; cu un trecut, prezent şi viitor învăluite în ură, violenţă şi disperare. Cu toate acestea, de-a lungul anilor am văzut, de asemenea, schimbări majore în aspecte importante ale conflictului, cum ar fi în conducere, politică, circumstanţele regionale, intensificarea şi de-escaladarea violenţei, diviziuni în interiorul grupului, sentiment popular şi strategii internaţionale de intervenţie. Cu alte cuvinte, am văzut schimbări extraordinare care au loc într-un context al unui model de relaţii distructive stabile. Acest paradox de stabilitate în mijlocul schimbării este evident în conflicte greu de rezolvat la toate nivelurile, de la fraţi înstrăinaţi şi vecini la facţiuni etnopolitice. Ele sunt îngheţate, neînduplecate - şi de multe ori persistă în state ostile de generaţii -, dar sunt, de asemenea, unele dintre procesele sociale cele mai volatile şi dinamice de pe pământ"[20].

Centrul Internaţional pentru Conflicte şi Complexitate din cadrul Universităţii din Varşovia introduce Teoria complexităţii în cercetarea conflictelor, punând un accent puternic pe aspectele socio-psihologice ale acestuia. Cercetătorii Centrului caracterizează conflictele greu de rezolvat drept sisteme complexe, nonliniare - menţinute într-o stare de distrugere printr-o varietate de procese emergente, integrate şi automate. În opinia acestora, „vizualizarea conflictului într-un singur punct în timp, sau concentrându-se pe un singur aspect, a fost în cele din urmă problematic pentru că nu a reuşit să surprindă faptul că acesta, în special conflictul greu de rezolvat, este cu multiple faţete; care implică mai multe experienţe şi întâlniri între mai multe părţi diferite, pe o varietate de probleme în condiţii diferite la diferite puncte în timp."[21]

De asemenea, în opinia lui Harrison, mediul afectează comportamentul sistemului în două moduri. În primul rând, constrânge ceea ce este posibil şi selectează comportamentele care sunt cele mai adecvate în aranjamentele instituţionale actuale. În al doilea rând, percepţia mediului influenţează modelele interne ale agenţilor[22].

Cu oimensă experienţă în intelligence, dr. Gregory F. Treverton a abordat complexitatea dintr-un nou şi interesant unghi. În cadrul unui articol integrat în proiectul pentru intelligence şi securitate naţională elaborat de Centrul RAND pentru Studiul Ameninţărilor Asimetrice, destinat Agenţiei suedeze pentru Managementul de Urgenţă[23], Treverton caracterizează „complexităţile" drept o nouă categorie de probleme în intelligence, acestea fiind prezente, în mod particular, în evaluarea grupărilor teroriste, protejând astfel siguranţa naţională.

Ceea ce este cu atât mai interesant, este comparaţia făcută de acesta între „mistere" şi „complexităţi", diferenţa majoră fiind că primele au o oarecare formă; ştim ce variabile contează mai mult în producerea unui rezultat şi putem avea şi o oarecare evidenţă istorică în privinţa felului în care ele interacţionează. Prin comparaţie, în complexitate, un număr mare de actori relativ mici reacţionează la un set schimbător, dinamic, de factori situaţionali, astfel încât ei nu se repetă, în mod neapărat, în vreun tipar cunoscut/ stabilit şi nu pot fi maleabili într-o analiză predictivă. Aceste caracteristici descriu multe ţinte transnaţionale, precum teroriştii – mici grupuri care se formează şi se reformează, căutând vulnerabilităţi, adaptându-se constant şi interacţionând în moduri care pot fi noi.

---

[20]Peter T. COLEMAN, Robin VALLACHER, Martin NOVAK, Lan BUI-WRZOSINSKA, *Intractable Conflict as an Attractor: Presenting a Dynamical Model of Conflict, Escalation and Intractability*, American Behavioral Scientist, 2007, vol. 50, p. 2

[21]Diane HENDRICK, *Complexity Theory and Conflict Transformation: An Exploration of Potential and Implications*, Working Paper 17, University of Bradford, Centre for Conflict Resolution, Department of Peace Studies, june 2009, p. 26

[22]HARRISON, *Complex Systems and the Practice of World Politics*, p. 35

[23]Gregory F. TREVERTON, *Adressing „Complexities" in Homeland Security*, The Swedish National Defense College, 2009

În cazul complexităţii, incertitudinea este foarte ridicată şi greu de redus, întrucât nu ştim exact ce factori vor fi mai importanţi, nici felul în care aceştia interacţionează. Evenimentul din 11 septembrie a transformat vechea credinţă că „ei (în sensul actorilor care ameninţă siguranţa naţională) n-ar putea sau n-ar vrea" în „*orice* se poate întâmpla". Astfel, Treverton subliniază necestatea de a importa noi concepte şi de a lua în calcul noi modele şi teorii pentru a rezolva provocarea terorismului privit prin prisma complexităţii.

Trecând în revistă o serie de caracteristici ale terorismului, Treverton descrie de fapt, în mare parte, complexitatea:

- Terorismul este predominant un fenomen al unui grup psihologic, unde un sistem social de simpatizanţi şi suporteri exercită multiple influenţe la nivel de comportament individual;
- Nu există o singură cauză de bază a terorismului, ci mai degrabă mai multe căi către acesta;
- Grupările teroriste şi sistemele lor sociale de susţinere sunt încorporate în structuri instituţionale şi politice evolutive şi în sisteme complexe de credinţă religioasă;
- Acţiunile teroriste au câţiva (poate chiar mulţi) spectatori şi evoluează ca răspuns în funcţie de aceştia;
- Teroriştii inovează şi îşi adaptează răspunsul la schimbări, atât în ceea ce priveşte măsurile contrateroriste, cât şi evenimentele independente;
- Grupările teroriste auto-organizate se creează, în principal, prin intermediul reţelelor sociale, astfel încât structura lor este o funcţie lărgită a acestor legături sociale;
- Reţelele teroriste descentralizate facilitează rezilienţa în operaţiuni, difuzia ideologiei şi inovării şi distribuţia resurselor şi a informaţiei.

Concluzii

Deşi nu s-a conturat încă o şcoală de gândire în materie de complexitate în ştiinţele de securitate/ relaţii internaţionale, o serie de concepte încep să fie elaborate, mai ales în ceea ce priveşte o nouă abordare în analiza de intelligence.

Complexitatea este, încă, destul de contestată în rândul analiştilor care utilizează modele predictive, întrucât gradul de incertitudine introdus în ecuaţie nu mai poate genera previziuni pentru următorii 50 de ani, aşa cum ne-ar place. Contestarea acestei abordări derivă cu atât mai mult din parcimonia elaborării unei metodologii şi a unor definiţii mai clare asupra termenelor utilizate. Astfel, în principiu, în materie de aplicabilitate la nivelul mediului de securitate internaţional, comunitatea ştiinţifică a agreat doar termenii de „auto-organizare" şi „rezilienţă", comuni în toate ştiinţele care utilizează Teoria complexităţii.

Avantajul complexităţii este dat tocmai de transdisciplinaritatea ei, mai ales dacă ţinem cont de faptul că trăim într-o lume a interdependenţelor şi a eludării coagulării intereselor.

BIBLIOGRAFIE:

1. ANDERSON,Philip.W.,*More is Different*. Science, 177:393:396, 1972.
2. BUZAN,Barry,*Popoarele, statele şi teama: O agendă pentru studii de securitateInternaţională în epoca de după Războiul Rece,* Chişinău: Cartier. Cap.I, II, III, IV, 2000.
3. COLEMAN,Peter T., VALLACHER,Robin, NOVAK,Martin, BUI-WRZOSINSKA,Lan,*Intractable Conflict as an Attractor: Presenting a Dynamical*

Model of Conflict, Escalation and Intractability, American Behavioral Scientist, 2007, Vol. 50.
4. COOPER, Robert,*Destrămarea naţiunilor. Ordine şi haos în secolul 21*, Bucureşti: Editura Univers Enciclopedic, 2007.
5. FONTANA, Walter, BALLATI, Susan, *Complexity; Introduction to Issues in and about „Complexity"*, în cadrul seminarului „Philanthropy and Social Change", New Jersey: Robert Wood Johnson Foundation, Princeton, 15 octombrie 1998.
6. HARRISON, Neil E., *Complex Systems and the Practice of World Politics*, în HARRISON, Neil E. (ed.), *Complexity in World Politics, Concepts and Methods of a New Paradigm*, State University of New York, 2006.
7. HENDRICK, Diane, *Complexity Theory and Conflict Transformation: An Exploration of Potential and Implications*, Working Paper 17, University of Bradford, Centre for Conflict Resolution, Department of Peace Studies, iunie 2009.
8. INNER, Judith E, BOOHER, David E. , *Consensus Building and Complex Adaptive Systems: A framework for Evaluating Collaborative Planning*, Journal of the American Planning Association, Vol. 65, No.4, toamna 1999.
9. McELROY, Mark W.,*Integrating Complexity Theory, Knowledge Management and Organizational Learning*, Journal of Knowledge Management, Vol. 4 No. 3, 2000.
10. ORTEGON-MONROY, Maria Carolina, *Chaos and Complexity Theory in Management: An Exploration from a Critical Systems Thinking Perspective*, Systems Research and Behavioral Science, Vol. 20 No. 5, 2003.
11. PARROTT, Lael, KOK, Robert, *Incorporating Complexity in Ecosystem Modelling*, Complexity International, Vol. 7, 2000.
12. PAVARD,Bernard, DUGDALE,Julie,*The Contribution of Complexity Theory to the Study of Sociotechnical Cooperative Systems*, disponibil la http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.70&rep=rep1&type=pdf.
13. PIGLIUCCI, Massimo,*Chaos & Complexity. Should We Be Skeptical?*, California: Skeptic Magazine, Vol. 8 No. 3, 2000.
14. SMITH,Aaron, HUMPHRIES, Clare,*Complexity Theory as a Practical Management Tool: ACritical Evaluation*, Organization Management Journal, Vol. 1 No. 2, 2004.
15. TALEB, Nassim Nicholas, *Lebăda neagră. Impactul foarte puţin probabilului*, Bucureşti: Editura Curtea Veche, 2010.
16. TREVERTON, Gregory F.,*Adressing „Complexities" in Homeland Security*, The SwedishNationalDefenseCollege, 2009.
17. WALTZ, Kenneth, *Theory of International Politics*, Boston: McGraw-Hill, 1979.
18. WENDT, Alexander, *Contructing International Politics*, International Security, 20 (1), vara 1995.
19. WOLFERS, Arnold, *„National Security" as an Ambitious Symbol*, Political Science Quarterly, Vol. 67, No. 4, 1952.

SECURITATE PRIN COMPLEXITATE

Maria – Cristina MURARU
Doctorand, Academia Naţională de Informaţii "MIHAI VITEAZUL"
e-mail cristina.muraru@gmail.com
Giorgiana – Raluca STOICA
Doctorand, Academia Naţională de Informaţii ""MIHAI VITEAZUL"
ralluca.stoica@gmail.com

Rezumat*: Mediul actual de securitate este perceput prin intermediul conectării evenimentelor aparent izolate, tendinţelor sezoniere şi evenimentelor episodice, ulterior unei ere cel mai bine descrise de o definiţie care include termeni precum fenomene cauză-efect, tendinţe pe termen lung şi, cel mai important, modelele ordonate, organizate.*

Fiind dată această mutaţie de paradigmă, se înţelege că metaforele aferente teoriei complexităţii – o ştiinţă care postulează că existenţa societăţilor, statelor interacţionează într-o manieră deloc lineară şi predictibilă – pot fi de asemenea aplicate în problematica mediului de securitate.

Lucrarea de faţă îşi propune să evidenţieze vechile şi noile metafore ale haosului lui Clausewitz şi teoriei complexităţii propuse de Institutul Santa Fe, metafore ascunse în strategiile şi politicile de securitate naţională.

Cuvinte cheie: *complexitate, haos, nelinear, ordine, strategie, securitate, sisteme.*

Introducere

Relaţiile dintre state şi grupuri de state sunt similare interacţiunilor dintre structurile microscopice din fizică: un număr redus de variabile sunt necesare pentru creionarea unui întreg proces.

În descrierea unor astfel de evenimente şi fenomene, cercetătorii şi experţii contemporani tind să utilizeze termeni precum *haos, complexitate, sisteme, incertitudine, emergenţă,* etc.

Este cunoscut faptul că paradigma haosului a fost asociată cu ideea de bătălie şi conflicte: volumul „Vom Kriege", elaborat de generalul prusac Carl Phillipp Gottlieb von Clausewitz's a fost prima lucrare militară în care s-au regăsit principiile şi aspectele care ulterior urmau să fie incluse în teoria haosului.

Mai târziu, oameni de ştiinţă renumiţi au propus şi explicat utilitatea conceptelor complexităţii şi haosului în descrierea relaţiilor internaţionale şi securităţii. Ceea ce au sugerat aceştia a fost, de fapt, aplicarea metaforelor precum atractori stranii, fractalii, auto-organizare etc., la domeniul militar şi cel de intelligence.

Este lesne de înţeles că un nou set de principii pentru înţelegerea regulilor ascunse care determină un sistem sau un grup de sisteme nu înseamnă noi comportamente ale acestor sisteme, ci o mai bună descriere şi, eventual, interacţiuni mai bune cu sistemele menţionate.

1. Teoria complexităţii

Eforturile ştiinţifice, de la începutul anilor 1960, de prognoză meteorologică au fost împiedicate de înţelegerea scăzută şi imposibilitatea de compilare a evoluţiei neliniare, non-cauză - efect a curenţilor de aer. Edward Norton Lorenz, meteorolog şi matematician american,

a fost primul care a descris aceste mişcări utilizând matematica superioară. Ulterior, în anii 1980, best-seller-ul lui James Gleick, "Chaos: Making a New Science", a popularizat ceea ce numim astăzi teoria haosului.

Teoria complexităţii sau teoria sistemelor complexe adaptive este o ramură ştiinţifică relativ nouă, adusă în atenţia lumii ştiinţifice de Institutul Santa Fe din New Mexico. Similar ciberneticii, teoriei sistemelor şi teoriei haosului, teoria complexităţii are la bază ideea interacţiunii şi mişcărilor continue şi coroborate atât a sistemelor, cât şi a componentelor acestora. Altfel spus, termenul de complexitate care astăzi tinde să fie utilizat pentru a descrie sisteme încâlcite şi complicate este de fapt asociat cu inter-conectivitatea dintre componentele unui sistem şi a acestuia cu mediul înconjurător[1].

Majoritatea sistemelor naturale (mintea umană, ecosistemele, grupurile), îndeosebi societăţile şi, mai nou, majoritatea sistemelor artificiale (sistemele computaţionale, programe evolutive şi, cel mai faimos, Internetul) tind să fie descrise de comportamente complexe care sunt rezultatul unui număr ridicat de interacţiuni neliniare între un număr la fel de ridicat dintre componentele sistemului. Dat fiind faptul că neliniaritatea a fost până acum câteva zeci de ani o Zonă Crepusculară a matematicii, emergenţa teoriei complexităţii a fost influenţată şi de dezvoltarea computerelor, având în vedere că un comportament neliniar este extreme de dificil de descris fără un sprijin automatizat.

1.1 Elemente de bază

Teoria complexităţii poate fi cel mai bine descrisă ca fiind maniera fundamentală de investigare a chintesenţei comportamentului sistemelor neliniare, în contrast cu matematica bazată pe o gândire simplă, Newtoniană axată pe calcule şi statistici.

Sistemele liniare sunt rezultatul a ceea ce numim simplu procese cauză şi efect. Sunt caracterizate de predicţii uşor de realizat, ca rezultat al unor proceduri meticuloase de planificare, monitorizare şi control, intrările şi ieşirile din sistem fiind direct proporţionale. De asemenea, sistemele liniare sunt ceea ce stă la baza reducţionismului: sistemele complicate, ample sunt analizate prin reducerea la părţi componente cât mai mici.

La polul opus se află sistemele neliniare, sau în cuvinte mai bine alese, *căile naturii:* medii în care sistemul reprezintă mai mult decât suma părţilor, în care ieşirile şi intrările sunt orice decât proporţionale, şi, poate cel mai important, fenomenele de tip cauză şi efect nu sunt observabile. În cazul sistemelor neliniare fenomenele sunt incerte, însă în anumite limite, concomitent auto-organizarea fiind o soluţie şi nu controlul convenţional.

Sistemele complexe adaptive sunt sisteme dinamice care posedă abilitatea de a se adapta şi de a evolua într-un mediu aflat în schimbare. De asemenea, sistemele complexe adaptive şi mediile care le înconjoară nu sunt separabile: nu există sistem complex adaptiv fără un mediu la care să se adapteze. În alte cuvinte, schimbarea constă în co-evoluţie cu toate sistemele din mediu, şi nu în adaptare care în majoritatea cazurilor duce la o stare fixă, deci la moartea sistemului.

1.2 Atributele sistemelor complexe adaptive

În mod tradiţional, caracteristicile de bază ale unui sistem complex adaptiv constau în:

- *Auto-organizare*

Atunci când un teoretician în complexitate aude sintagma „sistem complex", prima idee pe care o are este auto-organizarea. Ideea de auto-organizare a fost utilizată prima dată de Maturana şi Varela în cercetările privind sistemele biologice, fiind creat astfel termenul de

[1]Vasant, HANOVAR, *Complex Adaptive Systems Group,* Iowa State University, available at http://www.cs.iastate.edu/ ~honavar/alife.isu.html, accesat la 23.03.2015.

„autopoiază” – procesul intern prin care fiecare componentă a unui sistem este direct responsabilă de transformarea celorlalte component şi a sistemului în întregime.

În ceea ce priveşte sistemele complexe adaptive, componentele acestuia, numite agenţi, relaţionează cu vecinii lor, pentru propriile motive. Un sistem este auto-organizat când evoluează într-o formă şi mai complexă fără a fi administrat, manipulat sau controlat din exterior.

Având în vedere că relaţiile dintre agenţi sunt aproape mereu mutuale şi feedback-ul este constant, un sistem auto-organizat este prin definiţie neliniar. Mai mult, un sistem complex adaptativ este auto-organizat datorită componentelor sale conexe emergenţei şi feedback-ului.

- *Emergenţă*

Noţiunea de emergenţă se bazează pe ideea că întregul este mai signifiant decât suma componentelor sale. Altfel spus, comportamentul grupului sau sistemului este diferit de suma acţiunilor agenţilor. Prin intermediul emergenţei, sistemele complexe adaptive determină structuri interne noi şi coerente, modele, care, mai important, nu au fost anterior detectate. Fenomenele emergente sunt perceptibile la scară macro deşi au derivat din evenimente de dimensiune redusă.

Neliniaritatea joacă un rol imens când vine vorba de auto-organizare şi emergenţă: paradigma newtoniană, care a postulat că un input redus creează un output similar a constituit fundamentul cercetării ştiinţifice anterioare, însă în cazul teoriei sistemelor complexe adaptative, orice turbulenţă minoră în evoluţia sistemului, creată de mediul exterior sau de unul din agenţi, poate conduce la ajustări majore, inclusiv de natură a remodela structura sistemului.

- *Adaptabilitate*

Sistemul este deschis: fluxurile de energie şi informaţie sunt bidirecţionale. Informaţia nouă intră în ciclul de feedback, influenţând mai departe comportamentul agenţilor. Implicit tendinţa sistemului este de a se adapta la mediul înconjurător.

- *Co-evoluţie*

Această caracteristică este, de fapt, o versiune *evoluată* a evoluţionismului lui Darwin. În loc să fie înconjurat de un mediu stabil care să permit agenţilor să evolueze şi să se adapteze încet, teoria complexităţii sugerează că agenţii interacţionează cu alţi agenţi, care la rândul lor evoluează.

- *Feedback*

Informaţiile noi intră în iteraţiile de tip feedback şi influenţează comportamentul indivizilor, deci al întregului sistem.

- *Rezilienţă*

Se referă la capacitatea unui sistem de a absorbi şi utiliza, sau chiar beneficia de perturbaţii şi de schimbările aduse de acestea, reuşind să existe în continuare fără modificări de ordin calitativ în structura sistemului. Sistemele complexe adaptative sunt reziliente fiind capabile să răspundă într-o manieră care le permite să se redreseze sau să mascheze rapid efectele unui eveniment neaşteptat sau unei perturbaţii premeditate.

- *Sensibilitatea la condiţii iniţiale*

Teoria haosului semnalează că evoluţiile neliniare sunt extreme de sensibile la condiţiile iniţiale: o diferenţă minoră în oricare variabilă de stare a sistemului de la care porneşte evoluţia poate cauza traiectorii complet diferite, urmare a majorării amplificate de feedbackul pozitiv. Sensibilitatea la condiţiile iniţiale este cunoscută publicului sub numele de *efect de fluture.* Spre exemplu, cum ar fi arătat Europa astăzi dacă Arhiducele Franz Ferdinand de Austria nu ar fi vizitat Sarajevo la data de 28 iunie 1914 sau dacă tânărul combatant Adolf Hitler ar fi orbit în 1918?

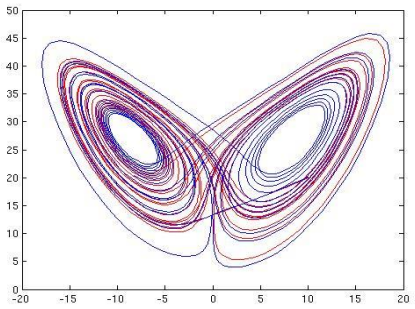


Figura nr. 1. The 'Butterfly Effect'

Cele două grafice colorate cu roşu şi albastru descriu două traiectorii diferite ale aceluiaşi sistem complex, care a evoluat de la două seturi de condiţii iniţiale extrem de similare

Se poate observa în figura de mai sus că deşi cele două traiectorii sunt diferite, au o structură similar – noţiunea de atractor. Un sistem complex orbitează în jurul unui atractor, niciodată în aceeaşi manieră, deşi un model este observabil, rezultatul fiind mişcări neprevăzute ale sistemului[2]. De asemenea, conform lui James Gleick, atractorii pot fi descrişi ca forţe care conduc activitatea sistemului spre o axă comună.

Noţiunea de atractor conectează teoria haosului cu geometria fractală – o nouă metodă de observare a lumii natural, care conţine modele nebănuite, însă uşor de recunoscut[3].

Cercetătorii consideră că fractalii nu ar trebui să fie definiţi, o definiţie riscând să elimine unele cazuri interesante, ci să fie descrişi ca *forme*, nu neapărat tridimensionale, care sunt auto-similare – se replică pe sine la orice nivel - şi care deţin un potenţial infinit – sunt generate un număr reduc de ecuaţii matematice, pornind de la puţină informaţie[4].

Enumerând caracteristicile şi atributele descrise anterior, putem concluziona că sistemele complexe adaptive pot fi creionate de figura următoare: agenţii sunt auto-organizati şi co-evoluează pe măsură ce sistemul schimbă informaţii cu mediul înconjurător şi primeşte feedback, care îi decide viitoarele transformări.

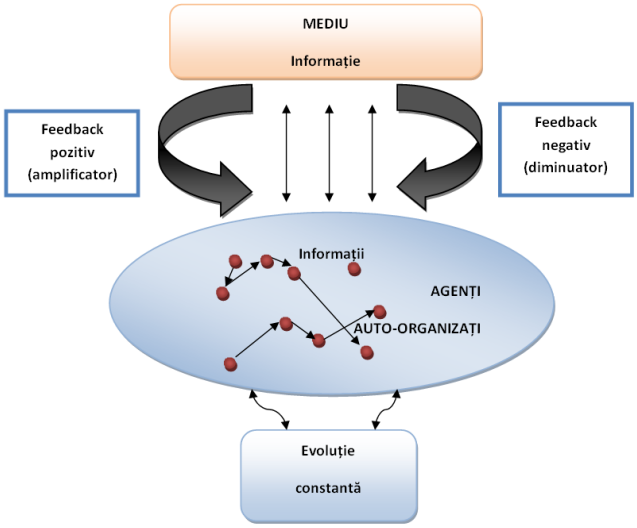


Figura nr. 2. Sistem complex adaptativ

[2] Sandra, L. BLOOM, *Chaos, Complexity, Self-Organization and Us,* Community Works, America Psychoterapy Review 2(8), August 2000.

[3] Michael, FRAME, Benoit B., MANDELBROT, Nial, NEGER, *Fractal Geometry,* Yale University, March 2015, available at http://classes.yale.edu/fractals/, accesat la 25.03.2015.

[4] Anirvan, SENGUPTA, *Towards a Theory of Chaos,* International Journal of Bifurcation and Chaos, vol.13, no. 11, pp. 31-49.

2. Intelligence-ul şi teoria sistemelor complexe adaptative

Trăim într-o epocă descrisă de incertitudine, emergenţă şi dubii, apariţia teoriei sistemelor complexe adaptative pe scena securităţii naţionale nefiind o surpriză pentru nimeni, dat fiind faptul că zona de intelligence şi decidenţii sunt mereu în căutarea unui panaceu.

Mai mult, urmare dizolvării Uniunii Sovietice, în prezent nu mai există ideea de stat ca sistem închis, rezultatul fiind schimburi constante de informaţii între toate statele lumii.

Este mai mult decât evident că teoria complexităţii este convingătoare în sensul în care se bazează pe studiul fenomenelor complexe şi pleacă de ipoteza că acestea sunt până la un punct derivate din modele, deci posibil de înţeles. Pe termen lung, teoria sistemelor complexe adaptative poate fi văzută ca baza propice pentru soluţionarea celor mai dificile dileme ale factorilor decidenţi.

Zona de intelligence este una dintre cele mai, sau poate cea mai recent în care teoria complexităţii este aplicată, ulterior implementării cu succes în management, economie şi pieţe financiare, ecologie şi prognoză meteorologică.

2.1 Aplicaţii ale atributelor sistemelor complexe adaptative

Serviciile şi comunitatea de intelligence dintr-un stat trebuie să fie capabile să se reinventeze prin colectarea progresivă a informaţiilor, învăţarea şi adaptarea la modificările mediului de securitate. Factorii de decizie din intelligence ar trebui să propună anumite obiective, care odată îndeplinite, sprijină evoluţia organizaţiei şi deci, încurajează o evaluare eficientă a unui mediu în tranziţie rapidă.

- *Activitate descentralizată*

Este o aplicaţie a auto-organizării pentru că susţine ideea că un număr redus de reguli conduce la rezultate mai bune a organizaţiei şi, implicit, un mediu de securitate mai sigur.

Având în vedere că un serviciu de informaţii înglobează atributele unui sistem complex adaptativ, este legitim ca toţi angajaţii – ofiţeri de execuţie şi manageri – să acţioneze independent atunci când modificările din mediul de securitate o cer.

Deci, ofiţerii de informaţii trebuie să aibă la dispoziţie posibilitatea de a acţiona *mai mult* pe cont propriu. Spre exemplu, furnicile dintr-o colonie decid mereu ce sarcină să rezolve şi în ce manieră o vor realiza. Extrapolând, angajaţii unui serviciu de informaţii ar trebui să poată reacţiona, în concordanţă cu normele legale şi instituţionale, în faţa evoluţiilor din mediul de securitate. În plus de auto-organizare, independenţa fiecărui angajat poate fi privită ca un fractal: coroborat cu experienţa şi expertiza fiecărui angajat şi manager, gradul de independenţă acordat fiecărui cadru ar trebui să includă aceleaşi criterii, conducând la forme similare de capacitate de decizie.

- *Căutarea constantă a cunoaşterii*

Practicienii din intelligence ar trebui să se afle într-o constantă căutare a expertizei şi cunoaşterii, cele două fiind principalele condiţii pentru posibilitatea unui cadru de a acţiona independent.

Similar atractorului unui sistem complex adaptativ, expertiza şi cunoaşterea ar trebui să se afle în centrul atenţiei fiecărui ofiţer.

- *Includerea şi evoluţia knowledge workers*

Peter Drucker a postulat în 1966, în volumul său 'The Effective Executive' că principalul factor de producţie este cunoaşterea. Organizaţiile ale căror obiective constau în crearea, distribuirea şi aplicarea cunoaşterii sunt direct influenţate: *knowledge workers,* sau analiştii din cadrul serviciilor de informaţii, sunt cei care dictează productivitatea şi eficienţa sistemului.

Un studiu elaborate la Universitatea Bar Ilan din Israel a dus ideea de *knowledge workers* mai departe. Potrivit cercetării conduse de Snunith Shohan şi Alon Hasgall această

categorie de angajaţi ar putea fi priviţi ca fractali pentru că stau la baza managementului cunoaşterii. Datorită responsabilităţii în integrarea în sistem a propriei cunoaşteri, managerii pot administra mai eficient operaţiunile de nivel strategic.

- *Schimburi interne de informaţii*

Revoluţia informaţională, creată de explozia Internet-ului şi de avansul masiv al comunicaţiilor a făcut umanitatea să uite de principiul *need-to-know* şi să îl adopte pe cel *need-to-share.*

Dacă un serviciu de informaţii doreşte să evolueze, şi nu doar să supravieţuiască, trebuie să eficientizeze utilizarea celor mai bune resurse: informaţii şi resursa umană. Practicienii în domeniu – colectorii de date, ofiţerii operative, analişti, unităţi tehnice şi manageri – ar trebui să renunţe la competiţie şi să facă schimb de informaţii.

Astfel, golurile umplute din cunoaşterea organizaţională nu doar vor încuraja progresul sau, în unele cazuri îl vor inhiba, ci vor şi permite practicienilor de la orice nivel ierarhic să se auto-organizeze şi să răspundă rapid la riscuri şi vulnerabilităţi.

- *Înţelegerea cadrului organizaţional*

Deşi problemele zilnice sunt percepute ca fiind prioritatea principală în activitatea curentă a unui practician, managerii ar trebui să precizeze clar obiectivele strategice, de lungă durată.

Ştiind că mediul de securitate este în sine un sistem complex şi deci evoluează, angajaţii unui serviciu de informaţii ar trebui să cunoască modul în care activitatea lor este inclusă în cea a organizaţiei cu scopul de a evolua şi de a se adapta.

- *Feedback constant*

Serviciile de intelligence şi întreaga Comunitate de Intelligence trebuie să primească mai multe răspunsuri din partea mediului de securitate naţională. Este singura manieră de învăţare şi adaptare la schimbările mediului de securitate.

Inexistenţa feedbackului poate crea întârzieri în răspunsul unei organizaţii la probleme de ordin critic şi poate provoca efecte dezastruoase.

Concluzii

Ştiinţele exacte au dominat cercetarea ştiinţifică încă de când Isaac Newton a descoperit gravitaţia. Paradigma newtoniană a oferit o descriere exactă şi satisfăcătoare a lumii şi a securităţii. Paradigma anterior menţionată, cu descrierea sa mecanică a organizaţiilor militare şi de informaţii, a conflictelor şi războaielor, nu este aplicabilă mediului actual de securitate.

Teoria complexităţii şi metaforele sale ne încurajează să ne referim la securitate utilizând alte sintagme, obţinând astfel o abordare distinctă a managementului în intelligence. De asemenea, aplicând principiile teoriei complexităţii la securitate, nu ne aşteptăm să identificăm soluţii universale care să asigure certitudine sau control precis, ci un mod de a discerne incertitudinea şi dezordinea aparentă.

Lucrarea de faţă şi-a propus să sublinieze ideile de evoluţie şi adaptare, atât pentru supravieţuirea, cât şi pentru asigurarea securităţii. Comunităţile actuale de intelligence necesită o gândirea Prigogineană: mediul de securitate, sau mai bine formulat, *de insecuritate,* nu este un bun dat. Complexitatea, alături de auto-organizare, atractori, fractali, utilizate ca metafore sunt extreme de utile pentru recrutarea, educarea şi instruirea şi, evident, gândirea solicitată ofiţerilor de informaţii din zilele noastre.

Pe de altă parte, teoria complexităţii nu oferă comunităţii de intelligence instrumente precise precum stabilirea unei probabilităţi precise pentru unele evenimente incerte. De asemenea, când vine vorba de luarea deciziilor, nu ar trebui căutată o soluţie universală, ci, mai degrabă, ar fi utilă aplicarea unui *cel mai bun* temporar, care permite adaptare rapidă.

Şi nu în ultimul rând, poate cel mai important aspect al metaforelor teoriei haosului şi complexităţii aplicate securităţii şi intelligence-ului este să prevină practicienii să nu cadă în capcana dezordinii.

BIBLIOGRAFIE:

1. ALBERTS, David; CZERWINSKI, Thomas J.; *Complexity, Global Politics, and National Security,* National Defense University, Washington D.C., 1997;
2. ANDRUS, Calvin; *Toward a Complex Adaptive Intelligence Community. The Wiki and the Blog;* Central Intelligence Agency, Studies in Intelligence, Vo. 49, No. 3, September 2005;
3. BLOOM, Sandra, L.; *Chaos, Complexity, Self-Organization and Us;* Community Works, America Psychoterapy Review 2(8), August 2000;
4. CHAN, Serena; *Complex Adaptive Systems;* Research Seminar in Engineering Systems, Massachusetts Institute of Technology, 2001;
5. DRUCKER, Peter, *The Effective Executive,* HarperCollins, 1967;
6. FRAME, Michael; MANDELBROT, Benoit B.; NEGER, Nial; *Fractal Geometry,* Yale University, disponibil la http://classes.yale.du/fractals/;
7. HANOVAR, Vasant, *Complex Adaptive Systems Group,* Iowa State University, available at http://www.cs.iastate.edu/~honavar/alife.isu.html, accesat la 23.03.2015;
8. PAVLOS, Antoniou; PITSILLIDES, Andreas; *Understanding Complex Systems: A Communication Networks Perspective,* Nicosia, Computer Science Department, University of Cyprus, 2007;
9. SENGUPTA, Anirvan; *Towards a Theory of Chaos,* International Journal of Bifurcation and Chaos, vol.13, no.11, pp.31-49, 2004;
10. SHOHAM, Snunith; HASGALL, Anon; *Knowledge Workers as Fractals in a Complex Adaptive Organization;* Knowledge and Process Management, volume 12, number 3, pp. 225-236, 2005;
11. TAYLOR, Robert L.V.; *Attractors: Non Strange to Chaotic;* Society for Industrial and Applied Mathematics, SIAM Undergrad Research Online, volume 4, 2010 disponibil la https://www.siam.org/students/siuro/vol4/S01079.pdf , accesat la 20.03.2015.

ASPECTE PRIVITOARE LA ELABORAREA PRINCIPIILOR DE DOCTRINĂ ALE SISTEMULUI DE ORDINE PUBLICĂ ŞI SIGURANŢĂ NAŢIONALĂ

Antonela-Alina ŞOFINEŢI
Ofiţer de poliţie în cadrul Direcţiei Generale Anticorupţie, doctorand în cadrul Academiei de Poliţie „Al. I. Cuza”, antonnella77@yahoo.com

Rezumat*: Articolul abordează principalele aspecte referitoare la valorile esenţiale, pilonii de bază, conduita profesională, standardele etice şi principiile fundamentale, precum şi la elementele de tradiţie întâlnite în procesul de elaborare a doctrinei sistemului naţional de ordine şi siguranţă publică. De asemenea, autorul evidenţiază şi importanţa elementelor de doctrină privitoare la complexitatea elaborării strategiilor în domeniul de referinţă. În plus, articolul face parte dintr-un proiect de cercetare mai amplu, desfăşurat în cadrul programului POSDRU/159/1.5/S/141086, finanţat de Academia Română.*

Cuvinte cheie: *valori, principii, doctrină, strategie, sistemul de ordine şi siguranţă publică.*

Introducere

Pornind de la definiţia dată „doctrinei” de dicţionarul explicativ al limbii române ca fiind totalitatea principiilor unui sistem politic, ştiinţific, religios etc. sau ansamblul de principii, de idei fundamentale ale unui sistem, prin analogie, putem afirma că doctrina ordinii şi siguranţei publice însumează totalitatea principiilor care guvernează acest domeniu, reflectând învăţătura sănătoasă care transmite valorile, direcţiile de acţiune, viziunea şi misiunea sistemului de ordine şi siguranţă publică.

Doctrina prezintă importanţă prin aceea că determină şi adecvează comportamente, atitudini, acţiuni, având scopul de a modela, de a forma gândirea sau mentalitatea celor cărora li se adresează; doctrina comunică cunoştinţe care transformă ceea ce e necesar sau doar modelează. Acolo unde lipseşte doctrina sănătoasă, sistemul apare mutilat, lipsit de consistenţă, iar beneficiarii doctrinei simpli diletanţi. Printre beneficiile aplicării unei doctrine sănătoase, revigorante şi dinamizante enumerăm: abordare şi înţelegere unitare, consecvenţă şi stabilitate, eficienţă şi eficacitate.

Analizând documentele programatice care reglementează şi fundamentează domeniul ordine şi siguranţă publică, pot fi reliefate o serie de elemente care se prefigurează în principii ce impregnează liniile directoare pentru acest domeniu.

Principalele documente de politici publice[1] avute în vedere pentru extragerea elementelor de doctrină asociate domeniului ordine şi siguranţă publică au fost strategiile

[1]Hotărârea nr. 62 din 17 aprilie 2006 privind Strategia de Securitate Naţională a Romaniei, adoptată de către Consiliul Suprem de Apărare a Ţării; Hotărârea nr. 30/2008 privind aprobarea Strategiei Naţionale de Apărare a Ţării publicată în Monitorul Oficial al României nr. 799/28.11.2008; Hotărârea Guvernului nr. 1040/2010 pentru aprobarea Strategiei Naţionale de Ordine Publică 2010-2013, publicată în Monitorul Oficial nr. 721 din 28 octombrie 2010; Hotărârea Guvernului nr. 784/2013 privind aprobarea Strategiei Naţionale Antidrog 2013-2020, publicată în Monitorul Oficial nr. 702 bis din 15 noiembrie 2013; Hotărârea nr. 498 din 18 mai 2011 pentru aprobarea Strategiei nationale privind imigratia pentru perioada 2011-2014, publicată în Monitorul Oficial nr. 391 din 3 iunie 2011; Hotărârea Guvernului 1156/2012 privind aprobarea Strategiei nationale pentru prevenirea şi combaterea fenomenului violentei in familie pentru perioada 2013-2017, publicată în Monitorul Oficial nr. 819/2012; Hotărârea nr. 498 din 18 mai 2011 pentru aprobarea Strategiei nationale privind imigratia pentru

nationale care definesc şi sunt circumscrise domeniului de referinţă, respectiv strategia de securitate naţională a României, strategia naţională de apărare, strategia naţională de ordine publică, strategia naţională împotriva traficului de persoane, strategia naţională antidrog, strategia naţională pentru prevenirea si combaterea fenomenului violentei in familie, strategia naţională privind imigraţia, strategia naţională de securitate cibernetică şi strategia naţională anticorupţie.

Astfel, documentele programatice menţionate prezintă elemente de doctrină comune care asigură aplicabilitatea, convergenţa şi coerenţa acţiunilor şi măsurilor de asigurare şi menţinere a ordinii şi liniştii publice la nivel naţional.

Totodată, documentele potenţează principiifundamentale ce pot susţine activitatea de zi cu zi şi pot oferi coordonatele unui sistem al ordinii şi siguranţei naţionale eficient şi sustenabil pentru misiunile, acţiunile şi măsurile întreprinse în domeniul de referinţă: legalitatea şi respectarea drepturilor omului, prioritatea interesului public, transparenţa, disponibilitatea, dialogul şi parteneriatul, independenţa operaţională, anticiparea, funcţionalitatea, pragmatismul, multidisciplinaritatea, echilibrul, continuitatea, specificitatea, subsidiaritatea şi corelarea internaţională.

De asemenea, alături de aceste principii comune se regăsesc valorile esenţiale, pilonii de bază, elementele ce ţin de conduita profesională şi standardele etice, toate stând la baza constituirii doctrinei sistemului ordinii publiceşi siguranţei naţionale.

1. Valorile esenţiale şi pilonii de bază

Forţele sistemului de ordine şi siguranţă publică exercită o profesie nobilă care presupune cunoştinţe de specialitate şi abilităţi specifice, precum şi înalte standarde de etică şi moralitate. Drept urmare, toate trebuie să adere şi să-şi însuşească *valorile esenţiale* de durată privitoare la respectul faţă de autoritate, devotamentul sincer şi în beneficiul tuturor cetăţenilor, responsabilitatea.

Forţele de aplicare a legii înţeleg că respectul pentru autoritate este o datorie individuală, dând dovadă de decenţă şi moralitate faţă de acest lucru. Respectul şi supunerea faţă de prevederile legale şi constituţionale,precum cele privitoare la România care este,,un stat de drept, democratic şi social, în care demnitatea omului, drepturile şi libertăţile cetăţenilor, libera dezvoltare a personalităţii umane, dreptatea şi pluralismul politic reprezintă valori supreme”[2], darşi recunoaşterea legitimităţii şi autorităţii conducerii, reprezintă însuşiri de bază. În plus, credinţa în dragostea de popor şi în respectul faţă de cetăţeni este de esenţă. Pentru atingerea acestui deziderat, implicarea lor în serviciul cetăţenesc trebuie să fie mai presus de orice interes personal.

În aceeaşi măsură, forţele de ordine şi siguranţă publică îşi fundamentează existenţa pe următorii *piloni de bază*: imagine, managementul carierei, managementul conducerii şi accesul egal al cetăţenilor la servicii.

Imaginea forţelor sistemului de ordine şi siguranţă publică, odată ştirbită, poate afecta moralul, dar şi mândria acestora. În acest sens, acuzaţiile defăimătoareale unor formatori de opinie apăruţi pe scena publică la un moment dat, cazurile denigratoare din justiţie, mediatizate agresiv, fără respectarea principiului universal valabil al prezumţiei de nevinovăţie până la adoptarea unei hotărâri definitive de condamnare, precum şi

---

perioada 2011-2014, publicată în Monitorul Oficial nr. 391 din 3 iunie 2011; Hotărârea Guvernului 215 din 20 martie 2012 privind aprobarea Strategiei naţionale anticorupţie pe perioada 2012-2015, publicată în Monitorul Oficial nr. 202 din 27 martie 2012; Hotărârea Guvernului 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României, publicată în Monitorul Oficial nr. 296 din 23.05.2015;

[2]Constituţia României din 21 noiembrie 1991, republicată în Monitorul Oficial nr. 767 din 31 octombrie 2003, art. 1;

comportamentele interpretate, în mod public, ca fiind inadecvate şi fără un fundament legal, de către factorii decidenţi din sistemul de referinţă, pot constitui exemple care să conducă la demoralizarea lucrătorilor, respectiv la scăderea autorităţii şi încrederii cetăţenilor. Astfel, fiecare lucrător trebuie să aibă o conduită care să reflecte cel mai bine statutul instituţiei în care îşi desfăşoară activitatea şi să urmeze valorile trasate de aceasta.

Implementarea unui sistem eficient de management al carierei va îmbunătăţi vizibil procesul de profesionalizare a lucrătorilor în ceea ce priveşte recrutarea, pregătirea profesională, promovarea, recompensarea şi ulterior, retragerea din activitate. O instituţie de aplicare a legiitrebuie să formuleze o politică stringentă şi să implementeze un sistem de resurse umane compatibil cu distribuirea echitabilă a funcţiilor privitoare la angajare, promovare pe criterii obiective şi abordare raţională a problematicii legate de distribuirea sarcinilor, dezvoltarea abilităţilor, recompensarea imediată şi un trai decent după retragerea din câmpul muncii.

În ceea ce priveşte managementul conducerii, eficienţa aplicării legii este reflectată asupra capacităţilor managriale şi a leadership-ului competent al celor care conduc instituţia de aplicare a legii. Aceste atribute trebuie, prin urmare, să fie esenţiale în selecţia personalului ce urmează să fie angajat sau redistribuit în câmpul muncii.

De asemenea, trebuie să existe o distribuţie judicioasă şi echitabilă a oportunităţilor pentru ca un lucrător să-şi dovedească competenţele într-o instituţie de aplicare a legii. Problema inechităţii, favorizarea unor cadre, şansele inegale la pregătirea profesională, promovarea pe criterii nedrepte, dar şi întârzierea în atingerea obiectivelor instituţionale pot genera o atmosferă tensionată. Rezultatul poate fi ineficienţa, pierderea de resurse materiale, informaţionale, financiare, dar şi lipsa muncii în echipă, în detrimentul instituţiei şi implicit a sistemului. Prin urmare, conducerea instituţiei trebuie să gestioneze eficient astfel de situaţii şi să implementeze o politică de aderare la un sistem bazat pe meritocraţie.

În consonanţă cu cerinţele legate de onoare şi integritate, forţele de ordine şi siguranţă publică trebuie să aibă curajul moral de a-şi sacrifica interesul personal în beneficiul comunităţii. Fără acest curaj moral, specific fiecărei structuri a sistemului de ordine şi siguranţă publică, nu ne-am mai afla în prezenţa unor lucrători calificaţi şi dispuşi să facă faţă unor provocări extraordinare pe care ritmul cotidian le impune. Sacrificiul care delimitează cetăţeanul de rând de lucrătorul specializat constă în disponibilitatea personală a celui din urmă, de a se dedica necondiţionat deservirii cetăţenilor, în orice situaţie, disponibilitate dictată de norme interioare de înalt devotament şi altruism. În plus, în ceea ce priveşte generarea unui exemplu, forţele de aplicare a legii trebuie să se constituie într-un model de etică şi moralitate.

2. Conduita profesională, standardele etice, obiceiurile şi tradiţiile

Privitor la *conduita profesională*, forţele de ordine şi siguranţă publică trebuie să se caracterizeze prin excelenţă şi expertiză în ceea ce priveşte îndeplinirea atribuţiilor de serviciu, dar şi integritate şi pregătire de specialitate în aplicarea competenţelor specifice şi a cunoştinţelor tehnice.

Profesionalismul presupune, în primul rând, pregătirea profesională temeinică a tuturor categoriilor de personal ce activează în cadrul sistemului naţional de ordine şi siguranţă publică. În al doilea rând, pentru a avea un sistem suplu şi dinamic în care toate structurile să performeze, acesta trebuie să se specializeze şi să-şi diversifice metodele şi mijloacele de acţiune, să reflecte o flexibilitate instituţională, un management proactiv de succes şi în special, o fundamentare a deciziilor pe bază de analiză.

Însuşirea şi exercitarea democraţiei trebuie să devină un stil de viaţă. Forţele de aplicare a legii trebuie să-şi însuşească viaţa şi valorile democratice şi să menţină principiul

responsabilităţii publice. În toate cazurile, trebuie să respecte prevederile constituţionale şi să fie loiale ţării, cetăţenilorşi instituţiei în care îşi desfăşoară activitatea.Totodată, prin creşterea gradului de conştientizare socială, forţele de aplicare a legii sunt încurajate să se implice în mod activ în activităţile sociale şi civice pentru a creşte imaginea pozitivă a instituţiilor de aplicare a legii.

În ceea ce priveşte*sănătatea fizică şi psihică,* forţele de ordine şi siguranţă publică trebuie să se asigure că fizic şi mental sunt, în permanenţă, în stare bună. În acest sens, se antrenează constant şi sunt supuse unor examene medicale periodice, participând la diferite programe de sănătate sau dezvoltare fizică.

Din punct de vedere al *disciplinei privind informaţiile clasificate*, toţi lucrătorii sistemului de referinţă au obligaţia de a păstra confidenţialitatea acestora, inclusiv a aspectelor legate de datele cu caracter personal, a comunicărilor, dosarelor sau oricăror altor documente care conţin informaţii clasificate sau de ordin operativ.

Independenţa profesională presupunecă forţele de ordine şi siguranţă publică caută să-şi îmbunătăţească permanent pregătirea profesională prin programe de dezvoltare a carierei, şi nu să solicite, în mod direct sau indirect influenţa sau recomandarea din sfera politicului ori a persoanelor influente ce ar putea avea legătură cu atribuţiile lor de serviciu. În plus, membrii de familie nu trebuie să intervină în activităţile lor, în special în ceea ce priveşte atribuţiile date în competenţă.

Utilizarea judicioasă şi *protecţia proprietăţii publice* presupune ca forţele sistemului de ordine şi siguranţă publică să promoveze şi să menţină un simţ al responsabilităţii în protejarea, asigurarea, dispunerea şi folosirea eficientă a bunurilor publice care sunt pentru folosul comunităţii. În acest sens, în concordanţă cu rigorile ierarhice, şefii nemijlociţi, dar şi fiecare lucrător individual, sunt responsabili pentru supravegherea eficientă, controlul şi dirijarea personalului şi veghează ca toate resursele publice să fie gestionate în consonanţă cu normele şi regulile în materie, astfel încât să se evite utilizarea lor în afara cadrului legal sau dispunerea de acestea după bunul plac.

Privitor la despre *standardele etice*, acestea se referă la valorile morale general stabilite şi acceptate. Valorile etice ce trebuie respectate sunt patriotismul, moralitatea, integritatea, devotamentul, loialitatea.

În ceea ce priveşte *patriotismul*, forţele de aplicare a legii sunt caracterizate de acest sentiment prin însăşi natura atribuţiilor de serviciu. Îşi manifestă iubirea de ţară cu un jurământ de credinţă faţă de drapel şi un jurământ de apărare a Constituţiei şi a prevederilor legale.

Forţelede ordine şi siguranţă publică aderă la înalte standarde de *moralitate şi decenţă*, generând astfel exemple demne de urmat pentru ceilalţi. Aceste norme de moralitate şi decenţă îşi găsesc rădăcinile în obligaţiile de serviciu generate de legile de organizare şi funcţionare care prevăd ca şi condiţii sine qua non, adoptarea unei conduite bazate pe integritate, onoare, respect faţă de cetăţeni şi stat. În plus, chemarea pentru moralitate şi decenţă trebuie să fie un atribut personal al celor care înţeleg să-şi lege destinul de o astfel de menire, respectiv aceea de a fi un protector al societăţii şi nu doar să aibă în minte partea materială conferită de statutul special. Atunci când obligaţiile profesionale ale lucrătorului de ordine şi siguranţă publică se întrepătrund în mod firesc cu convingerile sale interioare legate de respectarea legii, rezultatul nu poate fi altul decât cel de a da naştere unei atitudini de respect pentru ceilalţi cetăţeni.

De altfel, moralitatea trebuie să constituie o premiză în elaborarea şi adoptarea oricărei legi şi cu atât mai mult, un etalon pentru structurile angrenate în asigurarea şi menţinerea ordinii şi siguranţei publice. Pe parcursul exercitării atribuţiilor de serviciu, lucrătorii sistemului de ordine şi siguranţă publică nu trebuie, sub nicio formă, să fie implicaţi în activităţi ilegale ori să fie aplecaţi spre vicii, şi nu trebuie să tolerezeactivităţile ilicite. În acest

sens, testul integrităţii lor profesionale constă în prezenţa responsabilităţii morale individuale ce se dovedeşte prin conduită legală şi personal necompromis din toate punctele de vedere.

Totodată, cât priveşte *integritatea*, lucrătorii sistemului de ordine şi siguranţă publică nu îşi pot permite să fie victimele corupţiei ori a practicilor neoneste.Integritatea profesională presupune responsabilitate atât în cheltuirea banului public, cât şi în desfăşurarea activităţilor în domeniul ordinii şi siguranţei publice, în conformitate cu normele statuate în codul de etică şi deontologie profesională. Totodată, reprezentanţii instituţiilor şi autorităţilor publice au obligaţia de a declara orice interese personale care pot veni în contradicţie cu exercitarea obiectivă a atribuţiilor de serviciu; aceştia sunt obligaţi să ia toate măsurile necesare pentru evitarea situaţiilor conflictelor de interese ori incompatibilităţilor.

De asemenea, *devotamentul*faţă de muncă este de esenţă. Forţele de ordine şi siguranţă publică trebuie să exercite atribuţiile de serviciu cu meticulozitate, cu eficienţă, entuziasm şi determinare, precum şi să manifeste preocupare pentru avutul public şi să se abţină de la angajarea în orice activităţi care sunt în conflict cu statutul lor.Totodată,loialitateareprezintă ataşamentul faţă de instituţiile şi forţele de aplicare a legii, precum şi faţă de valorile promovate în cadrul sistemului de ordine şi siguranţă publică, valori care trebuie să primeze. Împărtăşirea valorilor promovate în cadrul sistemului de referinţă trebuie să fie voluntară, din proprie iniţiativă, iar respectul faţă de principiile unui stat de drept să fie fără echivoc.

În ceea ce priveşte *obiceiurile şi tradiţiile,* forţele de ordine publică şi siguranţă naţională adoptă obiceiurile şi tradiţiile general acceptate, bazate pe activităţile specifice sistemului. Acestea servesc la a-i inspira pentru a atinge obiectivele stabilite ale instituţiei de aplicare a legii.

Obiceiurile sunt definite ca fiind practicile sociale general stabilite şi adoptate, desfăşurate ca urmare a unor tradiţii împământenite ce au căpătat forţa unei legi. Tradiţiile includ ansamblul credinţelor, poveştilor, obiceiurilor şi uzanţelor transferate de la o generaţie la alta, ce au efectul unei legi nescrise.

Printre obiceiuri şi tradiţii regăsim disciplina, bunele maniere, camaraderia, curtoazia.

*Disciplina*ce caracterizează sistemul de ordine şi siguranţă naţională se manifestă printr-o supunere instinctivă faţă de ordinele legale şi faţă de acţiunile spontane derulate pentru atingerea obiectivelor instituţionale, caracterizate de norme morale, etice şi legale.Ea este o piatră de temelie în dezvoltarea unei cariere în sistemul de referinţă. În acest sens, forţele de aplicare a legii trebuie să aibă în permanenţă un comportament demn de urmat, respectând regulile şi obligaţiile ce decurg din restricţiile impuse de sistem.

Bunele maniere presupun ca forţele de aplicare a legii să aibă caracter, bună creştere, demnitate în conduită şi onestitate în toate activităţile pe care le desfăşoară.

Camaraderia stă la baza legăturilor dintre forţele de ordine publică şi eficientizează munca în echipă şi colaborarea, fiind astfel extinsă şi la cetăţenii în beneficiul cărora lucrează. Forţele de ordine publică manifestă o puternică implicare şi preocupare unul faţă de celălalt, şi mai ales faţă de comunitate.

Curtoazia este o formă de manifestare a expresiei consideraţiei şi respectului faţă de alţii. Reflectări ale curtoaziei în sistemul de ordine şi siguranţă publică pot fi: salutul adresat celorlalţi lucrători, salutul imnului şi drapelului naţional, adresarea cu gradul/funcţia către alţi lucrători.

3. Principii fundamentale

Termenul de principiu, din lat. principium[3] care înseamnă „început”, poate desemna în raport cu contextul în care este utilizat „bază, temei, punct de plecare” sau „teză

[3]Maria-Tereza Pirău, Introducere în pedagogie,Ed. Risoprint, 2005, p. 87;

fundamentală" ori „un rezultat al generalizării legilor care guvernează realitatea obiectivă, cunoaşterea sau acţiunea". Datorită gradului lor înalt de generalizare, de regulă, principiile nu pot fi demonstrate direct, ci pot fi confirmate prin consecinţele lor. Conceptul de principiu desemnează o normă de maximă generalitate, care generalizează efectele acţiunii unor legi obiective şi reglementează actul educativ.

Aşadar, aplicarea rigidă sau riguroasă a *principiilor fundamentale* în cadrul sistemului de ordine şi siguranţă publică este necesară pentru a evita încălcarea drepturilor omului şi pentru a menţine respectul faţă de profesie. Astfel, forţele de aplicare a legii au atribuţii legate de prevenirea şi combaterea criminalităţii în sensul cel mai larg, dar şi de asigurarea respectării legii.

Legalitatea este principiul care constituie fundament al problematicii gestionate de sistemul naţional de ordine şi siguranţă publică, potrivit căruia toate politicile în domeniu se constituie în strictă consonanţă cu respectarea drepturilor şi libertăţilor fundamentale ale omului, precum şi în conformitate cu supremaţia Constituţiei şi a legilor. Astfel, principiul respectarii drepturilor omuluipresupune garantarea drepturilor şi libertăţilor fundamentale ale omului, în scopul evitării discriminării, a insecurităţii şi excluziunii sociale.

Prioritatea interesului public reprezintă un alt principiu care trebuie aplicat, apărarea intereselor naţionale şi a valorilor, precumşi îndeplinirea obiectivelor naţionale de siguranţă, realizându-se în limitele unei arhitecturi de securitate şi în spiritul unei bune guvernări. Forţele sistemului naţional de ordine publică, în exercitarea funcţiilor, trebuie să acorde prioritate realizării serviciului în folosul comunităţii, aflându-se permanent în slujba cetăţeanului şi fiind prestatoare de servicii în beneficiul acestuia.În acest sens, forţele de ordine şi siguranţă publică caută să menţină cetăţenii aproape, nu prin dreptul la opinie, dar prin demonstrarea în mod constant a imparţialităţii lor, prin oferirea promptă a serviciilor şi prin disponibilitatea lor faţă de toţi cetăţenii, indiferent de statutulfinanciar, social sau de rasă.

Un alt principiu, *transparenţa*, presupune atât accesul cetăţenilor la informaţiile care privesc domeniul ordinii şi siguranţei naţionale, cât şi recunoaşterea şi respectarea drepturilor acestora de a înţelege măsurile şi acţiunile care se derulează în acest domeniu. În acest sens, considerăm oportună informarea, controlul şi participarea cetăţenilor la procesul decizional. Instituţiile cu rol în problematica ordinii şi siguranţei naţionale trebuie să manifeste deschidere faţă de societate, în limitele stabilite de reglementările legale.

Principiul prevenirii, în sensul cel mai larg, presupune identificarea anticipată şi înlăturarea în timp util a premiselor apariţiei oricăror fapte ce ar putea aduce atingere ordinii şi liniştii publice. În plus, forţele de ordine publică admit necesitatea de a se supune strict legii, de a se abţine de la orice abuz de puterea şi autoritatea conferite de lege, precum şi faptul că testul eficienţei acestora constă în absenţa criminalităţii în sensul cel mai larg, prevenirea fiind mai eficientă decât combaterea.

Disponibilitatea şi operativitatea presupun intervenţia forţelor de aplicare a legii în orice situaţie în care se aduce atingere unei valori apărate de lege, respectiv acţiunea, sprijinul sau îndrumarea pe care trebuie să le manifeste în orice moment. Receptarea mesajelor cetăţenilor, precum şi identificarea modalităţilor optime de răspuns la acestea trebuie să fie prompte, iar acţionarea cu celeritate şi eficacitate în prestarea serviciilor în folosul comunităţii, dar şi participarea la acţiuni concrete în beneficiul ţărilor din Uniunea Europeană, trebuie să fie linii directoare în acest domeniu.

Dialogul se bazează pe relaţionarea cu cetăţeanul, pe construirea unei relaţii de încredere cu acesta, prin transparenţă şi comunicare, în conformitate cu principiile toleranţei, respectului şi libertăţii de exprimare. Relaţionarea de tipul instituţii-cetăţeni este unul din instrumentele prin care se poate contribui la dinamizarea şi efervescenţa unui sistem care să vină în întâmpinarea nevoilor de securitate ale cetăţenilor.

Parteneriatul sau cooperarea împotriva criminalităţii, în sensul cel mai larg, sunt de strictă necesitate pentru realizarea unui climat de ordine şi siguranţă publică. Atât cetăţenii, cât şi instituţiile de aplicare a legii, la nivel naţional si internaţional, precum şi alte organizaţii publice sau private, trebuie să-şi aducă aportul la eficientizarea şi întărirea actului de guvernare în acestă zonă, în vederea consolidării interoperabilităţii şi a canalizării resurselor înspre securitatea publică şi cea individuală. Doar printr-un efort conjugat se pot obţine rezultate performante în acest domeniu. Caracterul participativ presupune abordarea integrată a sistemului de ordine şi siguranţă naţională, de tipul structuri-forţe-cetăţeni, în care acestea să fie parteneri în rezolvarea unor probleme de interes comunitar în domeniul de referinţă, inclusiv în situaţii de urgenţă. De asemenea, presupune şi consultarea societăţii civile, în ceea ce priveşte gestionarea problematicii ordinii şi siguranţei naţionale, societatea civilă fiind cea care oferă legitimitate politicii de ordine şi siguranţă naţională. Organizaţiile non-guvernamentale şi alte persoane juridice pot colabora cu instituţiile de aplicare a legii în acţiuni de prevenire şi înlăturare a riscurilor, ameninţărilor şi vulnerabilităţilor la adresa siguranţei naţionale.

Independenţa operaţională vine ca o contrapondere a caracterului participativ, dar nu îl exclude. Independenţa operaţională presupune ca misiunile şi atribuţiile specifice fiecărei instituţii de aplicare a legii să se realizeze potrivit competenţelor stabilite în conformitate cu actele normative şi nivelul ierarhic potrivit, fără imixtiunea ilegală a altor instituţii ori autorităţi. Însă accentuăm faptul că şi participarea celorlalte forţe este absolut necesară, abordând în mod sistemic problematica sistemului de ordine şi siguranţă publică.

Caracterul anticipativ şi activ presupune ca provocările la adresa ordinii şi siguranţei naţionale vor fi abordate şi adecvate cât mai devreme cu putinţă, cu celeritate, în acest sens fiind absolut necesară eficientizarea mijloacelor de identificare a riscurilor viitoare, posibile sau inerente, la adresa sistemului de ordine şi siguranţă naţională, precum şi dezvoltarea capabilităţilor de acţiune preventivă.

Caracterul funcţional este în strânsă legătură cu cel anticipativ, astfel că resursele trebuie corelate cu obiectivele, şi totodată, trebuie să existe planuri concrete de acţiune, respectiv politici sectoriale specifice pentru aducerea la îndeplinire a dezideratului de ordine şi siguranţă naţională. Pentru acest obiectiv, instituţiile cu rol în aplicarea legii trebuie să dezvolte un set de capacităţi puternice, echilibrate şi flexibile pentru a putea gestiona riscurile, ameninţările şi vulnerabilităţile sistemului de ordine şi siguranţă naţională, respectiv trebuie să dispună de forţe, resurse şi mijloace proprii, independente.

Principiul pragmatismului presupune adoptarea şi implementarea de măsuri şi intervenţii fundamentate pe evidenţe ştiinţifice în cadrul sistemului de ordine şi siguranţă publică,şi nu pe decizii ori interese politice.

*Multidisciplinaritatea*generează consolidarea demersurilor şi intervenţiilor statale prin îmbinarea diferitelor perspective disciplinare şi practici profesionale aplicabile domeniului de referinţă.

Principiul continuităţii presupune consolidarea şi optimizarea rezultatelor obţinute din implementarea documentelor de politici publice anterioare sau obţinute până la momentul evaluării ex-post.

*Principiul specificităţii*are în vedere definirea şi implementarea politicilor de răspuns care trebuie să fie canalizate la nevoile şi realităţile specifice fiecărei zone de intervenţie, precum şi implicarea potenţialului local pentru atingerea obiectivelor propuse.

Subsidiaritatea presupune asigurarea luării deciziilor cât mai aproape de cetăţean şi verificarea permanentă a necesităţii întreprinderii acţiunilor specifice realizării obiectivelor strategice, în lumina posibilităţilor existente la nivel naţional, regional sau local.

Corelarea internaţională presupune participarea şi sprijinul pe care România le oferă pentru ducerea la îndeplinire a misiunilor desfăşurate de organisme precum NATO, UE,

ONU, OSCE şi Consiliul Europei. Abordarea multilaterală, multidirecţională şi multiinstituţională a riscurilor şi vulnerabilităţilor la adresa sistemului de ordine şi siguranţă publică este cea mai potrivită, în vederea garantării reciproce a unui nivel rezonabil de siguranţă, ordine şi stabilitate.

Concluzii

Finalmente, principiile enumerate mai sus, ce decurg din documentele ce fundamentează domeniul ordine şi siguranţă publică pot fi sintetizate în: abordarea sistemică şi cuprinzătoare a problematicii ordinii şi sigurantei naţionale; convergenţa dintre politicile domeniului ordine şi siguranţă publică şi politicile de dezvoltare economico-socială; eforturileconcentrate asupra siguranţei cetăţeanului şi securităţii publice; concordanţa dintre concluziile rezultate din evaluarea mediului de securitate, opţiunea politică şi acţiunea strategică.

Analizând acest ansamblu format de principiile fundamentale, valorile esenţiale, pilonii de bază şi elementele ce ţin de conduita profesională şi de standardele etice, prin prisma calităţii de stat membru al U.E. şi N.A.T.O., remarcăm faptul că România împărtăşeşte valori similare celorlalte state membre: demnitatea omului, drepturile şi libertăţile cetăţeanului, legalitatea. Premisa asumării acestor valori fundamentale de către toate instituţiile de aplicare a legii trebuie să fie una efectivă şi tangibilă, vectorul acestora fiind voinţa politică prin care toate cele trei puteri în stat, respectiv puterea executivă, judecătorească şi cea legislativă trebuie să înţeleagă importanţa unei societăţi caracterizate de un sentiment de securitate şi să conlucreze pentru ducerea la îndeplinire a acestui deziderat.

În acest sens, *ansamblul acestor linii directoare*ale sistemului de ordine şi siguranţă publicătrebuie privit ca un vector dinamizant al sistemului, cu multiple avantaje. În primul rând, în urma implementării acestei palete de principii, avem în vedere*creşterea gradului de coordonare a formulării, implementării şi evaluării documentelor programatice ce definesc domeniul ordine şi siguranţă publică.* În al doilea rând, subliniem o *creştere semnificativă a predictibilităţii impactului documentelor programatice implementate,dar şi de ameliorarea calităţii politicilor guvernamentale în domeniu printr-un plus de coordonare interinstituţională* şi implicare a tuturor actorilor sociali. Totodată, constituie avantaje atât*creşterea eficienţei documentelor strategice în domeniul ordine şi siguranţă publică* prin rezultate concrete şi identificarea disfuncţiilor ce ar putea afecta aceste rezultate, cât şi creşterea gradului de implicare a cetăţenilor şi a societăţii civile în procesele de luare a deciziilor în acest domeniu.

Ansamblul de principii mai sus evidenţiate au menirea *de a informa decidenţii politici cu privire la necesitatea şi utilitatea parcurgerii, transpunerii şi implementării lor în practică*, dar şi reprezentanţii autorităţilor publice, societăţii civile ori organizaţiilor nonguvernamentalece pot fi cooptaţi în dinamizarea şi eficientizarea segmentului de ordine şi siguranţă publică, astfel încât siguranţa cetăţeanului, în context larg, să nu mai reprezinte o problemă.

Setul acesta de principii trebuie aplicat şi transpus. În acest sens, sunt necesare creşterea responsabilităţii decidenţilor autorităţilor ori instituţiilor publice cu privire la propriile acţiuni şi crearea unui cadru prin care să fie posibilă implicarea societăţii civile şi implicit,*creştereatransparenţei actului guvernării.* Totodată, transpunerea aplicată a acestor principii duce la creşterea eficienţei şi calităţii activităţilor desfăşurate în administraţia publică centrală pe segmentul ordine şi siguranţă publică.

Sistemul naţional de ordine şi siguranţă publică este unul dintre cele mai importante componente ale statului de dreptşi presupune prestarea unui serviciu public de bază pentru populaţie, cu finalitate în asigurarea securităţii şi siguranţei cetăţeanului. În vederea realizării

unei radiografii eficiente a sistemului de ordine şi siguranţă publică astfel încât să se asigure un climat de securitate este necesară o abordare holistică a elementelor sale componente şi tangenţiale. Printr-o fundamentare corectă, pot fi furnizate elemente de esenţă pentru *elaborarea, de către factorii de decizie, a unui model naţional unic de abordare a diverselor documente programatice* pe segmentul ordinii şi siguranţei publice, cu aplicabilitate pe diverse paliere ale vieţii sociale, în vederea unei mai bune canalizări a resurselor instituţionale, legislative, informaţionale şi mai ales umane.

Sistemul de ordine şi siguranţă publică trebuie să corespundă celor mai noi provocări[4] strategice şi de mediu, atât la nivel naţional, cât şi la nivel internaţional, iar în contextul evoluţiei factorilor interni şi externi, o coordonată majoră şi permanentă a politicii de securitate vizează reducerea influenţei riscurilor, vulnerabilităţilor şi ameninţărilor la adresa ordinii şi siguranţei publice, ca parte integrantă a securităţii naţionale, prin perfecţionarea mecanismelor instituţionale specifice.În acest context, rezultatele aplicării acestor elemente esenţiale de doctrină ar putea fi concretizate într-o *modificare pozitivă a mentalităţii factorilor de decizie din domeniu,* cu privire la modalitatea de abordare şi de legiferare a viitoarelor documente de politici publiceşi instituţionale incidente ordinii publice,pentru o mai bună gestionare a domeniului, darşi pentru furnizarea premiselor unei eficienţe sporite în materie.

BIBLIOGRAFIE:

1. Hotărârea nr. 30/2008 privind aprobarea Strategiei Naţionale de Apărare a Ţării publicată în Monitorul Oficial al României nr. 799/28.11.2008;
2. Hotărârea Guvernului nr. 1040/2010 pentru aprobarea Strategiei Naţionale de Ordine Publică 2010-2013, publicată în Monitorul Oficial al României nr. 721/28.10.2010;
3. Hotărârea Guvernului nr. 784/2013 privind aprobarea Strategiei Naţionale Antidrog 2013-2020, publicată în Monitorul Oficial al României nr. 702 bis/15.11.2013;
4. Hotărârea nr. 498/2011 pentru aprobarea Strategiei nationale privind imigratia pentru perioada 2011-2014, publicată în Monitorul Oficial al României nr. 391/03.06.2011;
5. Hotărârea Guvernului nr. 1156/2012 privind aprobarea Strategiei nationale pentru prevenirea şi combaterea fenomenului violentei in familie pentru perioada 2013-2017, publicată în Monitorul Oficial al României nr. 819/06.12.2012;
6. Hotărârea Guvernului nr. 215/2012 privind aprobarea Strategiei naţionale anticorupţie pe perioada 2012-2015, publicată în Monitorul Oficial al României nr. 202/27.03.2012;
7. Hotărârea Guvernului nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României, publicată în Monitorul Oficial al Românieinr. 296/23.05.2015;
8. Hotărârea Guvernului nr. 775/2005 pentru aprobarea Regulamentului privind procedurile de elaborare, monitorizare şi evaluare a politicilor publice la nivel central, publicată în Monitorul Oficial al României nr. 1163/22.12.2005;
9. Maria-Tereza Pirău, Introducere în pedagogie, Ed. Risoprint, Bucureşti 2005;
10. http://www.mai.gov.ro/index00_1.html (Programul de guvernare al Ministerului Afacerilor Interne).

[4]Strategia Europeană de Securitate – O Europă sigură într-o lume mai bună notează ca şi provocări globale: proliferarea armelor de distrugere în masă, terorismul, conflictele regionale, criminalitatea organizată, eşecul statal.

11. Constituţia României din 21 noiembrie 1991, republicată în Monitorul Oficial nr. 767/31.10.2003;
12. Strategia Europeană de Securitate, Bruxelles, 12 decembrie 2003;
13. Hotărârea nr. 62 din 17 aprilie 2006 privind Strategia de Securitate Naţională a Romaniei, adoptată de către Consiliul Suprem de Apărare a Ţării.

Această lucrare este elaborată şi publicată sub auspiciile Institutului de Cercetare a Calităţii Vieţii, Academia Română ca parte din proiectul co-finanţat de Uniunea Europeană prin Programului Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013 în cadrul proiectului Pluri şi interdisciplinaritate în programe doctorale şi postdoctorale Cod ProiectPOSDRU/159/1.5/S/141086.

IMPORTANŢA GÂNDIRII CRITICE ÎN IMBUNĂTĂŢIREA EVALUĂRILOR REALIZATE DE SERVICIILE DE INFORMAŢII

Giorgiana-Raluca STOICA
Doctorand la Academia Naţională de Informaţii "Mihai Viteazul" în domeniul "Informaţii şi Securitate Naţională", e-mail: ralluca.stoica@gmail.com

Maria-Cristina MURARU
Doctorand la Academia Naţională de Informaţii "Mihai Viteazul" în domeniul "Informaţii şi Securitate Naţională", e-mail: cristina.muraru@gmail.com

Rezumat: *În ultimii ani, cercetările în domeniul securitar au indicat că problemele legate de terorism de pe scena internaţională au fost determinate de erori ale analizei de intelligence, din cauza incapacităţii de a anticipa riscuri, în pofida semnalelor existente, sau a eşecului analizei predictive. Putem include în această categorie atacurile teroriste împotriva SUA, Spaniei, Federaţiei Ruse şi, mai recent, cele din Franţa.*

Utilizarea gândirii critice în analiza de intelligence vizează evitarea unor astfel de eşecuri atât prin îmbunătăţirea metodelor de argumentare ale analiştilor, îndeosebi depăşirea şi corectarea eşecurilor din sfera cognitivă, cât şi prin obţinerea unor rezultate cuantificabile necesare anticipării viitoarelor direcţii de acţiune.

Cuvinte cheie: *intelligence, analiză, eroare, eşec, gândire critică*

Introducere

Procesul informaţional din secolul XXI, în contextul unei lumi globalizate, implică nesiguranţă şi riscuri, precum şi necesitatea receptării rapide şi validării unui număr semnificativ de date, situaţie care presupune adaptarea analiştilor din serviciile de informaţii, inclusiv la nivel cognitiv. Întrebările pe care un analist le formulează nu reprezintă doar instrumente de atragere a dovezilor existente, ci şi o sursă generatoare de noi date, care, sprijinite de cele obţinute în plan tehnologic, conduc la identificarea de noi informaţii prin care sunt prevenite „surprizele strategice".

Raţionamentul necesar pentru o bună analiză a informaţiilor intră în contradicţie cu modul în care oamenii, inclusiv analiştii gândesc în mod firesc.

De obicei, se confirmă ipotezele iniţiale ale unei situaţii, utilizându-se în mod selectiv dovezile, chiar dacă există semnale demne de luat în considerare, conform cărora o ipoteză alternativă poate fi, de fapt, corectă.

Astfel, din inerţie, se adoptă o gândire deficitară, element întâlnit frecvent la majoritatea erorilor în procesul de intelligence.

Cum pot evita analiştii acest tip de gândire deficitară? Gândirea critică reprezintă un răspuns la această întrebare, analiştii care o adoptă îmbunătăţindu-şi propriile analize prin identificarea lacunelor şi utilizarea mijloacelor de raţionament reflexiv.

1. Abordări conceptuale

Gândirea critică este o acţiune intenţionată atât cognitivă (gândire), cât şi meta-cognitivă (gândirea despre gândire), prin intermediul căreia o persoană reflectă la calitatea procesului de raţionare concomitent cu identificarea unei soluţii plauzibile. Gânditorul are

două scopuri la fel de importante: identificarea unei soluţii şi îmbunătăţirea modului în care acesta raţionează[1].

Cu alte cuvinte, gândirea critică presupune folosirea acelor abilităţi cognitive sau strategii care argumentează probabilitatea unui rezultat dezirabil. Este un termen folosit pentru a descrie actul de gândire intenţional, raţional şi direcţionat către un scop – implicat în rezolvarea de probleme, formularea unor interferenţe, calculul sau luarea deciziilor atunci când cel care gândeşte foloseşte abilităţi selectate special, eficiente pentru contextul particular în care se găseşte şi pentru tipul de sarcină pe care o are de rezolvat. Acest mecanism implică, de asemenea, evaluarea procesului de gândire – raţionamentul care a condus la luarea unei anumite decizii sau tipul de factori care au fost luaţi în considerare. Gândirea critică este uneori numită şi „gândire direcţionată", deoarece este îndreptată spre obţinerea unui anumit rezultat.

Analiza semnifică tratarea informaţiilor prin folosirea metodelor de analiză logice, analogice, sistemice şi ale comunicării, în scopul stabilirii adevărului, incertului sau falsului ori identificării şi caracterizării disfuncţiilor, vulnerabilităţilor şi factorilor de risc ce pot constitui ameninţări.

Ca produs, este apanajul analistului de informaţii şi se realizează în cadrul unui proces de gândire cu valenţe preponderent critice, prin utilizarea unor metode şi tehnici specifice, pentru a stabili relaţia cauză-efect între disfuncţii, vulnerabilităţi, factori de risc şi ameninţări la adresa securităţii naţionale. Analiştii de intelligence sunt implicaţi în colectarea, evaluarea, analiza şi diseminarea informaţiilor de interes în domeniul securităţii naţionale. Fiecare analist de informaţii îşi construieşte propria versiune a „realităţii", în funcţie de experienţă, valori culturale, precum şi de specificul informaţiilor.

2. Procesul de realizare a gândirii critice

Pentru a adopta gândirea critică, persoana care raţionează are nevoie de 8 „elemente ajutătoare" (*elements of thought*) ale raţionamentului - scopul, subiectul în discuţie (problema), informaţia (faptele, observaţiile, experienţele), interpretarea (concluzii, soluţii), conceptele (teorii, axiome, principii, modele), ipotezele (supoziţii), implicaţiile şi consecinţele, punctele de vedere (perspective), care conduc la ridicarea unor întrebări clare referitoare la subiectul în cauză, precum şi la procesul de gândire[2].

Studiile în domeniu au relevat că oamenii gândesc întotdeauna cu un scop, gândire care presupune un punct de vedere şi este modelată de presupuneri conştiente şi inconştiente. Procesul gândirii implică ajungerea la concluzii care decurg din nevoia de a răspunde la nişte întrebări şi a soluţiona probleme, în baza datelor de care dispun. Raţionamentele conduc la decizii şi consecinţe.

Există 6 etape specifice procesului de gândire critică, respectiv interpretarea, analiza, evaluarea, deducţia, explicaţia şi autoreglarea[3].

Interpretarea se referă la înţelegerea şi exprimarea semnificaţiei situaţiilor, datelor, evenimentelor şi opiniilor.

Analiza presupune identificarea, prin deducţie, a relaţiei dintre anumite afirmaţii, întrebări, concepte.

---

[1]David T. MORE, *Critical Thinking and Intelligence Analysis,* Washington, National Defense Intelligence College, 2007, p. 8

[2]Richard PAUL, Linda ELDER, *Mini-guide de la Pensee Critique Concepts et instruments,* Foundation for Critical Thinking Press, 2008, pp. 1-17

[3]Peter A. FACIONE, *Critical Thinking: What It Is and Why It Counts, Academis Press,* 1998,articol disponibil la http://insightassessment.com/pdf_files/what&why98.pdf, accesat la data de 19.03.2015

Evaluarea constă în aprecierea credibilităţii unor afirmaţii şi a logicii relaţiilor dintre declaraţii şi evenimente.

Deducţia constă în identificarea elementelor necesare emiterii de ipoteze şi concluzii rezonabile, precum şi semnalarea posibilelor consecinţe.

Explicaţia se referă la prezentarea rezultatelor raţionamentelor, cu relevarea argumentelor care le susţin.

Autoreglarea vizează monitorizarea conştientă a propriilor activităţi şi a rezultatelor acestora, având ca scop validarea sau corectarea, după caz a raţionamentelor.

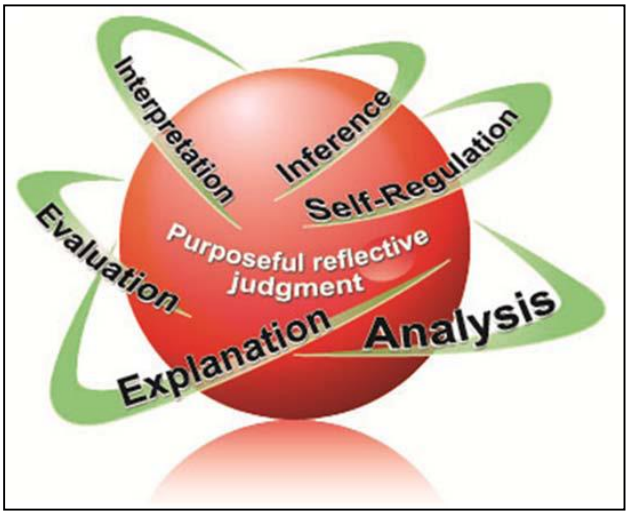


Figura nr. 1. Procesul gândirii critice

3. Utilizarea gândirii critice în procesul de analiză a informaţiilor

3.1. Cadru optim pentru formularea unor concluzii pertinente

Surprizele şi evenimentele dificil de anticipat reprezintă o constantă în istoria tuturor naţiunilor. Acestea nu sunt cauzate neapărat de lipsa de informaţii, ci de natura evenimentelor sau de apariţia bias-urilor cognitive. Astfel, pe de-o parte, tendinţele generale sunt mult mai uşor de anticipat faţă de evenimentele singulare (tendinţe versus fenomene), în timp ce, pe de altă parte, pot apărea dificultăţi în a face diferenţa între ce este adevărat şi ce reprezintă o încercare de inducere în eroare, sau în îndepărtarea analistului de ideile predefinite.

Pentru a reduce riscul situaţiilor neprevăzute într-o lume în continuă schimbare, analiştii de intelligence, mai mult ca oricare altă categorie de analişti, trebuie să dezvolte deprinderi de utilizare a instrumentelor analitice, care să îi ajute să îşi dea seama când vechile idei predefinite nu se mai pot aplica. În analiza de intelligence, gândirea critică oferă aparatul intelectual necesar reflecţiei.

Volumul semnificativ de informaţii din mediul virtual, coroborat cu riscul ridicat de manipulare prin intermediul surselor deschise, impun un calcul introspectiv privind modul de tratare a informaţiei şi de judecată a felului în care este gândită analiza.

Analistul poate aplica mai multe metode de analiză şi verifica care dintre acestea aduce cel mai bun rezultat sau poate compara rezultatele şi, în cazul în care apar diferenţe între acestea, să identifice de unde provin.

În emiterea de concluzii, analistul trebuie să-şi pună următoarele întrebări: ”Deducţiile mele decurg din datele pe care le am la dispoziţie?”, ”Sunt concluziile mele logice?”. De multe ori, concluziile la care se ajunge ar putea genera noi căutări de date şi releva scenarii conexe.

Procesul de elaborare a analizei informaţiilor necesită un efort intelectual prin care se diferenţiază datele în funcţie de gradul de importanţă, iar ulterior, printr-o evaluare individuală susţinută de exerciţiul judecăţii, se generează o concluzie pertinentă.

Exerciţiul judecăţii presupune utilizarea a trei procedee – inducţie, deducţie şi abducţie[4] - prin care se creează o conexiune obiectivă între convingerile analistului şi informaţiile care sugerează un trend diferit faţă de cel identificat anterior.

Raţionamentul inductiv determină, în spectru larg, o serie de rezultate sau acţiuni viitoare posibile. Este esenţial pentru emiterea unor avertismente/ prognoze, prin identificarea tendinţei unui anumit aspect. Astfel, în baza unor percepţii/ evenimente anterioare, acţiunile derulate în prezent ar putea indica un probabil trend, nefiind însă obligatoriu ca acesta să se şi materializeze.

Pe de altă parte, în particular, raţionamentul deductiv presupune identificare elementelor necesare emiterii de ipoteze şi ajungerii la o concluzie rezonabilă, precum şi semnalarea posibilelor consecinţe.

Raţionamentul abductiv reprezintă o alternanţă între inducţie şi deducţie, scopul fiind identificarea unor ipoteze. Astfel, dacă în cazul inductiei ne sunt date concluzia şi premisa minoră, fiind necesar de stabilit cea majoră, iar în deducţie sunt furnizate cele doua premise, fiind nevoie de o concluzia, abducţia constă în întemeierea premisei minore când sunt date premisa majoră şi concluzia[5].

Altfel spus, în timp ce raţionamentul inductiv dezvăluie „că ceva este probabil adevărat", raţionamentul deductiv certifică că „ceva este neapărat adevărat". Cu toate acestea, ambele metode sunt limitate, existând riscul ca raţionamentul inductiv să genereze soluţii multiple cu acelaşi grad de probabilitate, iar cel deductiv poate fi afectat de procesul de manipulare. În această situaţie, raţionamentul abductiv, care demonstrează că „ceva este în mod plauzibil adevărat", poate compensa limitarea celorlalte două procedee.

În pofida limitelor individuale, coroborarea celor trei procedee oferă o modalitate de examinare detaliată a informaţiilor în scopul elaborării unor concluzii pertinente. Gândirea critică furnizează acest cadru prin asigurarea faptului că fiecare formă de raţionament este utilizată în mod corespunzător. Acest procedeu se extinde la întregul proces de analiză a informaţiilor.

3.2. Răspuns la problema erorii

Analiştii de intelligence se confruntă în mod constant cu date incomplete şi neclare, cu surse contradictorii, precum şi cu încercările intenţionate de inducere în eroare (*denial and deception*) din partea regimurilor autoritare ale unor state, care resping accesul la date de interes (*precum programele de dezvoltare militară*). Literatura de specialitate denumeşte utilizarea, de către Rusia, a tehnicii de inducere în eroare, cu termenul „maskirovka"[6].

În scopul îmbunătăţirii gândirii analiştilor, precum şi pentru a evita tehnicile de inducere în eroare, este necesară schimbarea modului de gestionare a datelor de care aceştia dispun şi stabilirea metodei de analiză care poate genera o soluţie la problema cercetată. Astfel, în selectarea şi evaluarea datelor, analistul ar trebui să se ghideze după întrebările: „Care este şansa de a fi indus în eroare?", „De ce se întâmplă acest lucru?", „De ce este această sursă credibilă?", „Dacă scenariul opus este într-adevăr cel adevărat, ce date în sprijinul acestuia ar trebui să iau în considerare?", „Care îmi sunt ideile predefinite?".

---

[4]William MILLWARD, *Life in and aut of Hut 3, in F.H. HINSLEY and Alan STRIPP: The Codebreakers: The Inside Story of Bletchley Park,* Oxford University Press, 1993, p. 17

[5]Ioan Bus, *Argumente transcendentale şi inferenţa abductivă, 2003*, p. 45, articol disponibil la http://www.roslir.goldenideashome.com/archiv/2003_3-4/12IonBus2003.pdf, accesat la data de 24.04.2015

[6]David T. MORE, *Critical Thinking and Intelligence Analysis,* Washington, National Defense Intelligence College, 2007, p. 25

Criteriile în funcţie de care ar trebui evaluată credibilitatea datelor sunt autenticitate, acurateţe şi flexibilitate. Autenticitatea nu este totuşi absolută, ci este dependentă de vremuri şi context, în vreme ce flexibilitatea poate fi probată prin obţinerea aceloraşi date din surse diferite de culegere.

Gândirea critică se concentrează, de fapt, în procesul de elaborare de concluzii adevărate şi întemeiate (creare de cunoaştere). Cele patru probleme[7] ce reies din procesul de gândire în intelligence sunt insuficienţa, irelevanţa, indeterminarea şi utilitatea.

Insuficienţa rezultă din relaţia dintre date şi cunoaştere în reţeaua analitică. Marea majoritate a cunoştinţelor produse de analişti se bazează, în cele din urmă, pe date colectate, dar care se dovedesc insuficiente din cel puţin două puncte de vedere: sunt limitate ca scop şi nu acoperă, în consecinţă, toate aspectele pe care analistul trebuie să le evalueze; sunt limitate ca încredere, odată ce consistă doar în fapte afirmate (în speţă, unele care se pot dovedi false). În concluzie, profesionistul în *intelligence* nu are altă alternativă decât să se bazeze pe informaţii incomplete şi uneori inexacte şi ar trebui, astfel, să presupună că multe dintre datele relevante îi lipsesc, în timp ce, din cele avute la dispoziţie, unele sunt eronate sau induc în eroare.

Irelevanţa derivă din relaţia dintre informaţie şi cunoaştere în reţeaua analitică. Cunoaşterea pe care specialistul o deduce provine din informaţii la care are acces, dar care conţine mult mai mult decât ce era necesar pentru elaborarea de produse. Cea mai mare parte a informaţiilor se poate chiar dovedi irelevantă pentru soluţionarea problemei. Practicianul nu trebuie să presupună niciodată că informaţia pe care o deţine este relevantă pentru problema pe care o evaluează, ci că „cea mai mare parte" este, în pofida aparenţelor, irelevantă.

Indeterminarea este generată de legătura dintre cunoaştere şi întreaga reţea analitică şi lumea întreagă (evenimentele care sunt analizate). Cele mai multe dintre evenimentele pe care analistul încearcă să le înţeleagă şi mai ales să le anticipeze nu sunt inevitabile (nu pot fi dobândite toate informaţiile necesare pentru proiectarea lor). În schimb, chiar dacă ar şti tot ce se poate şti despre un terorist, de exemplu, tot nu ar putea determina cu certitudine ce va face acesta. Deciziile şi acţiunile agenţilor umani, dar şi unele procese naturale, nu pot fi determinate (nu reprezintă consecinţe inevitabile ale unor factori cauzali anteriori, ci doar un posibil deznodământ din multe probabil să se producă). Un singur set de evenimente viitoare se poate întâmpla, însă nu se poate spune că numai unul are „şanse reale" în acest sens. Analistul nu poate niciodată să presupună că lucrurile vor evolua într-un singur mod, ci că o serie de „viitoruri" diferite, incompatibile ar putea avea loc. Trebuie să determine ce ar fi dacă fiecare dintre aceste alternative s-ar întâmpla.

Utilitatea derivă din relaţia dintre înţelegere şi cunoaştere. Prin analiză se obţin cunoştinţe nu în interes propriu, ci pentru a face faţă „provocărilor" lansate de beneficiari, ceea ce creează constrângeri suplimentare în ceea ce priveşte „dobândirea de cunoaştere". Totodată, nu se poate stabili o perioadă de timp corespunzătoare pentru a desfăşura activitatea de analiză şi nici nu se poate presupune că factorul de decizie este doar un observator obiectiv, fără scopuri.

Gândirea critică poate diminua anumite cauze comune ale eşecurilor şi poate oferi mijloacele prin care acestea pot fi evitate, pe viitor. In mod specific, orice proces informativ bazat pe acest tip de gândire poate compensa următoarele eşecuri, atunci când:

Analiştii se înşeală. Nu este realist să ne aşteptăm ca analiştii să nu se înşele niciodată. Indiferent de procesele folosite, analiştii comit erori. Antropologul Rob Johnston defineşte astfel erorile „inadvertenţe reale în procesul de analiză ca urmare a lipsei de date sau a

[7]Noel HENDRICKSON, *Critical Thinking in Intelligence Analysis,* Londra, International Journal of Intelligence and CounterIntelligence, *vol. 21, no.4, 2008, pp. 679-693*

informaţiilor incomplete”[8]. La fel, eşecurile informative sunt „surprize sistemice organizaţionale care rezultă din ipoteze incorecte, incomplete sau inadecvate”. Gândirea critică reduce asemenea tipuri de erori, furnizând mijloacele de evaluare a erorilor de raţionament în momentul în care acestea au loc, ca şi înainte de a deveni eşecuri sistemice. O asemenea abordare meta-cognitivă a procesului analitic facilitează monitorizarea la cele mai înalte nivele a acestuia. Cercetările în domeniu au relevat că sursa cea mai importantă a eşecurilor în intelligence, care este şi cea mai dificil de remediat, constă în limitarea cognitivă[9]. Potrivit psihologiei cognitive, oamenii nu reuşesc să conştientizeze mecanismul mental prin care se formează percepţiile. Acesta este mai degrabă un proces activ decât pasiv, în care realitatea este construită, nu receptată, în baza datelor furnizate de simţuri. Ceea ce oamenii percep este influenţat de experienţă, educaţie, valori culturale şi norme organizaţionale. De regulă, persoanele tind să perceapă ceea ce se aşteaptă să perceapă. Evenimentele percepute în conformitate cu aşteptările sunt procesate mai rapid, în vreme ce acelea care sunt în contradicţie cu aşteptările tind să fie ignorate sau distorsionate în subconştient. Odată dezvoltată, predilecţia cognitivă condiţionează percepţiile viitoare ale unui fenomen. În acest fel, informaţia nouă este asimilată imaginilor deja existente[10]. Interpretarea iniţială este menţinută până când contradicţia devine atât de evidentă încât obligă la o schimbare de percepţie. Predilecţiile cognitive sunt definite aşadar ca erori mentale cauzate de strategiile simplificate de prelucrare a informaţiei. Principalele caracteristici ale predilecţiile cognitive sunt că se formează repede şi sunt rezistente la schimbare, datele noi sunt integrate în cadrul conceptual existent, impresia iniţială, bazată pe date incomplete sau inexacte va persista chiar şi după intrarea, de către analist, în posesia de noi date.

Factorii de decizie ignoră informaţiile. Pe de o parte, informaţiile trebuie să fie convingătoare şi să oblige factorii de decizie să acorde atenţie conţinutului. Pe de altă parte, informaţia nu ar trebui să indice factorilor de decizie ce au de făcut.

Adversarii neagă şi înşeală. Gândirea critică reduce efectele negărilor şi ale afirmaţiilor false ale adversarilor determinând analiştii să ia în calcul toate posibilităţile, să pună sub semnul întrebării presupunerile şi prejudecăţile, să examineze în mod sistematic autenticitatea dovezilor analizate şi să ia în serios anomaliile care apar.

Adversarul este mai capabil. In orice sistem în care există un adversar, există câştigători şi învinşi. Chiar dacă analiştii pot face tot posibilul pentru a se asigura că activitatea lor este corectă, aceştia folosesc rareori toate dovezile de care dispun şi se pot lăsa astfel înşelaţi. In asemenea cazuri, ei pot trage concluzii greşite. Totuşi, gândirea critică, furnizând structură şi control raţionamentului, poate funcţiona ca un organism de audit. In acest caz, mijloacele prin care se ajunge la concluzii analitice pot fi periodic revizuite, erorile şi afirmaţiile false pot fi descoperite şi se pot adopta măsuri pentru a îmbunătăţi procesul, astfel încât erorile să nu se mai repete. Intr-adevăr, din cauza accentului pus pe proces, gândirea critică devine un instrument serios în evaluarea şi îmbunătăţirea raţionamentului analitic[11].

---

[8]Rob JOHNSTON,*Analytic Culture in the U.S. Intelligence Community,* Central Intelligence Agency, Washington, 2005, p. 6, carte disponibilă la https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf, accesată la data de 24.03.2014

[9]Richard J. HEUER Jr., *Limits of Intelligence Analysis, Orbis, 2005*, pp. 75-94, carte disponibilă la http://www.worldaffairsboard.com/attachments/staff-college/20727d1273228985-ebo-sod-limits-intelligence-analysis-fpri-winter-2005-heurer-.pdf, accesată la data de 19.03.2015

[10]Magdalena A. DUVENAGE, *Intelligence Analysis in the Knowledge Age. An Analysis of the Challenges facing the Practice of Intelligence Analysis,* Stellenbosch University, 2010, p. 102, disponibil la http://hdl.handle.net/10019.1/46428, accesat la 24.03.2015

[11]David T. MORE, *Critical Thinking and Intelligence Analysis,* Washington, National Defense Intelligence College, 2007, pp. 79-80

3.3. Exemple de eşecuri analitice

Majoritatea eşecurilor în analiza de intelligence este generată de greşeli de interpretare, nu de erori de colectare - informaţia disponibilă a fost ignorată sau respinsă, întrucât nu se potrivea modelului mental al analistului.

Relevante din acest punct de vedere sunt concluziile emise anterior intervenţiei trupelor coaliţiei în Irak, în anul 2003 sau cele referitoare la stoparea programului nuclear american din 2008.

În cazul intervenţiei în Irak, un raport al Senatului american a relevat că „indiciile incerte au fost folosite ca dovezi, iar informaţiile care contraziceau tabloul de ansamblu au fost ignorate". În această situaţie, serviciile de intelligence au căutat acele date care corespundeau aşteptărilor decidentului politic[12]. Astfel, golul informaţional a fost umplut de modelul mental al analistului. Chiar şi în situaţia în care comunitatea de informaţii din SUA ar fi dispus de surse credibile apropiate Puterii de la Bagdad, este de aşteptat că ar fi pus la îndoială informaţiile obţinute, calificându-le drept încercare de înşelare.

Centrul Francez de Studii de Intelligence a catalogat Raportul prezentat de Direcţia Naţională de Intelligence în anul 2007, în care 16 agenţii de informaţii americane au susţinut că Iranul a stopat programul nuclear încă din 2003, drept o eroare de intelligence[13], deoarece s-a demonstrat că nici în prezent statul iranian nu a întreprins demersuri în acest sens, ci, dimpotrivă, este suspectat în continuare de construirea armelor nucleare.

Se poate aprecia că prejudecăţile şi mentalitatea analiştilor, precum şi falsele supoziţii ale acestora i-au împiedicat să identifice să identifice intenţiile reale ale Iranului, concluziile raportului având la bază interceptări telefonice în care autorităţile iraniene criticau stoparea programului militar. Totuşi, specialiştii americani nu au luat în calcul riscul unei manipulări din partea autorităţilor iraniene.

De asemenea, atacurile teroriste înregistrate la nivel mondial (printre care cele înregistrate la 11 septembrie 2001- Statele Unite ale Americii, 11.04.2003 - Spania, 6 februarie, 31 august 2004, 27 noiembrie 2009 - Federaţia Rusă), în ultimii ani, ar putea fi considerate erori ale analizei de intelligence, prin prisma faptului că organizaţiile de profil nu au putut anticipa riscul producerii unor asemenea evenimente.

Atât experţii în domeniul, cât şi mass-media au avansat posibilitatea ca producerea ultimelor atentate teroriste de o mai mare anvergură, -cel din Boston din luna aprilie 2013, precum şi cel petrecut în Franţa la începutul acestui an-, să fi fost favorizată de apariţia unei erori în analiza de intelligence a serviciilor de informaţii din cele două state vizate, care nu au putut anticipa riscul[14].

Se pare că Tamerlan Ţarnaev, principalul vinovat de producerea atentatului din Boston, a fost pierdut din atenţia serviciilor de informaţii odată cu plecare acestuia în Rusia, în 2012, reîntoarcerea ulterioară pe teritoriul SUA fiind trecută cu vederea, din cauza unei erori umane.

O abordare similară a fost avansată şi în Franţa, unde serviciile franceze de informaţii fuseseră avertizate la sfârşitul anului 2014 de omologii algerieni, de iminenta producere a unor atentate teroriste. Cherif şi Said Kouachi, cei doi fraţi care au comis atacul asupra sediului publicaţiei satirice Charlie Hebdo, Amedy Coulibaly, cel care a luat ostatici persoane

---

[12]Richard J. HEUER Jr., *Limits of Intelligence Analysis, Orbis, 2005, pp. 75-94,* carte disponibilă la http://www.worldaffairsboard.com/attachments/staff-college/20727d1273228985-ebo-sod-limits-intelligence-analysis-fpri-winter-2005-heurer-.pdf, accesată la data de 19.03.2015

[13]Alain RODIER, *„Pourquoi les americains ont plie devant les iraniens",* Centrul Francez de Studii de Intelligence, notă de actualitate nr.111, 2007, articol disponibil la http://www.cf2r.org/fr/notes-actualite/pourquoi-les-americains-ont-plie-devant-les-iraniens.php, accesat la 17.03.2015

[14]Christopher DICKEY, *The Boston Bombing Intelligence Failure, 16.04.2013,* articol disponibi la http://www.thedailybeast.com/articles/2013/04/16/the-boston-bombing-intelligence-failure.html, accesat la 18.03.2015,

dintr-un magazin şi prietena sa, Hayat Boumeddiene, toţi cei patru erau conectaţi atât între între ei, cât şi la o reţea extinsă de extremişti din Europa[15]. În plus, cele două persoane resposabile de atacul asupra sediului publicaţiei satirice Charlie Hebdo, s-ar fi aflat în atenţia serviciilor de informaţiile, mai ales că, una dintre ele a făcut închisoare acum 10 ani fiind suspectat de conexiuni cu mediul jihadist. Totuşi, supravegherea de către autorităţi a celor doi fraţi a încetat la jumătatea anului 2014, decizie care ar putea fi considerată o eroare de intelligence.

Concluzii

Gândirea critică nu este o gândire perfectă, pentru că şi cel care gândeşte critic face greşeli. Însă procesul de autoobservare şi autocorectare prin care trece mereu cel care o practică îl face să comită mai puţine greşeli decât cei care nu gândesc critic.

Astfel, în final gândirea critică este autodirijată, autodisciplinată, autocontrolată şi autocorectoare, ceea ce presupune criterii stricte de excelenţă şi o utilizare atentă a acesteia.

Utilizarea gândirii critice conduce la creşterea abilităţii de comunicare efectivă în scopul rezolvării problemelor.

Fără gândirea critică, oamenii ar fi mai uşor de exploatat, fiind de neimaginat, spre exemplu, un sistem economic sau juridic care să nu aplice gândirea critică, deoarece absenţa gândirii critice ar face imposibil de interpretat trendurile pieţei. Utilizara gândirii crtice de către o societate informată este o condiţie necesară pentru succesul instituţiilor democratice.

În activitatea de intelligence, gândirea critică are un rol extrem de benefic, acest mecanism cognitiv conducând la atenuarea erorilor inerente procesului analitic, generate de ideile predefinite; reevaluarea, de către factorii de decizie, a propriilor percepţii şi evaluări pe anumite subiecte; limitarea riscului inducerii voluntare în eroare a analiştilor de către adversari; transparentizarea mecanismului de gândire, astfel încât toate etapele raţionamentului să fie explicitate şi uşor de urmărit şi revizuit.

În acest fel, atât ofiţerii de intelligence cât şi beneficiarii informaţiilor nu se vor mai axa pe rezultatul analizei, ci pe procesul elaborării acesteia**,** fapt care va genera o realizare mai eficientă a evaluărilor realizate de specialişti.

BIBLIOGRAFIE:

1. BUS, Ioan, *Argumente transcendentale şi inferenţa abductivă, 2003*, p. 45, articol disponibil la http://www.roslir.goldenideashome.com/archiv/2003_3-4/12IonBus 2003.pdf
2. DICKEY, Christopher, *The Boston Bombing Intelligence Failure*, The Daily Beast, 16.04.2013, articol disponibil la http://www.thedailybeast.com/articles/2013/04/16/the-boston-bombing-intelligence-failure.html
3. DUVENAGE, Magdalena, A., *Intelligence Analysis in the Knowledge Age. An Analysis of the Challenges facing the Practice of Intelligence Analysis*, Stellenbosch University, 2010, articol disponibil la http://hdl.handle.net/10019.1/46428

[15]Shashank JOSHI,*Charlie Hebdo attack: A French intelligence failure?,* 10.01.2015, articol disponibil la http://www.bbc.com/news/world-europe-30760656, accesat la data de 26.03.2015

4. FACIONE, Peter, A., *Critical Thinking: What It Is and Why It Counts*, Academis Press, 1998, articol disponibil la http://insightassessment.com/pdf_files/what&why98.pdf
5. HENDRICKSON, Noel, *Critical Thinking in Intelligence Analysis*, Londra, International Journal of Intelligence and CounterIntelligence, vol. 21, no.4, 2008
6. HEUER, Richard J., Jr., *Limits of Intelligence Analysis*, Orbis, 2005, carte disponibilă la http://www.worldaffairsboard.com/attachments/staff-college/20727d1273228985-ebo-sod-limits-intelligence-analysis-fpri-winter-2005-heurer-.pdf
7. JOHNSTON, Rob *Analytic Culture in the U.S. Intelligence Community*, Central Intelligence Agency, Washington, 2005, p. 6, carte disponibilă la https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf
8. JOSHI, Shashank, *Charlie Hebdo attack: A French intelligence failure?,* 10.01.2015, articol disponibil la http://www.bbc.com/news/world-europe-30760656
9. MILLWARD, William, *Life in and aut of Hut 3*, HINSLEY**,** F.H.; STRIPP, Alain: *The Codebrakers: The Inside Story of Bletchley Park*, Oxford University Press, 1993, p. 17
10. MORE, David T., *Critical Thinking and Intelligence Analysis*, Washington, National Defense Intelligence College, 2007
11. PAUL, Richard; ELDER, Linda, *Mini-guide de la Pensee Critique Concepts et instruments*, Foundation for Critical Thinking Press, 2008,
12. RODIER, Alain, *Pourquoi les americains ont plie devant les iraniens,* Centrul Francez de Studii de Intelligence, notă de actualitate nr.111, 2007, articol disponibil la http://www.cf2r.org/fr/notes-actualite/pourquoi-les-americains-ont-plie-devant-les-iraniens.php

ÎMBUNĂTĂŢIREA PERFORMANŢEI ÎN INTELLIGENCE – O ABORDARE EXPERIMENTALĂ

Răzvan ŢUREA
Doctorand, Academia Naţională de Informaţii "MIHAI VITEAZUL", Bucureşti,
email: razvan.turea@yahoo.com

Rezumat: *În general, există o legătură strânsă între performanţa umană şi conştientizare, ca parte a inteligenţei emoţionale şi sociale. Conştientizarea implică o conexiune cu memoria şi atenţia ca factori cognitivi, o cale pentru a creşte performanţa umană fiind antrenarea acestora. Aptitudinile crescute legate de memorie şi atenţie pot creşte performanţa, inclusiv cea legata de activitatea de intelligence. Pentru aceasta, am gasit un set de patru tehnici ce ameliorează nivelul conştientizării subiecţilor. Designul experimental folosit a fost unul de tip plan factorial cu doi factori, aplicaţi în câte două nivele. Lotul experimental a fost format din 24 de studenţi ai Facultăţii de Psihologie a Universităţii Bucureşti cu vârste 18 şi 23 de ani. Studiind diferenţa dintre tehnicile aplicate, prin aplicarea testului statistic MANOVA, pentru analiza varianţei mediilor variabilelor dependente, am arătat că există o diferenţă semnificativa statistic între aceste tehnici, fapt ce a permis identificarea celei mai eficiente tehnici, pentru îmbunătăţirea performanţei.*

Cuvinte cheie: *intelligence, performanţa umană, conştientizare, memorie, atenţie, efect Kirlian.*

Introducere

Performanţa umană a fost definită pornind de la conceptul de "performanţă" specifică (de exemplu mentală, sportivă etc), în acest sens, fiind o capacitate a individului, ca fiinţă umană, de a face faţă, de a se adapta, la condiţii deosebite. Aceste condiţii se referă la cele care depăşesc "parametrii funcţionali" obişnuiţi, consideraţi normali, factori ce s-au dezvoltat în decursul evoluţiei ontologice şi genetice.

Depăşirea acestor dotări, aptitudini, poate fi determinată de anumite condiţii adverse (ca o reacţie la condiţii de mediu extreme, stres ridicat, etc.) sau de o intenţie bine precizată (activităţi sportive de performanţă, activităţi mentale deosebite, etc.). Mai multe aspecte ale performanţei umane, pot fi evaluate, antrenate şi în acest fel, îmbunătăţite. Uneori, exersând un anumit tip de performanţă specifică, se pot obţine efecte care să implice îmbunătăţirea, oarecum neaşteptată, a performanţei într-un alt domeniu, fără o legătură directă cu aptitudinea antrenată.

Antrenamentul interspecific al aptitudinilor poate fi orientat spre un scop precis. Acest proces este folosit pentru a atinge noi nivele de performanţă şi în activitatea de intelligence. Astăzi activitatea de intelligence a devenit, mai mult ca oricând, una care se desfăşoară pe un adevărat *câmp de luptă mental*[1]. În acest context, performanţa în activitatea de intelligence (de exemplu, achiziţia de informaţii) este legată foarte puternic pe performanţele mentale (ca atenţia şi memoria) ale celor care sunt actorii acestui teatru de război, câmpul mental. „Mintea este un instrument de rezolvare a problemelor, de stocare, extragere şi prelucrare a informaţiilor, precum şi de evaluare a datelor. Ea realizează acest lucru prin concentrare pe anumite senzaţii, pe gânduri şi imagini mentale care sunt prezente în memorie şi pe care le

[1]Emil STRĂINU*, Războiul psihotronic. Câmpul de luptă mental*, Editura Solaris Print, Bucureşti, 2008, p.1.

procesează”[2]. Prin urmare, există o legătură foarte puternică între performanţele mentale şi unele procese psihice ca atenţia şi memoria.

Prin ameliorarea acestor procese psihice conform unor metodologii şi cu tehnici adecvate, se poate obţine performanţă îmbunătăţită şi în ce priveşte conştientizarea, ceea ce va potenţa şi va accelera procesul transformare a activităţii în intelligence, în conformitate cu noile tendinţe precizate prin sintagma „nevoia de schimbare”[3]. În cercetarea experimentală pe care am desfăşurat-o, am urmărit să evaluez actul de conştientizare versus performanţa umană în acţiunile de intelligence. Două aptitudini specifice unui bun lucrător în intelligence şi nu numai, sunt reprezentate de memorie şi atenţie. Caracteristica definitorie a experimentului este dată de faptul că nivelul conştientizării, surprins prin aplicarea itemilor *Scalei de Evaluare a Conştientizării (CQ-I,)* este stabil temporal. Modificarea acestuia necesită serioase intervenţii manipulative, atât energetice cât şi psihoemoţionale, astfel încât am corelat itemii înregistraţi prin aplicarea scalei CQ-I, cu parametrii specifici câmpului cuantic uman (CCU), în dinamica mecanismului de adaptare la solicitările mediului, inclusiv la cel socio-profesional. În acest context, evaluarea unei tehnici sau a unor ansambluri de tehnici de activare a potenţelor proprii, aplicate în scopul creşterii performanţelor în activitatea de intelligence, corelată cu actul de conştientizare poate fi efectuată, chiar şi în mod indirect, folosind aparate şi intrumente psihometrice.

Deoarece folosirea scalei de conştientizare CQ-I, pentru a valida un model de intervenţie asupra subiecţilor umani, ar necesita intervale temporale de mărimea anilor calendaristici am împărţit crcetarea în două etape. La momentul iniţial am evaluat subiecţii cu *Scala de Evaluare a Conştientizării şi am obţinut valorile numerice ale itemilor caracteristici. În condiţiile de pretest le-am măsurat parametrii personali cu aparatele* GDV (Gas Discharge Visualisation) şi cu aparatul AV5.1 (AuraVision). În continuare am efectuat evaluarea corelaţiilor dintre itemii scalei de conştientizare şi parametrii psihoemoţionali măsuraţi. În această etapă am folosit testul FVW, pentru a reliefa performanţele iniţiale ale subiecţilor supuşi studiului, privitoare la atenţie şi memorie.

În etapa a doua a cercetării experimentale, am subiecţii au efectuat un set de tehnici specifice care au urmărit creşterea performanţelor proprii. După efectuarea acestor tehnici am repetat măsurătorile, cu aceleaşi aparate şi am aplicat acelaşi instrument psihometric, pentru a obţine valorile variabilelor dependente

Cu ajutorul testului statistic t student, ce se aplică grupurilor pereche pentru variabilele dependente cu valori normal distribuite, şi cu ajutorul testului neparametric Wilcoxon, ce se aplică variabilelor dependente cu valori ce nu respectă distribuţia normală, am evaluat statistic efectele tehnicilor specifice de activare a potenţelor umane.

1. Descrierea experimentului

1.1 Scopul demersului ştiinţific de cercetare

Scopul demersului de cercetare a fost acela de a arăta legătura dintre conştientizare - prin componentele ei memorie şi atenţie - şi performanţele fiinţei umane, în general, şi în special în activitatea de intelligence.

[2]http://www.dezvoltarium.ro/detalii- articol/legatura_dintre_creier_ si_constientizare, accesat la 20 iunie, 2013
[3]Lucian Ion PETRAŞ, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014, p. 120.

1.2 Obiective

Obiectivul nr.1 Demonstrarea experimentală a legăturii dintre valorile parametrilor câmpului cuantic uman şi valorile itemilor testului CQ-I.

Obiectivul nr.2 Demonstrarea experimentală a legăturii dintre valorile parametrilor câmpului cuantic uman şi nivelul atenţiei şi al memoriei vizuale şi auditive.

Obiectivul nr.3 Demonstrarea eficacităţii tehnicilor de activare a potenţelor proprii prin aplicarea unor tehnicilor specifice, utilizând metode de evaluare a nivelului atenţiei concentrate şi al memoriei vizuale şi auditive şi metode de evaluare a caracteristicilor câmpului cuantic uman.

Obiectivul nr.4 Demonstrarea experimentală a faptului că există un efect sinergic obţinut de subiecţii care au efectuat pregătirea specifică prin combinarea mai multor tehnici, iar acesta este semnificativ mai mare decât efectul aplicării unei singure tehnici.

Obiectivul nr. 5 Identificarea, interpretarea şi determinarea unui mod specific de acţiune pentru îmbunătăţirea parametrilor specifici câmpului cuantic uman necesari pentru ofiţerii de intelligence, care să le permită dezvoltarea anumitor calităţi psihice.

1.3 Ipotezele cercetării

Ipoteza nr.1 Subiecţii care înregistrează valori scăzute ale parametrilor câmpului cuantic uman, măsuraţi cu aparatura GDV şi AV5.1, prezintă un nivel mai scăzut conştientizării determinate prin aplicarea testului CQ-I.

Ipoteza nr.2 Subiecţii care înregistrează valori scăzute ale itemilor Testului CQ-I, prezintă un nivel

mai scăzut al atenţiei şi al memoriei vizuale şi auditive.

Ipoteza nr.3 Subiecţii, ale căror potenţe proprii au fost activate prin aplicarea tehnicilor specifice, înregistrează creşterea semnificativă a nivelului atenţiei concentrate şi al memoriei vizuale şi auditive.

Ipoteza nr.4 Subiecţii, ale căror potenţe proprii au fost activate prin aplicarea tehnicilor specifice, înregistrează creşterea semnificativă a parametrilor câmpului cuantic uman măsuraţi cu aparatura GDV şi AV5.1

Ipoteza nr.5 Efectul sinergic obţinut de subiecţii care au efectuat pregătirea specifică prin combinarea mai multor tehnici, este semnificativ mai mare decât efectul aplicării unei singure tehnici.

2. Metoda

2.1 Participanţi

Dimensiunea grupului experimental am stabilit-o la un număr de 24 de subiecţi, împărţiţi în patru grupuri de câte şase.

Grupului i s-a aplicat procedura de optimizare a parametrilor câmpului cuantic uman prin activarea specifică a potenţelor proprii.

2.2 Aparate şi instrumente

Metoda folosită este cea electrofizică de cercetare a stărilor şi a energiilor[4]. Ea permite vizualizarea şi analiza prin înregistrare computerizată a radiaţiilor optice şi emisiilor biologice

[4]Aliodor MANOLEA *„Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă”*,Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012, p. 116.

umane stimulate de câmpul electromagnetic şi amplificate prin descărcare în gaze[5], preluarea datelor folosind senzori dermali pentru descrierea câmpului cuantic uman. Sistemul folosit permite ca datele să fie prelucrate şi interpretate prin intermediul programului statistic SPSS.

Toate măsurătorile descrise anterior, se vor face automat, pentru fiecare subiect în parte. În cea ce priveşte determinarea efectelor care apar după sesiunile experimentale voi folosi următoarele indicii:

-modificări în emisia biologică şi optică stimulate de câmpuri electromagnetice prin descarcăre în gaze, prin efect Kirlian;

-schimbări ale parametrilor câmpului cuantic uman puse în evidenţă cu aparatul Aura Vision.

Pentru punerea în evidenţă a efectelor menţionate am folosit GDV (Gas Discharge Visualisation), aparatură ce caracterizează starea psihoemoţională şi starea somatică a subiecţilor din grupul experimental atunci când se acţionează conform designului experimental.

Metoda GDV de măsurare a emisiei biofotonice, oferă posibilitatea de a studia starea emoţională, psihică şi fizică a omului prin determinarea unui set de 42 de variabile. Rezultatele obţinute se prelucrează cu ajutorul programelor speciale care oferă informaţii cu privire la starea psihoemoţională şi fiziologică a subiectului supus investigării. Parametrii imaginii obţinute prin descărcare în gaze, depind de proprietăţile obiectului cercetat şi, în felul acesta, analizând caracterul luminescenţei induse de către obiecte, apare posibilitatea de a emite judecăţi de valoare privitor la starea energetică a obiectului într-un moment concret (figura 1). Programul de analiză statistică, implementat în aparatul GDV, este conceput pentru procesarea multiplă a parametrilor statici şi dinamici ai diagramelor, şi pentru compararea statistică cu parametrii calculaţi pentru una sau mai multe dintre probele ce se efectuează. Printre testele statistice folosite de acest program sunt criteriul Student, criteriul Wilcoxon, criteriul Mann-Whitney şi Valde-Volfovitz, ca şi criteriul semnelor[6]. O metaanaliză[7] a cercetărilor ştiinţifice efectuate folosind metoda GDV, care au fost publicate în reviste de specialitate între anii 2003-2012, estimează că:

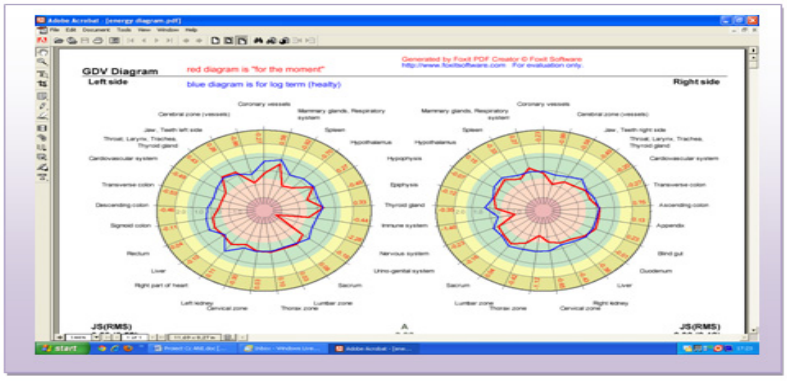


Figura nr.1 Evidenţiere grafică a parametrilor cuantici umani cu ajutorul aparaturii GDV

-sunt corelaţii semnificative între parametrii măsuraţi cu GDV şi diverşi parametri medicali, fiziologici şi psihologici, validând astfel aparatura şi metoda utilizată;

---

[5]K. KOROTKOV, *Human energy field: study with GDV bioelectrography*, Fair Lawn, NJ, Backbone Publishing, 2002.

[6]*Ibidem.*

[7]K. G. KOROTKOV, P. MATRAVERS, D.V. ORLOV, *Application of Electrophotonic Capturing (EPC) Analysis Based on Gas Discharge Visualization (GDV) Technique in Medicine: a Systematic Review,* J Altern Complement Med. 2010, 16(1): 13-25.

-software şi echipamentul EPC/GDV este un dispozitiv viabil şi uşor de utilizat şi oferă o gamă largă de aplicaţii şi metode de evaluare psiho-fiziologică.

2.2.1 Metoda de evidenţiere a câmpului cuantic uman cu Aura Vision 5.1[8]

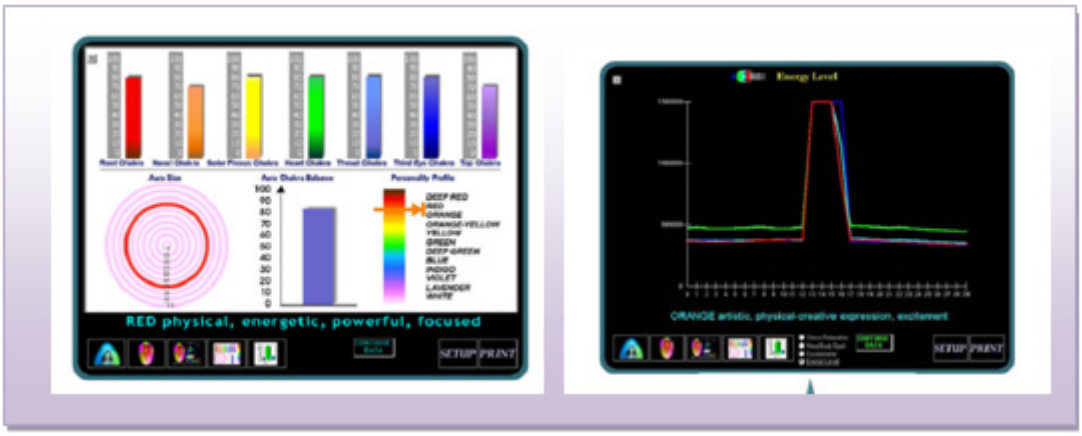


Figura nr. 2 Modalităţi de prezentare grafică a parametrilor înregistraţi cu aparatul AV 5.1

Aparatul AV 5.1 se bazează pe interpretarea informaţiilor despre activitatea electrodermală şi emisia termică, la nivel palmar. Prelucrarea acestor informaţii cu ajutorul unui sistem informatic specific oferă informaţii despre echilibrul minte-corp-spirit, nivelul stresului, nivelul şi calitatea activităţii centrilor cuantici principali ai CCU şi în legătură cu aceştia despre funcţionarea glandelor endocrine asociate. De asemenea sunt precizate şi diverse informaţii despre personalitatea subiectului investigat (figura 2).

2.2.2 Instrumente psihometrice folosite

Scala de Evaluare a Conştientizării – CQ-I

Scala a fost elaborată pornind de la aspectaţia că există un nivel curent/actual de conştientizare care reflect nivelul evolutiv prezent al persoanei în stare de veghe, în condiţii obişnuite de viaţă. Cele şase dimensiuni ale experienţei conştiente care au fost luate în calcul la evaluarea gradului de conştientizare, şi care au devenit Factori principali ai Scalei de Evaluare a Conştientizării, sunt următoarele: Conştientizare Concretă, Conştientizare Emoţională, Conştientizare Mentală, Conştientizare Spirituală şi Conştientizare Socială-Relaţională. Coeficientul de conştientizare[9] se obţine din media celor şase factori principali. Cei şapte subfactori identificaţi pentru a descrie şi alte faţete relevante pentru experienţa conştientizării sunt: Conştientizarea stării interne, Reflectarea de Sine, Detaşare, Autonomie, Dezvoltare Personală, Relaţionare pozitivă cu ceilalţi şi Scop în viaţă.

Testul FVW[10]

Pentru evaluarea atenţiei şi a capacităţii de memorare am folosit testul FVW-Recunoaşterea vizuală continuă, care face parte din sistemul de teste Vienna.

Respondentul trebuie să decidă dacă un item este arătat pentru prima dată sau se repetă pe ecran.

---

[8]Aliodor MANOLEA, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012, p.116.

[9]Ovidiu BRAZDĂU, *Coeficientul de Conştientizare (CQ) The Consciousness Quotient & The CQ Inventory-Theory and Research,* Ed. Reţeaua Info-Sănătate, Bucureşti, 2011, pp. 110-125.

[10]Uli PUHR, *User manual for FVW Test*, Copyright for Test by Garching Instrumente G.m.b.H, Mödling, Austria, September 2003, pp. 3-4.

2.3 Procedura de lucru

Am utilizat în manieră test-retest testul FVW pentru evaluarea performanţelor memoriei şi atenţiei fiecărui subiect şi scala CQ-I pentru determinarea coeficienţilor de conştientizare.

Toate măsurătorile valorilor variabilelor dependente s-au efectuat pentru fiecare subiect în parte, înainte şi după activarea potenţelor proprii prin utilizarea tehnicilor respiratorii şi a cogniţiilor funcţionale.

În ceea ce priveşte determinarea efectelor care apar înainte, în timpul şi după sesiunile experimentale (după caz) am urmărit diferenţierile înregistrate de valorile variabilelor în cadrul etapele experimentului privind:

-emisiile cuantică, biologică şi optică, stimulate de câmpuri electromagnetice prin descărcare în gaze folosind efectul Kirlian;

-starea psihoenergetică;

-parametrii câmpului cuantic uman;

-starea echilibrului emoţional afectiv al subiecţilor din grupul experimental;

2.3.1 Etape de lucru

Etapa I-a Prelevarea datelor iniţiale de la întreg eşantionul

Grupul experimental a efectuat testul FVW, a aplicat scala CQ-I şi s-au înregistrat parametrii câmpurilor cuantice ale fiecărui subiect

Etapa a II-a Aplicarea tehnicii pentru activarea potenţelor proprii ale subiecţilor participanţi la experiment

În această etapă s-a efectuat exerciţiul de respiraţie cu contractura muşchiului bazinului inferior, în patru modalităţi, fiecare grup experimental (de câte şase subiecţi) abordând o singură modalitate:

- Modalitatea A: exerciţiul a fost însoţit de concentrarea cognitivă pe numărarea mentală a timpilor corespunzători etapelor respiraţiei.
- Modalitatea B: exerciţiul a fost însoţit de concentrarea mentală pe o structură lingvistică cu semnificaţie spirituală deosebită.
- Modalitatea C: exerciţiul a fost însoţit de rularea bazinului şi de concentrarea cognitivă pe numărarea mentală a timpilor corespunzători etapelor respiraţiei.
- Modalitatea D: exerciţiul a fost însoţit de rularea bazinului şi de concentrarea mentală pe o structură lingvistică cu semnificaţie spirituală deosebită.

Grupurile experimentale A, B, C şi D au efectuat aceasta activitate consecutiv, după ce pentru grupul precedent s-au efectuat toate măsurătorile valorilor variabilelor dependente.

Etapa a III-a Prelevarea datelor finale ale cercetării

Cu ajutorul aparaturii s-au înregistrat variabilele dependente sub forma numerică a valorilor parametrilor electrodermali personali cât şi parametrii specifici câmpului cuantic. Întregului lot experimental i s-a aplicat din nou testul FVW pentru evaluarea performanţelor memoriei şi atenţiei.

Etapa a IV-a Analiza şi interpretarea datelor

În această etapă s-a folosit setul de programe Excel, SPSS 20, Qpower, pentru extragerea rezultatelor statistice.

2.4 Designul experimental

Designul experimental (figura 3) folosit a fost unul de tip plan factorial cu doi factori, aplicaţi în câte două nivele, adică un plan factorial de tip 2x2.

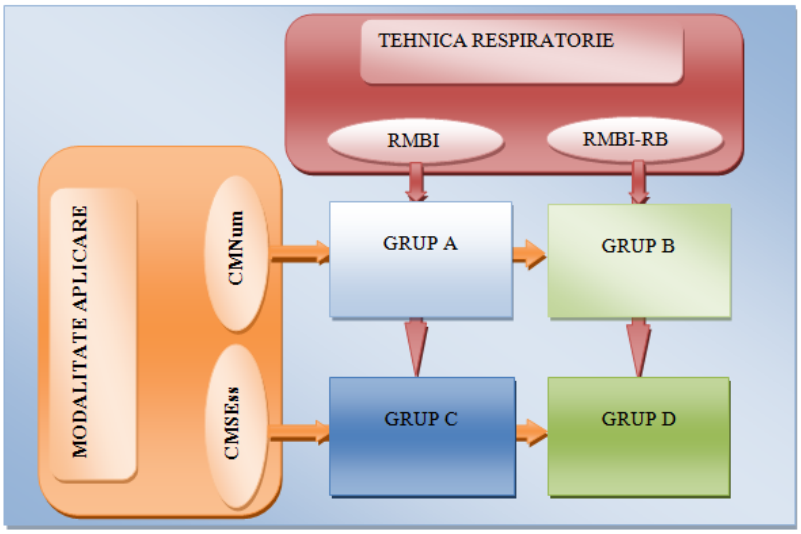


Figura nr. 3 Designul experimental – plan factorial 2x2

Variabilele independente (factorii) au fost tehnica respiratorie (cu contractura muşchiului bazinului inferior (RMBI) şi rularea bazinului (RMBI-RB)), iar modalitatea de aplicare (cu concentrare mentală pe numărare (CMNum) şi cu concentrare mentală pe o structură cu elemente semantice spirituale deosebite (CMSEss)). Modalităţile, prezentate în paranteze, reprezintă nivelele în care se aplică factorii. De aici rezultă denumirea de plan factorial 2x2, adică un plan experimental în care se studiază două variabile independente, fiecare cu câte două niveluri. Astfel, în acest experiment sunt cuprinse de fapt, patru experimente unifactoriale.

3. Discuţii

Analiza corelaţiilor dintre itemii testului CQ-I şi variabilele dependente măsurate cu GDV, AV5.1, arată că este posibil să utilizăm aceste instrumente şi teste pentru a face o evaluare a unei stări momentane a conştientizării unui subiect, chiar dacă conştientizarea este o calitate a fiinţei umane care are o variaţie relativ lentă. Acesta a fost, de altfel şi scopul testării acestor două ipoteze. Analiza corelaţiilor dintre itemii testului FVW şi itemii Testului CQ-I, demonstrează că există o legătură între aptitudinile măsurate cu testul FVW, adică memoria şi atenţia şi conştientizare aşa cum este ea caracterizată de testul CQ-I.

Aplicând un complex de tehnici pentru creşterea performanţelor umane (îmbunătăţirea parametrilor câmpului cuantic uman), am arătat că există un efect semnificativ statistic al acestora asupra fiinţei umane. Acest efect se traduce printr-o capacitate mai mare de memorare şi într-o abilitate mai însemnată de a menţine atenţia concentrată asupra unui obiectiv. Aspectul respectiv a fost relevat prin testarea statistică a ipotezelor trei şi patru, care au arătat o creştere a parametrilor câmpului cuantic, corelată cu o îmbunătăţire semnificativă a memoriei şi atenţiei.

Analiza multivariată aplicată asupra tehnicilor de creştere a câmpului cuantic uman, s-a soldat cu relevarea faptului că tehnica respiratorie este determinantă în obţinerea efectului, în timp ce modalitatea în care se execută (cu concentrare mentală pe numărare (CMNum) şi cu concentrare mentală pe o structură cu elemente semantice spirituale deosebite (CMSEss)), nu are un efect semnificativ statistic. Acest lucru ne permite sa alegem modalitatea mai simplă pentru subiecţi şi anume respiraţie cu rularea bazinului şi cu concentrare mentală pe numărare.

Concluzii

Fără prezenţa conştientizării, probabil că nu am şti de existenţa propriile noastre percepţii. În mod real suntem conştienţi numai de o mică parte dintre acestea, una din modalităţile de conştientizare fiind îndreptarea atenţiei, sau concentrarea mentală. „C*onştientizarea este precum un ecran pe care apar toate gândurile si senzaţiile, iar mintea devine conştientă de ele prin concentrare asupra lor"* [11]. Mintea rezolvă probleme, stochează şi extrage informaţii prin concentrare pe anumite senzaţii, pe imagini mentale şi gânduri prezente în memorie si pe care le procesează. Astfel că, există o legătură puternică între conştientizare şi calităţile atenţie şi memorie. Este legătura pe care am testat-o în acest studiu, arătând ca există o corelaţie relativ puternică între itemii testului CQ-I (chestionar de evaluare a conştientizării) şi cei ai testului FVW (test pentru evaluarea performanţei la memorie şi atenţie). A fost necesar să fac acest lucru pentru că testul CQ-I pune în evidenţă modificări lente ale procesului de conştientizare, fiind necesare intervale lungi de timp, de ordinal anilor, pentru a releva o schimbare în nivelul conştientizării unui subiect. Am avut nevoie de un instrument care să evidenţieze aceste schimbări în structura constientizării în timp foarte scurt, testul FVW fiind potrivit acestui scop. Am arătat, de asemenea, că există o corelaţie puternică între itemii testului CQ-I şi variabilele dependente măsurate cu aparatele GDV şi AV5.1, putând astfel să arăt că există o corelaţie puternică între caracteristicile câmpului cuantic uman, determinate cu acestea, şi conştientizarea subiecţilor, aşa cum a rezultat ea în urma evaluării cu testul CQ-I.

Am elaborat un set de tehnici de activare a potenţialului fiinţei umane pe care le-am aplicat subiecţilor experimentului şi am testat apoi efectul acestora asupra caracteristicilor câmpului cuantic uman, determinate cu aparatele GDV şi AV5.1. Astfel, am tras concluzia că tehnicile respective au fost eficiente, înregistrând modificări pozitive ale câmpului cuantic uman, dublate şi de îmbunătăţirea performanţelor la testul FVW, care măsoară aptitudinile memorie şi atenţie şi interacţiunea lor. Prin urmare, am găsit un set de tehnici de activare a potenţialului fiinţei umane care să amelioreze şi nivelul conştientizării subiecţilor, care prin intermediul aptitudinilor crescute legate de memorie şi atenţie, pot duce la creşterea performanţei umane inclusiv cea legată de activitatea de intelligence. Studiind diferenţa dintre tehnicile aplicate, utilizând analiza varianţei mediilor variabilelor dependente MANOVA, am arătat că există o diferenţă între acestea în ce priveşte variabila independentă Tehnica respiratorie, în timp ce din punctual de vedere al variabilei Modalitatea de aplicare, nu a fost înregistrată nici o diferenţă semnificativă. Aceasta implică utilizarea celei mai simple modalităţi de aplicare a tehnicii mai eficiente de respiraţie, anume respiraţie cu contractura muşchiului bazinului inferior şi rularea bazinului cu numărarea mentală a timpilor respiraţiei.

Concluzionând, am realizat un instrument de evaluare şi îmbunătăţire a performanţei umane compus dintr-o tehnică de activare a potenţialului uman (respiraţie cu contractura muşchiului bazinului inferior şi rularea bazinului cu numărarea mentală a timpilor respiraţiei-RMBI_RB) al cărui efect se măsoară utilizând aparatura GDV, AV5.1 iar performanţele la testarea memoriei şi atenţiei se evaluează cu testul FVW.

[11] http://www.dezvoltarium.ro/detalii- articol/legatura_dintre_creier_ si_constientizare, accesat la 20 iunie, 2013

BIBLIOGRAFIE:

1. ANITEI, Mihai, *Psihologie experimentală*, ed. Polirom, 2007.
2. BRAZDĂU, Ovidiu, *Coeficientul de Conştientizare (CQ) The Consciousness Quotient & The CQ Inventory-Theory and Research*, Ed. Reţeaua Info-Sănătate, Bucureşti, 2011
3. KOROTKOV, K.G., MATRAVERS, P., ORLOV, D.V., *Application of Electrophotonic Capturing (EPC) Analysis Based on Gas Discharge Visualization (GDV) Technique în Medicine: a Systematic Review*. J Altern Complement Med., 2010, 16(1).
4. KOROTKOV, Konstantin, *Human energy field: study with GDV bioelectrography*, Fair Lawn, NJ, Backbone Publishing, 2002.
5. MANOLEA, Aliodor, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012.
6. MANOLEA, Doina Elena, MANOLEA, Aliodor, *Energetica Subtilă a fiinţei umane*, Ed. Aldomar Extrasenzorial, 1996.
7. PETRAŞ Lucian Ion, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014.
8. PUHR, Uli, *Manual for FVW Test*, Garching Instrumente G.m.b.H, Mödling, Austria, 2003.

DE LEGE FERENDA ÎN DOMENIUL INTRĂRII, STAŢIONĂRII, DESFĂŞURĂRII DE OPERAŢIUNI SAU AL TRECERII TRUPELOR STRĂINE PE TERITORIUL ROMÂNIEI

Dr. Florin MACIU
General de brigadă, consilier juridic Ministerul Apărării Naţionale,
Bucureşti, România; e-mail: fmaciu@yahoo.com

Rezumat*: În ultima perioadă, s-a creat o situaţie complexă şi extrem de serioasă cu posibile consecinţe foarte grave la adresa securităţii zonei Mării Negre, dar şi a spaţiului euro-atlantic, cu elemente care caracterizează perioadele dinainte de începerea unui conflict militar, făţiş, de mare amploare – anexări de teritorii străine, sprijin al rebelilor dintr-un stat străin, mii de victime în rândul civililor şi militarilor, comiterea de fapte abominabile precum doborârea unui avion de transport civil, fără legătură cu litigiul, diminuarea substanţiala a canalelor diplomatice sau practicarea unui dialog al surzilor, acuzaţii şi ameninţări reciproce, luarea de contramăsuri şi contra-contramăsuri, încălcări de înţelegeri internaţionale, escaladarea numărului de exerciţii militare de forţă în vecinătatea apropiată a presupusului oponent, impunerea de măsuri coercitive de natură economică, înfiinţarea de noi baze militare în interiorul suprafeţei de conflict.*

Pentru întărirea capacităţii de apărare a ţării, prin prezenţa permanentă a unor forţe aliate pe teritoriul României, ar trebui să luăm măsurile necesare pentru a nu ne încurca singuri în hăţişul legislativ propriu, adică să amendăm legislaţia în vigoare pentru a ne netezi calea implementării intenţiilor de a primi în ţară forţe militare aparţinând statelor aliate, care să joace, în primul rând, rolul de disuasiune a oricărui agresor, dar şi pe cel de participant activ la apărarea împotriva ameninţărilor cu invazia. Din timp, trebuie adoptate măsuri legislative de optimizare a regulilor privind staţionarea forţelor străine pe teritoriul ţării. Unele dintre zonele textelor de lege, susceptibile de sancţionare, precum şi recomandările corespunzătoare sunt prezentate în cadrul acestei lucrări. Altele se referă la exploatarea unor instrumente juridice internaţionale.

Cuvinte cheie: *securitate, anexare, alianţă, reglementare, modificare, completare, amendare, prezenţă militară străină, teritoriu românesc, facilităţi fiscale, sprijin*

Introducere

De mai bine de un an, românii sunt copleşiţi de ştirile extrem de grave, referitoare la evenimentele dramatice legate de agresiunea asupra Ucrainei, constând în acţiuni care, fără exagerare, pot conduce la o nouă conflagraţie mondială. Securitatea regiunii Mării Negre a fost dintotdeauna un subiect fierbinte, caracterizat de numeroase complicaţii ale situaţiei din zonă, precum şi de elemente complexe care interacţionează generând instabilitate. Totuşi, în prezent, mult mai serios ca în vremurile trecute, luăm cunoştinţă despre violenţe exacerbate, iar tulburările ajung la paroxism.

Rând pe rând, depăşindu-ne imaginaţia, se derulează întâmplări semnificative, menite să producă nu numai panică, dar şi modificări în geografia administrativă sau secvenţe memorabile în istoria contemporană. Lumea spaţiului euro-atlantic se cutremură când este martoră a anexării unor teritorii străine, a sprijinului acordat cu impertinenţă rebelilor dintr-o altă ţară, a numeroaselor acte de violenţă soldate cu mii de victime între civili şi militari. Rămânem consternaţi de intensificarea faptelor abominabile, culminând cu doborârea unui avion de transport civil de mare capacitate, aparţinând unui stat neimplicat în litigiu şi ai cărui

pasageri erau complet nevinovaţi. Canalele diplomatice între oponenţi se diminuează substanţial, iar atunci când mai există sunt folosite pentru un dialog al surzilor, împestriţat cu acuze şi ameninţări reciproce.

Înţelegerile internaţionale sunt ignorate sau interpretate părtinitor, se iau contramăsuri şi contra-contramăsuri, se impun măsuri economice coercitive, iar preţul energiei este folosit ca o veritabilă şi eficientă armă în confruntare, numărul exerciţiilor militare care trebuie să intimideze prin parada de forţă este escaladat şi mai toate sunt desfăşurate în vecinătatea apropiata a oponentului. In acest context, ajungem la situaţia în care statele vecine ariei de conflict doresc, pentru garantarea sau sporirea propriei securităţi, permanentizarea prezenţei unor forţe militare străine, aliate pe teritoriul lor şi chiar se întrec în punerea la dispoziţie a infrastructurii necesare pentru înfiinţarea aşa-ziselor baze militare străine.

În aceasta conjunctură, este evident că şi România, aflată la flancul de est al alianţei nord-atlantice şi având Ucraina drept stat vecin, este adânc preocupată de consolidarea factorilor care contribuie la propria apărare. Intr-un punct de vedere prezentat într-o altă lucrare, reliefam faptul că este mult mai sănătos, dată fiind situaţia actuală, să avem toţi aliaţii o poziţie caracterizată de pragmatism, adică să ne orientăm temeinic spre crearea şi menţinerea unei solide capacităţi de apărare, inclusiv prin înfiinţarea de entităţi militare străine permanente pe teritoriul ţării, în detrimentul efectuării unor analize pur teoretice legate de identificarea părţii care a comis o încălcare a înţelegerii internaţionale dintre NATO şi Federaţia Rusă, semnate la Paris în 1997[1]. În opinia noastră, interesul vital al României este prezervarea statului naţional, a independenţei acestuia şi a optimizării funcţionarii principiilor democraţiei reale, obiective care nu pot fi atinse sub ocupaţie străină, coşmar care, din păcate, în opinia noastră şi nu numai, poate deveni realitate.

1. Situaţia de facto

Atât SUA cât şi Uniunea Europeană reafirmă consecvent şi la unison că nu sunt de acord cu acţiunile întreprinse de Federaţia Rusă în Ucraina. Astfel, la un an de la referendumul controversat organizat în Crimeea, Jennifer Psaki, purtătoarea de cuvânt a Departamentului de

[1]Aflat într-o vizită oficială la Riga în Letonia, cancelarul german Angela Merkel a respins cererile unor politicieni şi intelectuali locali pentru înfiinţarea unei forţe militare vestice permanente în regiune, deşi a garantat că susţine ţările baltice împotriva unei posibile ameninţări ruseşti („*Merkel Promises Support for Baltic States Alarmed by Russia*", Juris Kaža, August 18, 2014, The Wall Street Journal, World News, http://www.wsj.com/articles/merkel-promises-support-for-baltic-states-alarmed-by-russia-1408383489, accesat pe 12 martie 2015). Motivul invocat de cancelar pentru refuz a fost că instalarea unei prezenţe permanente militare la estul Alianţei ar încălca înţelegerea dintre NATO şi Rusia.
Cererea letonilor a fost generată, în mod natural, de anexarea Peninsulei Crimea de către Rusia, fapt care a alarmat mai ales fostele state din spaţiul ex-sovietic dar şi statele membre NATO din estul Alianţei. Încercând să-şi explice poziţia adoptată, care presupunea acordul pentru pregătiri sporite în vederea desfăşurării de trupe în zonă fără însă a fi de acord cu prezenţa permanentă a NATO, cancelarul a subliniat faptul că prin Tratatul Internaţional de Cooperare din 1997 dintre NATO şi Federaţia Rusă, ambele părţi au garantat să nu se trateze una pe alta ca adversari şi a reiterat că o prezenţă permanentă a NATO în zonă ar viola înţelegerea respectivă.
La începutul lunii iunie 2014, miniştrii apărării din statele membre NATO au fost de acord ca, în răspuns la criza din Ucraina, să amplifice măsurile de protecţie din Europa de Est („*NATO Agrees To 'Readiness Action Plan' To Counter Russia*", By AGENCE FRANCE-PRESSE, June 03, 2014, DefenseNews, http://archive.defensenews.com/article/20140603/DEFREG01/306030034/NATO-Agrees-Readiness-Action-Plan-Counter-Russia, accesat pe 12 martie 2015) ca răspuns la criza din Ucraina, dar au precizat că se va acţiona numai în limitele tratatului cu Moscova de după războiul rece. Ambasadorul Rusiei la NATO, Alexander Grush, spusese numai cu o zi înainte că desfăşurarea temporară de trupe şi avioane aparţinând Alianţei peste numărul celor existente în state membre NATO cum ar fi Polonia şi ţările baltice, echivalează cu o încălcare a tratatului. Acuzaţiile părţii ruse, aşa cum am prezentat mai sus, au avut unele ecouri în rândul aliaţilor, în sensul că unii au opinat că tratatul interzice cu claritate aducerea de trupe şi mijloace de luptă pentru a crea noi prezenţe permanente în Europa de Est.

Stat american, la mijlocul lunii martie 2015, a declarat, aproape simultan cu intervenţia Federicăi Mogherini, şeful diplomaţiei europene, că respectivele structuri statale militează împotriva anexării ilegale a peninsulei de către Rusia. Dmitri Peskov, purtătorul de cuvânt al preşedintelui rus, Vladimir Putin, nu a întârziat să răspundă, prin a face public faptul că teritoriul Crimeii este parte a Rusiei şi că aceasta temă nu va fi discutată cu nimeni[2].

În convergenţă cu poziţia statelor din Uniunea Europeană şi America de Nord, europarlamentarul Ioan Mircea Paşcu prezintă subcomisiei pentru securitate şi apărare a Parlamentului European un proiect de raport care abordează, din punct de vedere strategic militar, situaţia din regiunea Mării Negre, de după anexarea Crimeii. Potrivit acestuia, situaţia strategică şi militară din Marea Neagră s-a schimbat dramatic. Forţa ruşilor devine o grupare militară de lovire, cu potenţial ofensiv însemnat, inclusiv de debarcare[3]. In acest context, nu sunt de neglijat anumite elemente precum o evoluţie a conflictului la nivelul folosirii armamentului nuclear, o agravare a situaţiei minorităţilor sau implicaţii economice periculoase pentru Uniune.

1.1. Scenarii

Mircea Paşcu, în materialul susmenţionat, aminteşte, foarte pe scurt, şi despre posibile evoluţii ale situaţiei, conform cărora Rusia s-ar putea apropia de graniţele României, prin anexări sau ocupări de teritorii ucrainene. Menţionam că nu este vorba despre prognoze ci despre posibilităţi teoretice, cu şanse de a se materializa.

A. *Rusia ocupă, la malul Mării Negre, un coridor la de 50 de km, care să facă legătura între teritoriul recunoscut al federaţiei, teritoriile ocupate de rebeli şi peninsula Crimeea.*

La acest scenariu, există şi varianta A+, în care Rusia ajunge până la Odessa. Această variantă a fost construită de analiştii de la Stratfor[4], dar a fost prezentată şi de fostul ministru de externe, Cristian Diaconescu, alături de istoricul Armand Gosu[5]. In situaţia descrisă, deplasarea ruşilor până la Galaţi ar dura două ore, un avion rusesc ar ajunge la Bucureşti în câteva minute, iar o rachetă la fel. Platoul continental românesc, o viitoare sursă de mari cantităţi de energie, ar fi, de asemenea, expus, odată cu o posibilă independenţă energetică a ţării noastre.

B. *Rusia ocupă tot sudul Ucrainei, şi ajunge până în Transnistria, construind o punte de legătură între teritoriile cu populaţie rusofonă, din sudul Ucrainei.*

Acest scenariu este tot rodul gândirii celor de la Stratfor şi ar dura 3-4 săptămâni până la atingerea finalităţii,iar plauzibilitatea lui o confirmă şi fostul ministru de externe al Germaniei, Joschka Fischer. Pentru ruşi se pare că acest plan este mai costisitor, fiind nevoie de efective mari de luptători. Efortul Rusiei nu ar fi, însă, nicidecum imposibil.

---

[2] *„Moscova sărbătoreşte un an de la anexarea Crimeii printr-un miting-concert în Piaţa Roşie, la care este aşteptat şi Vladimir Putin”*, Flori Tiulea, Agerpres, Martie 18, 2015, http://www.agerpres.ro/externe/2015/03/18/moscova-sarbatoreste-un-an-de-la-anexarea-crimeii-printr-un-miting-concert-in-piata-rosie-la-care-este-asteptat-si-vladimir-putin-11-34-24, accesat pe 18 martie 2015;

[3] *„Ioan Mircea Paşcu: Echilibrul militar din regiunea Mării Negre s-a schimbat în favoarea Rusiei”*, Ionuţ Mareş, Agerpres, Martie 17, 2015, http://www.agerpres.ro/externe/2015/03/17/ioan-mircea-pascu-echilibrul-militar-din-regiunea-marii-negre-s-a-schimbat-in-favoarea-rusiei-12-22-03, accesat pe 18 martie 2015;

[4] *„Stratfor analizeaza ce sanse ar avea Romania in fata unei invazii rusesti”*, e-politic.ro, Martie 11, 2015, http://e-politic.ziuanews.ro/dezvaluiri-investigatii/stratfor-analizeaza-ce-sanse-ar-avea-romania-in-fata-unei-invazii-rusesti-168420, accesat pe 12 martie 2015;

[5] *„E lucrul cel mai grav trait de Romania in ultimele decenii. Un diplomat si un istoric, despre pericolul razboiului cu Rusia”*, Pro TV, Februarie 22, 2015,http://stirileprotv.ro/emisiuni/dupa-20-de-ani/e-lucrul-cel-mai-grav-trait-de-romania-in-ultimele-decenii-un-diplomat-si-un-istoric-despre-pericolul-razboiului-cu-rusia.html, accesat pe 12 martie 2015

C. Rusia lansează un atac convenţional asupra unui stat est-european, membru al NATO, urmărind neutralizarea Ucrainei şi punerea în discuţie a capacităţii de răspuns a Alianţei, adică verificarea funcţionării prevederilor art. 5 al tratatului NATO.

Veridicitatea ipotezei este confirmată de sir Adrian Bradshaw, adjunctul comandantului forţelor NATO din Europa, care subliniază riscul de confruntare nucleară, într-o asemenea situaţie. Generalul în rezervă Degeratu Constantin, fost şef al Statului Major General, întăreşte exactitatea acestui scenariu şi, mai mult, identifică posibilele state victimă: Estonia sau România[6].

După cum se poate constata, scenariile generate de intervenţia Federaţiei Ruse în Ucraina au, ca numitor comun, un viitor apropiat foarte sumbru pentru România.

1.2. Poziţia vecinilor României

Să trecem succint în revista poziţia statelor vecine României, cu scopul de a stabili elementele străine pe care ţara noastră se poate baza ca să îşi întărească, în timp scurt, apărarea, în cazul că unul dintre scenariile de coşmar, menţionate mai sus, se pune în practică.

Moldova, un stat pe care ne place să-l considerăm frăţesc, care aspiră la Uniunea Europeană, dar care, de fapt, depinde din punct de vedere energetic aproape total faţă de ruşi, are Armata a XIV-a pe propriul teritoriu, este parte a unui conflict latent cu separatiştii transnistreni. Apreciem că mulţi dintre cetăţenii moldoveni sunt rusofoni sau/şi cu vederi cvasicomuniste, deloc prietenoase României.

Ucraina, dezmembrată de ruşi, ocupată parţial de către aceştia, cu datorii externe foarte mari şi adusă în pragul falimentului.

Ungaria, care pare preocupată numai de interesele proprii, uneori deviaţioniste, întreţinând foarte bune relaţii cu Federaţia Rusă, ignorând avertismentele colegilor din Uniunea Europeană şi neexcelând la capitolul de bună vecinătate cu România, câteodată manifestându-şi evident ostilitatea prin diferite personaje care se bucură de popularitate în aceasta ţară. Fostul model pe care l-am urmat pentru intrarea în NATO şi-a pierdut aureola şi se remarcă negativ la capitolul democraţie.

Serbia, prin tradiţie un bun partener al ruşilor, ca şi Bulgaria, care, chiar dacă e membru NATO, poate oricând deveni un avanpost al Federaţiei Ruse[7].

Dintre toate aceste state, în zonă, România plăteşte către Gazprom cel mai mare preţ la gaz rusesc, ceea ce demonstrează ca vecinii s-au asigurat printr-un comportament oarecum duplicitar de bunăvoinţa ruşilor.

1.3. Politica de apărare a României

Date recente scot în evidenţă elemente noi în legătură cu activitatea militară a Federaţiei Ruse în zona peninsulei Crimeea. Aici vor fi aduse avioane strategice Tu-22M3, capabile să transporte rachete nucleare[8]. Preşedintele Ucrainei, Petro Poroşenko, menţiona, zilele acestea, riscul unui conflict de mare amploare, în regiunea Mării Negre[9].Aceste ştiri îngrijorătoare nu

---

[6] *„Dacă ROMÂNIA ar fi atacată de RUSIA”*, QMagazine, Martie 10, 2015, http://qmagazine.ro/ce-nu-se-vede-la-tv/daca-romania-ar-fi-atacata-de-rusia/, accesat pe 12 martie 2015;

[7] *„Stimulentul Putin. Oportunitatea unui tandem România-Polonia”*, Laurenţiu Mihu, România Liberă, Martie 11, 2015, http://www.romanialibera.ro/politica/institutii/stimulentul-putin--oportunitatea-unui-tandem-romania-polonia-370623, accesat pe 12 martie 2015;

[8] *„Rusia iar joacă cartea intimidării. Mută armele nucleare mai aproape de Europa”*, Oleg Cojocaru, Pagina de Rusia.ro, Martie 17, 2015, http://www.paginaderusia.ro/rusia-iar-joaca-cartea-intimidarii-muta-armele-nucleare-mai-aproape-de-europa/, accesat pe 19 martie 2015;

[9] *„Poroşenko: Amplasarea de rachete ruseşti în Crimeea creşte riscul unui conflict major în zona Mării Negre”*, Lilia Traci, Agerpres, Martie 19, 2015,http://www.agerpres.ro/externe/2015/03/19/porosenko-amplasarea-de-

fac altceva decât să sublinieze justeţea măsurilor luate la începutul lunii februarie, la reuniunea miniştrilor apărării din NATO, de la Bruxelles. Atunci s-a decis înfiinţarea unor structuri multinaţionale de comandă şi control, pentru integrarea forţelor NATO, pe teritoriile statelor de la graniţa de est a organizaţiei.

România nu numai că a agreat această propunere, dar s-a angajat să realizeze rapid tot ceea ce depinde de ea în acest sens. Mai mult, România a fost de acord să găzduiască pe teritoriul ei un comandament multifuncţional de divizie, operaţional în 2016. De la ministrul de externe, Bogdan Aurescu, până la Klaus Iohanis, Preşedintele României, incluzându-l, în special, pe ministrul apărării, Mircea Duşa, persoanele cu funcţii de mare responsabilitate au fost de acord cu măsurile luate, iar armata a trecut imediat şi cu profesionalism la întocmirea documentelor şi întreprinderea acţiunilor necesare.

2. De lege ferenda în domeniul intrării, staţionării, desfăşurării de operaţiuni sau al trecerii trupelor străine pe teritoriul României. Concluzii

Pentru întărirea capacităţii de apărare a ţării, prin prezenţa permanentă a unor forţe aliate pe teritoriul României, ar trebui să luăm măsurile necesare pentru a nu ne încurca singuri în hăţişul legislativ propriu, adică să amendăm legislaţia în vigoare pentru a ne netezi calea implementării intenţiilor de a primi în ţară forţe militare aparţinând statelor aliate, care să joace, în primul rând, rolul de disuasiune a oricărui agresor, dar şi pe cel de participant activ la apărarea împotriva ameninţărilor cu invazia. Din timp, trebuie adoptate măsuri legislative de optimizare a regulilor privind staţionarea forţelor străine pe teritoriul ţării. Unele dintre zonele textelor de lege interna, susceptibile de sancţionare, precum şi recomandările corespunzătoare sunt prezentate în cadrul acestei lucrări. Altele sugestii se referă la exploatarea unor instrumente juridice internaţionale.

2.1. Abrogarea Hotărârii Parlamentului nr. 29/2007[10] privind aprobarea intrării şi staţionării forţelor Statelor Unite al Americii pe teritoriul României în vederea desfăşurării activităţilor stabilite prin Acordul dintre România şi Statele Unite ale Americii privind activităţile forţelor Statelor Unite staţionate pe teritoriul României, semnat la Bucureşti la 6 decembrie 2005, ratificat prin Legea nr. 268/2006

In baza art. 5 din Legea apărării naţionale a României nr. 45/1994[11], aşa cum a fost modificată prin Ordonanţa de urgenţă a Guvernului nr. 13/2000[12], a fost adoptată, la solicitarea Preşedintelui României, Hotărârea Parlamentului nr. 29/2007, care prevedea limitarea numărului membrilor forţelor Statelor Unite ale Americii ce se pot afla la un moment dat pe teritoriul României la cel mult 3000, cu posibilitatea de suplimentare a numărului maxim de persoane cu încă 500.

Mai târziu, a fost adoptată Legea nr. 291/2007 privind intrarea, staţionarea, desfăşurarea de operaţiuni sau tranzitul forţelor armate străine pe teritoriul României[13]. Legea reglementează, pe de o parte, condiţiile ce trebuie respectate pe teritoriul României de către forţele armate străine aparţinând unor state care nu sunt membre NATO sau ale Parteneriatului pentru Pace, iar, pe de altă parte, prevede măsuri juridice pentru aplicarea anumitor dispoziţii din tratatele bi şi multilaterale privind statutul forţelor.

---

rachete-rusesti-in-crimeea-creste-riscul-unui-conflict-major-in-zona-marii-negre-14-02-22, accesat pe 19 martie 2015;

[10]Act publicat în: Monitorul Oficial nr. 294 din 3 mai 2007;

[11]Act publicat în: Monitorul Oficial nr. 172 din 7 iulie 1994;

[12]Ordonanţa de urgenţă a Guvernului nr. 13 din 13 martie 2000 pentru modificarea art. 5 din Legea apărării naţionale a României nr. 45/1994. Act publicat în: Monitorul Oficial nr. 111 din 14 martie 2000;

[13]Act publicat în: Monitorul Oficial nr. 758 din 8 noiembrie 2007;

Acest act normativ schimbă radical concepţia referitoare la prezenţa forţelor armate străine pe teritoriul României. Dacă mai susmenţionata Hotărâre a Parlamentului făcea referire la numărul de militari şi amploarea operaţiunilor desfăşurate şi conţinea anumite restricţii la perioada de timp cât aceste prevederi se puteau aplica, noua reglementare a vizat o abordare fundamental diferită. Astfel, au fost eliminate orice limitări în ceea ce priveşte numărul şi amploarea forţelor participante. Prin art. 55 din Legea 291/2007 se abrogă în mod expres art. 5 din Legea nr. 45/1994, articol invocat ca temei legal pentru Hotărârea Parlamentului nr. 29/2007. Prin abrogarea susmenţionată, a dispărut şi baza legală ca preşedintele României să se adreseze Parlamentului cu solicitări privind intrarea, staţionarea ori trecerea trupelor străine pe teritoriul României.

Într-o opinie, s-a susţinut că această hotărâre e căzută în desuetudine. În opinia unor specialişti, această hotărâre a Parlamentului este încă în vigoare. Existând şi argumente pro dar şi contra, s-a hotărât ca acest act juridic să fie pus în atenţia Parlamentului care ar urma să decidă calea de urmat pentru încetarea aplicabilităţii lui, fiind în totală discordanţă cu prevederile Legii 291/2007, act cu aceeaşi forţă juridică, dar mai nou.

2.2. Semnarea şi ratificarea acordului suplimentar la protocolul de la Paris privind Statutul comandamentelor militare internaţionale aparţinând Tratatului nord atlantic, semnat la Paris la 28 august 1952[14]

Până în prezent, România nu a simţit o nevoie acută de a legifera această înţelegere internaţională, unde o parte este NATO, reprezentată de Comandamentul suprem al puterilor aliate în Europa şi Comandamentul suprem aliat pentru transformare, iar cealaltă este statul membru. Tratatul se refera, în special la inviolabilităţi, imunităţi, statutul membrilor etc.. Remarcăm că proiectul are un capitol dedicat facilităţilor în legătură cu achiziţiile, importuri şi exporturi, fonduri, donaţii, cumpărături, carburanţi şi lubrifianţi, folosirea porturilor, aeroporturilor etc..

2.3. De lege ferenda în ceea ce priveşte Legea nr. 291/2007 privind intrarea, staţionarea, desfăşurarea de operaţiuni sau tranzitul forţelor armate străine pe teritoriul României[15]

Prima intervenţie de modificare a legii, ar putea fi efectuată prin completarea acesteia cu aspecte referitoare la procedura de aprobare a înfiinţării bazelor militare străine. Trebuie să se precizeze cine anume face propunerea forului legislativ al ţării pentru permanentizarea existenţei forţelor străine pe teritoriul naţional şi de ce avize are nevoie pentru aceasta. Aici opinăm ca autorul propunerii să fie Preşedintele României, având avizul Consiliului Suprem de Apărarea Ţării, al cărei preşedinte este. Tot aici, este nevoie să lărgim sectorul prezenţelor militare străine permanente, pentru a evita interpretarea nedorită, conform căreia legea conţine o enumerare strict limitativă – comandamente, baze militare sau reprezentanţe militare. Părerea noastră este că legea ar trebui să conţină, în aceasta privinţă, expresii mai generale, de genul „entităţi" sau „structuri", care să confere flexibilitate dispoziţiilor.

A doua sugestie, ar fi ca, în legea respectivă, să se reglementeze „prepoziţionarea", odată cu stabilirea unei definiţii pentru aceasta sintagmă. In accepţiunea noastră, pentru pregătirea minuţioasă a unor operaţiuni şi desfăşurarea eficientă a acestora, este necesar ca trupele să aibă, din timp, adăpostite în anumite locaţii cu caracter public, materiale şi echipamente de care vor avea nevoie, poate chiar însoţite de personal de pază, întreţinere, transport etc.. Legea trebuie să conţină şi o trimitere la înţelegeri tehnice, care privesc

[14]Act publicat în: Monitorul Oficial nr. 845 din 15 septembrie 2004;
[15]Ibidem pag. 5;

prepozitionarea, această dispoziţie constituind o bază legală pentru încheierea acestora între români şi forţele armate străine.

O a treia recomandare are legătură cu intrarea forţelor străine pe teritoriul nostru prin metode mai puţin uzuale, cum ar fi paraşutarea. În prezent, legea vorbeşte de trecerea frontierei de stat „prin alte locuri", fapt ce poate conduce la interpretări restrictive.

O ultimă situaţie supusă atenţiei este aceea că, tot spre profitul securităţii naţionale, România poate pune la dispoziţia forţelor armate străine, cu suportarea cheltuielilor de către statul român, o serie de facilităţi, produse, materiale, bunuri şi servicii. În prezent, nu există o asemenea posibilitate decât contra cost şi nu este exclus să ne dorim să oferim ceva cu titlu gratuit în scopul protejării unor interese vitale ale statului român.

2.4. Amendarea Codului fiscal[16]

Ne gândim aici la modificări şi completări ale Codului fiscal în vederea oferirii partenerilor aliaţi a unor condiţii de desfăşurare a trupelor proprii pe teritoriul romanesc, lipsite de povara unor taxe descurajatoare. Dacă cetăţenii români sunt obligaţi prin legea fundamentala şi prin alte legi să plătească taxe şi impozite pentru statul român, care, la rândul său, foloseşte aceşti bani, pentru a presta servicii indispensabile pentru cetăţenii lui, nu putem afirma acelaşi lucru şi pentru cetăţenii altor state, membri ai forţelor străine, aliate, care îşi plătesc contribuţiile faţă de statele lor, şi sunt în România pentru a contribui la creşterea capacităţii de apărare a ţării noastre.

Pentru binele României, aceştia nu trebuie să se supună reglementarilor fiscale ale statului român, fiindcă în acest fel nu pot fi motivaţi să participe la misiuni militare pe teritoriul nostru. Nici ei şi nici statele de care aparţin. La fel de corect este ca şi cetăţenii români, membri ai unui comandament internaţional, atunci când acţionează în interesul serviciului, să beneficieze de scutiri, facilităţi, excepţii etc., exact ca şi colegii lor străini.

2.5. Amendarea Legii 346/2006 privind organizarea şi funcţionarea Ministerului Apărării Naţionale[17]

Actul normativ susmenţionat ar putea suferi câteva modificări sau completări care ţintesc strict un singur ţel: întărirea capacităţii de cooperare cu aliaţii pe teritoriul nostru, prin reglementări ce vizează o mai eficientă şi pragmatică re-structurare a armatei în situaţii critice, modul de trecere sub autoritatea Alianţei a unor structuri de comandă sau execuţie ale Armatei României, precum şi posibilitatea acordării de către Ministerul Apărării Naţionale de sprijin contra cost sau gratuit pentru entităţile internaţionale de apărare ce se înfiinţează pe teritoriul ţării.

Când vorbim de o re-structurare pragmatică, facem referire la faptul că o subordonare flexibilă a comandamentelor create pentru a îndeplini anumite misiuni, într-o anumită conjunctură, nu poate fi decât benefică, în opoziţie cu o gândire veche, rigidă, care nu se poate adapta noilor situaţii. Astfel, comandamentele s-ar putea afla fie în subordinea nemijlocită a unei structuri centrale, cum este Statul Major General, dar separate de structura de forţe, fie în interiorul structurii de forţe, ca element într-o categorie de forţe a armatei ori în afara acesteia.

2.6. Altele

La această dată, se pot anticipa doar, fără pretenţia de a prezice cu exactitate, toate intervenţiile legislative necesare pentru a facilita înfiinţarea şi buna desfăşurare a activităţii entităţilor militare internaţionale permanente înfiinţate cu acordul României pe teritoriul

[16]Act publicat în: Monitorul Oficial, Partea I nr. 927 din 23 decembrie 2003;
[17]Act publicat în: Monitorul Oficial, Partea I nr. 654 din 28 iulie 2006;

acestei ţări, cu participarea aliaţilor. Am trecut în revistă unele puncte nevralgice, care pot face obiectul unor amendamente, fără a închide însă lista.

Evident, pentru înfiinţarea comandamentului de divizie NATO la Bucureşti, probabil că va fi necesară semnarea câte unui memorandum de înţelegere cu fiecare ţară participantă, după cum, pentru buna funcţionare a entităţii NATO de integrare a forţei, Alianţa va dezvolta o întreagă arhitectură de acte normative, având în vedere că vor fi înfiinţate cinci structuri de acest gen în ţări diferite.

De asemenea, este necesar să punem în aplicare prevederile Memorandumului de înţelegere între Guvernul României şi cele două comandamente menţionate la punctul 2.2. privind acordarea sprijinului naţiunii gazdă pentru executarea operaţiilor şi exerciţiilor NATO.

Nu excludem ca, în anumite privinţe, să localizăm problemele *din mers* şi să venim cu soluţii legislative la vremea respectivă. Sarcina noastră este să diminuăm pe cât posibil producerea unor astfel de situaţii, care suprapunându-se cu incertitudinile şi tulburările inerente, generate de iminenţa unei agresiuni, pot genera nesiguranţă, instabilitate, panică, haos. Iată de ce, în această perioadă, este imperios necesar să ne sporim, prin maximă concentrare şi luciditate, capacitatea de predicţie.

BIBLIOGRAFIE:

1. *„Dacă ROMÂNIA ar fi atacată de RUSIA”*, http://qmagazine.ro/ce-nu-se-vede-la-tv/daca-romania-ar-fi-atacata-de-rusia/;
2. *„E lucrul cel mai grav trait de Romania in ultimele decenii. Un diplomat si un istoric, despre pericolul razboiului cu Rusia”*, http://stirileprotv.ro/emisiuni/dupa-20-de-ani/e-lucrul-cel-mai-grav-trait-de-romania-in-ultimele-decenii-un-diplomat-si-un-istoric-despre-pericolul-razboiului-cu-rusia.html;
3. *„Ioan Mircea Paşcu: Echilibrul militar din regiunea Mării Negre s-a schimbat în favoarea Rusiei”*, http://www.agerpres.ro/externe/2015/03/17/ioan-mircea-pascu-echilibrul-militar-din-regiunea-marii-negre-s-a-schimbat-in-favoarea-rusiei-12-22-03;
4. „*Merkel Promises Support for Baltic States Alarmed by Russia*”, http://www.wsj.com/articles/merkel-promises-support-for-baltic-states-alarmed-by-russia-1408383489;
5. *„Moscova sărbătoreşte un an de la anexarea Crimeii printr-un miting-concert în Piaţa Roşie, la care este aşteptat şi Vladimir Putin”*, http://www.agerpres.ro/externe/2015/03/18/moscova-sarbatoreste-un-an-de-la-anexarea-crimeii-printr-un-miting-concert-in-piata-rosie-la-care-este-asteptat-si-vladimir-putin-11-34-24;
6. „*NATO Agrees To 'Readiness Action Plan' To Counter Russia*”, http://archive.defensenews.com/article/20140603/DEFREG01/306030034/NATO-Agrees-Readiness-Action-Plan-Counter-Russia
7. *„Poroşenko: Amplasarea de rachete ruseşti în Crimeea creşte riscul unui conflict major în zona Mării Negre”*, http://www.agerpres.ro/externe/2015/03/19/porosenko-amplasarea-de-rachete-rusesti-in-crimeea-creste-riscul-unui-conflict-major-in-zona-marii-negre-14-02-22.
8. *„Rusia iar joacă cartea intimidării. Mută armele nucleare mai aproape de Europa”*, http://www.paginaderusia.ro/rusia-iar-joaca-cartea-intimidarii-muta-armele-nucleare-mai-aproape-de-europa/;
9. *„Stimulentul Putin. Oportunitatea unui tandem România-Polonia”*, http://www.romanialibera.ro/politica/institutii/stimulentul-putin--oportunitatea-unui-tandem-romania-polonia-370623;

10. *„Stratfor analizeaza ce sanse ar avea Romania in fata unei invazii rusesti”*, http://e-politic.ziuanews.ro/dezvaluiri-investigatii/stratfor-analizeaza-ce-sanse-ar-avea-romania-in-fata-unei-invazii-rusesti-168420;
11. Codul Fiscal din 2003, publicat în Monitorul Oficial, Partea I nr. 927 din 23 decembrie 2003;
12. Hotărârea Parlamentului nr. 29/2007 privind aprobarea intrării şi staţionării forţelor Statelor Unite al Americii pe teritoriul României în vederea desfăşurării activităţilor stabilite prin Acordul dintre România şi Statele Unite ale Americii privind activităţile forţelor Statelor Unite staţionate pe teritoriul României, semnat la Bucureşti la 6 decembrie 2005, ratificat prin Legea nr. 268/2006, publicată în Monitorul Oficial nr. 294 din 3 mai 2007;
13. Legea apărării naţionale a României nr. 45/1994, publicată în Monitorul Oficial nr. 172 din 7 iulie 1994;
14. Legea nr. 291/2007 privind intrarea, staţionarea, desfăşurarea de operaţiuni sau tranzitul forţelor armate străine pe teritoriul României, publicată în Monitorul Oficial nr. 758 din 8 noiembrie 2007;
15. Legea nr. 346/2006 privind organizarea şi funcţionarea Ministerului Apărării, publicată în Monitorul Oficial, Partea I nr. 654 din 28 iulie 2006;
16. Legea nr. 362/2004 pentru aderarea României la Acordul dintre statele părţi la Tratatul Atlanticului de Nord cu privire la statutul forţelor lor, semnat la Londra la 19 iunie 1951, şi la Protocolul privind statutul comandamentelor militare internaţionale, înfiinţate în temeiul Tratatului Atlanticului de Nord, semnat la Paris la 28 august 1952, publicată în Monitorul Oficial nr. 845 din 15 septembrie 2004;
17. Ordonanţa de urgenţă a Guvernului nr. 13/2000, pentru modificarea art. 5 din Legea apărării naţionale a României nr. 45/1994, publicată în Monitorul Oficial nr. 111 din 14 martie 2000;

Această lucrare a fost posibilă prin sprijinul financiar oferit prin programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului POSDRU/159/1.5/S/138822, cu titlul „Reţea Transnaţională de management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile „Ştiinţe Militare”, „Securitate şi Informaţii” şi „Ordine Publică şi Siguranţă Naţională” – Program de Formare Continuă a Cercetătorilor de Elită – „SmartSPODAS”.”

CONSTITUIREA GRUPĂRII DE FORŢE ÎN VEDEREA ÎNDEPLINIRII UNEI MISIUNI ÎN CONTEXTUL GEOSTRATEGIC DIN PROXIMITATEA ROMÂNIEI

Dr. Virgil-Ovidiu POP
General de brigadă, comandantul Brigăzii 282
Infanterie Mecanizată "UNIREA PRINCIPATELOR"

Ilie MELINTE
Locotenent-colonel, doctorand la Universitatea Naţională de Apărare "CAROL I",
Brigada 282 Infanterie Mecanizată "UNIREA PRINCIPATELOR",
e-mail: imelinte@hotmail.com.

Bogdan TUDORACHE
Locotenent-colonel, Brigada 282 Infanterie Mecanizată "UNIREA PRINCIPATELOR",
e-mail: bogdantudorache28@yahoo.com.

Rezumat: *Lucrarea prezintă posibilităţile constituirii unei grupări de forţe de reacţie imediată, de nivel tactic, capabilă să execute o misiune de luptă.*

Beneficiind de activitatea practică şi de lecţiile identificate, autorii aduc în atenţie capabilităţile forţei constituite, limitările actuale şi o analiză prin care efectele acestora să fie diminuate.

Concluziile şi propunerile vin în sprijinul factorilor de decizie privind pregătirea pentru luptă a acestor structuri şi identificarea relaţiilor de subordonare / cooperare între structurile aparţinând diferitelor categorii de forţe ale Armatei Române.

Cuvinte cheie: *transformare, organizare, model, acţiune, reacţie, grupare de forţe, misiune.*

Introducere

Perioada ultimilor ani a fost în general cea în care s-a impus caracterul integrat, intercategorii de forţe al acţiunilor militare. În această perioadă, urmare a revoluţiei tehnico-ştiinţifice, în special în domeniul informaticii, au fost lansate diverse concepte, care descriu acţiunile militare ca o competiţie în care câştigă acea parte implicată care înţelege mai bine spaţiul de luptă şi care transferă mai rapid această cunoaştere elementelor luptătoare proprii, pentru a aplica forţa necesară cu rapiditate şi precizie la distanţe mari. Succesul este reprezentat de utilizarea puterii de luptă în interacţiunea şi cooperarea dintre diferitele sisteme de armament şi structuri militare.

Reducerea efectivelor militare şi crearea structurilor de luptă cu posibilităţi de proiectare în orice zonă de operaţii, suple şi flexibile, apariţia şi utilizarea noilor tehnologii şi sisteme de armament au condus către schimbarea concepţiei de desfăşurare a acţiunilor, la adoptarea de noi strategii de tip JOINT, precum şi la o altfel de pregătire a forţelor pe timp de pace.

Componenta terestră va rămâne în continuare decisivă în acţiunile militare întrunite, în special datorită faptului că procesul de transformare pe care îl suferă va duce la posibilitatea

executării de către acestea a întregii game de acţiuni militare, cu caracter terestru şi aeromobil, indiferent de locaţie şi timp.

În abordarea conţinutului noilor concepte de ducere a acţiunilor militare trebuie să se ia în considerare precizia, viteza, raza de acţiune şi eficacitatea noilor tehnologii militare în curs de aplicare şi implementare.

Întrebuinţarea grupărilor de forţe are ca scop atingerea obiectivelor stabilite prin planul / ordinul de acţiune a marii unităţi.

1. Aspecte generale

Gruparea de forţe se poate defini, principial, ca o uniune temporară de structuri (unităţi şi subunităţi) de aceeaşi armă sau specialitate sau de specialităţi diferite, care fac parte din una sau mai multe categorii de forţe şi, mai nou, în urma creşterii nivelului de interoperabilitate între Armata României şi celelalte state membre NATO, ale unei alianţe, care acţionează sub o comandă unică şi care au ca misiune destinată realizării unui dispozitiv de luptă în vederea îndeplinirii unei anumite misiuni.

De aici rezultă caracterul temporar al constituirii acestei grupări de forţe, care este determinat de durata misiunii, de necesitatea creşterii mobilităţii şi flexibilităţii, elemente care vor conttribui decisiv la realizarea surprinderii inamicului, conform concepţiei de acţiune a comandantului.

Aceasta se constituie datorită nevoilor acţionale, doar pentru rezolvarea anumitor situaţii şi în condiţii specifice, nefiinţând pe timp de pace. Se vor constitui în perioada de preconflict, în special pentru executarea unor misiuni de apărare naţională sau colectivă, pe teritoriul naţional sau al altor state ale alianţei, în cadrul angajamentelor asumate.

Constituirea grupărilor de forţe, este determinată, atât în perioada preconflict cât şi pe timpul acţiunii militare, de: organizarea forţelor pe timp de pace şi la război; misiunile de executat; organizarea pentru luptă pe structuri acţionale; nivelul de operaţionalizare al unităţilor şi marilor unităţi; nevoile acţionale; dinamica acţiunilor militare; resursele necesare pentru atingerea nivelului de operaţionalizare ale forţelor; capacitatea de refacere şi redimensionare a forţelor; nivelul de dezvoltare al tehnicii şi armamentului; capacitatea statelor majore de a elabora, planifica şi conduce acţiunile militare.

Pentru constituirea grupărilor de forţe şi atingerea obiectivelor stabilite în cadrul operaţiei trebuie să se identifice soluţii eficiente, care să ia în considerare efectul cumulativ al factorilor enumeraţi mai sus.

Structurile care vor face parte din compunerea acesteia trebuie să îndeplinească următoarele condiţii:

– mobilitate şi dislocabilitate, adică posibilitatea de a le putea disloca rapid în orice arie de operaţii – pe teritoriul naţional sau în afara ţării (când situaţia impune acest lucru);

– susţinere şi autosusţinere – atât posibilitatea de a se asigura sprijinul logistic propriu pentru cel puţin 30 zile, cît şi posibilitatea de a putea fi aprovizionate ulterior pentru executarea operaţiilor de lungă durată;

– angajare efectivă – capacitatea de a angaja, în întreg spectrul operaţional, orice adversar, atât în operaţiile cu intensitate scăzută cât şi în cele cu intensitate ridicată;

– capabilitatea de supravieţuire – posibilitatea de a asigura protecţia forţelor şi a infrastructurii proprii împotriva acţiunilor inamicului;

– comunicaţii interoperabile – sisteme de comandă-control compatibile în cadrul tuturor structurilor din compunerea grupării de forţe, dar şi cu ale celorlalte structuri militare cu care se cooperează.

Conducerea Grupării de Forţe poate fi exercitată la nivel operativ de Comandamentul Grupării de Forţe Întrunite, iar, la nivel strategic, direct de către CNMC. Analizând situaţiile

posibile de constituire a Gruparii de Forţe pe teritoriul naţional considerăm că acestea pot fi: demonstraţie de forţă (pentru descurajarea unei potenţiale agresiuni), prin dislocarea acesteia într-o anumită zonă / poligon sau executarea acţiunilor militare întrunite pe teritoriu naţional, în cadrul apărării naţionale. Comandamentului Grupării de Forţe Întrunite va avea sarcina de a constitui o grupare de forţe, sub o comandă unică, în măsură să acţioneze pe teritoriul naţional sau, conform angajamentelor asumate în cadrul Alianţei, în afara acestuia. De altfel, în contextul geostrategic actual, României i se va atribui în cadrul alianţei un rol deosebit.

Necesitatea de a constitui şi de a proiecta o grupare naţională de forţe întrunite este determinată de existenţa mai multor imperative: strategic, tehnologic, al ameninţărilor şi respectiv, al diminuării riscurilor[1].

Imperativul strategic al constituirii grupării de forţe la nivel naţional este generat de faptul că în momentul de faţă nu ne putem permite să nu reacţionăm la ameninţări. Aceasta presupune că este nevoie de o forţă puternică, care să aibă o putere sporită de luptă, viteză şi manevrabilitate ridicate, pentru a acţiona, înfrânge sau respinge orice adversar. De asemenea nu trebuie scăpată din vedere executarea unei apărări active pe întreg teritoriul naţional.

Datorită ritmului rapid de dezvoltare a tehnologiei, *imperativul tehnologic* ne obligă la modificări structurale corespunzătoare şi la o reanaliză a conceptelor operaţionale. Gruparea de forţe astfel constituită, cu un nivel de operaţionalizare ridicat poate fi o soluţie.

Luând în considerare că ”majoritatea ameninţărilor, provocărilor sau pericolelor aferente societăţii umane prezintă un profil voalat, ceea ce împiedică o identificare a lor în mod facil şi o adoptare de soluţii de contracarare în timp scurt”[2] trebuie acordată consideraţie şi imperativului ameninţărilor.

Imperativul ameninţărilor identificate în contextul actual ne face să considerăm că necesitatea constituirii unei (sau mai multe) grupări de forţe va răspunde la ameninţările relativ noi[3]. Printre acestea amintim: creşterea instabilităţii regionale şi a ameninţărilor asimetrice crescute (intensificarea acţiunilor teroriste, achiziţionarea de arme de distrugere în masă, etc.); preluarea puterii militare de către grupări separatiste / naţionaliste, prin sponsorizarea acestora de organizaţii sau guverne cu interes în zonă; diversitatea, numărul mare de surse şi impredictibilitatea locului conflictelor. Toate acestea determină imposibilitatea folosirii unui anumit tip / categorie de forţe capabil să anihileze un adversar într-o anumită zonă.

Pentru a răspunde *imperativului diminuării riscurilor*, putem considera că pentru constituirea grupării de forţe trebuie luat în considerare faptul că riscurile identificate la adresa securităţii naţionale pot fi în următorii ani şi de natură militară şi convenţională, ceea ce impune, în primul rând operaţionalizarea şi dotarea corespunzătoare a unor structuri capabile să execute o ripostă imediată în spaţiul terestru, aerian sau naval şi, ulterior, de alte structuri destinate apărării naţionale cu termene de operaţionalizare mai mari.

Aşadar, în actualul context de securitate, este de aşteptat ca acţiunea militară, în primele momente ale crizei, să poată fi executată doar de o grupare de forţe întrunite şi integrate, cu putere de luptă ridicată, cu grad ridicat de dislocabilitate, flexibilă şi capabilă să desfăşoare o gamă variată de misiuni de luptă, sub diverse subordonări, naţionale sau NATO. Această grupare ar putea reprezenta o structură militară de vârf a Forţelor Armate, complet

---

[1]Colectiv de autori (coordonator Gl.lt.dr.Eugen BĂDĂLAN), *Concepte strategice şi operative de actualitate,* Editura CTEA, Bucureşti, 2004, p.32.

[2]BUŢA, Viorel, Gl.bg.(r) prof. univ. dr., *EVOLUŢIA CONCEPTULUI STRATEGIC AL NATO – continuitatea şi flexibilitatea unei alianţe în mediul internaţional de securitate*, Revista de Ştiinţe Militare, Editată de Secţia de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România, Nr. 1 (22), Anul XI, 2011, p.53.

[3]Colectiv de autori (coordonator Gl.lt.dr.Eugen BĂDĂLAN), *Concepte strategice şi operative de actualitate,* Editura CTEA, Bucureşti, 2004, p.34

integrată, care să includă structuri din cadrul forţelor terestre, aeriene şi (eventual) navale, cu un grad de organizare, dotare şi instruire ridicat, capabile să acţioneze întrunit.

Luând în considerare cele prezentate mai sus, apreciem că gruparea de forţe întrunite ar trebui să răspundă următoarelor cerinţe:

a) structurale: grad ridicat de completare cu personal; tehnică de luptă, sisteme de armament operaţională, echipamente militare moderne şi compatibile; nivel de instruire şi de interoperabilitate ridicat;

b) acţionale: capacitate de reacţie ridicată; sisteme de comandă, control, comunicaţii şi informaţii care să asigure desfăşurarea acţiunilor militare; capacitate de luptă şi de sprijin logistic adaptate întregului spectrul de operaţii militare; grad ridicat de autosusţinere şi independenţă logistică.

2. Managementul informaţiilor pentru luptă

Câmpul de luptă necesită luarea de către comandanţii fiecărei structuri luarea deciziilor oportune, susţinute de informaţii la toate nivelurile. La acest moment constatăm o creştere a cantităţii de informaţii şi foarte important este cum şi ce anume folosim din acestea în procesul planificării şi conducerii forţelor în acţiunile militare.

Caracteristicile şi cerinţele confruntărilor militare curente şi complexitatea situaţiei actuale politico-militare au dus la confirmarea şi acordarea unei mai mari atenţii rolului informaţiilor militare pentru luptă şi la integrarea structurilor de informaţii militare, dotate cu tehnică modernă şi bine pregătite, capabile să planifice şi desfăşoare acţiuni de culegere a informaţiilor pentru a putea fi analizate şi diseminate.

Informaţiile deţin un rol deosebit de important în sprijinul acţiunilor militare, urmărindu-se permanent asigurarea superiorităţii informaţionale în scopul asigurării unui suport informaţional sigur şi ancipativ luării deciziei. Acestea provin din surse specializate sau nespecializate, umane sau tehnice, obţinute prin acţiuni specifice, sau prin alte modalitaţi aflate la dispoziţia comandantului.

Pentru comandantul grupării de forţe de nivel brigadă aflat în zona de operaţii este important ca, pentru misiunea viitoare, să cunoască nivelul de instruire al personalului inamicului, starea operaţională a mijloacelor de luptă ale acestuia, sprijinul populaţiei din zona de acţiune.

În acest context se pot identifica capabilităţi ale structurilor HUMINT[4], IMINT[5] şi SIGINT[6] care vin în sprijinul grupării de forţe de nivel brigadă, mai ales în cadrul conflictelor moderne, în care acţiunile sunt bazate pe efecte:

- culegerea de informaţii;
- protecţia informaţiilor;
- interzicerea accesului la informaţii;
- managementul informaţiilor.

Pentru neutralizarea sau respingerea inamicului, atât elementele din cadrul structurilor de informaţii, cât şi forţele din subordinea brigăzii acţionează pentru a influenţa sau controla domeniul fizic (spaţiul, logistica, manevra, personalul sau echipamentele), informaţional (baze de date, fluxuri de informaţii) şi cognitiv (înţelegere, conştientizare, evaluare sau decizie)[7].

---

[4] Human Intelligence – informaţii culese de la surse umane

[5] Imagery Intelligence – informaţii culese de la surse specializate în prelucrarea imaginilor

[6] Signal Intelligence – informaţii obţinute din surse care acţionează în spectrul electromagnetic

[7] Conferinţa doctrinară a Forţelor Terestre, ed. V, 2007, p. 247

Succesul misiunii brigăzii este esenţial influenţat de folosirea unuia sau mai multor mijloace de acţiune INFOOPS[8]. Astfel, între fazele de observare şi orientare ale inamicului este indicată folosirea dezinformării şi înşelării militare, ulterior, pe timpul luării deciziei de către acesta fiind recomandată folosirea PSYOPS[9], pentru ca, în final, pe timpul ducerii acţiunii militare folosindu-se acţiuni de război electronic.

Forţele brigăzii, sprijinite informativ de elementele HUMINT, IMINT sau SIGINT urmăresc exploatarea, înşelarea, distrugerea, influenţarea sau degradarea unor categorii diverse de ţinte pe timpul confruntării: puncte de comandă, centre şi reţele de comunicaţii, radare, structuri de artilerie şi apărare antiaeriană.

Echipele HUMINT furnizează comandantului brigăzii informaţii despre intenţiile liderilor inamicului, care pot fi folosite ca avertizări în beneficiul protecţiei forţei, iar în cooperare cu structurile IMINT, identifică locaţiile cheie ale inamicului.

În cazul în care mijloacele tehnice nu pot fi întrebuinţate pentru culegerea de informaţii, echipele HUMINT pot reprezenta singura sursă de informaţii la dispoziţia comandantului grupării de forţe. Pentru a avea eficienţă maximă, în scopul coordonării efortului de culegere a informaţiilor, verificării valabilităţii acestora şi eliminării potenţialelor erori, echipele HUMINT trebuie să fie într-un contact continuu cu structura de informaţii a brigăzii şi alte mijloace de informaţii, supraveghere şi cercetare.

Structurile SIGINT şi război electronic oferă informaţii referitoare la capabilităţile, dispunerea, compunerea de luptă şi intenţiile inamicului. În plus, oferă informaţii referitoare la obiective importante din dispozitivul inamic, pentru angajarea acestora cu sistemul de foc din dotare. Totodată, sprijină acţiunile grupării de forţe executând atât atacuri electronice, cât şi protecţia electronică a forţelor şi mijloacelor acesteia.

Contribuţia majoră a IMINT la îndeplinirea misiunii brigăzii este adusă de detaşamentul UAV[10], ale cărui dotări satisfac nevoile informative la nivel tactic. În cadrul brigăzii, aceste acţiuni vizează cercetarea câmpului de luptă, ziua şi noaptea, stabilirea coordonatelor ţintelor şi efectele focului asupra acestora, marcarea / iluminarea cu radiaţii laser a obiectivelor în vederea lovirii cu rachete autodirijate.

Imaginile obţinute prin platformele IMINT îmbunătăţesc adesea nivelul înţelegerii de către statul major al grupării de forţe a situaţiei câmpului de luptă, sprijinindu-l pe acesta în concentrarea efortului şi protejarea puterii de luptă. Cu excepţia observării directe efectuată de observatorii de artilerie şi subunităţile de cercetare, imaginile obţinute de UAV sunt singurele care oferă posibilitatea comandantului să observe în timp real câmpul de luptă pe măsură ce acţiunile sunt în plină desfăşurare.

Deşi structurile centrale conduc acţiunile structurilor de informaţii, este evident că trebuie realizată o coordonare perfectă cu comandamentul grupării de forţe nivel brigadă. Informaţiile culese şi transmise la structura centrală sunt analizate şi diseminate ulterior, conform principiului „nevoii de a cunoaşte”. Totuşi, avertizările iminente sunt, însă transmise imediat comandantului şi ulterior structurilor superioare pentru elaborarea ordinelor de acţiune către gruparea de forţe. Între timp însă comandantul a reuşit să adopte măsurile minime necesare pentru evitarea pericolului.

Comandantul brigăzii sprijinite cu informaţii are responsabilitatea realizării unui sistem de comunicaţii şi informatică adecvat, care să permită valorificarea integrală a informaţiilor prelucrate şi puse la dispoziţie de structurile de informaţii sau subunităţile de cercetare.

---

[8] Information Operations – Operaţii Informaţionale
[9] Psychological Operations – Operaţii Psihologice
[10] Unmanned Aerial Vehicle - avioane fără pilot tip SHADOW 600

Produsul final al acţiunilor desfăşurate de structurile HUMINT, IMINT şi SIGINT este informaţia, care reprezintă de fapt cunoaşterea dimensiunilor câmpului de luptă – fizică, culturală, politică şi de moral, cunoaşterea inamicului şi a posibilităţilor lui de acţiune. Datorită progreselor tehnologice, acurateţea capabilităţilor de cercetare şi supraveghere au crescut, ceea ce a generat o reducere a implicării factorului uman în procurarea de informaţii, în favoarea folosirii HI-TECH-ului, respectiv senzoriilor montaţi pe UAV-uri. De asemenea, sistemele deservite de structurile SIGINT au devenit foarte eficiente, nelăsând inamicului multe şanse de folosire în deplină securitate sistemele de comunicaţii. Singura excepţie este dată de structurile HUMINT, care rămâne o importantă sursă de informaţii procurate prin metode inaccesibile sistemelor tehnice.

Pentru comandantul unei grupări de forţe de nivel brigadă, care acţionează independent sau în cadrul unui eşalon superior, informaţiile primite de la structurile specializate de culegere a acestora sunt un important sprijin în luarea unor decizii oportune şi constituie elemente esenţiale ale acţiunilor militare desfăşurate pentru folosirea puterii de foc a forţelor şi mijloacelor din subordine, mai ales datorită faptului că ele vizează ceea ce înseamnă de cele mai multe ori centrul de greutate al inamicului, şi anume sistemul de comandă şi control.

Brigada trebuie să dispună de informaţii pentru a desfăşura cu succes acţiunile militare. Acestea trebuie să fie relevante, esenţiale, oportune şi prezentate într-o formă accesibilă, pentru a fi înţelese şi utilizate rapid de către forţele de lovire, pentru a acţiona optim în scopul îndeplinirii misiunilor.

3. Organizarea pentru luptă

Schimbările de formă şi de conţinut care configurează conflictele de azi, impun ca reforma militară să promoveze crearea unor forţe de elită formate din unităţi selecţionate şi antrenate la standarde riguroase, dotate şi organizate conform misiunilor predilecte a fi primite şi, nu în ultimul rând, care au şi continuă să-şi îmbunătăţească experienţa de luptă.

Este probabil că în viitor armatele de masă vor continua să-şi atingă acele scopuri clare (intimidarea, presiunea, obţinerea succesului necondiţionat împotriva celor mai mici şi mai puţin dotaţi). Observăm însă tot mai des că, în condiţiile prelungirii unor situaţii de incertitudine, respectiv pe fondul indeciziilor şi a reacţiilor prompte de amploare, formaţiunile mici, profesioniste şi care se ghidează după planuri atent comandate au devenit capabile să nimicească inamicul sau să obţină succesul scontat fără să intre în conflict direct.

Vrem să evidenţiem aici faptul că în constituirea şi în modul de implicare în acţiunile militare a unei grupări de forţe, în special a celei de nivel brigadă, „se impune o atentă analiză a mediului operaţional şi a evoluţiei modurilor de acţiune a adversarului, lucru ce poate garanta menţinerea eficienţei structurii în operaţiile desfăşurate.”[11]

Continuând spre argumentarea celor de mai sus, aducem în discuţie două aspecte complementare care stau la baza eficienţei pe câmpul de luptă a unei structuri militare: organizarea pentru luptă şi instruirea.

Vorbind despre organizarea pentru luptă, se ştie că în cazul unei grupări de forţe de nivel brigadă din armata noastră putem discuta despre două maniere de organizare şi folosire a structurilor componente: cea clasică, în care unităţile şi subunităţile sunt angajate în formatul standard şi cea a organizării pe misiune, respectiv sub formatul grupurilor de luptă (battle groups).

---

[11]MITULEŢU, Ion, Col. prof. univ. dr., *Brigada mecanizată (infanterie, vânători de munte). Principii generale, organizare, loc, rol, destinaţie, principii de întrebuinţare în luptă, generalităţi privind operaţiile* – Curs universitar ARTĂ MILITARĂ FORŢE TERESTRE,Universitatea Naţională de Apărare „Carol I”, 2012, p.12.

Analiza condiţiilor în care se decide să folosirea forţelor în maniera grupurilor de luptă, diferită de cea clasică are motivaţii multiple. Aici facem referire atât la aspectele primare cum ar fi răspunsul cerut la 5 „C"(cine, ce, unde, când, de ce ?) dar şi la aspectele extinse privind necesitatea modelării tacticilor şi adaptării sistemelor de luptă la condiţiile speciale ale unor situaţii tactice.

Constituirea grupurilor de luptă presupune analiza detaliată a necesităţilor şi a posibilităţilor, ceea ce stă la baza organizării optime a forţelor de manevră, de sprijin de luptă şi de logistică, raportat la misiunea de îndeplinit[12]. Cazul ideal presupune ca resursa alocată să fie întărită proporţional cu misiunea de îndeplinit, respectiv cu ameninţarea. Dar realitatea ne obligă să luăm în considerare faptul că forţele şi mijloacele brigăzii sunt limitate, în situaţia constituirii unei grupări de forţe, baza o constituie structura de forţe şi mijloace avută la dispoziţie la momentul respectiv.

Scopul principal al constituirii a grupurilor de luptă este de a susţine concepţia acţiunii, în special privind cursul acesteia şi angajarea eficientă în operaţii a grupării de forţe de nivel brigadă. Activităţile desfăşurate pentru constituirea grupurilor de luptă ţin cont de următorii factori:

- structura brigăzii şi a elementelor primite din cadrul altor eşaloane;
- nivelul de încadrare şi dotare a structurilor;
- specificul brigăzii şi misiunile în care poate fi angajată;
- efectele şi nevoile de acţiune rezultate din analiza situaţiei;
- criteriile timp/spaţiu ale acţiunii militare;
- elementele flexibile ale sistemului logistic.

Avantajul major al grupurilor de luptă trebuie să fie determinat de sinergia creată prin gruparea de arme pentru o misiune specifică. Organizarea pe misiune presupune că grupurile de luptă sunt în măsură să se regrupeze rapid (în orice condiţii de anotimp, stare a vremii, ziua şi noaptea) în cadrul operaţiei ce se desfăşoară şi că acestea sunt compuse din subunităţi instruite în comun, lucruri care concură la succesul angajării în operaţie.

Mai mult, pe baza experimentării în cadrul exerciţiilor desfăşurate în poligoane, am adnotat că în condiţiile oricărei grupări, întregul potenţial al grupurilor de luptă poate fi dezvoltat şi pus în valoare doar prin instruirea colectivă şi unitatea de comandă manifestate la cel mai înalt grad de disciplină.

Aici avem în vedere cele două principii care trebuie să fie deplin înţelese şi implementate la toate eşaloanele: abordarea manevrieră şi comanda misiunii (incluse deja în doctrina Forţelor Terestre).[13]

Dezvoltând aceste principii susţinem ideea potrivit căreia acţiunile ofensive trebuie adoptate oricând este oferită oportunitatea, conform concepţiei de manevră a comandantului nemijlocit şi respectând intenţia celui cu două eşaloane mai sus. Grupurile de luptă trebuie să dezvolte şi să susţină astfel un ritm ridicat al operaţiei, element care se atinge doar prin instruirea efectivă, leadership puternic, o doctrină comună, repetiţii în comun, o bază logistică solidă şi eficienţa procedurilor în câmpul de luptă.

De regulă, un grup de luptă organizat în cadrul brigăzii mecanizate, include:

- comandamentul batalionului în jurul căruia se organizează forţa;
- până la 5 subunităţi de manevră, de regulă constituite din infanterie şitancuri;
- o subunitate de cercetare;

---

[12]MARTIN, Iulian, dr., *Structura, misiunile, standardele de instruire şi certificare a grupurilor de luptă europene*, în IMPACT STRATEGIC Nr. 4[37]/2010, Editura Universităţii de Apărare „Carol I", Bucureşti, p. 86.

[13]FT 1 / 2007- Doctrina Forţelor Terestre.

– până la 3 subunităţi de sprijin a manevrei (artilerie terestră, inclusiv armament antitanc);

– o subunitate de artilerie şi rachete antiaeriene;

– o structură de geniu la care se adaugă organizarea pentru misiune a mijloacelor specifice armei;

– logistică: detaşament suport logistic, parte din logistica unităţii „mamă" pentru fiecare subunitate, o subunitate medicală.

Principiile de întrebuinţare în operaţie a brigăzii mecanizate sau a unei grupări de forţe de acest nivel sunt: acţiunea în toate tipurile de teren; realizarea surprinderii; implicarea în acţiuni decisive; întrebuinţarea în acţiuni manevriere pe spaţii mari; întrebuinţarea modulară; sprijinul eficient şi oportun. Fiecare din principiile menţionate trebuie să fie însuşite de către comandantul de brigadă înaintea deciziei privind organizarea forţelor pe structuri de tip grup de luptă.

Analizând „câte" astfel de grupuri de luptă poate să genereze o brigadă mecanizată, observăm că se pot forma atâtea grupuri de luptă căte unităţi luptătoare are în subordine, deoarece regruparea se va face în jurul comandamentelor respective. Se pot organiza grupuri de luptă, în mod excepţional, sub comanda unor comandamente generate ad-hoc din cadrul batalioanelor sau al eşaloanelor superioare.

Disponibilitatea vine totuşi din faptul că se pot organiza grupuri de luptă diferite: mai puternice, mai uşoare, sau echilibrate, aspect dat de numărul de subunităţi de tancuri şi de infanterie din compunere. Organizarea se va decide în funcţie de misiunea brigăzii în cadrul eşalonului superior, de rezultatele obţinute din analiza misiunii, de manevra adoptată şi chiar în funcţie de rezultatele jocurilor de război.

Alte motivaţii sau situaţii care pot sta la baza deciziei formării grupurilor de luptă la nivelul brigăzii mecanizate sunt cele de natură externă: la ordinul eşalonului superior şi cea impusă de situaţia forţelor la un moment dat (pierderi, detaşări, resubordonări etc).

În primul caz avem situaţia în care brigada primeşte ordin să pună la dispoziţia eşalonului superior forţe, până la valoarea unei unităţi, pentru îndeplinirea unor sarcini.

A doua este situaţia în care comandantul de brigadă poate fi obligat să recurgă la reorganizarea forţelor, în urma unor acţiuni independente de comanda sa (pierderi, distrugeri), pentru continuarea luptei sau îndeplinirea unor sarcini de luptă utilizând forţele rămase la dispoziţie.

Deşi s-ar putea considera că „grupul de luptă" înlocuieşte vechiul „detaşament", argumentele privind diferenţa cum sunt date de caracteristici şi destinaţie. În primul caz avem gradul ridicat de independenţă, rolul manevrier accentuat, independenţa în acţiuni şi posibilităţi sporite de obţinerea efectului dorit al puterii de luptă. Privind detaşamentele, conform literaturii de specialitate, acestea se organizează în mod deosebit pentru o singură acţiune, precisă şi condusă de regulă de eşalonul superior.

Comanda şi controlul în cadrul unui grup de luptă nu diferă faţă de structurile militare obişnuite, în acest caz apărând doar particularităţi reieşite din caracterul de independenţă accentuată a structurii şi poate din limitările specifice privind folosirea în luptă a unor forţe cu statut aparte.

Comandamentul grupului de luptă păstrează organica comandamentului de batalion pe cadrul căruia se formează dar, în mod obligatoriu este augmetat cu specialişti în utilizarea forţelor care vin în compunere, altele decât dispune unitatea respectivă. Din practica la nivelul brigăzii am dedus că se impune prezenţa specialiştilor pentru întrebuinţarea structurilor care vin din afara brigăzii mecanizate sau a batalionului cum sunt: aviaţia, tancurile/infanteria, artileria, elementele ISTAR, CIMIC, PSYOPS).

Un alt adevăr desprins din experienţa misiunilor de luptă şi al aplicaţiilor este că eficienţa acţiunii unui grup de luptă depinde covârşitor de abilităţile profesionale şi de personalitatea comandantului, elemente care sunt evidenţiate în toate activităţile.

4. Instruirea

Instruirea trupelor trebuie să vină în completarea unor concepţii ale operaţiilor care pun accentul pe neprevăzut şi contracararea sa. Pe timpul instruirii, trupele şi statele majore trebuie puse în situaţii cât mai puţin familiare şi forţate astfel să gândească creativ.

Aspectele prezentate mai sus iniţiază crearea unei imagini asupra modului de constituire a structurilor de tip grup de luptă; trebuie subliniat însă faptul că, pentru asigurarea criteriilor de angajare decisivă în operaţii atât a componentelor cât şi a întregii grupări de forţe de nivel brigadă, trebuie aplicată foarte precis componenta instruire. Instruirea structurilor trebuie să fie orientată eficient spre dezvoltarea sau îmbunătăţirea caracteristicilor specifice unei forţe credibile cum sunt mobilitatea, puterea de foc, flexibilitatea, capacitatea de autosusţinere şi care-i conferă capacitatea de a duce la îndeplinire orice misiune ce-i este încredinţată.

Un pas important în domeniul instruirii forţelor îl constituie implementarea scenariului, respectiv al aplicaţiei unice la nivelul întregii categorii de forţe terestre. Implementarea acestei decizii o găsim oportună nu doar datorită faptului că asigură o necesitate imperativă dată de situaţia militară din proximitatea ţării noastre, ci şi pentru că se sprijină pe o bogată activitate de experimentare şi aplicare desfăşurată în ultimii ani.

Facem referire aici la activitatea Brigăzii 282 Infanterie Mecanizată, unde, începând cu anul de instrucţie 2008, a fost propusă şi aplicată varianta „aplicaţiei unice" cu scopul precis de îmbunătăţire şi de perfecţionare a concepţiei şi a asigurării cadrului tactic adecvat pentru exerciţiile, taberele de instrucţie şi aplicaţiile tactice care se desfăşoară de către marea unitate şi unităţile subordonate (până la brigadă inclusiv) pe o perioadă de un an.

Succesul „aplicaţiei unice" a fost bine înţeles la nivelul întregii categorii de forţe, ceea ce a determinat ca în anii următori, la nivelul tuturor brigăzilor, să fie stabilit un scenariu tactic, care să poată fi folosit pentru îndeplinirea obiectivelor şi cerinţelor de instruire ale acestora, funcţie de destinaţia şi misiunile acestora, nivelul de performanţă atins anterior şi de capabilităţile acţionale specifice structurilor implicate.

Această aplicaţie unică reprezintă „cadrul tactic general prin care se integrează instrucţia la nivelul unităţilor şi marilor unităţi, se asigură o concepţie unitară şi modernă de desfăşurare şi prin care se răspunde cerinţelor de pregătire ale unităţii şi marii unităţi"[14]; aceasta are un grad de complexitate ridicat, dar oferă totodată flexibilitate comandanţilor în procesele de planificare şi de execuţie.

Această variantă de elaborare şi organizare a scenariilor pentru exerciţiile de comandament şi cu forţe, aplicată pe perioada unui an de instrucţie, asigură desfăşurarea procesului de instrucţie într-o o concepţie unitară.

Valoarea acestei idei a crescut exponenţial an de an, lucru remarcat prin natura şi amploarea exerciţiilor cu trupe în teren desfăşurate la nivelul brigăzilor mecanizate, caracteristici care au antrenat fără echivoc toate tipurile de structuri operaţionale din forţele terestre dar şi din celelalte categorii de forţe.

---

[14]TOMESCU, Cătălin, T., Gl.bg., Dr., Teză de doctorat: *Consideraţii privind instruirea Forţelor Terestre în contextul participării acestora la gestionarea conflictelor militare la nivel naţional şi global*, Universitatea Naţională de Apărare „Carol I", Bucureşti, 2010, p. 146-147.

Seria de avantaje ale aplicaţiei unice şi care au impus-o ca soluţie în abordarea procesului de instruire a întregii categorii de forţe în ultimul an cuprinde următoarele:

– asigură caracterul interarme[15] şi întrunit[16] prin modul de elaborare şi executare a fazelor exerciţiului. Astfel, pot fi cuprinse toate etapele specifice participării unei grupări de forţe la o acţiune militară (perioada de creştere a capacităţii operaţionale, dislocarea în teatrul / zona de operaţii, desfăşurarea acţiunilor militare specifice luptei armate, urmate de cele de stabilitate);

– se poate adopta cu uşurinţă în pregătirea forţelor pentru desfăşurarea de acţiuni militare, în special pe teritoriul naţional;

– la nivelul brigăzii mecanizate, asigură coerenţa în îndeplinirea obiectivelor exerciţiilor şi a celor de instruire şi caracterul unitar al concepţiei (vizează întreg ansamblul operaţiunii militare preconizate);

– asigură parcurgerea sistematică de către structura instruită a tuturor fazelor şi etapelor, de la activare şi până la refacere;

– asigură comandanţilor (indiferent de eşalon) o mai mare flexibilitate, oferindu-le posibilitatea alegerii setului de exerciţii fără temerea că se pot abate de la obiectivele anului de instrucţie şi a rămâne în corelaţie cu cerinţele imediate naţionale şi aliate;

– simplifică activitatea statelor majore de brigadă şi de batalion şi cultivă iniţiativa privind adoptarea propriilor concepţii de pregătire;

– trasează cadrul general asigurând corelaţia dintre obiectivele de instruire naţionale şi cele ale NATO şi permite dezvoltarea oricărui scenariu de acţiune;

– permite tuturor unităţilor (de manevră, sprijin de luptă sau sprijin logistic) antrenarea repetată şi implementarea lecţiilor învăţate atât pe timpul instrucţiei specifice armelor şi specialităţilor, cât şi pe parcursul acţiunii interarme şi întrunite.

Această variantă se impune ca liant între categoriile de forţe (terestre, aeriene şi navale) dar şi ca soluţie în aplicarea unei formule coerente de asigurare a instruirii grupărilor de forţe care se activează sau se pot forma după necesităţile imediate privind securitatea ţării. Cu siguranţă, pe baza experienţei de luptă, aplicaţia unică va fi adaptată misiunilor specifice şi obiectivelor stabilite fiecărei structuri. Totodată, ea va fi îmbunătăţită pe baza experienţei câştigate de la an la an, a lecţiilor învăţate şi prin participarea la operaţii externe.

Importanţa optimizării instruirii în forţele terestre s-a impus în fiecare an sau etapă având mereu ca obiectiv principal pregătirea forţelor în vederea executării întregii game de acţiuni militare în cadrul unor operaţii interarme şi întrunite pe teritoriul naţional sau în afara acestuia. Cele două valenţe majore în acest caz sunt realizarea capabilităţilor operaţionale necesare participării la misiuni de apărare colectivă, tip art. 5, în cadrul structurilor NATO şi asigurarea securităţii spaţiului terestru al României prin acţiuni de luptă cu caracter limitat şi acţiuni de securizare în zona de responsabilitate.

Concluzii

Pentru o mai bună abordare a instruirii tactice în cele două domenii, individual şi colectiv, aplicaţia unică a venit în sprijinul tuturor structurilor de instruit prin stabilirea sistematică a tematicii de pregătire conform scenariului adoptat pentru anul de instrucţie (orientat pe formele principale de luptă apărarea sau ofensiva), asigurându-se atingerea nivelului de instruire scontat pentru participarea cu succes la un anumit tip de operaţie. Acest lucru s-a preferat în defavoarea stilului anterior în care structurile erau obligate să parcurgă

[15] Armele şi specialităţile specifice unei categorii de forţe
[16] Intercategorii de forţe armate

întreaga gamă de operaţiuni militare dar fără a atinge un nivel maxim de pregătire specific unui anume tip de acţiune militară.

În acest context, apreciem modul cum s-a impus ca pe timpul desfăşurării procesului de instrucţie, la nivelul Forţelor Terestre, să se intensifice şi permanentizeze exerciţiile şi aplicaţiile tactice de comandament şi/sau cu trupe, în format interarme şi întrunit. Mai mult, am observat deschiderea şi interesul celorlalte categorii de forţe privind participarea la activităţile importante ale Forţelor Terestre dar şi în concentrarea eforturilor spre aducerea instruirii cu caracter întrunit la nivelul de condiţie obligatorie pentru desfăşurarea exerciţiilor de comandament şi a aplicaţiilor.

Activităţile de instrucţie în comun, aduc un plus de valoare pentru toate categoriile de forţe şi asigură îndeplinirea obiectivelor privind asigurarea securităţii atât pe plan naţional cât şi în cel aliat. La nivelul brigăzii mecanizate s-a atins performanţa de a combina exerciţiile de la nivelul grupurilor de forţe, din Forţele Terestre (battlegroup – pe structură de nivel batalion) cu exerciţiile structurilor de aviaţie, exemple sugestive fiind exerciţiile MĂLINA 14, DANUBE EXPRESS 14 şi WIND SPRING 15, activităţi cu profund caracter interarme şi întrunit şi cu participare multinaţională.

Susţinem ideea că aspectul întrunit trebuie practicat şi la nivele mai mici, respectiv la task force – de nivel companie. Ca exemplu luăm instruirea elicopterelor de atac, a căror misiune de bază este sprijinul cu foc al structurilor din Forţele Terestre, care au accelerat instruirea în comun cu unităţile şi subunităţile din cadrul brigăzilor mecanizate. Progresele realizate la ultimele exerciţii din poligoane au asigurat accesul spre perfecţionarea metodelor de realizare a sprijinului aerian apropiat în formele principale de luptă armată.

Implementarea acestei proceduri, a eficientizat semnificativ procesul decizional, şi a produs deja o schimbare fundamentală în planificarea, desfăşurarea şi evaluarea exerciţiilor în comun Forţe Terestre - Forţe Aeriene, desfăşurarea aplicaţiilor tactice (de la nivel companie la nivel brigadă) în cadru întrunit fiind o condiţie obligatorie.

Activităţile întrunite de pregătire sunt demarate din acest an şi în relaţia cu Forţele Navale, în special pentru structurile din Forţele Terestre dislocate în Dobrogea şi a celor care nemijlocit sunt în cooperare cu structurile din Flotila de Dunăre. Acest lucru s-a asigurat tot prin adoptarea scenariului unic al exerciţiilor.

Caracterul integrat al scenariului unic aplicat la nivelul întregii armate oferă o oportunitate specială, bine sesizată şi folosită de către şefii instrucţiei şi doctrinei, respectiv conectivitatea exerciţiilor naţionale cu cele aliate (ale unui partener NATO sau multinaţionale). Acest lucru asigură atât atingerea reală a nivelului de interoperabilitate al grupărilor de forţe generate pe plan naţional necesar participării la operaţii în sistem aliat, cât şi posibilitatea verificării practice a reacţiei acestor grupări şi a forţelor aliate la apariţia unor ameninţări iminente sau pentru soluţionarea unor situaţii de agresiune militară.

Avem creată astfel puntea între eforturile naţionale şi cele ale partenerilor din Alianţă pentru pregătirea structurilor destinate să îndeplinească misiunile de luptă conform conceptelor strategice şi angajamentelor asumate.

Toate cele prezentate argumentează nu doar eficienţa implementării unui sistem întrunit de desfăşurare a pregătirii prin exerciţii şi aplicaţii pentru cele trei categorii de forţe, ci însuşi principiul acţiunii întrunite inerente în cazul apariţiei unei agresiuni la adresa ţării noastre sau a altei ţări membre NATO.

Mulţumiri:

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului POSDRU/159/1.5/S/138822, cu titlul „Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile "Ştiinţe Militare", "Securitate şi Informaţii" şi "Ordine Publică şi Siguranţă Naţională" - Program de Formare Continuă a Cercetătorilor de Elită –" SmartSPODAS"."

BIBLIOGRAFIE:

1. ***, Conferinţa doctrinară a Forţelor Terestre, ed. V, 2007.
2. ***, CRIZA, CONFLICTUL, RĂZBOIUL Volumul IV: Sisteme militare şi civil-militare folosite în gestionarea crizelor şi conflictelor. Pericole, ameninţări, riscuri la adresa acestora. Criterii şi metodologii de evaluare şi de testare, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2007.
3. ***, FT 1 Doctrina Forţelor Terestre.
4. ***, Ordinul privind instrucţia în Forţele Terestre în anul 2015.
5. BUŢA, Viorel, Gl.bg. (r) prof. univ. dr., EVOLUŢIA CONCEPTULUI STRATEGIC AL NATO – continuitatea şi flexibilitatea unei alianţe în mediul internaţional de securitate, Revista de Ştiinţe Militare, Editată de Secţia de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România, Nr. 1 (22), Anul XI, 2011.
6. Colectiv de autori (coordonator gl.lt.dr.Eugen BĂDĂLAN), Concepte strategice şi operative de actualitate, Editura CTEA, Bucureşti, 2004.
7. FRUNZETI, Teodor, Gl.lt. prof. univ. dr., Putere naţională şi putere militară, în "LUMEA 2011 – Enciclopedie politică şi militară (studii strategice şi de securitate)", Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2011, p.21.
8. MARTIN, Iulian, dr., Structura, misiunile, standardele de instruire şi certificare a grupurilor de luptă europene, în IMPACT STRATEGIC Nr. 4[37] / 2010, Editura Universităţii de Apărare „Carol I", Bucureşti.
9. MITULEŢU, Ion, Col. prof. univ. dr., Brigada mecanizată (infanterie, vânători de munte). Principii generale, organizare, loc, rol, destinaţie, principii de întrebuinţare în luptă, generalităţi privind operaţiile – Curs universitar ARTĂ MILITARĂ FORŢE TERESTRE, Universitatea Naţională de Apărare „Carol I", 2012.
10. TOMESCU, Cătălin, T., Gl.bg.dr., Teză de doctorat: Consideraţii privind instruirea Forţelor Terestre în contextul participării acestora la gestionarea conflictelor militare la nivel naţional şi global, Universitatea Naţională de Apărare „Carol I", Bucureşti, 2010.
11. www.buletinul.unap.ro.
12. www.cssas.ro.
13. www.dresmara.ro.
14. www.impactstrategic.ro.
15. www.infocercetare.ro.
16. www.strategii21.ro.

AUTORITATEA ADMINISTRAŢIEI MILITARE. DREPTUL DE A COMANDA ÎN ARHITECTURA ADMINISTRAŢIEI MILITARE

Marian Paul FUSEA
Doctorand în Ştiinţe militare al Universităţii Naţionale de Apărare „CAROL I ”
Bucureşti, România, e-mail: fuseapaul@gmail.com

Rezumat: *Delimitări teoretice în spectrul conceptul al autorităţii militare. Autoritatea militară, ca semnificaţie formală a „puterii” administraţiei militare de a comanda. Autoritatea militară – domeniu special al autorităţii şi şi puterii publice. Principalele proiecţii normative relative la structura şi faptul aplicat al autorităţii militare. Transferul de autoritate şi delegarea de autoritate – procedee de asigurarea a continuităţii autorităţii militare în administraţiile militare multinaţionale şi/sau autohtone.*

Cuvinte cheie: *administraţie, autoritate militară, delegare de autoritate, transfer de autoritate*

Introducere

Cercetarea teoretică a problematicii relative la *administraţia militară*, domeniu cu determinări complexe în spaţiul sistemic al construcţiei sociale, nu poate ocoli, ba, dimpotrivă, impune, abordarea *autorităţii* acesteia, ca vector fundamental al îndeplinirii misiunlor care îi sunt atribuite constituţional, precum şi a celor derivate din acestea, misiunile administraţiei militare, constituind, într-un fel, „pretextul” imperativ al definirii *autorităţii instituţionale* a administraţiei militare. Spre a înţelege semnificaţia instituţională şi operaţională a *autorităţii administraţiei militare*, ne vom opri, iată, un „punct obligatoriu de trecere”, doar definindu-l, asupra conceptului care o determină şi o presupune, respectiv *administraţia militară*. În planul înţelegerii sistemice a societăţii, opinăm că administraţia militară constituie un subsistem al administraţiei publice şi, în egală măsură, o componentă subsistemică a sistemului social global, înţelegând prin acesta sistemul social definit prin coordonatele sale statale şi naţionale. *Stricto sensu*, modelul conceptual invocat în abordările de specialitate consacră *administraţiei militare* definiri prin care este abordată fie ca *„totalitate a activităţilor privind organizarea, înzestrarea, asigurarea materială şi financiară a forţelor armate, precum şi elaborarea regulilor specifice pentru aplicarea în armată a legislaţiei şi actelor normative de stat”*[1], fie ca ansamblul de acţiuni al căror scop vizează *„organizarea şi conducerea de către autorităţile militare a întregii activităţi desfăşurate pe un teritoriu inamic ocupat în timp de război sau ca urmare a acestuia.”*[2] Admiţând cele două componente ale definiţiei, ca părţi inseparabile ale conceptului şi având în vedere raporturile sistemice dintre sistemul social, administraţia publică şi administraţia militară, putem accepta definiţia potrivit căreia *administraţia militară* este *„activitatea de organizare a executării şi de executare în concret a legilor ţării în domeniul militar prin acţiuni cu*

[1] *** Lexicon militar, Editura Saka, 1994, p.15
[2] Ibidem, p.15

caracter dispozitiv sau prestator"[3], activitate care *„se realizează de către Ministerul Apărării, ca organ central al administraţiei publice, prin organele sale de specialitate şi structurile deconcentrate şi/sau descentralizate în teritoriu."*[4]

1. Autoritatea militară

1.1 Autoritatea militară în legislaţia românească

În aria delimitărilor conceptuale relative la administraţia militară, caracteristica de fond a impunerii prerogativelor în cadrul administraţiei militare, în starea aplicată a formulei sale operaţionale, este *autoritatea militară*.

Opinăm că *autoritatea militară* este semnificată de *dreptul administraţiei militare de a comanda, de a da dispoziţii sau de a impune, în cazuri anume stipulate în lege, supunerea necondiţionată informal faţă de propriile decizii.*

Excursul relativ la invocarea specifică a *autoritatea militară*, precum o regăsim conceptual în fondul legislativ românesc, denotă situaţii de excepţie, în care rolul determinant îl are administraţia militară. Astfel, urmărind referirea nemijlocită în exprimările legislative a noţiunii de *autoritate militară*, o regăsim, mai întâi, în legea cu privire la actele de stare civilă în care se precizează că, în mod special, în documentele de acordare a cetăţeniei, în condiţiile în care un anumit teritoriu se află sub jurisdicţia administraţiei militare, sunt prezentate : "... *extrase de pe actele de stare civilă ce au fost eliberate de autorităţile militare în baza legii*"[5]. O utilizare mai accentuată a sintagmei o regăsim în legea[6] în care sunt reglementate preponderent activităţi specifice administraţiei militare, precizându-se aspecte, precum: *„bunurile se rechiziţionează numai în baza ordinului de predare emis de autorităţile militare"*[7]; *„Ordinul de predare a bunurilor ce se rechiziţionează va cuprinde, obligatoriu, denumirea autorităţii militare emitente şi a unităţii beneficiare, temeiul legal al rechiziţiei, datele de identificare a bunurilor, a proprietarului sau a deţinătorului acestora, precum şi menţiunile despre locul şi termenul predării bunurilor"*[8]; *„Ordinul de chemare va cuprinde, obligatoriu: denumirea autorităţii militare emitente şi a unităţii beneficiare, temeiul legal al chemării, numele, prenumele şi domiciliul persoanei chemate, termenul şi locul unde trebuie să se prezinte."*[9] Într-un alt context normativ[10], reglementând activitatea administraţiei militare pe durata stării de asediu, invocându-se rolul *autorităţii militare*, sunt specificate drepturile legale ale acesteia, semnificative fiind cele care decurg din următoarele prevederi ale legii: „*În exercitarea atribuţiilor ce le revin pe durata stării de asediu sau a stării de urgenţă, autorităţile militare emit ordonanţe militare care au putere de lege(...)*[11] ... *„informaţiile cu privire la starea de asediu sau la starea de urgenţă, cu excepţia celor referitoare la dezastre, se dau publicităţii numai cu avizul autorităţilor militare"*[12] ... *„Ordonanţele militare se emit pe durata stării de asediu de ministrul apărării naţionale sau*

---

[3] Eugen Bădălan, *Administraţia militară – Lucrare de dizertaţie*, Şcoala Naţională de Studii Politice şi Administrative, Facultatea de administraţie publică, 2003, p.49

[4] Ibidem, p. 50.

[5] Legea nr. 119 din 16 octombrie 1996, republicată şi actualizată, *cu privire la actele de stare civilă*, Monitorul Oficial nr. 339 din 18 mai 2012.

[6] Legea nr.132 din 15 iulie 1997**,** *privind rechiziţiile de bunuri şi prestările de servicii în interes public***,** Monitorul Oficial, nr. 161 din 18 iulie, 1997.

[7] Ibidem, Art.14, alin.(1)

[8] Ibidem, alin.(2)

[9] Ibidem, Art.17, alin. (2)

[10] Ordonanţa de urgenţă a Guvernului nr. 1/1999, *privind regimul stării de asediu şi regimul stării de urgenţă***,** Monitorul Oficial nr. 22 din 21 ianuarie 1999

[11] Ibidem, Art.8.

[12] Ibidem, Art.20, pct. „i"

de şeful Statului Major General, ca autorităţi militare exclusive la nivel naţional, când starea de asediu a fost instituită pe întregul teritoriu al ţării."[13] *... „Ordonanţa militară cuprinde (...) autoritatea militară emitentă, baza legală a acesteia, perioada de aplicare, data, ştampila şi semnătura autorităţii emitente."*[14] *... „Pe durata stării de urgenţă, (...) a) aplicarea de către autorităţile militare a măsurilor prevăzute în planurile aprobate conform dispoziţiilor prezentei ordonanţe de urgenţă şi ale decretului de instituire, este obligatorie."*[15]

De asemenea, rolul definit al *autorităţii militare* este invocat în legea relativă la a*cordul dintre statele părţi la Tratatul Atlanticului de Nord şi statele participante la Parteneriatul pentru Pace*[16], în care sunt definite, în special, *autorităţile militare* ale statului trimiţător, precum şi principalele atribute ale acestora, specificându-se: *„autorităţile militare ale statului trimiţător înseamnă acele autorităţi investite cu atribuţii de comandă şi de aplicare a legislaţiei acestui stat cu privire la membrii forţei sale sau ai componentei civile"*[17] *... „Autorităţile militare ale statului trimiţător vor acorda tot sprijinul pentru a asigura ca bunurile susceptibile de a fi confiscate de autoritatile vamale sau fiscale române ori în numele acestor autorităţi să fie puse la dispoziţie autorităţilor respective."*[18] *... „autorităţile militare ale statului trimiţător vor avea dreptul să exercite jurisdicţia penală sau competenţa disciplinară care le este conferită de legea statului trimiţător în privinţa persoanelor supuse legilor militare ale acestui stat"*[19] *... „autorităţile militare ale statului trimiţător vor avea dreptul să îşi exercite jurisdicţia exclusivă asupra persoanelor supuse legilor militare ale acestui stat pentru infracţiunile, inclusiv cele referitoare la securitatea sa, incriminate de legea statului trimiţător, dar nu şi de legea română."*[20]

Localizarea interbelică a conceptului operaţional relativ la *autoritatea militară*, ca instrument de operaţionalizare performantă a actelor administraţiei militare, o identificăm în consfinţirea constituţională a *puterii armate*, prin care, în fapt, era desemnată puterea publică, cu caracter militar, a statului. Specifică dar şi semnificativă acestei perioade, este opinia potrivit căreia *„autoritatea militară în mâinile căreia se trec puterile referitoare la menţinerea ordinii publice şi siguranţei statului este comandantul pe lângă care fiinţează un tribunal (Comandamentul militar al Capitalei, comandamentele de armată şi unele comandamente de divizii). Toţi acesşti comandanţi exercită aceste puteri fie în direct, fie delegând cu anumite atribuţii, pe comandanţii de garnizoane dincircumscripţia juridică respectivă."*[21]

Cu privire la conceptul operaţional prin care definim *autoritatea militară*, evidenţa manifestării acestuia în practica militară consemnează unele caracteristici, mai importante fiind aspecte, precum: în fondul legislativ românesc actual, sintagma autoritate militară/autorităţi militare nu are o utilizare insistentă, efect, în ultimă instanţă, al metamorfozei greoaie a culturii de apărare şi de securitate din modelul predecembrist în paradigma evoluţiei democratice a societăţii; în lipsa unei definiţii care să o consacre conceptual, sintagmei *autoritate militară* sau, după caz, *autorităţi militare*, îi sunt subsumate comprehensiv, în cuantumul ideatic al aceluiaşi înţeles, denumiri ale unor structuri militare cu

---

[13] Ibidem, Art.23, alin. (1)
[14] Ibidem, Art. 24. lit. b,c,d,e,h
[15] Ibidem, Art. 26, alin.(1)
[16] Legea nr. 61 din 24 aprilie 2000, pentru aplicarea Acordului dintre statele părţi la Tratatul Atlanticului de Nord şi celelalte state participante la Parteneriatul pentru Pace, cu privire la statutul forţelor lor, încheiat la Bruxelles la 19 iunie 1995, Monitorul Oficial nr. 185 din 28 aprilie 2000
[17] Ibidem, Art. 1, pct.5
[18] Ibidem, Art.29, alin.(2)
[19] Ibidem, Art.38, alin. (1), lit. b)
[20] Ibidem, lit. d)
[21] Paul NEGULESCU, Tratat de drept administrativ, vol. I, p.521

o puternică şi cunoscută imagine publică – Statul Major General sau fiecare din statele majore ale categoriilor de forţe ale armatei, centrele militare zonale, comandamentele specifice; afirmarea târzie şi, oarecum, timidă, în literatura juridică de specialitate a noţiunii *autoritate militară*, poate fi explicată şi prin faptul că, în acelaşi sens semantic, au fost larg folosite sintagmele *„organe militare”* şi *„cadre militare”*, atribuindu-li-se, practic, subliminal, calitatea de autorităţi militare. Mai consemnăm că, potrivit consacrării în faptul operaţional al *autorităţii militare*, aceasta nu face referire la raporturile manifeste în cadrul organismului militar, al instituţiei militare, ci, exclusiv, la raporturile directe şi legale ale acesteia cu cetăţenii sau cu autorităţile publice.

În ceea priveşte legislaţia specifică domeniului militar, dar şi actele normative interne care decurg din aceasta, aflăm sintagma despre care facem vorbire – *autoritate militară*, în Regulamentul disciplinei militare, în ediţia sa din anul 2000[22]. În corpul Regulamentului, este tratată distinct problematica relativă la *"Autoritatea militară şi obligaţiile care decurg din aceasta"*[23], însă, în continuarea dezvoltării sale normative, sunt mai frecvente expresiile „comandanţi”, „superiori”, „şef ierarhic”, „structuri militare”, „eşalon superior”, toate folosite subliminal în înţelesul *autorităţii militare*. Dar, constatăm, probabil dintr-o scăpare a meticulozităţii elaboratoare, că în contextul definirii abaterilor disciplinare[24] se apreciază că *"lipsa de respect manifestată faţă de comandanţi, superiori, egali sau inferiori în grad şi faţă de autorităţi"*[25], formularea ca atare conducând indirect către presupunerea că autorităţile despre care se face vorbire ar fi exclusiv cele civile. Apreciem că este o lacună a culturii şi operaţiunii teoretice de definire şi delimitare conceptuală a ceea ce înseamnă şi presupune *autoritatea militară*, construcţia acestui concept nefiind împlinită în paradigme statornice consacrate instituţional.

Dar, documentul ce uzează frecvent de utilizarea noţiunii conceptuale de *autoritate militară*, într-un fel consacrându-l în literatura normativă de profil, este Regulamentul general pentru conducerea acţiunilor militare[26]. Subscriindu-l sistematic noţiunii de *autoritate*, regăsim conceptul în construcţii care vizează şi normativizează: dispoziţia în sensul căreia *"comandantul este autoritatea investită sau asumată legal care exercită actul de comandă asupra personalului structurilor subordonate, precum şi asupra celui avut temporar în subordine"*[27] ... prevederea potrivit căreia *"actul de comanda include autoritatea şi responsabilitatea pentru folosirea eficientă a resurselor disponibile şi pentru planificarea acţiunii, organizarea, coordonarea şi controlul forţelor în vederea îndeplinirii misiunilor"*[28] ... rolul organizaţional al locţiitorului comandantului, definindu-l drept *"autoritatea învestita care participa la actul de comanda în limitele stabilite de comandant"*[29], precum şi pe cel al şefului de stat major, ca *"autoritate învestita cu exercitarea actului de comanda asupra statului major, el putând lua decizii care privesc întreaga unitate numai în absenţa comandantului şi a locţiitorului acestuia"*[30]. De asemenea, în componenta ajutătoare a Regulamentului este definită *„autoritatea asumată legal"*, ca *"drept de a da ordine, pe care*

---

[22] „R.G.-3, Regulamentul disciplinei militare, aprobat prin Ordinul ministrului Apărării Naţionale nr. M.70/2000, cu modificările şi completările ulterioare. Ordinul nu a fost publicat în Monitorul Oficial al României, Partea I, deoarece avea ca obiect reglementări din sectorul de apărare şi securitate naţională

[23] Ibidem, Capitolul II

[24] Ibidem, Art.44

[25] Ibidem

[26] A.N.-2, Regulamentul general pentru conducerea acţiunilor militare, Bucureşti, Editura Militară, 1998

[27] Ibidem, Art.3

[28] Ibidem, Art.4

[29] Ibidem, Art.7

[30] Ibidem, Art.17

un militar şi-l asumă potrivit actelor normative în vigoare, a ierarhizării gradelor, funcţiilor şi a competentelor în domeniu"[31].

Amintim, în sensul pledoariei noastre, nu în ultimul rând, regulamentul în vigoare al disciplinei militare[32]. Documentul atribuie un sector distinct *autorităţii militare*[33], ceea ce ne îndrituie presupunerea că referirile concrete la roluri instituţionale ale ierarhiei militare sunt abordate având suportul conceptual al *autorităţii militare*. Reţinem ca fiind reprezentativă pentru argumentarea discursului nostru, aserţiunea potrivit căreia *„Comandantul/şeful reprezintă autoritatea militară învestită legal cu responsabilităţi şi drepturi pentru exercitarea actului de comandă în cadrul unei structuri militare."*[34] În spiritul unei concluzii, cu evident caracter endemic, putem aprecia *„autorităţile militare ca fiind autorităţi publice învestite de lege cu exerciţiul puterii publice, care au atribuţii de comandă şi de aplicare a legislaţiei militare în zona lor de responsabilitate în timp de pace, de criză şi de război, exercitându-se sub controlul civil al autorităţilor publice constituţionale, de către organe militare cu caracter unipersonal sau colectiv, în conformitate cu principiile şi normele dreptului public."*[35]

1.2. Transferul de autoritate şi delegarea de autoritate

Abordarea conceptului *autoritate militară*, impune luarea în considerare a substitutelor sale operaţionale legale, respectiv *delegarea de autoritate* şi *transferul de autoritate*, foarte importante în exercitarea faptelor administrative şi de comandament ale administraţiei militare. Le consemnăm, definindu-le, după cum se manifestă în spaţiul operaţional al administraţiei militare. În principiu, *delegarea de autoritate* se realizează potrivit regulilor generale prin care, în situaţii anume prevăzute de lege, se recurge la exercitarea atribuţiilor specifice funcţiilor publice, de către persoane, altele decât cea care îndeplineşte calitatea instituţională de titular. În acest sens, sistemul normativ militar[36] conţine prevederi clare, precizându-se că, în funcţie de situaţie, *„Comandantul unităţii militare, în exercitarea actului de comandă, poate atribui, temporar, prin delegare de competenţă, o parte din atribuţiile şi responsabilităţile sale unor persoane subordonate."*[37] Analiza descriptivă a atribuţiilor comandantului[38], indică faptul că din suma reglementată a acestora (32 de responsabilităţi, definite şi delimitate prin enunţuri distincte), numai două nu pot fi supuse delegării autorităţii sale, respectiv răspunderea potrivit căreia *„asigură capacitatea operaţională a unităţii"*[39] şi obligaţia în temeiul căreia *„informează locţiitorul/şeful de stat major cu datele necesare preluării comenzii."*[40]

Relativ la *transferul de autoritate*, această procedură este specifică contextului operaţional în care este angajată o forţă multinaţională. Practic este modalitatea prin care, potrivit unor reguli asumate prin consens, se asigură comanda militară unică a tuturor forţelor participante la operaţie/misiune, indiferent de ţara de unde provin, ceea ce înseamnă că mai puţin una din forţele naţionale participante, toate celelalte admit să fie sub comanda unui

---

[31] Ibidem, Glosarul de termeni şi locuţiuni
[32] Regulamentul disciplinei militare, aprobat prin Ordinul ministrului Apărării Naţionale, M.64 din 10 iunie 2013, publicat în Monitorul Oficial nr.399 bis, 3 iulie 2013
[33] Ibidem, Secţiunea 2
[34] Ibidem, Art.11, alin. (1)
[35] Ion DRAGOMAN, *Actele autorităţilor militare,* Editura LUMINA LEX, Bucureşti, 2003, p.108
[36] Regulamentul de ordine interioară în unităţile militare, aprobat prin Ordinul M.92, din 17.09.2008, publicat în Monitorul Oficial nr.815, din 05.12.2012
[37] Ibidem, Art.40
[38] Ibidem, Art. 43
[39] Ibidem, Art. 43, lit. a)
[40] Ibidem, Art. 43, lit. u)

militar străin. De asemenea, înseamnă că *transferul de autoritate* reprezintă modalitatea de a asigura neîntrerupt şi unitar, din punct de vedere al concepţiei şi al totalităţii forţelor participante, conducerea forţei multinaţionale, altfel spus, a organizării executării şi a executării de către *administraţia militară multinaţională* a misiunilor primite. Pentru că, din perspectiva conceptuală a temei noastre, organismul de conducere a forţelor multinaţionale participante la o astfel de misiune, poate fi asimilat, din perspectiva faptelor administrative şi de comandament cu care este responsabilizată şi de care este responsabilă, *administraţiei militare multinaţionale*. Aşadar, rezultă o primă caracteristică a *transferului de autoritate*, în sensul că, dacă *delegarea de autoritate*, al cărei statut operează, la toate nivelurile administraţiei militare, în interiorul instituţiei militare naţionale, *transferul de autoritate* rezidă în trecerea deplină a conducerii operaţionale a forţelor participante la misiune în responsabilitatea unor comandanţi militari, alţii decât cei aparţinând structurii naţionale. *Transferul de autoritate* este un procedeu extrem de bine pus la punct, fiind precedat de asumarea de către admistraţiile militare ale statelor participante la forţa multinaţională, dar şi de către decidenţii politici din ţările respective, prin consens, a Regulilor de Angajare (Rules of Engagement - ROE)[41]. Acestea, în fond, sunt *„directive emise de către autoritatea politică/militară, către structurile militare participante la operaţia militară în care sunt precizate circumstanţele şi limitele în cadrul cărora acestea pot iniţia sau continua acţiuni de luptă cu forţele adverse.”*[42] Întemeiate pe legalitate, exercitarea controlului politic naţional asupra militarilor şi înţelegerea asumată a necesităţii militare, ROE asigură *transferului de autoritate* cadrul administrativ de operaţionalitate a forţelor multinaţionale, fără disfuncţii, stagnări sau involuţii specifice.

Transferului *de autoritate*, îi sunt proprii o serie de caracteristici care îl individualizează ca procedeu specific administraţiei militare multinaţionale.

Din această perspectivă, semnificative sunt cele care denotă aspecte care evidenţiază realităţi operaţionale cursive, precum:

- *transferul de autoritate* se produce fără alterarea principiului unităţii de comandă, care determină coeziunea operaţională a fortelor multinaţionale, orice contigent naţional, parte a forţei multinaţionale, putând primi ordine şi instrucţiuni exclusiv de la comandantul forţei, implicit şi al administraţiei militare multinaţionale;
- *transferul de autoritate* nu afectează autoritatea administrativă şi jurisdicţională, sub care acţionează comandantul unui contingent naţional, acesta, chiar aflându-se sub autoritatea operaţională a administraţiei militare multinaţionale, rămânând deplin subordonat autorităţilor naţionale ale ţării de proveniență (nu este o dublă subordonare, subordonarea faţă de autorităţile naţionale evitând divizarea responsabilităţii faţă de resursele, ordinea si disciplina forţelor pe care le comandă);
- *transferul de autoritate* conferă autorităţii militare un cadru juridic bine delimitat, în faptele administrative şi de comandament ale administraţiei militare multinaţionale, în sensul că în timp ce în interiorul organizaţional al contingentului naţional forţele participante se supun exigenţelor legislaţiei naţionale, în cadrul forţei mulţinationale acestea îndeplinesc întocmai faptele administrative şi de comandament al organizării executării şi, evident, ale executării misiunilor, în conformitate cu documentele şi procedurile standard de operare ale alianţei sau coaliţiei multinaţionale.

---

[41] Cf. Doctrina pentru operaţiile întrunite multinaţionale, Bucureşti, 2001, art. 123, alin. (1)

[42] Lt-col Ion PÎRGULESCU Col. (r.) prof. univ. dr. Lucian STĂNCILĂ, *„Comanda şi controlul structurilor de forţe din armata României pe timpul participării la misiuni specifice stării postconflict, în context multinaţional”*, Revista *Colocviu Strategic*, nr. 5/2009, p. 2

Concluzii

- Argumentele conceptuale expuse, îndrituiesc concluzia că autoritatea militară, prin atributele operaţionale care o reclamă, constituie suportul decizional al administraţiei militare. Mai mult decât atât, autoritatea administraţiei militare consistă legal în actul de comandă, de fapt în exercitarea acestuia, ca modalitate de înfăptuire a actelor şi faptelor administrative şi de comandament.

- De asemenea, excursul conceptual relativ la *autoritatea administraţiei militare* degajă un pachet coerent de concluzii a căror valoare teoretică este semnificată în următoarele enunţuri:

- în fondul legislativ şi normativ românesc actual, sintagma autoritate militară/autorităţi militare nu are o utilizare insistentă şi cursivă, efect, în ultimă instanţă, al metamorfozei greoaie a culturii de apărare şi de securitate din modelul predecembrist în paradigma evoluţiei democratice a societăţii;

- în lipsa unei definiţii care să o consacre conceptual, sintagmei *autoritate militară* sau, după caz, *autorităţi militare*, îi sunt subsumate comprehensiv, în cuantumul ideatic al aceluiaşi înţeles, denumiri ale unor structuri militare cu o puternică şi cunoscută imagine publică – Statul Major General sau fiecare din statele majore ale categoriilor de forţe ale Armatei, centrele militare zonale, comandamentele specifice;

- afirmarea târzie şi, oarecum, timidă, în literatura juridică de specialitate a noţiunii *autoritate militară*, poate fi explicată şi prin faptul că, în acelaşi sens semantic, au fost larg folosite sintagmele *„organe militare”* şi *„cadre militare”*, atribuindu-li-se, practic, subliminal, calitatea de autorităţi militare;

- potrivit consacrării *autorităţii militare* în faptul operaţional, aceasta nu face referire la raporturile manifeste în cadrul organismului militar, al instituţiei militare, ci, exclusiv, la raporturile directe şi legale ale acesteia cu cetăţenii sau cu autorităţile publice.

BIBLIOGRAFIE:

1. A.N.-2, Regulamentul general pentru conducerea acţiunilor militare, Bucureşti, Editura Militară, 1998
2. Bădălan, E., Administratia militara, *Lucrare de dizertaţie*, Şcoala Naţională de Studii Politice şi Administrative, Facultatea de administraţie publică, 2003
3. Doctrina pentru operaţiile întrunite multinaţionale, Bucureşti, 2001
4. Dragoman, I., *Actele autorităţilor militare,* Editura LUMINA LEX, Bucureşti, 2003
5. Legea nr. 119 din 16 octombrie 1996, republicată şi actualizată, *cu privire la actele de stare civilă*, Monitorul Oficial nr. 339 din 18 mai 2012
6. Legea nr.132 din 15 iulie 1997**,** *privind rechiziţiile de bunuri şi prestările de servicii în interes public***,** Monitorul Oficial, nr. 161 din 18 iulie, 1997
7. Legea nr. 61 din 24 aprilie 2000, pentru aplicarea Acordului dintre statele părţi la Tratatul Atlanticului de Nord şi celelalte state participante la Parteneriatul pentru Pace, cu privire la statutul forţelor lor, încheiat la Bruxelles la 19 iunie 1995, Monitorul Oficial nr. 185 din 28 aprilie 2000
8. Lt-col Pîrgulescu, I., Col. (r.) prof. univ. dr. Stăncilă, L., *„Comanda şi controlul structurilor de forţe din armata României pe timpul participării la misiuni specifice stării postconflict, în context multinaţional”*, Revista *Colocviu Strategic*, nr. 5/2009

9. Negulescu, P., *Tratat de drept administrativ*, vol.I, II, Ediţia a IV-a, Institutul de arte grafice, Bucureşti, 1934
10. Ordonanţa de urgenţă a Guvernului nr. 1/1999, *privind regimul stării de asediu şi regimul stării de urgenţă***,** Monitorul Oficial nr. 22 din 21 ianuarie 1999
11. R.G.-3, Regulamentul disciplinei militare, aprobat prin Ordinul ministrului Apărării Naţionale nr. M.70/2000, cu modificările şi completările ulterioare
12. Regulamentul de ordine interioară în unităţile militare, aprobat prin Ordinul M.92, din 17.09.2008, publicat în Monitorul Oficial nr.815, din 05.12.2012
13. Regulamentul disciplinei militare, aprobat prin Ordinul ministrului Apărării Naţionale, M.64 din 10 iunie 2013, publicat în Monitorul Oficial nr.399 bis, 3 iulie 2013

SUPORTUL DECIZIONAL AL ADMINISTRAŢIEI MILITARE

Marian Paul FUSEA
Doctorand în Ştiinţe militare al Universităţii Naţionale de Apărare "Carol I"
Bucureşti, România
fuseapaul@gmail.com

Abstract: *Angajarea teoretică a delimitărilor conceptuale cu privire la autoritatea militară, administraţia militară, comandant, organe militare, cadre militare. Decizia, responsabilitatea maximă a autorităţii militare. Relaţia decizională dintre administraţia militară şi autoritatea militară. Rolul autorităţii militare în proiectarea, materializarea şi maximizarea deciziei administraţiei militare. Actul de comandă – act al autorităţii militare. Semnificaţia ordinului, ca act al autorităţii militare. Fundamente juridice ale autorităţii şi deciziei militare.*

Cuvinte-cheie: administraţie militară, război, organe centrale, organe deconcentrate, structuri militare

1. Introducere

Problematica relativă la *administraţia militară*, cu complementarităţile care îi maximizează operaţionalizarea – autoritatea militară, faptele administrative şi de comandament, a fost dintru început în atenţia sistemului legislativ, dar şi a preocupărilor diriguitorilor publici ai construcţiei militare naţionale. Atenţia acordată *administraţiei militare* evidenţiază, deopotrivă, importanţa acesteia în sistemul naţional statal al administraţiei publice centrale, precum şi nevoia imperativă ca această componentă a organizării administraţiei centrale să fie riguros validată juridic din perspectivă legislativă. Din această perspectivă, vom centra discursul nostru pe evidenţierea evoluţiei conceptului de administraţie militară, precum şi a suportului decizional al acesteia, încheind prin relevarea interdpendenţelor operaţionale dintre autorităţile publice, administraţia publică şi administraţie militară.

2. Evoluţii în fondul conceptual al administraţiei militare

O restrospectivă asupra realităţii militare româneşti, dirijată spre perioadele nodale ale evoluţiei sale, ne înfăţişează instituţia militară, la momentul constituirii statului român, 1859, drept un corp profesional, racordat organizaţional, conceptual şi ca filozofie a pregătirii, la cele mai avansate metode, principii şi proceduri specifice ale epocii.

Dată fiind importanţa care se acorda disciplinei, în instituirea şi menţinerea unui status organizaţional coerent, activ şi performant administraţiei militare, nu surprinde că unul din primele documente juridice, unic prin caracterul său atotcuprinzător, este *Condica Penală Ostăşească*[1], intrată în vigoare în anul 1860, înlocuită, prin perfecţionarea elaborării sale, în anul 1873, cu un document cu profil similar – *Codicele de Justiţie Militară*, document care a îndrituit starea şi conduita disciplinară a administraţiei militare până în anul 1937.

Atenţia acordată consolidării administraţiei militare este reflectată de perfecţionarea continuă a legislaţiei penale cu caracter special, semnificative fiind, în acest sens, *Codul Justiţiei Militare*[2], document a cărui apariţie a fost impusă de reaşezarea juridică a statului

[1] Monitorul Oastei nr.13, din 1873
[2] A fost promulgat, prin Înaltul Decret Regal nr. 1297, la 17 martie 1937, în Monitorul Oficial nr. 66 din 20 martie 1937

român pe temelia şi în coordonatele Codului Penal „Carol al II-lea”[3], act intrat în vigoare în anul 1936.[4] Documentul a conferit faptelor administrative şi de comandament al administraţiei militare legitimitate juridică, dar şi cadrul legal de organizare a executăriii atribuţiilor şi misunilor specifice, precum şi de executare concretă a acestora.

După prăbuşirea edificiului teritorial care definea Statul Naţional Unitar Român, reconsiderarea normativă a sistemului juridic militar, în care urma să identificăm noile coordonate ale administraţiei militare, în contextul unui alt sistem al administraţiei publice centrale, era imperativă. În context, la 31 iulie 1940[5], Codului Justiţiei Militare sunt operate modificări semnificative, devenind ulterior *Codul justiţiei militare „Mihai I”*[6].

Perspectiva legislativă şi normativă adiacentă pragmatic şi conceptual temei noastre – *administraţia militară*, relevă o preocupare cursivă, mereu mai aplicată, a factorilor instituţionali pentru maximizarea publică a administraţiei militare. Exemplificările următoare sunt relevante.

Cea dintâi referire neechivocă, cu caracter normativ, la instituţia publică a *administraţiei militare* este stipulată în *„Decretul privind înfiinţarea de consilii de administraţie în toată oastea”*,[7] în care se menţionează că *„până la publicarea regulamentelor de administraţie şi contabilitate, corpurile militare sunt autorizate să execute aprovizionarea prin încheierile consiliilor de administraţie.”*[8] În aceeaşi perioadă, într-un act referitor la compunerea şi organizarea corpului de intendenţă militară, argumentându-se necesitatea organizării ca atare a acestei diviziuni a logisticii armatei, se milita pentru *„necesitatea de a organiza un corp de funcţionari însărcinaţi cu controlul şi supravegherea tuturor sarcinilor administrative ale armatei, sub autoritatea şi prin delegaţia ministrului secretar de stat de la Ministerul de Resbel, voind mai cu seamă a asigura economia în cheltuieli, buna întrebuinţare a fondurilor şi bunul trai al soldaţilor.”*[9] Apreciat ca fiind *„de cea mai mare importanţă pentru conservaţia apărătorilor statului, şi pentru menajarea veniturilor sale”*[10], consecinţă a solicitarii sale dinspre structurile reprezentative ale administraţiei militare, acest organism s-a dezvoltat continuu, în raport cu dezvoltarea instituţiei militare a statului. Apoi, noua organizare a „Ministerului de Resbel”, elaborată în anul 1862, includea în structura acestuia o direcţie destinată *„administraţiei generale”*, al cărei scop lucrativ consta în asigurarea serviciilor sanitare, de intendenţă, de transport şi de administraţie.[11]

În cristalizarea organizatorică şi conceptuală a administraţiei militare, ca instituţie destinată serviciului public al apărării naţionale, un rol important l-a avut elaborarea unui număr important de instrucţiuni şi regulamente militare care, practic, au pregătit înţelegerea necesităţii publice a administraţiei militare, semnificative fiind:

- *„Regulamentul pentru comandamentele militare”*, un capitol distinct al acestuia fiind atribuit *„administraţiei generale”*[12]; *„Instrucţiunile pentru determinarea atribuţiilor ofiţerilor de intendenţă militară”*[13], care operau o distincţie clară între raporturile operative

[3]Denumirea „ Carol al II-lea a fost stabilită conform legii intitulată „Denumirea Codurilor de unificare a legislaţiei”, decretată sub numărul 577/1936, publicată în Monitorul Oficial, partea I, nr. 73/27.03.1936
[4]Înaltul Decret Regal nr. 471 din 17 martie 1936, publicat în Monitorul Oficial nr. 65 din 18 martie 1936
[5]Decretul Lege nr. 2530/1940, publicat în Monitorul Oficial nr. 194, 31 iulie 1940
[6]*Codul Justiţiei Militare „ Regele Mihai I*”, Editura ziarului „Universul”, Bucureşti, 1941
[7]Monitorul Oastei, nr. 19, 28 ianuarie 1860
[8]Ibidem
[9]Monitorul oastei, an II, nr. 11, din 16 februarie 1861, p.161
[10]Ibidem, p.168
[11]Maior Ioan I. POPOVICI, *Organisarea armatei române*, vol.I, Schiţă istorică a organisărei de la 1830-1877, Partea a II-a, Roman, 1900, p. 196
[12]Monitorul oastei, an III, nr.37 din 25 martie 1863
[13]Monitorul oastei, an IV, nr.25/1864

dintre comandamentele militare şi structurile administrative, preconizând şi evoluţia acestora în contextul trecereii de la starea de pace la cea de război, în sensul că, în caz de război, *„comandantu-şef exercită toată autoritatea militară şi administrativă”*[14];

- *„Instrucţiunile asupra inspecţiei administrative”*[15], prin care se cerea *„oficiunilor de control ale corpului ofiţeresc, calitate, severitate şi onoare desăvârşită în inspecţiunile pe care le petrece la orice fel de companie, batalion, regiment sau divizie”*;
- *„Regulamentul asupra serviciilor miliţiilor”*[16], act care instituie şi reglementează constituirea consiliilor de administraţie, începând de la eşalonul batalion;
- *„Regulamentul asupra administraţiei şi contabilităţii corpurilor de trupă”*[17], în care erau stipulate *„îndatoririle agenţilor Consiliului de administraţie (...), principala atribuţie a acestuia fiind de a dirija administraţia în toate amănunte ei.”*[18]
- Consemnăm, de asemenea, Legea pentru înfiinţarea Consiliului Superior al Ministerului de Război[19] ale cărei prevederi îi stipulau menirea în sensul că scopul său era *„de a-l ajuta pe ministru în administrarea generală a armatei şi în elaborarea şi aplicarea legilor şi regulamentelor militare”*[20].

Un rol decisiv în configurarea şi consacrarea instituţiei militare, aflată în serviciul public al naţiunii, ca administraţie militară, l-a avut elaborarea, în temeiul Constituţiei din 1866[21] a *„Legii de organizare a puterii armate”*[22], consolidată conceptual, organizatoric şi juridic prin modificările aduse în anii 1872[23] şi 1874[24]. Potrivit acestei legi, care stipula fără echivoc că „organul central al organizării şi administrării *« intereselor de fiecare zi ale oastei »* este Ministerul de Resbel[25], în organica activă a armatei permanente se înfiinţa de sine stătător *comandamentul trupelor de administraţie*, care subordona *Corpul ofiţerilor de administraţie*, *Escadronul echipajelor de tren*, *Compania sanitară* şi *Compania lucrătorilor de administraţie*. Dar, decisive în sensul şi afirmarea demersului nostru, sunt înfiinţarea *Comitetului consultativ general*, ale cărui atribuţii constau în *„conducerea şi administraţiunea oastei”*[26], şi *Comitetul permanent de administraţie*[27], cu rolul de a asigura oportun şi operativ elaborarea regulamentelor şi a instrucţiunilor specifice formaţiunilor cu atribuţii administrative.

În definirea organizatorică, dar şi a necesităţii impunerii publice a structurilor operative al armatei, ca entităţi de/ale administraţiei militare, un rol aparte îl are *Legea asupra organizării comandamentelor armatei*[28] , în temeiul căreia *„au fost înfiinţate marile unităţi (corp de armată, divizie, brigadă) ca entităţi militare permanente încă din timp de pace, cu stat major şi compunere fixe, (...) cea mai mare diviziune a armatei devenind corpul de armată”*[29]. Consecinţă a acestei legi, *„teritoriul era împărţit sub aspectul organizării militare*

[14]Ion DRAGOMAN, *Actele autorităţilor militare*, Editura LUMINA LEX, Bucureşti, 2003, p.161
[15]Monitorul oastei, an VII, nr. 22 /1867
[16]Monitorul oastei, an VIII, nr. 21/1868
[17]Monitorul oastei, nr.27/1871
[18]Ion DRAGOMAN, Op. cit. p.163
[19]Monitorul oastei, nr.16/1878
[20]Ion DRAGOMAN, Op. cit. p.163
[21]Monitorul. Jurnal oficial al României”, nr.142 din 1/13 iulie 1866, pp.637-658
[22]„Monitorul oastei, an XI, nr.21 din 22 iunie 1868, pp.257-271
[23]Ibidem, nr.14 din 26 mai 1872, pp.265-275
[24]Ibidem, nr.14 din 1 iunie 1874, pp.597-608
[25]Ibidem, nr.21 din 22 iunie 1868, p.257
[26]“Monitorul oastei”, an XIX, nr.21 din 22 iunie 1868, p.260
[27]Ibidem, p. 274
[28]„Monitorul oastei”, an XIII, din 8/20 iunie 1882, p.143
[29]Maria GEORGESCU, *Istoria Marelui Stat Major*, 1830-1914, p.147

în patru mari regiuni, atribuite noilor comandamente, corpurile de armată, cu reşedinţele la Craiova, Bucureşti, Galaţi şi Iaşi."[30]

În evoluţia sistematizată, funcţional şi conceptual, a administraţiei militare naţionale, un rol definitivant a avut *Legea asupra administraţiei armatei*[31], care conferă problematicii militare a ţării un caracter sistemic, în acord sensibil cu organismele militare reprezentative ale epocii. În acest sens, dintre prevederile legii, sunt edificatoare aspectele care definesc axiomatic următoarele teze/principii: *„ministrul de război este şeful oastei şi poartă responsabilizaţiunea administraţiunii armatei"*[32]; *„administraţiunea armatei cuprinde serviciile intendenţei, artileriei, geniului, flotilei, sanitar, tezaurului şi al poştelor"*[33]; *comandantul de corp de armată are autoritatea de a dispune în conformitate cu legile, regulamentele şi deciziile ministeriale de toate fondurile şi materialele afectate comandamentului său, asigurând aplicarea cu exactitate a legilor, regulamentelor şi deciziilor ministeriale în toate serviciile"*[34]; *„comandanţii diviziilor au, sub autoritatea comandantului de corp de armată, faţă de trupele, stabilimentele şi serviciile din diviziile lor, aceleaşi îndatoriri de priveghere prescrise pentru comandanţii corpurilor de armată"*.[35]

În sensul aceluiaşi demers, de evidenţiere a evoluţiei conceptuale şi instituţionale a administraţiei militare, se înscrie nodal şi *Legea pentru organizarea armatei*[36], din care reţinem că în capitolul relativ la rolul Comandamentului[37] se stipula că Regele este capul puterii armate[38]; administraţia armatei este condusă de Ministerul de Război, organizat după o lege specială[39]; iar comandanţii de corpuri de armată şi divizie au sub ordinele lor toate trupele, serviciile şi stabilimentele generale ale armatei, precum şi cetăţile depinzând administrativ direct de Ministerul de Război.[40]

După constituirea Statului Naţional Unitar Român, în contextul reaşezării României în paradigmele juridice şi constituţionale ale întregirii naţionale, condiţia conceptuală a administraţiei militare este marcată de *Legea relativă la organizarea armatei*[41]. Din prevederile sale reţinem: proiectarea unei noi organizări militare, potrivit noilor realităţi naţioanle; constituirea inspectoratelor generale de armată prin delimitarea structurală de comandamentele de corp de armată şi de cele de divizie; segmentarea strategică a teritoriului naţional în şapte regiuni militare, corespunzător celor 7 corpuri de armată din organica armatei române; proiectarea responsabilităţilor privind conducerea armatei, Regele fiind „capul puterii armatei care, în timp de răsboiu poate delega comandamentul de căpetenie unui general"[42]

În condiţiile premergătoare celui de-Al Doilea Război Mondial, este promulgat *Decretul-Lege pentru organizarea şi funcţionarea Ministerului Apărării Naţionale*[43], care

---

[30]Ibidem, p. 179
[31]Monitorul oastei, nr. 11/1883, citat după Ion DRAGOMAN, Actele autorităţilor militare, Editura LUMINA LEX, Bucureşti, 2003, p.165
[32]Ibidem, Art.1
[33]Ibidem, Art.2
[34]Ibidem, Art.7
[35]Ibidem, Art.9
[36]Monitorul oastei, nr.15/1908, citat după Ion DRAGOMAN, Actele autorităţilor militare, Editura LUMINA LEX, Bucureşti, 2003, p.171
[37]Ibidem, Cap. X
[38]Ibidem, Art.35
[39]Ibidem, Art.36
[40]Ibidem, Art.37
[41]Monitorul Oficial nr.134 din 24 iunie 1924
[42]Costinel PETRACHE, *Apărarea naţională în România contemporană.Înţelegerea politică,* Editura CTEA, Bucureşti, 2006, p.81
[43]Cioflină DUMITRU, Alexandru OŞCA, *Istoria Statului Major General Român. Documente*, 1859-1947, Editura Militară, Bucureşti, 1994, p.280

consolidează statutul conceptual al *administraţiei militare*, în titluri distincte, reglementând *atribuţiile generale ale Ministerului Apărării Naţionale*[44], prin stipularea responsabilităţilor privind conducerea, administrarea şi modalitatea de control a armatei de uscat şi coordonarea, de către Marele Stat Major, a întregului ansamblu de operaţiuni subsumate apărării naţionale; structura, *componenţa şi atribuţiile organelor de conducere superioară, de comandament şi de pregătire*[45], în principal ale Subsecretariatului de Stat al M.Ap.N., ale Consiliului Superior al Armatei, Marelui Stat Major şi ale Inspectoratelor generale de armată.

Complementar, dar şi în susţinerea preocupărilor de esenţă strict juridică, problematica relativă la administraţia militară a fost în atenţia unor teoreticieni din linia întâi a gândirii militare româneşti. Subliniem această evidenţă prin câteva exemple. Astfel, în documentele specifice memoriei militare, în anul 1870, în „Studiul asupra serviciului intendenţei în campanie"[46] se apreciază că *„administraţia armatei, care are ca scop întreţinerea şi conservarea armatelor, este una din ramurile importante ale războiului, în acelaşi timp fiind o ramură a administraţiei publice"*.[47] Acelaşi autor, în *„Cursul de administraţie militară, pe scurt"*[48], plecând de la teza potrivit căreia *„orice armată care aspiră la onoarea de a se constitui pe baze solide şi durabile are nevoie şi de o bună administraţie, diferită de comandamentele care-i asigură disciplina şi instrucţia"*[49], afirmă tutelar: *„Comandamentul şi administraţia, iată temeiul ştiinţei militare, iată căpătâiele pe care se reazimă acea aglomeraţiune de oameni înarmaţi a căror sfântă misiune constă în a apăra patria şi cămninele părinţilor lor, iată în fine acel secret care face ca o mulţime de indivizi să se mişte ca un singur om, să lucreze şi să se agite sub impulsiunea unui singur cap"*.[50] Interesante, din perspectiva viziunii lor conceptuale, sunt şi aprecierile mr. Sergie Voinescu[51] potrivit cărora *„comandamentul este un cap cu mai multe braţe: capul este generalul, iar braţele sunt statul major"*[52], constatând că *„prea numeroşi în timp de pace, ofiţerii sunt insuficienţi în timp de război"*.[53] Găsim a fi deopotrivă interesantă şi folositoare edificiului epistemologic al conceptului, teza prin care se afirmă că „una din ramurile administraţiei publice este administraţia militară, care are ca obiect întreţinerea şi conservarea armatelor, fiind şi una din ramurile importante ale artei războiului, condusă de un corp de ofiţeri ce poartă numele de intendenţă militară."[54]

O contribuţie cu totul aparte pe frontul teoretic al dezvoltării conceptuale şi, implicit, aplicate a administraţiei militare, cu determinări în dezvoltarea doctrinară a dreptului administrativ militar, a avut-o colonelul de justiţie Vasile D. Chiru. Teoretician prodigios în domeniul dreptului şi al justiţiei militare, Vasile D. Chiru s-a aplecat detaliat asupra condiţiei, semnificaţiei şi importanţei administraţiei militare, ca domeniu atotcuprinzător al organizării, susţinerii şi acţiunii militare, din studiul său de referinţă[55], impunându-se atenţiei avizate teze, precum: necesitatea aplicată a delimitării şi a specializării organelor de conducere administrativă, „problema separării administrative impunându-se nu

---

[44]Ibidem, Titlul I, p.281
[45]Ibidem, Tilul II, p.287
[46]Adj.Cls.I Constantin MOVILĂ, *„Studiul asupra serviciului intendenţei în campanie",* Monitorul Oastei nr.27/1870
[47]Ibidem, p.211
[48]Monitorul Oastei, nr.28/1872, pp.83-197
[49]Monitorul Oastei, nr.28/1872, parafrazat de Ion DRAGOMAN, Actele autorităţilor militare, Editura LUMINA LEX, Bucureşti, 2003, p.181
[50]Monitorul Oastei, nr.28/1872, p.84
[51]Mr. Sergie VOINESCU, *Studiu asupra statlui major în luptă*, Monitorul Oastei, nr.10/1883, pp.42-65
[52]Ibidem, p.45
[53]Ibidem, p.57
[54]Dimitrie MIHĂILESCU, *Curs de legislaţie şi administraţie*, Tipografia GOLDSLEGER, Botoşani, 1889, citat de Ion DRAGOMAN, Actele autorităţilor militare, Editura LUMINA LEX, Bucureşti, 2003, p.183
[55]Chiru V., *Comandament şi administraţie*, Editura *Curierul Justiţiei Militare*, Sibiu, 1934

numai pentru armata combatantă, unde destinele administraţiei sunt înfrăţite şi sudate cu cele de comandament, ci şi pentru celelalte unităţi şi servicii ale armatei, pentru care separarea administrativă constituie o poruncă a vremii, categorică şi de neînlăturat"[56]; crearea unui organism administrativ temeinic specializat în săvârşirea totală a actelor şi a faptelor administrative, astfel încât componenta militară combatantă, destinată pregătirii pentru luptă şi ducerii luptei să fie degrevată de orice alte responsabilităţi, alte decât cele care rezultă din natura combatantă a menirii lor. Într-o altă lucrare[57], militând pentru delimitarea atribuţională clară între faptele de comandament şi cele administrative, sancţiona *„concepţia eronată a ofiţerilor combatanţi (...) perpetuată până în zilele noastre"*[58], potrivit căreia *„problemele de administraţie militară erau considerate chestiuni de prea mică importanţă, de care trebuie să se ocupe asimilaţii, administratorii şi intendenţii, aceasta fiind meseria lor, iar pentru treburiele administrative privitoare la subunităţi era arhisuficientă priceperea majurului."*[59]

3. Suportul decizional al administraţiei militare

Suportul decizional al administraţiei militare este reprezentat – instituţional, organizatoric şi tehnic, de către *organele centrale ale administraţiei militare* şi *organele deconcentrate ale administraţiei militare*, la care ne vom referi distinct în continuare, cu precizarea principalelor atribuţii şi responsabilităţi ale acestora.

Întrebarea care, inevitabil, se pune, şi nu în sens retoric, vizează nu doar anatomia actului decizional, în acest caz suportul instituţional, ci şi fiziologia acestuia, în care regăsim faptele administrative şi de comandament ale administraţiei militare, potrivit nivelurilor de funcţionare, implicit de responsabilitate militară sau politico-militară, fapte determinate şi/sau posibil a fi desfăşurate ca urmare a actului decizional. Din această perspectivă, într-o înţelegere extinsă, apreciem că, în expresie conceptuală, *suportul decizional al administraţiei militare* este configurat *suprastructural*, de totalitatea ideilor, teoriilor, concepţiilor şi a doctrinelor specifice naturii speciale a administraţiei militare şi a relaţiilor determinate de acestea, care, prin consacrare instituţională, fac posibilă proiectarea şi desfăşurarea actelor şi a faptelor administraţiei militare. În „creuzetul" preparator al suportului decizional al administraţiei militare, al deciziei însăşi, un rol important, inevitabil de altfel, îl are *sprijinul decizional*, exprimat prin totalitatea acţiunilor, administrative şi de comandament, care vin în susţinerea concretă a adoptării unei anume decizii, ca urmare a examinării unei probleme, reclamată de o situaţie concretă.

3.1. Organele centrale ale administraţiei militare

Strict, din perspectiva raportării conceptuale, organizatorice şi sistemice la ceea ce presupune instituţional *administraţia centrală*, ***organele centrale ale administraţiei militare*** sunt: Statul Major General, departamentele şi direcţiile centrale ale Ministerului Apărării Naţionale şi statele majore ale categoriilor de forţe. Actele şi faptele de comandament, dar şi cele administrative, ale ***organelor centrale ale administraţiei militare*** au caracter strategic şi sunt eminamente militare. Potrivit legii[60], în plaja organelor centrale ale Ministerului Apărării Naţionale sunt admise: Departamentul pentru politica de apărare şi planificare, Departamentul pentru relaţia cu Parlamentul şi informare publică, Departamentul pentru armamente, Statul Major General, Secretariatul general, Direcţia generală de informaţii a apărării, Direcţia

[56]Ibidem, p.5
[57]Vasile D. CHIRU, *„Dreptul administrativ militar"*, Editura Curierul Justiţiei Militare, Sibiu, 1936
[58]Ibidem, p.4
[59]Ibidem, p.5
[60]LEGE nr.346, din 21 iulie 2006, privind organizarea şi funcţionarea Ministerului Apărării, publicată în Monitorul Oficial nr. 654 din 28 iulie 2006, cu modificările ulterioare, Art.6, alin.(1)

management resurse umane, Direcţia financiar-contabilă, Direcţia instanţelor militare, Corpul de control şi inspecţie, Direcţia audit intern şi Direcţia medicală.

În continuare, vom sublinia principalele acte şi fapte de comandament ale Statului Major General, precum şi actele şi faptele administrative ale departamentelor centrale ale administraţiei militare.

❖ *Statul Major General* – Este organul administraţiei centrale cu atribuţiile cele mai importante, eminamente militare, în domeniul apărării naţionale, practic, prin actele şi faptele de comandament care-i sunt proprii gestionând în integralitatea sa procesuală apărarea armată a ţării. Din perspectiva prevederilor legale[61] care configurează public rolul Statului Major General în cadrul administraţiei militare naţionale, singurul cu rol bine determinat de organ central al acesteia, atribuţiile sunt generate de răspunderea cu care este învestit să asigure:

- conducerea, organizarea, planificarea şi operaţionalizarea forţelor;
- ridicarea graduală a capacităţii de luptă şi mobilizarea armatei;
- conducerea operaţiunilor întrunite şi conducerea sprijinului logistic operaţional;
- antrenarea comandamentelor şi trupelor şi pregătirea de bază şi de specialitate a personalului militar în activitate şi în rezervă;
- managementul carierei individuale a personalului militar;
- planificarea înzestrării structurii de forţe;
- definirea necesarului de echipamente militare, conform măsurilor şi cerinţelor operaţionale şi standardizarea în domeniul militar;
- implementarea sistemului de comandă, control, comunicaţii, computere, informaţii, informatică, supraveghere şi recunoaştere;
- cooperarea cu forţele armate străine şi desfăşurarea relaţiilor militare internaţionale;
- încheierea înţelegerilor tehnice cu armatele altor state şi cu organizaţiile internaţionale la care România este parte;
- asistenţa religioasă în Ministerul Apărării Naţionale şi promovarea valorilor specifice tradiţiilor militare, a culturii militare, educaţiei civice şi ceremoniilor militare.

În acelaşi timp, din perspectiva menirii sale de organ central al administraţiei militare, Statului Major General îi revin responsabilităţi privind:

- organizarea sistemului de pregătire a miniştrilor, secretarilor şi subsecretarilor de stat, precum şi a demnitarilor cu rang corespunzător acestora, prefecţilor, subprefecţilor şi a persoanelor cu responsabilităţi de conducere din administraţiile publice centrale şi locale, în vederea îndeplinirii atribuţiilor ce le revin pe linia apărării naţionale;
- avizarea documentaţiilor ministerelor, autorităţilor administraţiei publice şi agenţilor economici cu privire la amplasarea noilor obiective de investiţii şi dezvoltarea celor existente, în scopul încadrării acestora în infrastructura sistemului naţional de apărare;
- cuantificarea, maximizarea şi gestionarea operaţională a *direcţiilor de acţiune în domeniul apărarii*, respectiv: lupta împotriva terorismului; combaterea proliferării armelor de distrugere în masă; transformarea militară; managementul crizelor; informaţii pentru apărare; economia şi industria de apărare; punerea în valoare şi dezvoltarea potenţialului cultural, ştiintific şi uman de care dispune România; angajarea permanentă a preocupării pentru protecţia mediului şi a securităţii ecologice; gestionarea eficientă a resurselor pentru apărare;
- conducerea operaţională a forţelor pentru operaţii speciale, iar în situaţia participării la operaţii militare în afara teritoriului statului naţional, potrivit înţelegerilor tehnice încheiate cu partenerii străini;
- avizarea anuală a obiectivelor şi a programului de pregătire a teritoriului pentru apărare;

[61]Ibidem, Art.12, alin. (1)

• verificarea periodică a stadiului pregătirii populaţiei, economiei şi teritoriului pentru apărare, prin exerciţii şi antrenamente de mobilizare;

• elaborarea cadrului normativ, precum şi conducerea, îndrumarea şi controlul activităţii de evidenţă militară a cetăţenilor încorporabili şi a rezerviştilor, pe întregul teritoriu naţional.

❖ *Departamentul pentru politica de apărare şi planificare* – Fundamentala menirea instituţională a Departamentului rezidă în coordonarea îndeplinirii obligaţiilor internaţionale asumate, asigurarea aplicării politicii de apărare şi planificarea integrată a apărării şi coordonarea cooperarea politico-militară internaţională[62].

❖ *Departamentul pentru relaţia cu Parlamentul şi informare publică* – Esenţial, coordonează relaţia cu Parlamentul şi activitatea legislativă, asigură asistenţa juridică şi reprezintă interesele Ministerului Apărării Naţionale în faţa instanţelor de judecată şi a altor organe cu activitate jurisdicţională, asigură relaţiile cu alte autorităţi publice, precum şi cu organizaţiile neguvernamentale, îndrumă activitatea de armonizare a actelor normative şi asigură asistenţa juridică pentru încheierea înţelegerilor tehnice în vederea cooperării cu forţele armate străine, conduce activităţile care privesc informarea publică şi mass-media militare, regimul juridic al patrimoniului imobiliar al Ministerului Apărării Naţionaleşi coordonează activitatea de soluţionare a problemelor sociale ale personalului.[63]

❖ *Departamentul pentru armamente* – Elaborează şi coordonează politicile de achiziţii în cadrul Ministerului, în calitate de autoritate de reglementare în domeniu, gestionează relaţiile cu industria naţională de apărare, asigură managementul programelor de achiziţii pentru sisteme de armamente şi echipamente majore şi al contractelor aferente, precum şi al activităţilor de cercetare-dezvoltare, planifică şi desfăşoară activitatea de cooperare internaţională în domeniul armamentelor, realizează supravegherea calităţii la furnizorii de echipamente şi tehnică militară, coordonează activitatea de formare, specializare şi perfecţionare a ofiţerilor de logistică în domeniul tehnico-ingineresc şi a altor specialişti necesari armatei, activitatea de metrologie şi standardizare tehnică şi realizează controlul specific domeniului de competenţă pentru importurile şi exporturile de produse speciale.[64]

3.2. Organele deconcentrate ale administraţiei militare

Organele deconcentrate ale administraţiei militare sunt asimilate structurilor militare care înfăptuiesc acte şi fapte de comandament, cu caracter operativ sau tactic. În principal, ca nivel de organizare, responsabilitate specifică şi mod de acţiune, la modul general, în organele deconcentrate ale administraţiei militare sunt cuprinse comandamentele teritoriale, comandamentele diviziilor, brigăzilor, batalioanelor şi diverselor formaţiuni cu rol ajutător în procesul pregătirii pentru luptă şi al luptei.

Fără a subestima importanţa tuturor organelor deconcentrate ale administraţiei militare, pentru edificarea gnoseologică a conceptului le vom menţiona doar pe cele care aparţin categoriilor de forţe ale Armatei.

• *Statul Major al Forţelor Terestre*[65]*:*

- 3 Divizii de infanterie, în organica fiecăreia intrând brigăzi luptă, regimente sprijin de luptă, o bază logistică, batalioane sprijin de luptă şi un batalion de sprijin logistic;

- brigăzi sprijin luptă; centre de sprijin luptă şi sprijin logistic; un centru de instruire pentru luptă al forţelor terestre; batalioane de sprijin luptă şi sprijin logistic; poligoane de instrucţie şi trageri; structuri de învăţământ (Academia Forţelor Terestre, Şcoala Militară de Maiştri Militari şi Subofiţeri, şcoli de aplicaţie ale armelor, colegiile militare liceale).

• *Statul Major al Forţelor Aeriene*[66]

[62]Ibidem, Art.8
[63]Ibidem, Art.9
[64]Ibidem, Art.19
[65]https://www.forter.ro/content/structura

- Bazele 71, 86 şi 95 aeriene, Baza 90 Transport, Brigada 1 Rachete Sol-Aer, Baza 91 Logistică, Regimentul 70 Geniu de Aviaţie, Centrul 85 Comunicaţii Aero şi Informatică, Centrul de Operaţii Aeriene, Poligonul Capu Midia, structuri şi unităţi de învăţământ (Academia Forţelor Aeriene, Şcoala de Maiştri Militari de Aviaţie, şcoli de aplicaţie)

- *Statul Major al Forţelor Navale*[67]*:*

Flota, compusă din: Flotila de Fregate, Divizionul 150 rachete navale, Divizionul 50 corvete, Divizionul 146 nave minare - deminare, Batalionul 110 comunicaţii şi informatică, Serviciul fluvial, Divizionul 67 nave purtătoare de artilerie, Divizionul 88 vedete fluviale.

*Baza Logistică Navală:*Divizionul nave speciale, Centrul 338 Mentenanţă Tehnică Navală; Secţiile 335, 329, 330 şi 325 Logistică, dispuse la Mangalia, Brăila, Constanţa şi Tulcea.

Unităţi de învăţământ şi cultură: Academia Navală, Şcoala Militară de Maiştri de MarinăŞcoala de Aplicaţie, Muzeul Marinei.

*Structuri distinct specializate:*Centrul de scafandri, Centrul radioelectronic şi observare "Callatis,"

Centrul de informatică,

Centrul de instruire, simulare şi evaluare,

Direcţia hidrografică maritimă,

Centrul de medicină navală, Batalionul 307 infanterie marină,Batalionul de Sprijin al Forţelor Navale. Acestora mai adăugăm *organele militare teritoriale* care au în compunere comandamente militare teritoriale, centre militare judeţene, municipale şi de sector[68].

Ca rol şi atribuţii, în general, organele deconcentrate ale administraţiei militare: transmit sau, după caz, îndeplinesc ordinele şi dispoziţiilor eşaloanelor superioare; organizează, conduc şi desfăşoară aplicaţii tactice şi de mobilizare, în regimul antrenamentelor de comandament; participă şi gestionează pregătirea, prin convocări periodice, a personalului cu funcţii şi responsabilităţi de conducere din sistemul administraţiei publice locale; organizează şi desfăşoară activităţi de promovare a profesiei şi carierei militare, precum şi, în situaţii şi forme anume stabilite de către organele eşaloanelor superioare, activităţi de recrutare pentru profesia militară; desfăşoară activităţi specifice de formare a militarilor, precum şi a cadrelor militare din rezervă; execută antrenamente de specialitate şi de stat major, în scopul perfecţionării şi maximizării pregătirii personalului din subordine; verifică sistematic îndeplinirea de către agenţii economici a obligaţiilor ce le revin în scopul punerii în aplicare a sarcinilor cuprinse în documentele de mobilizare.

4. Autorităţi şi administraţie publica, administraţie militară. Interdependenţe operaţionale

În sprijinul conceptual al discursului teoretic angajat în această comunicare, vom trata succint, rezumativ, unele aspecte care, în opinia noastră, întregesc, prin complementaritate, înţelegerea comprehensivă a suportului decizional al administraţiei militare. Un prim aspect îl reprezintă sistemul corelaţional dintre administraţiile publice locală şi centrală, la pace, în situaţii de criză şi în caz de război, precum şi cel dintre administraţia publică şi administraţia militară. Sub aspect constituţional, definirea reprezentativă a acestora este limpede, în sensul că vizează:

a. *autorităţile publice*[69]care cuprind explicit Parlamentul, Preşedintele şi Guvernul;

b. *administraţia publică centrală de specialitate*[70], a cărei structură[71] cuprinde ministerele ce se organizează exclusiv în subordinea Guvernului, precum şi alte organe de

---

[66]https://www.afahc.ro

[67]http://www.navy.ro/

[68]Legea Apărării Naţionale, Art.10

[69]Constituţia României, Titlul III, publicată în Monitorul Oficial nr.767, din 31 octombrie 2003

specialitate organizate fie în subordinea Guvernului ori a ministerelor, fie ca autorităţi administrative autonome;

c. *şi administraţia publică locală*[72], organizată pe principii administrativ-teritoriale, exercitată prin consiliile comunale, orăşeneşti(sectoriale, la nivelul municipiului Bucureşti), municipale şi judeţene, toate ca autorităţi deliberative, şi primăriile, ca autorităţi executive.

Relaţia distinctivă dintre administraţia publică centrală şi administraţia publică locală, a cărei conducere generală este exercitată de către Guvern[73], este evidenţiată de un cumul de criterii exprimate prin: competenţa materială şi teritorială a organelor administraţiei publice şi natura intereselor comunitare pe care le susţine şi le promovează; diferenţa de anvergură dintre cele două domenii ale administraţiei publice, administraţia publică centrală exercitându-şi teritorial competenţa asupra întregului teritoriu naţional, cea locală exercitându-şi responsabilităţile şi competenţa la nivelul unităţilor administrativ-teritoriale, la care au fost legitimate prin voinţa democratică a comunităţilor locale; organele din alcătuirea instituţională a administraţiei publice centrale dispun, după caz, fie de o competenţă materială cu caracter general, recte Guvernul, fie de una cu caracter sectorial, precum ministerele, în timp ce autorităţile publice locate dispun de o compoetenţă eminamente materială, angajată în scopul înfăptuirii interesului local, bunăoară în primul caz este promopvat interesul general-naţional, iar în cel de-al doilea cel local. Denotarea explicită a acestor diferenţe cu caracter atribuţional, face posibilă înţelegerea rolului acestora în mecanismele operaţionale ale apărării naţionale, la pace, în situaţii de criză şi în caz de război, dar şi în timpul *stării de asediu*, asupra acestui aspect oprindu-ne succint în continuare, cu menţiunea că regimul stării de asediu şi declararea stării de asediu sunt atributele constituţionale ale Parlamentului[74] şi ale Preşedintelui[75].

În mod absolut firesc, între *administraţia militară* şi *administraţia publică*, vectori vitali ai sistemului social, se stabilesc, esenţial şi necesar, raporturi de interdependenţă, cu finalitate în maximizarea rolului instituţional al fiecăreia. Complexitatea şi natura funcţională a raporturilor social-statale dintre administraţia militară şi administraţia publică sunt evidenţiate prin meticulozitatea legislaţiei aferente, precum şi prin conţinutul unora dintre prevederile actului constituţional. Totodată, natura şi, mai cu seamă, amploarea operaţională a acestor raporturi este evidentă prin angajarea instituţională, în spectrul administraţiei militare, în funcţie de condiţiile specifice în care aceasta se poate manifesta, respectiv, la pace, în situaţii de criză sau în caz de război, după declararea stării de asediu. Această angajare administrativ- instituţională necesită o coordonare judicios planificată a apărării armate a ţării, deziderat asumat prin lege organică[76]. Din perspectiva constituţională a administraţiei militare, planificarea apărării este *„atribut şi componentă esenţială a politicii de apărare”* şi *„reprezintă un complex de activităţi şi măsuri care vizează promovarea intereselor naţionale, definirea şi îndeplinirea obiectivelor securităţii naţionale a României în domeniul apărării.”*[77]Planificarea apărării, cu a cărei responsabilitate, în oricare dintre condiţiile menţionate, este îndrituită administraţia militară, *„se realizează pe baza deciziilor politice ale Preşedintelui, Parlamentului şi Guvernului României, precum şi a măsurilor şi acţiunilor întreprinse la nivelul celorlalte instituţii publice, care, potrivit legii, au răspunderi în*

---

[70]Ibidem, Capitolul V, Secţiunea 1
[71]Ibidem, Art.116
[72]Ibidem, Secţiunea 2
[73]Ibidem, Cap. III, Art. 102
[74]Ibidem, Art.73, lit. g)
[75]Ibidem, Art.93, alin.(1)
[76]Legea nr. 473 din 4 noiembrie 2004, privind planificarea apărării, Monitorul Oficial nr. 1052 din 12 noiembrie 2004
[77]Ibidem, Art.1

domeniul apărării"[78], *„Strategia naţională de apărare a României fiind documentul de bază care fundamentează planificarea apărării la nivel naţional."*[79]

Evidenţa dimensiunii naţionale a responsabilităţilor care decurg din complexitatea materializată a planificării apărării, responsabilităţi atribuite administraţiei militare, pe care le îndeplineşte cu caracter dispozitiv sau prestator, impune, în fapt, existenţa *Autorităţii Naţionale de Comandă*[80]. Instituţie nonformală, care, prin cuantumul total de responsabilităţi nemijlocite în domeniul apărării, poate fi asemănată, forţând oarecum semantica aplicată a conceptului, cu o *paraadministraţie militară*, este alcătuită din *Parlament, Preşedintele României, Guvern* şi *Consiliul Suprem de Apărare a Ţării*.

Evidenţierea expozitivă a componentelor nodale ale *Autorităţii Naţionale de Comandă*, acestea având constituţional calitatea de *autorităţi publice* sau de *autorităţi ale administraţiei publice centrale de specialitate*, în contextul determinărilor legale cu privire la *planificarea apărării*, pune în lumină caracterul necesar interdependent al raporturilor dintre *administraţia publică* şi *administraţia militară*, aceste raporturi ajutând la structurarea, pe de o parte, a obiectivelor operaţionale ale administraţiei militare şi la pregătirea materializării acestora şi, pe de altă parte, la definirea posibilităţilor specifice de a le executa.

Această interdependenţă impune în mod necesar şi funcţional aspecte referitoare la:

- concretizarea posibilităţii de a utiliza elemente din sistemul de comunicaţii, în cazuri de forţă majoră, bine definite de procedurile operaţionale ale administraţiei militare;
- proiectarea doctrinelor specifice fiecărei categorii de forţe ale Armatei, dar şi a doctrinelor întrunite, a regulamentelor şi a standardelor specifice operaţiunilor de apărare, în corelaţie cu potenţialul diversificat aflat în gestiunea administraţiei publice;
- folosirea, în condiţii de maximă eficienţă, a agenţilor economici, recurgând la externalizarea unor activităţi;
- coordonarea şi controlul întregului efort de apărare, neîntrerupt şi unitar;
- degrevarea comandamentelor de mari unităţi şi unităţi, prin externalizarea operativă a serviciilor şi preluarea semnificativă a acestora de către organe ale administraţiei publice centrale şi locale, fapt posibil prin angajarea unor forţe logistice cu structură modulară;
- perfecţionarea aplicată a activităţii şi a mecanismelor de colaborare, pe obiective concrete ale responsabilităţilor comune privind apărarea naţională, între structurile administraţiei militare şi cele ale administraţiei publice;
- optimizarea sistematică a comunicării, la toate nivelurile de definire instituţională şi organizaţională, între structurile operative ale administraţiei militare şi ale celei publice;
- folosirea cu maximă eficienţă a resurselor financiare, materiale şi de altă natură, prin aplicarea nedeturnată a procedurilor de achiziţie centralizată;
- standardizarea procedurilor referitoare la acţiunile desfăşurate în comun de către administraţia publică şi administraţia militară, mai cu seamă a celor care presupun executarea concretă a legislaţiei naţionale în domeniul militar, concret, prin activităţi cu caracter dispozitiv sau prestator;
- stabilirea şi definirea cu maximă claritate a activităţilor sau responsabilităţilor care pot fi transferate în competenţa organelor administraţiei publice centrale sau locale, în scopul maximizării timpului de reacţie în situaţii speciale, dar şi al folosirii eficiente a resurselor de care se dispune la un moment dat.

Tot acest adevărat sistem interrelaţional, pune pregnant în evidenţă, *relaţiile civili-militari*, de a căror calitate depinde decisiv răspunsul specific al statului la

[78]Ibidem, Art.3
[79]Ibidem, Art.4
[80]General dr. Eugen Bădălan, *Administraţie militară. Note de curs*, Editura Academiei Forţelor Terestre, Sibiu, 2004, p.54

oricare dintre situaţiile posibile generate de ameninţările externe, la pace, în situaţii de criză sau de război, sau la declararea stării de asediu.

Fără a detalia excesiv aspectul abordat, apreciem că relaţiile civili-militari, de fapt natura acestora, în contextul stării de asediu, sunte evidenţiate prin însăşi definirea *stării de asediu* care *„reprezintă ansamblul de măsuri excepţionale de natură politică, militară, economică, socială şi de altă natură aplicabile pe întreg teritoriul ţării ori în unele unităţi administrativ-teritoriale, instituite pentru adaptarea capacităţii de apărare a ţării la pericole grave, actuale sau iminente, care ameninţă suveranitatea, independenţa, unitatea ori integritatea teritorială a statului”*[81], situaţie în care *„se pot lua măsuri excepţionale aplicabile pe întreg teritoriul ţării ori în unele unităţi administrativ-teritoriale.”*[82] De asemenea, în spiritul pledoariei noastre, remarcăm că *„la instituirea stării de asediu sau a stării de urgenţă, unele atribuţii ale administraţiei publice centrale de specialitate şi ale administraţiei publice locale trec în competenţa autorităţilor militare şi a altor autorităţi publice, prevăzute în decretul de instituire a stării de asediu sau de urgenţă.”*[83] În acest context, *„autorităţile civile ale administraţiei publice continuă exercitarea atribuţiilor care nu au fost transferate autorităţilor militare, având obligaţia de a acorda sprijin acestora.”*[84]

5. Concluzii

Analiza şi exigenţele asumate ale temei noastre, impun, esenţial, câteva ***concluzii***. *Prima*, potrivit căreia de la întemeierea sa pe baze moderne, organismul militar românesc a corespuns exigenţelor operaţionale ale condiţiei administraţiei militare, exercitând atribuţii de comandament, dar şi specifice actelor administrative, în sensul lor instituţional. Mai mult, chiar dacă exemplele la care am recurs sunt minimale numeric, apreciem că, în perioada care a marcat evoluţia statului român de la întemeierea sa, în anul 1859, până la intrarea României în paradigma dezvoltării totalitare a societăţii, s-a cristalizat o adevărată doctrină juridică relativă la administraţia militară. Cea de-*a doua*, în sensul că Statul Major General este principala şi cea mai importantă instituţie a administraţiei militare, singura ale cărei acte şi fapte de comandament au caracter strategic, eminamente militar; *a treia*, potrivit căreia, la nivelul organelor centrale ale administraţiei militare, se adoptă nu numai deciziile majore ale construcţiei militare, ci şi actele şi faptele administrative şi de comandament de punere în operă a strategiei politico-militare de apărare a ţării; cea de-*a patra*, care confirmă că suportul instituţional decizional al administraţiei militare este constituit de ansamblul structurilor militare care intră în componenţa organelor centrale şi deconcentrate ale administraţiei militare; *a cincea,* ultima pe care o menţionăm, potrivit căreia relaţiile dintre organele centrale şi locale ale administraţiei publice, pe de o parte, şi organele centrale şi deconcentrate ale administraţiei militare, pe de altă parte, sunt semnificativ determinate de calitatea operaţională a relaţiilor instituţionale, dar şi sociale, dintre civili şi militari.

BIBLIOGRAFIE:

1. Bădălan E., *Administraţie militară. Note de curs*, Editura Academiei Forţelor Terestre, Sibiu, 2004
2. Chiru V., *Comandament şi administraţie*, Editura *Curierul Justiţiei Militare*, Sibiu, 1934

[81]Legea 453, privind regimul stării de asediu şi regimul stării de urgenţă, publicată în Monitorul Oficial nr.1052, dn 12 noiembrie 2004, Art. 2
[82]Ibidem
[83]Ibidem, Art.7, alin.(1)
[84]Ibidem, alin.(2)

3. Chiru, V., „*Dreptul administrativ militar”*, Editura Curierul Justiţiei Militare, Sibiu, 1936
4. Cioflină D., Oşca, A., Istoria Statului Major General Român. Documente, 1859-1947, Editura Militară, Bucureşti, 1994
5. *Codul Justiţiei Militare „ Regele Mihai I*”, Editura ziarului „Universul”, Bucureşti, 1941
6. Dragoman, I., Actele autorităţilor militare, Editura LUMINA LEX, Bucureşti, 2003
7. Georgescu, M., Istoria Marelui Stat Major, 1830-1914, Editura Militară, 2011
8. Mihăilescu, D., *Curs de legislaţie şi administraţie*, Tipografia GOLDSLEGER, Botoşani, 1889, citat de Ion Dragoman, Actele autorităţilor militare, Editura LUMINA LEX, Bucureşti, 2003
9. Movilă C.,, *„Studiul asupra serviciului intendenţei în campanie”,* Monitorul Oastei nr.27/1870
10. Petrache C.,, *Apărarea naţională în România contemporană.Înţelegerea politică,* Editura CTEA, Bucureşti, 2006
11. Popovici, I., Organisarea armatei române, vol.I, Schiţă istorică a organisărei de la 1830-1877, Partea a II-a, Roman, 1900
12. Voinescu S.,, *Studiu asupra statlui major în luptă*, Monitorul Oastei, nr.10/1883

Legislaţie

1. Colecţiile „Monitorul Oastei” din anii 1860, 1861, 1863, 1864, 1866, 1867, 1868, 1871, 1873, 1882, 1908, 1924,
2. Colecţiile Monotorul Oficial, din anii 1924, 1936, 1937, 1940
3. LEGE nr.346, din 21 iulie 2006, privind organizarea şi funcţionarea Ministerului Apărării, publicată în Monitorul Oficial nr. 654 din 28 iulie 2006, cu modificările ulterioare
4. Legea nr. 45 din 1 iulie 1994, a apărării naţionale a României, Monitorul Oficial nr. 172 din 7 iulie 1994
5. Legea 453, privind regimul stării de asediu şi regimul stării de urgenţă, publicată în Monitorul Oficial nr.1052, dn 12 noiembrie 2004
6. Legea nr. 473 din 4 noiembrie 2004, privind planificarea apărării, Monitorul Oficial nr. 1052 din 12 noiembrie 2004
7. Constituţia României, publicată în Monitorul Oficial nr.767, din 31 octombrie 2003

Link-uri utile

1. https://www.forter.ro/content/structura accesat intre 20 si 30 martie 2015
2. https://www.afahc.ro accesat intre 20 si 30 martie 2015
3. http://www.navy.ro/ accesat intre 20 si 30 martie 2015

CONTRACARAREA RĂZBOIULUI HIBRID. DIRECŢII ŞI MODALITĂŢI DE CONTRACARARE A AMENINŢĂRILOR /RĂZBOIULUI DE TIP HIBRID

Marian RĂDULESCU
Locotenent-colonel, instructor superior, Şcoala Militară de Maiştri Militari şi Subofiţeri a Forţelor Terestre "Basarab I", Piteşti, România.
e-mail: mradulescu1969@yahoo.com

***Rezumat**: Mediul internaţional de securitate cunoaşte schimbări majore, generând adaptarea strategiilor, capacităţilor statale, inclusiv militare, transformarea organizaţiilor cu rol în asigurarea securităţii regionale şi globale, pentru a contracara noile riscuri şi ameninţări.*

Ameninţările noi, asimetrice, exced cadrul convenţional al războiului, fiind atât de natură militară (guerila, războiul civil, terorismul, insurgenţa), cât şi non-militară (crima organizată, asasinatele, agresiuni politice, economice, psihologice, mediatice, informaţionale, cibernetice, războiul climatic, geofizic, separatismul etnic etc).

O provocare distinctă pentru NATO şi partenerii săi o reprezintă ameninţările de tip hibrid, care combină inovator, amplificând astfel, efectele mijlocelor convenţionale, cu cele neregulate, asimetrice, sursa ameninţării fiind, în mare măsură, actori non-statali, cu sprijinul din umbră al unor state partenere.

Problematica Counter-Hybrid Warfare necesită o abordare cuprinzătoare, unitară şi coerentă, la nivelul tuturor elementelor de putere statală, regională şi internaţională pentru descurajarea acestui tip de ameninţare, identificarea şi facilitarea măsurilor pro-active de răspuns la nivel strategic, operativ şi tactic .

***Cuvinte cheie:** hibrid, asimetric, neconvenţional, ameninţări, NATO, planificare operaţională, operaţii speciale.*

Introducere

Mediul de securitate internaţional coagulează noi elemente de risc şi ameninţare: schimbările demografice, criza energetică, modificările climatice, criza economică, dimensiunea spaţială a războiului, sporirea importanţei aspectelor non-militare, accesibilitatea la informaţie, migraţia tehnologiilor militare de vârf către puteri nelegitime, separatismul etnic şi religios.

Evitând confruntarea clasică, pentru a diminua superioritatea militară convenţională a unor armate moderne, actori non-statali, organizaţii şi chiar state apelează cu succes la metode complexe de ducere a războiului, care eludează sau sfidează legile conflictelor armate, îmbină forţe şi mijloace letale şi nonletale, tactici de luptă convenţionale cu cele neconvenţionale, inclusiv atacuri teroriste, asasinate, operaţii informaţionale şi atacuri cibernetice, proiectează spaţiul de luptă în mass media, practică pe scară largă dezinformarea şi propaganda, încercând să legitimizeze propriile acţiuni şi să slăbească elementele de putere ale adversarului.

Accesul facil la înalta tehnologie militară, înzestrarea unor organizaţii teroriste cu sisteme de arme avansate, asociate în mod normal, unor armate convenţionale, predilecţia de a opera în medii urbane, dens populate, tendinţa de a combina într-un efect sinergic tehnologii, acţiuni militare, politice, mediatice şi de influenţare a opiniei publice conturează viitorul conflictelor.

Imaginea „războiului fără restricţii" practicat de organizaţii teroriste, actori statali şi non-statali este completată de exploatarea prezenţei civililor în zona de conflict, prin acţiuni

deliberate de sporire a numărului victimelor colaterale, cu încălcarea principiilor *LOAC (Law of Armed Conflict),* pentru a prezenta ulterior, pe canalele de informare, falsificând realitatea, operaţiile militare, legitime de altfel, ale părţii adverse, ca fiind disporporţionate şi nediscriminatorii, în scopul influenţării factorilor de decizie şi obţinerii avantajului strategic.

Aceşti actori modifică substanţial cadrul operaţional al războiului, pentru care grupările de forţe regulate trebuie să-şi adapteze tehnologiile, structura organizatorică, strategiile, tacticile şi procedurile de acţiune.

1. Idei doctrinare privind războiul hibrid

Analizând conflictele recente, teoreticieni, planificatori şi comandanţi militari au anticipat tendinţele mediului de confruntare, încercând să definească ameninţările şi implicit, tipurile de războaie prezente şi viitoare. Au apărut astfel conceptele de *unconventional warfare, irregular warfare*, şi, mai nou, *hybrid warfare*. Dacă asupra primelor concepte opiniile specialiştilor militari sunt convergente, generând strategii de răspuns eficiente, *hybrid warfare* cunoaşte interpretări şi nuanţări diferite.

1.1 Delimitări conceptuale

Conceptul de *ameninţare hibridă* reprezintă e evoluţie a artei operaţionale, aducând un important potenţial de revoluţie doctrinară şi organizaţională în domeniul militar. Termenul a apărut după conflictul din Liban (2006) dintre Israel şi Hezbollah, din necesitatea caracterizării complexităţii sporite şi non-linearităţii ameninţărilor actorilor statali şi non-statali.

Văzută ca un amalgam sofisticat de căi, mijloace, tehnologii şi metode nerestricționate, prin care actori statali şi non-statali combină în mod inovator şi simultan capacități regulate și neregulate pentru a crea efecte strategice, proliferarea ameninţărilor hibride a condus la numeroase dezbateri. Dezbaterea asupra ameninţărilor hibride este susținută și de lipsa unei definiții universal acceptate.

În 1996 istoricul Thomas Huber avansează termenul de "războiul compus" pentru a descrie amestecul de forțe regulate și neregulate care luptă pentru un scop comun.

Un rol determinant în definirea şi dezvoltarea conceptului l-a avut Frank G. Hoffman. În articolul *Future Warfare: The Rise of Hybrid Wars* (2005), autorul arată că, deşi războiul convenţional nu va dispărea, forţele armate menţinând capabilităţile necesare ducerii unei operaţii majore, este necesară adoptarea unor modalităţi de răspuns în faţa unor ameninţări noi, de tip hibrid. Acesta apreciază că pot fi utilizate simultan o varietate de forme de război. Actorii non-statali folosesc cu predilecţie forme de război neregulat, dar vor sprijini participarea la un conflict convenţional, dacă acesta serveşte scopurilor lor.

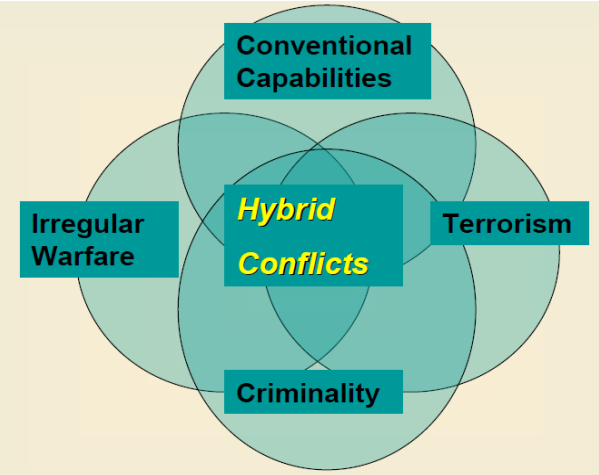


Figura nr. 1. Conflictele viitorului, după Hoffman[1]

[1] Disponibil la adresa http://indianstrategicknowledgeonline.com/web/DIRIWCSCBriefv3.pdf, accesat la 01.04.2015

În lucrarea *Conflict in the 21st Century: The Rise of Hybrid Wars*, publicată doi ani mai târziu, Frank Hoffman analizează acţiunile Hezbollah împotriva *Israel Defense Forces* (IDF) în campania din 2006, arătând capacitatea în creştere a Hezbollah de a întrebuinţa cu succes capacităţi, tactici şi metode difuze în zone dens populate, care îmbină într-un mod complex caracteristicile operaţiilor convenţionale cu cele neconvenţionale. În opinia autorului, într-un război hibrid, părţile adverse „urmăresc să obţină victoria prin fuziunea dintre tacticile neregulate şi cele mai letale mijloace aflate la îndemână, în scopul de a ataca adversarul şi a-şi îndeplini propriile obiective politice”[2].

În anul 2009, în articolul *Hybrid vs. compound war*, Frank Hoffman discută conceptul de *război compus* lansat de Thomas Huber, apreciind că acesta presupune existenţa a două forţe distincte (regulate şi neregulate) care acţionează în diferite părţi ale spaţiului de luptă, dar nu combină în luptă. Forțele neregulate sunt folosite în această situaţie pentru acţiuni de uzură și pentru a susține o strategie de epuizare, creând condiţiile de succes pentru forțele convenționale. Pe de altă parte, ameninţările hibride par să aibă un mai mare grad de coordonare şi combinare operaţională şi tactică, existând practic o singură forţă, sub comandă unică, care acţionează concentrat, prin mijloace convenţionale şi neconvenţionale pentru un obiectiv strategic.

Dr. Russell Glenn, un reputat analist militar, extinde dezbaterea dintre război compus și amenințări hibride. El interpretează războiul compus ca o acţiune sinergică şi combinată la nivel strategic, dar nu de complexitatea şi simultaneitatea realizată la nivel operaţional şi tactic, în care forţele combină întreaga gamă de metode şi moduri de acţiune în spaţiul de luptă.

Russell Glenn defineşte ameninţarea de tip hibrid ca venind din partea unui “ adversar care adoptă simultan acţiuni politice, militare, economice, sociale şi informaţionale, precum şi metode ale războiului convenţional, neregulat, terorism şi acţiuni criminale” [3], acesta putând fi o combinaţie de state şi actori non-statali.

În 1999, Qiao Liang și Wang Xiangsui prezintă în lucrarea *Unrestricted Warfare* alternative inovatoare la angajare militară tradițională, folosind o mare varietate de mijloace fără restricții. Ei susțin că noile abordări permit găsirea unor căi alternative pentru a face față costurilor în creștere ale războiului convenţional. Aceştia pledează pentru formarea unei forţe compozit, care combină metodele militare şi non-militare, inclusiv aparţinând cadrului juridic şi economic, pentru a plasa un ipotetic adversar în dezavantaj, în locul confruntării militare directe.

David Kilcullen în cartea *Out of the Mountains: The Coming Age of the Urban Guerrilla* oferă o perspectivă revoluţionară asupra războiului hibrid, subliniind patru megatendinţe privind evoluţia societăţii umane: modificarea structurii populaţiei, urbanizarea, creşterea rolului zonelor costiere, conectivitatea.

Kilcullen susține că viitoarele conflicte pot să apară în orașe de coastă, în localitățile periurbane, sugerând că ***oraşele, mai degrabă decât ţările, sunt unităţile critice de analiză pentru viitoarele conflicte*** (observaţie justă, având în vedere că până în anul 2050 aproximativ 75% din populaţia globului va fi urbanizată). Degradarea condiţiilor de mediu, competiţia pentru resurse şi spaţiu, lipsa mijloacelor minime de trai, dificultăţi în asigurarea unui nivel acceptabil de educaţie şi sănătate, proliferarea reţelelor criminale, ar putea transforma părţi importante din megaaglomerările urbane în „teritorii ale nimănui“. În abordarea problematicii conflictelor urbane este nevoie de flexibilitate, singură soluţia

---

[2] HOFFMAN, Frank, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, pp. 29.

[3] RUSSELL, Glenn, *Evolution and Conflict: Summary of the 2008 Israel Defense Forces*, disponibil la adresa https://www.doria.fi/bitstream/handle/10024/92639/Y2622_HuovinenKPO_YEK56.pdf, accesat la 01.04.2015

militară fiind neindicată. Implicarea populaţiei locale în domenii precum planificarea urbană, ingineria sistemelor, soluţionarea conflictelor şi mediere ţine mai mult de aspecte referitoare la politicile de dezvoltarea durabilă.

Potrivit NATO, „ameninţările hibride sunt lansate de adversari, cu capacitate de a utiliza simultan mijloace convenţionale şi neconvenţionale de o manieră adaptativă pentru a-şi atinge obiectivele”[4].

Problematica războiului hibrid a intrat şi în atenţia oficialilor Departamentului pentru Apărare al SUA, care au definit în mod corect caracteristicile şi particularităţile acestui tip de conflict. Potrivit oficialilor *Air Force*, războiul hibrid este mai puternic şi complex decât războiul neregulat din cauza tempo-ului crescut, complexităţii şi diversităţii manifestărilor, fiind caracterizat de accesul facil al adversarilor la comunicaţii şi resurse. Oficialii *Special Operations Command, Navy* şi *Marine Corps* consideră că războiul hibrid cuprinde forme de război convenţional şi neconvenţional, combaterea ameninţării potenţiale fiind acoperită din punct de vedere doctrinar de *operaţiile în spectru complet.*

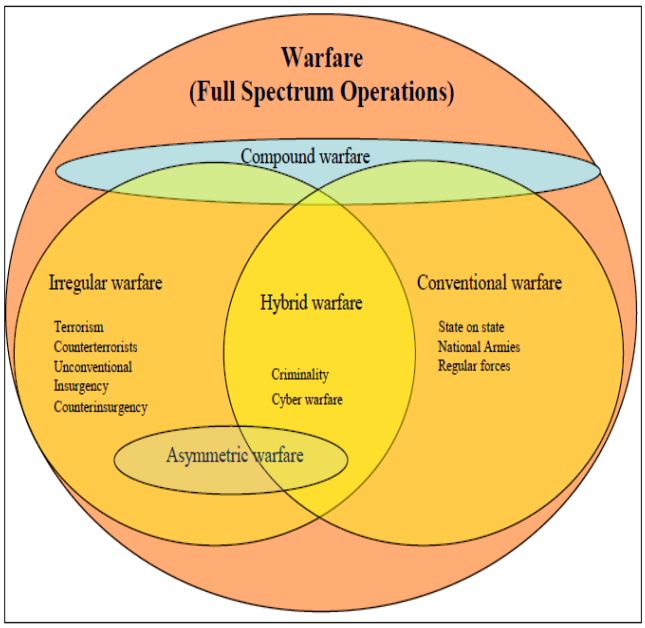


Figura nr. 2. Operaţii în spectru complet [5]

Având în vedere opiniile exprimate mai sus, apreciem că războiul hibrid este acea formă de război bazat pe o strategie flexibilă care combină inovativ capacităţi convenţionale, neregulate, teroriste şi criminale, integrând simultan forţe şi mijloace militare, paramilitare şi civile[6] ale unor actori statali sau non-statali, care exploatează vulnerabilităţile părţii adverse, pentru obţinerea unor efecte strategice.

1.2 Necesitatea adoptării unei doctrine Counter-Hybrid Warfare

Margaret S. Bond, în lucrarea *Hybrid War: A New Paradigm for Stability Operations in Failing States* descrie războiul hibrid dintr-o perspectivă strategică largă, prin prisma spaţiilor neguvernate. În lucrare se propune necesitatea adoptării unui nou concept strategic pentru operarea forţelor SUA în medii non-permisive, în state eşuate[7], unde guvernul nu are

---

[4] IMSM-0292-2010, *Hybrid threats description and context*, 2010, disponibil la adresa http://cco.dodlive.mil/files/2014/02/Prism_111-124_Aaronson-Diessen.pdf, accesat la 01.04.2015

[5] HUOVINEN, Petri, *Hybrid warfare – Just a Twist of Compound Warfare?* , disponibil la adresa https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf, accesat la 01.04.2015

[6] Unele activităţi infracţionale pot fi incluse ca făcând parte dintre cele proprii războiului hibrid, întrucât destabilizează administraţia publică, sau sprijină forţele insurgente prin furnizarea de resurse (provenite din acţiuni de contrabandă, trafic de droguri, comerţ ilicit, transferuri de muniţie sau arme avansate, exploatarea de reţele criminale urbane)

[7] BOND, Margaret, *Hybrid war: a new paradigm for stability operations in failing states*, disponibil la adresa http://www.dtic.mil/dtic/tr/fulltext/u2/a468398.pdf, accesat la 25.03.2015

un control efectiv asupra teritoriului său, nu oferă securitate națională sau servicii publice de bază pentru cetățenii săi și nu controlează forțele armate.

Războiul viitorului va fi, în opinia autorului, un război hibrid, care presupune ***proiectarea tuturor elementelor de putere națională de-a lungul unui continuum de activități simultane***, de la misiuni umanitare, la acţiuni militare, operaţii de stabilitate, securitate şi reconstrucţie. Acesta include un spectru larg de forţe convenţionale, capabilităţi de informaţii militare, arme neconvenţionale, unităţi de sprijin, echipament de luptă, disponibile pentru dislocare rapidă dacă elementele forţelor regulate sau neregulate adverse, organizaţiile teroriste sau alţi actori statali sau non-statali depăşesc un anumit prag al ostilităţii şi constituie o ameninţare directă.

În documentul *Future Character of Conflict Paper* [8]*,* elaborat de către ministerul britanic al apărării, se avansează ideea că în viitoarele conflicte caracterul hibrid al acestora va creşte semnificativ. Lucrarea explică faptul că ameninţărilor hibride nu li se pot opune operaţii de contrainsurgenţă sau stabilizare. Ideea principală este că într-o ameninţare hibridă se urmărește exploatarea slăbiciunilor adversarului, combinând metode convenționale, neregulate și amenințări asimetrice, în același timp și spațiu, inclusiv în domeniile economic, financiar, juridic și diplomatic.

Counter-Hybrid Warfare C-HW diferă astfel de *Counter-Terrorism (CT)* sau de *Counter-Insurgency (COIN).* Operațiunile CT tind să se desfăşoare pe termen scurt, rezultatele fiind vizibile imediat. C-HW, prin contrast, este o doctrină proactivă ce presupune desfăşurarea unor operaţii directe şi indirecte pe o lungă perioadă de timp, asemenea războiului de uzură - *attrition war*.

Operaţiunile COIN au o importantă încărcătură cinetică, conţin o amprentă fizică consistentă, având scopul de a învinge formaţiunile insurgente, în timp ce operaţiunile de C-HW combină metode directe şi indirecte, militare şi de altă natură, executate de (sub)unităţi diferite ca natură, valoare, organizare, având drept scopuri interzicerea posibilităţii adverarului de a exploata vulnerabilităţile proprii, de a-şi concentra capabilităţile de care dispune pentru realizarea efectului sinergic, de a obţine sprijinul populaţiei din zona de conflict, condiţii necesare pentru realizarea succesului strategic.

Războiul din Fâșia Gaza (2014) a demonstrat insuficienţa unor concepte precum Counter-Terrorism, Counter-Insurcency, sau Operaţii bazate pe efecte (EBO) într-un război de tip hibrid, fiind necesară elaborarea unei doctrine aparte, care să abordeze acest tip de conflict.

Extinderea conflictului din Afganistan şi Irak a dezvăluit o deficienţă sistemică privind operaţiile de contrainsurgenţă, remediată oportun prin elaborarea, în 2006, a unui nou manual de contrainsurgenţă FM 3-2, precum şi prin instruirea forţelor în planificarea şi executarea acestui gen de operaţii. Privind noile ameninţări, *United States Army Special Operations Command* a conceput în septembrie 2014 *Counter-Unconventional Warfare - White Paper,* ce ar putea fi elementul pivotant în adoptarea unei doctrine C-HW. Este important să nu se pună semnul de egalitate între C-UW şi C-HW, întrucât C-UW nu abordează toate ameninţările, iar nu toate ameninţările sunt neconvenţionale.

---

[8] *** Ministry of Defence UK, *Future Character of Conflict Paper (FCOC),* disponibil la adresa *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33685/FCOCReadactedFinalWeb.pdf,* accesat la 23.03.2015

2. Direcţii şi modalităţi de contracarare a ameninţărilor hibride

Prefigurat de acţiunile iraniene în Orientul Mijlociu şi de către chinezi prin conceptul de *război fără restricţii*, războiul hibrid a ajuns acum "soluţia" adoptată de insurgenţii separatişti din Ucraina. Acest tip de război, caracterizat prin integrarea acţiunilor clasice cu cele neconvenţionale, completat de extinderea conflictului către domeniile economic, civil, diplomatic, cultural, mediatic şi informaţional, la care se pot adăuga acţiuni de distrugere a infracţiunilor critice, sau atacuri cu arme de distrugere în masă, necesită acţiuni energice, preventive, convergente, având la bază o doctrină specifică, care să abordeze întreaga gamă de ameninţări şi care să cuprindă directive strategice politico-militare de acţiune. Aceasta va permite adoptarea unor măsuri preventive şi de răspuns coerente, asumate de întreaga societate şi puse în practică de instituţiile cu atribuţii în domeniul securităţii.

2.1 Abordare cuprinzătoare la nivelul tuturor elementelor de putere

Contracararea ameninţărilor de tip hibrid necesită aşadar o abordare cuprinzătoare, la nivelul tuturor elementelor de putere. Cooperarea dintre instituţii, agenţii guvernamentale şi non-guvernamentale, organizaţii de securitate regionale şi mondiale, structuri militare, agenţii de informaţii este vitală pentru adoptarea unor măsuri active de prevenire şi răspuns la ameninţare: măsuri politice şi diplomatice, sancţiuni economice, sprijin din partea naţiunilor şi organizaţiilor partenere, acţiuni militare, acţiuni de comunicare şi informare strategică pentru demascarea ameninţării.

O capacitate naţională de C-HW reprezintă o opţiune pe termen lung şi depinde de dorinţa liderilor de a angaja elementele de putere naţională în operaţii prelungite, purtate în medii sensibile, inclusiv angajarea forţelor armate în acţiuni militare de uzură.

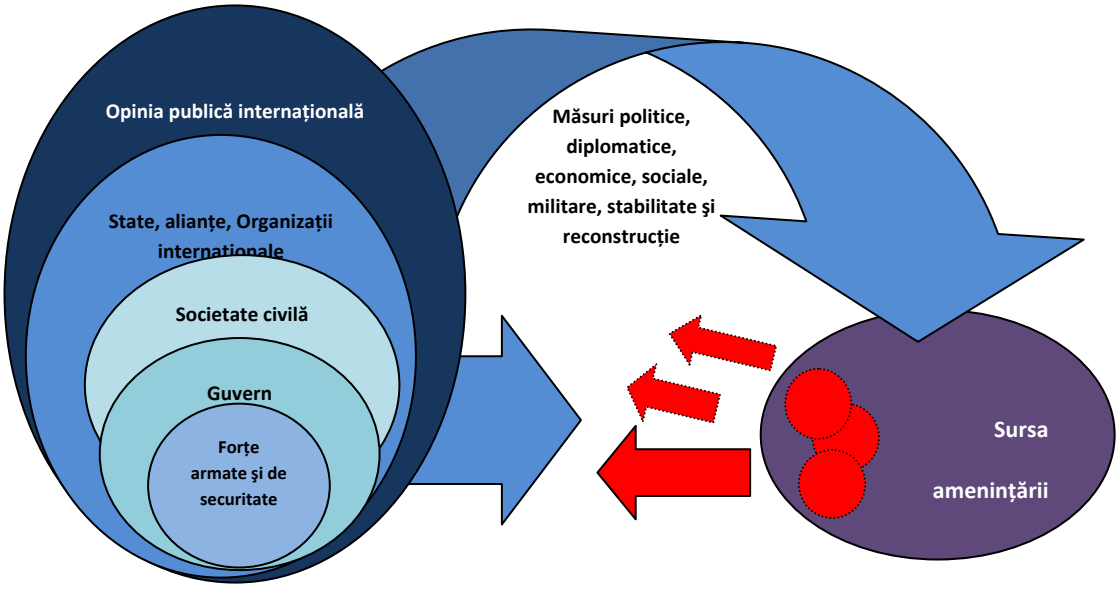


Figura nr. 3. Abordarea cuprinzătoare a ameninţării de tip hibrid

Naţiunile trebuie să fie în măsură să-şi adapteze strategiile naţionale, mecanismele de cooperare, dar şi conceptele de luptă şi structurile de forţe, să combine adaptiv şi eficient toate capabilităţile civile şi militare pentru reducerea tuturor riscurilor şi ameninţărilor care aduc perturbări şi disfuncţionalităţi majore şi care pot conduce la conflicte, acestea putând fi, în majoritatea cazurilor, de tip hibrid.

La nivel strategic, coordonarea şi sincronizarea eforturilor pentru realizarea obiectivelor generale ar putea fi asigurată de un grup mixt de coordonare interagenţii, cu personal din cadrul forţelor armate şi reprezentanţi ai altor ministere, instituţii şi agenţii. La nivel tactic, coordonarea interagenţii ar putea fi asigurată de ofiţeri de legătură *(Liaison officers - LNOs)*.

Plecând de la descrierea ameninţării, se impune elaborarea unei doctrine de *Counter-Hybrid Threats / Warfare*, pe baza căreia pot fi implementate concepte, proceduri, documente de planificare şi modificări importante ale structurii de forţe.

2.2 O nouă abordare în planificarea operaţiilor militare

După războiul rece, comunitatea militară a încercat să definească tipurile de ameninţare, numeroase idei conceptualizând complexitatea şi tendinţa de transformare a mediului operaţional, în care vechile doctrine deveniseră caduce. Conceptele dezvoltate în ultimele decenii au definit cadrul de planificare a operaţiilor militare, în acord cu transformările mediului operaţional. Acestea au inclus *Fourth Generation Warfare*, *Network-Centric Warfare, Counter-Terrorism* şi *Counter-Insurgency (COIN)*.

Conflictele în viitor nu vor fi caracterizate exclusiv de acţiuni convenționale sau neregulate. Adversarii vor folosi cu ingeniozitate combinații de metode tradiționale, neregulate și disruptive pentru a obține un avantaj operațional și strategic. Prin urmare, *amenințarea hibridă* oferă un ***cadru pentru a descrie caracterul evolutiv al amenințării***, contestă metodologiile convenționale de evaluare a amenințărilor și evidențiază dinamica mediului operațional contemporan.

Amenințările hibride furnizează deopotrivă provocări pentru planificarea operațională și strategică militară. Caracterul haotic și complex al amenințării hibride, analizat după metodologii tradiționale, poate duce la prognoze evazive.

Conceptul de amenințare hibridă sintetizează aspectele relevante ale acestor construcții, coroborate cu o tendință pragmatică a artei operaționale de ***a sincroniza toate elementele de putere în planificarea acțiunilor tactice și operative pentru atingerea obiectivelor strategice.***

În 2011, Centrul pentru lecţii învăţate al Armatei SUA, în studiul *Irregular Warfare: A SOF Perspective* , avansează ideea cooperării şi interoperabilităţii dintre forţele convenţionale şi forţele pentru operaţii speciale împotriva unor adversari care utilizează tactici specifice războiului hybrid[9].

Joint Vision 2020[10] este un document care proclamă necesitatea dominaţiei în întreg spectrul de luptă, oferind răspunsuri doctrinare la ameninţările militare ale secolului XXI.

Documentul pune accent pe aspectele legate de interoperabilitate (tehnologică, organizaţională şi procedurală), superioritate informaţională, decizională şi acţională, putând oferi un punct de plecare în găsirea unor soluţii doctrinare la ameninţările / războiul de tip hibrid.

Amenințările hibride aduc numeroase provocări pentru planificatorii militari. Gama diversificată a ameninţărilor impun ***adoptarea unor soluţii personalizate pentru fiecare provocare distinctă***. Planificarea trebuie să abordeze cu prioritate ***măsuri indirecte de perturbare şi fracţionare a ameninţării hibride***, prin introducerea unor tensiuni interne sau

---

[9] *** *Irregular Warfare: A SOF Perspective*, Center for Army Lessons Learned, Newsletter 11-34, Fort Leavenworth - Kansas, June 2011, p. 25, accesibil la adresa http://www.globalsecurity.org /military/ library/report/call/call_11-34.htm, accesat la 01.04.2015

[10] http://www.fraw.org.uk/files/peace/us_dod_2000.pdf, accesat la 23.03.2015, http://www.defense.gov/news/ newsarticle.aspx?id=45289, accesat la 23.03.2015

anularea efectului sinergic al componentelor ameninţării hibride, în locul metodelor fizice de contracarare a mijloacelor şi capabilităţilor adversarului.

Definirea şi descrierea ameninţării într-un cadru operaţional ambiguu, ***flexibilitate*** în gândire, ***revizuirea permanentă a planurilor*** şi adaptarea deciziilor la modificările din mediul operaţional, ***cooperare dinamică intra- şi inter-organizaţinală***, ***analiza preemptivă a implicaţiilor acţiunilor militare în plan mediatic*** (acesta trebuie să devină un criteriu de bază în compararea diferitelor cursuri de acţiune !), ***integrarea şi selectarea*** atentă a sistemelor de ripostă militare şi non-militare pentru evitarea pagubelor inutile şi suferinţelor din partea populaţiei civile sunt caracteristicile viitoarelor procese de planificare operaţională.

Analiza privind cultura strategică a potențialelor ameninţări venite din partea statelor-națiune, grupărilor transnaționale și regionale poate oferi prognoze privind comportamentul lor strategic viitor.

Ameninţările hibride sfidează preferinţa tradiţională a planificatorilor pentru campanii militare scurte, decisive, fiind continue, difuze, necesitând o abordare flexibilă şi nuanţată. Planificarea trebuie, de asemenea, ***să menţină iniţiativa*** în faţa ameninţărilor hibride, decât să adopte soluţii reactive de răspuns.

2.3 Necesitatea respectării LOAC

Comandanţii militari răspund de respectarea principiilor *LOAC* în conflictele armate şi a prevederilor Convenţiilor de la Geneva din 1949 referitoare la prizonierii de război, răniţi, bolnavi, persoanele care se abţin de la ostilităţi.

Principiul necesităţii militare cere forţelor să se angajeze în numai acele acţiuni necesare pentru a realiza un scop legitim, atacurile limitându-se strict la obiective militare. La aceasta se adaugă necesitatea utilizării echipamentelor militare în conformitate cu legile conflcitelor armate, fiind interzise sisteme de arme care contravin dreptului internaţional.

Principiul distincţiei presupune deosebirea între obiectivele militare şi cele civile, inclusiv interzicerea folosirii forţei asupra personalor care se abţin de la acţiunea militară. Ideea centrală este de a se angaja doar ţinte militare valide. Acest principiu cere totodată oponenţilor de a amplasa obiectivele militare în afara zonelor civile.

Principiul proporţionalităţii se referă la folosirea graduală a forţei în raport cu ameninţarea, pentru evitarea pierderilor excesive, în timp ce *principiul evitării suferinţelor inutile* are la bază interdicţia de a utilize arme şi metode de luptă de natură a cauza un prejudiciu sau suferinţe inutile.

Adversarii neconvenţionali - gherile, insurgenţi, teroriști şi grupuri armate nestatale – vor exploata restricţiile impuse forţelor armate care respectă *LOAC* şi principiile dreptului internaţional umanitar, prin atragerea acestora în zone de conflict populate, cautând să exploateze prezenţa civililor în aceste arii, unde forţele convenţionale sunt nevoite să acţioneze restrictiv. Această strategie de a pune în mod deliberat civilii în situaţii de pericol, are menirea şi de a obţine, prin dezinformare şi propagandă, atât atragerea civililor în acţiuni de ripostă împotriva forţelor armate, cât şi condamnarea internaţională.

În operaţiunea *Protective Edge* din fâşia Gaza (2014), *IDF* a aplicat o serie de metode extraordinare pentru a reduce pierderile în rândul populaţiei civile: evaluarea riscurilor întrebuinţării loviturilor aeriene şi reducerea acestor atacuri, maximizarea utilizării muniţiilor ghidate, selectarea unor explozivi cu randament acceptabil, avertizarea populaţiei civile prin mesaje text, transmisii radio şi apeluri telefonice privind iminenţa unor atacuri, chiar cu riscul anulării surprizei operaţiei, ceea ce reprezintă un angajament de bună credinţă faţă de respectarea *LOAC*. Am fost numeroase cazuri în care *IDF*, din aceste constrângeri excepţionale, a anulat misiuni de foc asupra unor ţinte militare valabile, dacă aceste misiuni prezentau un risc ridicat de daune colaterale. Eforturile IDF pentru atenuarea suferinţelor populaţiei din Gaza au fost extinse prin trimiterea de alimente şi medicamente, misiuni de

evacuare medicală, asigurarea resurselor energetice şi de repunere în funcţiune a infrastructurii avariate.

Într-un război de tip hibrid, în care acţiunile de luptă se duc, cu precădere, în zone intens populate, iar adversarul se poziţionează cu predilecţie în obiective civile, folosirea forţei este restricţionată, fiind necesare luarea unor măsuri suplimentare de precauţie pentru a evita pierderile colaterale în rândul populaţiei civile. Acţiunile de luptă vor fi punctiforme, duse de subunităţi şi unităţi mixte (forţe regulate şi forţe pentru operaţii speciale) de valoare redusă, dotate cu armament de înaltă precizie, având la bază informaţii exacte şi oportune privind poziţia, natura, valoarea, intenţia şi capacitatea de luptă a adversarului. În acest sens, structurile de informaţii vor juca un rol decisiv în succesul operaţiei. Este necesară revizuirea regulilor de angajare şi eventual, adoptarea unor restricţii suplimentare privind utilizarea puterii de luptă în medii urbane puternic populate.

2.4 Reorganizarea structurilor de forţe

Plecând de la ideea că ameninţările hibride sunt cu adevărat eficiente împotriva organizaţiilor mari, birocratice, cu ierarhii şi sisteme relaţionale rigide, este necesar regândirea structurilor de forţe, pentru a fi reproiectate modular, rapid dislocabile şi flexibile, cu un lanţ de comandă-control simplificat, după modelul unităţilor de reacţie rapidă, şi având un caracter integrat (inclusiv la eşaloane mici) şi întrunit, capabile să răspundă tuturor provocărilor mediului de luptă, preponderent urban.

Structura de forţe care acţionează într-un conflict hibrid va trebui ţinută într-o stare de operativitate ridicată, gata pentru desfăşurare chiar *înainte de izbucnirea conflictului*. Această forţă de reacţie rapidă ar putea fi susţinută de o forţă convenţioanală importantă, pentru asigurarea securităţii zonei de operaţii.

Este indicat ca pentru combaterea ameninţărilor hibride să existe o grupare de forţe întrunită, combinată, hibridă în esenţă, cu elemente din cadrul tuturor structurilor implicate (forţe convenţionale, forţe speciale, agenţii de informaţii, structuri de ordine publică, forţe specializate în contracararea acţiunilor cibernetice, teroriste, psihologice, de război electronic etc), având un sistem de comandă control simplificat, capabil să accelereze fluxul informaţional-decizional, pentru menţinerea iniţiativei la nivel strategic, operativ şi tactic.

Utilizarea simultană, sub o comandă unică, a unei forţe regulate sau principale și a unei forţe neregulate oferă avantajul sinergic al unei presiuni asupra adversarului conform căreia întregul este mai mare decât suma părţilor. Acest mod de abordare diferită de conceptul *compound,* în care forţele acţionează simultan într-o direcţie unică, însă separat, existând diferite grade de coordonare în luptă.

Pentru normalizarea situaţiei şi sprijinirea populaţiei indigene, element cheie într-un război de tip hibrid, forţele care intervin trebuie ca în paralel cu operaţiile de tip combat, sau imediat ce situaţia din teren permite, să desfăşoare rapid operaţii de stabilitate şi sprijin pentru restabilirea securităţii, reconstrucţia şi dezvoltarea elementelor de bază ale economiei, asigurarea serviciilor esenţiale pentru populaţie, sprijin acordat administraţiei locale şi forţelor de ordine publică.

În aceeaşi măsură se impune regândirea posibilităţilor de înzestrare a forţelor, în funcţie de particularităţile mediului în care acţionează şi de nivelul ameninţării. Adversarii neconvenţionali pot adopta soluții low-tech pentru a depăși avantajele tehnologice de care se bucură armatele convenționale, în aceeași măsură putând întrebuinţa sisteme de arme avansate. Aceste tehnologii folosite simultan pot genera confuzii şi dificultăţi în planificarea şi executararea operaţiilor militare.

Există riscul ca războiul să se extindă în toate mediile, incluzând, pe lângă cele trei medii cunoscute (terestru, maritim, aerian-cosmic), mediul subteran (tuneluri pentru aprovizionare, manevră omnidirecţională şi acces către facilităţi de comandă-control

subterane, a căror eficienţă a fost dovedită în războaiele din Vietnam, Cecenia şi Fâşia Gaza) sau cel subacvatic (utilizarea luptătorilor subacvatici pentru atacuri asupra unor obiective critice din zonele costiere).

Se impune ca unităţile care acţionează în medii urbane, dens populate, să fie înzestrate şi cu sisteme de arme neletale, iar cercetările privind modalităţile de utilizare a tehnologiei neletale în operaţiuni urbane să fie amplificate. Totodată apreciez ca fiind necesar continuarea cercetărilor privind dezvoltarea şi implementarea unor sisteme active de protecţie contra-artilerie care să permită detectarea punctului de lansare, distrugerea proiectilelor (rachetelor) înainte de impact, dar şi a instalaţiilor de lansare.

2.5 Adaptarea instrucţiei şi exerciţiilor la noul cadru operaţional

Inovaţia şi creativitatea sunt liniile de forţă într-un război de tip hibrid. Un adversar motivat, liber de orice constrângeri juridice, tactice şi morale, va căuta să utilizeze întreg arsenalul avut la dispoziţie în moduri neaşteptate, imprevizibile, maximizând pierderile în rândul forţelor proprii. Tacticile de luptă ale guerilelor urbane vor cunoaşte perfecţionări, adaptări şi ajustări. Utilizarea simultană şi combinată a formelor şi procedeelor de luptă convenţională cu cele neconvenţionale, atacuri cibernetice, acţiuni teroriste şi criminale, subversive şi difuze, precum şi creşterea nivelului "joint" al operaţiilor sunt caracteristicile mediului de confruntare hibrid.

Sursa ameninţării va fi dificil de desluşit, adversarul real mascându-şi intenţiile şi acţiunile prin interpunerea unor structuri paramilitare, organizaţii non-militare, mişcări separatiste, grupuri de presiune, state-pion, sau state-troian. Adversarul poate fi de neînţeles, insesizabil şi iraţional.

Recentele conflicte au arătat că actori non-statali utilizează deja concepte operaţionale şi capabilităţi militare bazate pe tehnologie avansată, asociate în mod tradiţional ca aparţinând armatelor naţionale.

Tocmai de aceea, apreciem că este necesar ca instrucţia şi exerciţiile să se bazeze pe scenarii multinaţionale, întrunite, aplicate mediului urban, cu exersarea aplicării principiilor *LOAC* şi gestionării relaţiilor cu societatea civilă. La exerciţiile naţionale şi multinaţionale, comandamentul grupării de forţe întrunite, dar şi comandamentele tactice vor putea interacţiona cu factorii de decizie (autorităţi publice centrale / locale), structuri militare şi civile cu atribuţii în domeniul securităţii, precum şi cu vectorii de imagine (mass media, ONG-uri, lideri locali) din zona de operaţii. Forţele armate trebuie astfel să dispună de capacitatea de a opera cu succes în toate mediile, în cadrul unor conflicte complexe.

2.6 Dezvoltarea unor capacităţi pro-active privind informarea publică

Într-un conflict de tip hibrid adevăratul război se duce pe canalele de comunicare şi reţelele de socializare, fiecare parte căutând să obţină înţelegerea opiniei publice privind legitimitatea acţiunilor sale. O entitate statală sau organizaţie, victimă a unei agresiuni de tip hibrid, trebuie să dispună de metode şi tehnici eficiente pentru a contracara dezinformarea şi propaganda lansată pe canalele media, pierderea campaniei de informare având magnitudinea unei înfrângeri.

Negarea, nesinceritatea, manipularea, intimidarea și amenințarea îndreptate împotriva populației și mass-media sunt instrumente folosite imediat şi cu intensitate de grupări teroriste, actori non-statali sau state nedemocratice pentru a manipula domeniul informațiilor, a influența publicul, a pune sub semnul întrebării legitimitatea unor acţiuni de răspuns din partea comunităţii internaţionale, diminuând astfel voinţa de a lupta din partea unei entităţi militare legitime.

Nu este suficient ca elementele militare angajate în operaţie să respecte legile conflictelor armate, să protejeze populaţia civilă, să utilizeze forţa în mod proporţionat, distinctiv şi conform necesităţii militare. Trebuie ca aceste măsuri legale să fie aduse la cunoştinţa publicului intern şi extern în timp real.

Comandanţii militari trebuie să dispună de autoritatea de a transmite, prin intermediul structurilor proprii de relaţii publice (care trebuie să fie extrem de active !), agenţiilor de relaţii publice partenere, ministerului afacerilor externe şi misiunilor dipomatice, în mediile naţionale şi internaţionale, informaţii de interes privind operaţiile în curs de desfăşurare, având la bază probe relevante (video şi imagini) în susţinerea acestora. Mesajele transmise vor fi adaptate publicurilor ţintă, utilizându-se toate canalele de informare disponibile. Experţii în comunicare trebuie să se implice în planificarea strategică şi operaţională, unde să se analizeze "efectul media" al operaţiilor, inclusiv acţiuni de răspuns proactive la campania de dezinformare practicată de adversar.

În aceeaşi măsură, se impune revizuirea procedurilor privind transmiterea documentaţiilor către mass media, având în vedere că produsele de planificare operaţională sunt clasificate. Balansul între necesitatea informării opiniei publice şi restricţiile pe linia securităţii informaţiilor privind operaţiile încheiate, în curs şi viitoare trebuie corectat printr-o revizuire atentă a procedurilor.

Gestionarea şi vehicularea informaţiilor de interes public va necesita o abordare cuprinzătoare, unitară, coerentă şi conjugată din partea tuturor factorilor responsabili şi vectorilor de comunicare, civili şi militari, cu spriinul societăţii civile şi beneficiind de noi tehnologii, inclusiv instrumente analitice de social-media.

Concluzii

Natura conflictului a cunoscut o evoluţie rapidă în ultimele decenii, de la cele tradiţionale, simetrice, către forme neregulate, asimetrice. Deşi ameninţările asimetrice nu sunt o noutate, recentele conflicte au fost marcate de utilizarea unor tehnici şi tactici inovative, marcând o evoluţie periculoasă în spectrul războiului.

În conflictele viitoare, nu vor fi folosite exclusiv acţiuni convenţionale sau asimetrice, ci o combinaţie a acestora, sub forma războiului hibrid. Acesta încorporează o varietate de capabilităţi, strategii şi metode de ducere a luptei, incluzând forţe convenţionale, formaţiuni şi tactici neregulate, acţiuni teroriste şi dezordine criminală. Forţele armate trebuie astfel să dispună de capacitatea de a opera cu succes în toate mediile, în cadrul unor conflicte complexe.

Pentru contracararea ameninţărilor de tip hibrid este necesară adoptarea unei strategii eficiente de răspuns, având la bază o doctrină comună, precum şi direcţii generale fundamentale.

Este necesară o *abordare cuprinzătoare la nivelul tuturor elementelor de putere*, prin cooperare, integrare şi viziune strategică. Acţiunile militare vor fi parte a unui ansamblu de măsuri care includ acţiuni politico-diplomatice, economice, sociale, informaţionale.

Întărirea dialogului la nivel regional şi global pentru diminuarea tensiunilor geostrategice şi dezvoltarea proceselor de consultări privind creşterea încrederii şi securităţii vor asigura cadrul principal de acţiune pentru coordonarea eforturilor comune de contracarare a ameninţărilor simetrice, asimetrice şi hibride.

Monitorizarea transferurilor de fonduri financiare, capabilităţi militare moderne şi sisteme de arme avansate către state sau actori non-statali poate permite o evaluare anticipativă a ameninţărilor hibride, evitând astfel surprinderea strategică.

Plecând de la o nouă strategie de securitate, sistemul militar trebuie să adapteze programele privind educaţia militară, planificarea apărării, înzestrarea şi instruirea forţelor la ameninţările şi provocările secolului XXI.

Totodată, este necesară *crearea unor structuri de comandă şi control flexibile, adaptabile şi capabile* să asigure condiţiile de succes pentru forţele implicate în întreg spectrul de operaţii militare, inclusiv în contracararea ameninţărilor hibride.

Operaţiile militare trebuie susţinute de *campanii intense de informare publică pentru contracararea încercărilor de propagandă şi dezinformare, menţinerea iniţiativei strategice* în media internă şi internaţională, câştigarea încrederii opiniei publice.

Abordarea ameninţărilor hibride şi transformarea forţelor armate trebuie să corespundă directivelor strategice ale Alianţei Nord Atlantice şi Uniunii Europene, în cadrul unui proces amplu de reorientare a politicilor de securitate europeană şi euroatlantică. O soluţie strict naţională la ameninţările de tip hibrid nu este de dorit, riscurile şi ameninţările regionale determinând o reacţie comună, unitară la nivelul întregului continent european şi a întregii comunităţi internaţionale.

BIBLIOGRAFIE:

1. AARONSON, Michael, *NATO Countering the Hybrid Threat*, disponibil la adresa http://cco.dodlive.mil/files/2014/02/Prism_111-124_Aaronson-Diessen.pdf, accesat la 01.04.2015
2. BOND, Margaret, *Hybrid war: a new paradigm for stability operations in failing states*, disponibil la adresa http://www.dtic.mil/dtic/tr/fulltext/u2/a468398.pdf, accesat la 25.03.2015
3. CASEY, George, *America's Army in an Era of Persistent Conflict*, Army Magazine (October 2008), disponibil la adresa http://www.ausa.org/publications/ armymagazine/archive/2008/10/Documents/Casey_ 1008.pdf, accesat la 01.04.2015
4. DUŢU, Petre, *Ameninţări asimetrice sau ameninţări hibride*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2013, disponibil la adresa http://cssas.unap.ro/ro /pdf_studii/amenintari_asimetrice_sau_amenintari_hibride.pdf, accesat la 01.04.2015
5. HOFFMAN, Frank ,*Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, pp. 29
6. HUOVINEN,Petri, *Hybrid warfare–Just a Twist of Compound Warfare*, disponibil la adresa https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf, accesat la 01.04.2015
7. Johnson, David E., *Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza*, disponibil la http://www.rand.org/content/dam/rand /pubs/occasional_papers/2010/RAND_OP285.pdf, accesat la 20.03.2015
8. McCUEN, John , *Hybrid Wars*, disponibil la adresa http://www.au.af.mil/au/awc/ awcgate/milreview/mccuen08marapr.pdf, accesat la 01.04.2015
9. RUSSELL, Glenn, *Evolution and Conflict*, disponibil la adresa https://www.doria.fi/bitstream/handle/10024/92639/Y2622_HuovinenKPO_YEK56.pdf, accesat la 01.04.2015

10. WEITZ, Richard, *Countering Russia's Hybrid Threats*, disponibil la adresa http://www.diplomaatia.ee/en/article/countering-russias-hybrid-threats/, accesat la 01.04.2015
11. ***, *FM 5-0 The operations process,* disponibil la adresa https://fas.org/irp/doddir/army/fm5-0.pdf, accesat la 01.04.2015
12. ***, IMSM-0292-2010, *Hybrid threats description and context*, 2010, disponibil la adresa http://cco.dodlive.mil/files/2014/02/Prism_111-124_Aaronson-Diessen.pdf, accesat la 01.04.2015
13. ***, *Irregular Warfare: A SOF Perspective*, Center for Army Lessons Learned, Newsletter 11-34, Fort Leavenworth - Kansas, June 2011, p. 25, accesibil la adresa http://www.globalsecurity.org/military/library/report/call/call_11-34.htm, accesat la 01.04.2015
14. ***, JP 5-0 Joint Operation Planning, 2011, disponibil la adresa http://fas.org/irp/doddir/dod/jp5_0.pdf, accesat la 01.04.2015
15. *** Ministry of Defence UK, *Future Character of Conflict Paper (FCOC),* disponibil la adresa *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33685/FCOCReadactedFinalWeb.pdf,* accesat la 23.03.2015
16. http://indianstrategicknowledgeonline.com/web/DIRIWCSCBriefv3.pdf, accesat la 01.04.2015
17. http://www.jinsa.org/files/2014GazaAssessmentReport.pdf, accesat la 20.03.2015
18. https://info.publicintelligence.net/USASOC-CounterUnconventionalWarfare.pdf, accesat la 20.03.2015
19. http://fas.org/irp/doddir/army/fm3-0.pdf, accesat la 20.03.2015
20. https://fas.org/irp/doddir/army/fm3-05-130.pdf, accesat la 20.03.2015
21. http://fas.org/irp/doddir/army/fm3-24fd.pdf, accesat la 20.03.2015
22. http://www.nato.int/cps/en/natolive/topics_69482.htm, accesat la 20.03.2015
23. http://www.aco.nato.int/page134134653.aspx, accesat la 20.03.2015
24. http://en.wikipedia.org/wiki/Hybrid_warfare, accesat la 20.03.2015
25. http://smallwarsjournal.com/blog/training-a-hybrid-warrior-at-the-infantry-officer-course, accesat la 20.03.2015
26. http://cgsc.contentdm.oclc.org/cdm/singleitem/collection/p4013coll3/id/2752/rec/1, accesat la 20.03.2015
27. http://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/, accesat la 20.03.2015
28. http://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm, accesat la 20.03.2015
29. https://info.publicintelligence.net/USJFCOM-IrregularThreats.pdf, accesat la 20.03.2015
30. http://www.defenceiq.com/air-land-and-sea-defence-services/articles/the-21st-century-hybrid-threat-part-terrorist-part/, accesat la 20.03.2015
31. http://www.warcouncil.org/blog/2015/1/18/dynamic-doctrine-for-hybrid-threats-and-the-four-killer-es, accesat la 20.03.2015
32. http://www.ndc.nato.int/news/current_news.php?icode=758, accesat la 20.03.2015
33. http://www.globalsecurity.org/military/library/report/call/call_11-34_ch4.htm, accesat la 20.03.2015
34. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/, accesat la 20.03.2015

35. http://smallwarsjournal.com/jrnl/art/review-essay-fighting-and-learning-against-hybrid-threats, accesat la 20.03.2015
36. http://smallwarsjournal.com/jrnl/art/review-essay-history-and-hybrid-warfare, accesat la 20.03.2015
37. https://www.eda.europa.eu/info-hub/news/2015/01/26/increased-cooperation-to-counter-hybrid-threats, accesat la 20.03.2015
38. http,://www.act.nato.int/act-countering-hybrid-threats-task-force-identifies-future-challenges, accesat la 20.03.2015
39. http://www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment, accesat la 20.03.2015
40. http,://iripaz.org/listado_docs/res_conflictos/Hofmann%20Naturaleza%20evolutiva%20del%20conflicto.pdf, accesat la 20.03.2015
41. http://www.armedforcesjournal.com/hybrid-vs-compound-war/, accesat la 20.03.2015
42. http://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybrid-warfare/97259/, accesat la 20.03.2015
43. http://www.specialforcestraining.info/topics/hybrid-warfare.htm, accesat la 20.03.2015
44. http://www.dtic.mil/whs/directives/corres/pdf/300007p.pdf, accesat la 20.03.2015
45. https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf?sequence=1, accesat la 20.03.2015
46. http://jsou.socom.mil/JSOU%20Publications/JSOU%2013-4_McCulloh, Johnson_Hybrid%20Warfare_final.pdf, accesat la 20.03.2015
47. http://www.fraw.org.uk/files/peace/us_dod_2000.pdf, accesat la 23.03.2015
48. http://www.defense.gov/news/newsarticle.aspx?id=45289, accesat la 23.03.2015.

CREŞTEREA PERFORMANŢEI ÎN ACTIVITATEA DE INTELLIGENCE PRIN CONŞTIENTIZARE

Răzvan ŢUREA
Doctorand la Academia Naţională de Informaţii „MIHAI VITEAZUL”,
email:razvan.turea@yahoo.com

Rezumat: *Produsul final al activităţii de intelligence, bazat pe cunoaştere şi obiectivitate, în conformitate cu noua paradigmă a serviciilor secrete, este rezultatul efortului depus de pionul principal – analistul de intelligence. Calitatea rapoartelor sale este condiţionată de performanţa atinsă în asimilarea pregătirii specifice. Două dimensiuni ale conştientizării, ca modalitate de creştere a performanţei, sunt importante în acest sens, inteligenţa emoţională şi inteligenţa socială. Acestea sunt, conform noilor concepte din neuroştiinţă, două laturi ale personalităţii umane posibil de manipulat prin metode specifice, ce implică conceptul de neuroplasticitate. Apare, în mod surprinzător poate, o puternică legătură între metodele neuroştiinţei şi creşterea performanţei în intelligence la toate nivelurile, atât din punctul de vedere al individului cât şi al organizaţiei. În activitatea de evaluare a lucrătorilor în intelligence se pot folosi metode şi practici ale psihologiei moderne, instrumente psihometrice adecvate diferitelor aspecte ale personalităţii specifice unui analist de intelligence performant.*

Cuvinte cheie*: intelligence, analist, conştientizare, performanţă, inteligenţa emoţională, neuroplasticitate.*

Introducere

Lumea de astăzi este un conglomerat de societăţi puternic diferenţiate atât social, economic, politic, cultural, militar, cât şi informaţional. Procesul de globalizare determină, pe lângă efectele pozitive ale dezvoltării economice şi ale progresului ştiinţei, tehnicii şi tehnologiei, şi puternice disfuncţionalităţi sociale şi în mod deosebit, militare, ce duc, în cele din urmă, la conflicte de toate tipurile.

În procesul de înşelegere şi combatere a acestora au apărut noi modele teoretice ale conflictului, care au determinat reconfigurarea conceptului de securitate naţională şi crearea unei noi paradigme de securitate.

Ca parte a acestei paradigme, misiunea serviciilor de informaţii a fost regândită şi reconfigurată astfel încât să satisfacă necesităţile de asigurare a securităţii în condiţiile provocărilor din ce în ce mai complexe şi mai bine proiectate, dispunând de resurse dintre cele mai sofisticate, atât materiale cât şi umane. Factorul uman nu a putut fi încă, depăşit de tehnologie în ce priveşte esenţa individului supravegheat/studiat[1]. Natura umană excede nivelul tehnologiei, tehnologiile avansate rămânând esenţiale în ce priveşte structura activităţii de informaţii.

Pe câmpul de luptă, de orice fel ar fi el, inclusiv pe cel *mental*, informaţia corectă trebuie să ajungă în timp real la luptător, acesta fiind obligat de dinamismul acţiunii să decidă şi să acţioneze singur sau împreună cu alţii. Primii, în acest adevărat război al minţii[2], sunt agenţii, sursele secrete umane, care culeg şi verifică informaţiile de securitate naţională.

---

[1]Stan PETRESCU**,** *Despre Intelligence, spionaj si contraspionaj*, Bucuresti, Editura Militară, 2007.
[2]*Ibidem.*

Următorul nivel, cel al elaborării analizei de intelligence, este asigurat de analistul de intelligence care "generează cunoştinţele (analiza primară, structurată, comparaţie, studiu de relevanţă, ordonare, ierarhizare, nuanţare, studiu de context etc.), le conferă atributul de informaţie strategică şi le organizează şi sintetizează în rapoarte de expertiză"[3].

1. Analistul de intelligence, calităţi şi trăsături mentale

Noile tendinţe, teoria nevoii de schimbare continuă, aşează analiza de intelligence în centrul ciclului de intelligence[4], orientând atât culegerea cât şi producţia şi diseminarea informaţiilor (figura nr.1).

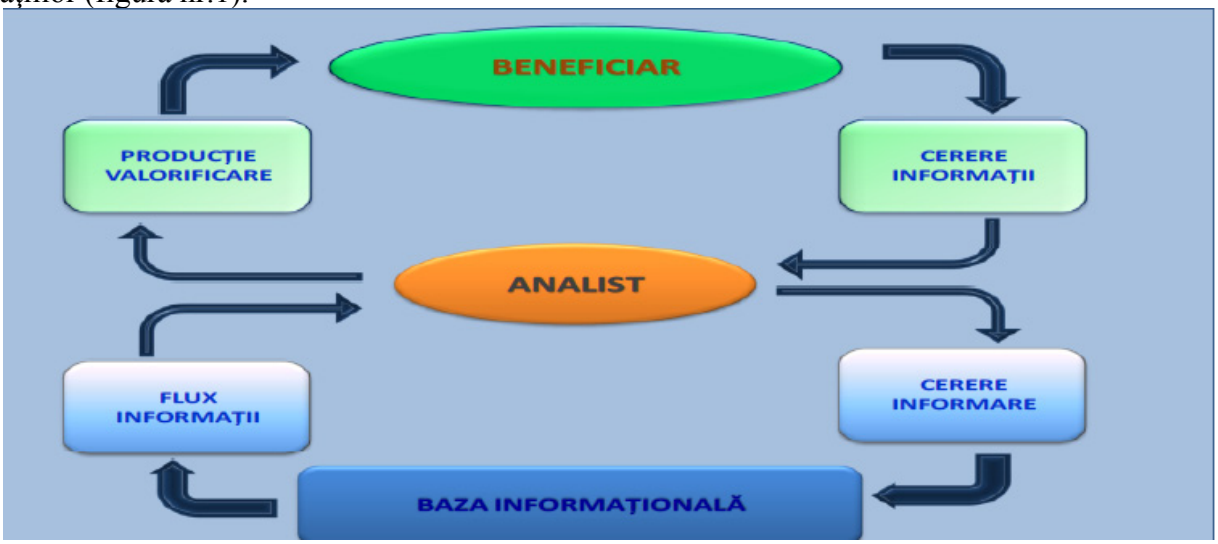


Figura nr. 1 Analistul în fluxul de intelligence.
(Sursa: Niţu Ionel, Ghidul analistului de intelligence: compendiu pentru analiştii debutanţi, Editura ANI MV, 2011, p. 31)

Deşi aparent simplu, "*este vorba de un proces de rafinare foarte complex, care implică în egală măsură inteligenţa, gândirea critică şi creativitatea analistului de informaţii, dar şi o foarte bună cunoaştere a domeniului analizat. Mai exact, analistul evaluează informaţiile din perspectiva relevanţei lor, sesizează schimbări şi tendinţe în manifestarea ameninţărilor, schiţează scenarii alternative de evoluţie, evidenţiază implicaţii şi indică eventuale variante de acţiune în raport cu fiecare scenariu prognozat.*"[5]

În munca lui analistul are datoria *„de a depăşi prejudecăţi, de a separa informaţia de emoţie, impulsul de raţional, strategicul de tactic"*[6].

Cercetările asupra luării deciziilor în grup, au arătat că acestea sunt dependente de procesul de distribuire a informaţiilor în cadrul grupului, în timp ce teoria achiziţei de informaţii sugerează că analistul de intelligence este un adevărat devorator de informaţii care utilizează strategii de adaptare pentru realizarea unor puncte de vedere obiective.

„Intelligence – ca disciplină teoretică – prezintă un grad redus de conceptualizare şi teoretizare, raportat la alte ramuri ale ştiinţelor sociale. Totuşi, aşa cum sublinia şi Stephen

---

[3]https://andreivocila.wordpress.com/2010/10/29/intelligence-ul-privat, accesat la 13 martie 2015.
[4]Lucian Ion PETRAŞ, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014, p. 119.
[5]http://www.sri.ro/analiza-intelligence.html, accesat la 12 sept. 2014.
[6]George Cristian MAIOR, *Incertitudine. Gandire strategica şi relaţii internaţionale în secolul XXI*, Bucureşti, Editura RAO, 2009, p. 36.

Marrin[7]*, obţinerea unui nivel de abstractizare care să permită analiza cazurilor specifice prin raportare la un cadru conceptual riguros este esenţială pentru a putea răspunde la întrebări precum: Ce tipuri de structuri şi procese organizaţionale maximizează calitatea produsului analitic? Ce modificări pot fi aduse structurilor şi proceselor pentru a îmbunătăţi acest produs? Ce bune practici din alte domenii pot fi utilizate pentru a optimiza procesul analitic? Ce ar trebui să facem pentru a maximiza performanţele analiştilor? Care sunt caracteristicile analiştilor de intelligence performanţi?"* – spunea George Maior în introducerea la lucrarea lui Ionel Nițu „Analiza de intelligence – o abordare din perspectiva teoriilor schimbării"[8]. Ultimele două chestiuni vor fi abordate în această lucrare, într-o ordine care se potriveşte mai bine cu tematica cercetată. Prin urmare, voi căuta să răspund mai întâi la întrebarea, care sunt caracteristicile analiştilor de intelligence performanţi?

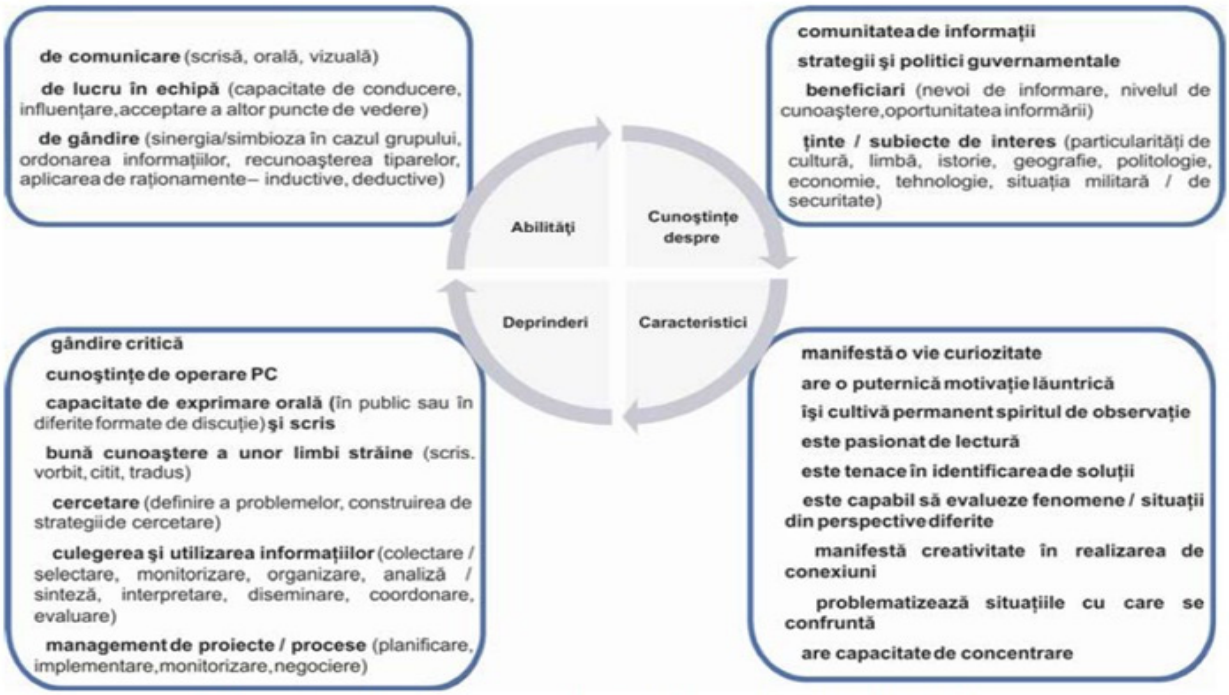


Fig. nr. 2 Competenţele de bază ale analistului de intelligence
Sursa: Nițu Ionel, Ghidul analistului de intelligence: compendiu pentru analiştii debutanţi, Editura ANI MV, 2011, p. 37

Modul în care gândeşte un analist de intelligence ar trebui să fie unul cât mai obiectiv, mai neutru, pentru a asigura calitatea primordială a unei analize, aceea de a descrie realitatea cât mai fidel. Gândirea critică[9] privită ca un act cognitiv şi metacognitiv (observare a actului gândirii, *conştientizare* a modului în care sunt abordate problemele), în acelaşi timp, poate fi un model de abordat. Nu este suficient să se ştie care sunt aptitudinile necesare pentru gândirea critică. Un bun analist trebuie să aibă anumite atitudini, dispoziţii, aptitudini şi trăsături ale minţii, pe care să le perfecţioneze prin folosirea modului de gândire critică. Anumite studii empirice precizate de Peter A. Facione şi alţii, indică faptul că, pentru

[7]Stephen MARRIN, , *Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful*, în Intelligence and National Security, vol 27, nr. 3, 2012, pp. 398-422.
[8]http://www.ziaristionline.ro/2012/12/05/george-maior-despre-analiza-de-intelligence, accesat la 3 august 2013
[9]Peter A. FACIONE, Noreen C. FACIONE, Carol A .GIANCARLO, *The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill*, Informal Logic 20, no. 1 2000, pp. 61–84.

atingerea scopului propus este necesar ca analistul, nu numai să aibă aptitudini pentru gândirea critică, dar şi să fie dispus să le folosească, ceea ce nu se întâmplă mereu.

Sunt câteva abilităţi esenţiale, atribute mentale asociate cu gândirea critică, aşa cum le precizează Faciones şi Giancarlo[10]: căutarea adevărului, deschidere la abordări noi, insolite ale evenimentelor, putere de analiză, gândire sistematică, încredere în sine, maturitate în gândire. Pe de altă parte, Richard Paul şi Gerald Nosich[11] afirmă că *„printre caracteristicile modelului de gândire critică se pot menţiona şi: gândirea independentă, înţelegerea egocentrismului şi a sociocentrismului, modestia intelectuală, suspendarea judecării persoanelor şi evenimentelor, curajul susţinerii ideilor, loialitatea şi integritatea, perseverenţă intelectuală, încrederea în raţiune, explorarea sentimentelor şi a emoţiilor, curiozitatea intelectuală”*. Ambele seturi de abilităţi au puncte comune cu aptitudinile necesare unui analist de intelligence aşa cum au fost ele identificate de David Moore şi Lisa Krizan[12] şi anume: curiozitatea permanentă, fascinaţie pentru identificarea evenimentelor fără a le cunoaşte în totalitate, motivarea pentru cunoaşterea intelectuală continuă, privirea realităţii din perspective inedite. Toate acestea îl ajută să facă conexiuni surprinzătoare pentru a rezolva cele mai dificile probleme. În final, tensiunile emoţionale create de aceste probleme sunt eliberate prin găsirea soluţiei optime. În plus, emoţiile, sentimentele şi intuiţia joacă un rol semnificativ în gândirea critică, aşa cum arată expertul în învăţare Stephen Brookfield[13]. El crede că este vorba de a găsi un alt mod de gândire decât cel folosit în mod curent de analist, unul care cere creativitate şi intuiţie, calităţi ce se consideră a nu aparţine gândirii raţionale.

Aptitudinile şi abilităţile menţionate (figura 2) nu sunt caracteristice numai analistului de intelligence, ele ar trebui să caracterizeze marea majoritate a celor ce activează în acest domeniu. Ionel Niţu afirmă[14] că între cei care colectează informaţia (agenţii) şi cei care procesează această informaţie (analiştii) există o diferenţă devenită deja clasică în comunităţile de informaţii, şi reuşeşte să demonstreze, cu o argumentare ştiinţifică solidă, că aceasta s-a mai redus astăzi, în secolul XXI, din mai multe raţiuni. Una dintre ele este nevoia de schimbare pentru a putea face faţă noilor provocări apărute în domeniu.

2. Performanţă umană

Conceptul de performanţă umană a fost definit pornind de la conceptul de "performanţă" specifică (de exemplu mentală, sportivă etc), de către un grup de specialişti în domeniul medicinii, bio-motricităţii şi teoriei informaţiei. În acest sens, performanţa umană este o capacitate a individului, ca fiinţă umană, de a face faţă, de a se adapta, la condiţii deosebite. Condiţiile deosebite se referă la cele care depăşesc "parametrii funcţionali" obişnuiţi, consideraţi normali, care s-au dezvoltat în decursul evoluţiei ontologice şi genetice.

Depăşirea acestor dotări, aptitudini, poate avea loc în condiţii adverse (de ex.: ca o reacţie la condiţii de mediu extreme, stres ridicat, etc.) sau poate fi făcută cu o intenţie bine precizată (activităţi sportive de performanţă, activităţi mentale deosebite, etc.). Există diferite

---

[10]Peter A. FACIONE, Noreen C. FACIONE, Carol A .GIANCARLO, *Professional Judgment and the Disposition Toward Critical Thinking,* Milbrae, CA: California Academic Press, 2002.

[11]Richard W. PAUL, Gerald NOSICH, *Model for the National Assessment of Higher Order Thinking*, Dillon Beach, CA: Foundation for Critical Thinking, 2013, p.23.

[12]David MOORE, Lisa KRIZAN, *Intelligence Analysis: Does NSA Have What it Takes,* reprint NSA Center for Cryptologic History, Cryptologic Quarterly 20, nos. 1/2 , 2001, pp. 8–11.

[13]Stephen D. BROOKFIELD, *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting,* San Francisco, CA: Jossey–Bass Publishers, 1987, p. 12.

[14]Lucian Ion PETRAŞ,*Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014, p. 120.

aspecte ale performanţei umane, care pot fi evaluate, antrenate şi în acest fel, ameliorate. Prin antrenarea unui anumit tip de performanţă specifică se pot obţine efecte care să implice îmbunătăţirea, oarecum neaşteptată, a performanţei în alt domeniu, aparent fără o legătură directă.

Antrenamentul interspecific al aptitudinilor poate fi orientat spre un scop precis. Acest proces este folosit pentru a atinge noi nivele de performanţă şi în activitatea de intelligence. În acest context, performanţa în activitatea de intelligence, îmbunătăţită conform unor metodologii şi cu tehnici adecvate, va potenţa şi va accelera procesul transformator a lucrătorului în intelligence, în conformitate cu noile tendinţe precizate prin sintagma „nevoia de schimbare”[15].

3. Conştiinţă, conştientizare

Etimologia cuvantului (con-ştiinţă, con-scientia; con-science) arată că organizarea conştientă este o reflectare cu ştiinţă. Este vorba despre o reflectare a realităţii în care fiinţa umană, având la dispoziţie un număr suficient de informaţii, le foloseşte pentru a înţelege şi interpreta un nou obiect, fenomen, eveniment, apărut în câmpul conştiinţei. *„Sub raport psihologic, omul îşi dă seama de „ceva" anume şi îl reproduce în subiectivitatea sa sub forma de imagini, noţiuni, impresii”*[16]. În virtutea experienţei anterioare, obiectul are un ecou informaţional în subiect, în sensul că este conştientizat aproape imediat.

Conştientizarea, fiind o observare a actului gândirii, presupune o recunoaştere a particularului în general şi regăsirea generalului în particular. De asemenea, conştientizarea implică prezenţa unui scop în plan mental, ca element esenţial în reflectarea conştientă. Scopurile, fiind stabilite înainte de desfăşurarea activităţii, permit individului să anticipeze rezultatul acţiunilor sale, înainte de realizarea lor într-o formă concretă. Regăsim, în aceste câteva caracteristici ale procesului de conştientizare, unele puncte comune cu aptitudinile şi abilităţile necesare unui analist de intelligence aşa cum au fost ele precizate anterior. Pe scurt, putem spune că în activitatea de intelligence este nevoie de indivizi cu o mare putere de conştientizare văzută ca o cunoaştere obiectivă a realităţii (sociale, în cazul nostru).

4. Inteligenţa emoţională şi conştientizare

Conceptul de inteligenţă, presupune, după unii autori[17], o abordare cognitivă, care evidenţiază abilităţi mentale cum ar fi: capacitatea de a raţiona, de a planifica, de a rezolva probleme, de gândire abstractă, de a înţelegere a unor idei complexe, de a învăţa în general.

Inteligenţa de tip cognitiv, academic, a fost considerată mult timp, un predictor al performanţei în domeniile ce aparţin de ştiinţă, tehnologie sau, într-un sens mai larg, al eficienţei în activitate. Dar, studiile efectuate în ultimele două decenii, au arătat că inteligenţa cognitivă nu este întotdeauna corelată cu performanţa[18], chiar şi în domeniile academice.

Situaţiile în care află o persoană nu pot fi judecate, clasificate dintr-o singură perspectivă, deoarece nu s-ar putea spune că indivizii au întotdeauna aceleaşi reacţii la aceeiaşi stimuli sociali. Aspectele de ordin afectiv, emoţional au început să fie luate în consideraţie atunci când se vorbeşte de cunoaşterea omului şi a mediului social în care se dezvoltă şi activează. Starea emoţională a unui individ condiţionează modalitatea de interpretare a situaţiilor. Dispoziţia emoţională pozitivă generează o gândire optimistă, care

---

[15] *Ibidem*, p. 121.
[16] http://www.aticmd.md/wp-content/uploads/2012/03/S_4_01_Todoroi.pdf
[17] Daniel GOLEMAN, *Inteligenţa emoţională*, editura Curtea Veche, 2008.
[18] *Ibidem,* p. 56.

determină soluţionarea într-un grad ridicat a problemelor, în timp ce emoţiile negative determină pesimism, blocând capacitatea de acţiune şi decizie.

Ar fi eronat să fie negat rolul afectivităţii al sentimentelor şi emoţiilor, atunci când scopul acţiunii sociale este îndreptat spre relaţionarea eficientă, cu atât mai mult cu cât aceste aspecte au un rol pregnant adaptiv. De aceea opoziţia emoţie – raţiune, este inexactă. Atât procesele cognitive (raţiunea) cât şi cele afective (emoţia) sunt inseparabile în cadrul acţiunii umane, chiar dacă sunt diferite prin modul de operare şi de organizare a formelor psihice[19]. Un aspect surprinzător, este că emoţiile şi sentimentele conştientizate, par a fi indispensabile luării unor decizii raţionale adecvate[20] situaţiilor sociale reale, decizii neafectate de prejudecăţi sau de trecutul emoţional al individului.

Comportamentul uman este foarte complex, fiind modulat de emoţii, astfel încât uneori, nu putem aprecia cu acurateţe reacţiile unei persoane, chiar dacă o cunoaştem. De aceea, abilitatea de a descifra, de a percepe emoţiile proprii sau ale altora, de a le interpreta şi utiliza pentru atingerea unui scop, este aceea care asigură succesul social şi nu numai. Această abilitate a fost denumită inteligenţă emoţională, Daniel Goleman considerând-o un predictor mai bun pentru performanţa socială decât inteligenţa cognitivă, referitoare la raţiune. Un individ cu un nivel ridicat al inteligenţei emoţionale poate foarte uşor să recunoască şi să şi înţeleagă comportamentul psihoemoţional al altor parteneri sociali. Inteligenţa emoţională dezvoltată, presupune aptitudini înnăscute ca sensibilitate (abilitatea de a recunoaşte structuri emoţionale manifestate la nivel subtil), memorie emoţională, capacitate ridicată de procesare atât propriilor emoţii cât şi ale partenerilor sociali şi nu în ultimul rând, abilitatea de învăţare emoţională, permanentă. Aceste caracteristici pot suferi un proces de ameliorare şi dezvoltare, după cum se şi pot degrada. În acelaşi timp, deşi inteligenţa emoţională crescută, este corelată cu un comportament social pozitiv, ea poate fi utilizată şi pentru a manipula comportamentul partenerilor sociali în propriul interes[21]. Aceasta nu este neapărat un element de negativitate, dacă luam în considerare specificul activităţii de intelligence.

Pe de altă parte, există şi o teorie a inteligenţei multiple, sau cu mai multe faţete, propusă de Howard Gardner[22] şi rezumată de Karl Albrecht cu acronimul ASPEAK[23] astfel:

Categoriile Inteligenţei multiple		
Acronim	**Categoria**	**Descriere**
A	inteligenţa abstractă	raţionamentul simbolic
S	inteligenţa socială	interacţiunea cu oamenii
P	inteligenţa practică	organizarea şi realizarea sarcinilor
E	inteligenţa emoţională	conştiinţa de sine şi autocontrolul
A	inteligenţa estetică	simţul formei, al design-ului, al muzicii, artei şi literaturii
K	inteligenţa kinestezică	aptitudini legate de mobilitatea corporală

Tabel nr. 1 Aspecte, categorii ale inteligenţei multiple

[19] Mielu ZLATE, *Introducere In Psihologie*, Ed. Polirom, Bucureşti, 2007

[20]Antonio DAMASIO, *Eroarea lui Descartes. Emoţiile,raţiunea şi creierul uman*, Ed. Humanitas,Bucureşti, 2005, p.38.

[21]Y. NOZAKI, M. KOYASU, *The Relationship between Trait Emotional Intelligence and Interaction with Ostracized Others' Retaliation,* PLoS ONE 8(10): e77579. doi:10.1371/journal.pone.0077579, 2013.

[22]Howard GARDNER,.*Assessment of intellectual profiles: A perspective from multiple intelligences theory*. In D. Flanagan, C. Graham (Eds.), Contemporary intellectual assessment, New York, Guilford Press.2011, pp. 145-155.

[23]https://www.karlalbrecht.com/articles/pages/socialintelligence.htm, accesat 20 martie 2015.

Aceste categorii pot fi imaginate ca fiind feţele unui cub, care constituie un tot, ce descrie mai bine fiinţa umană. Remarcăm că în acest model este inclus şi aspectul social al inteligenţei, un fel de conştientizare a unei strategiei sociale, combinată cu un set de aptitudini, pentru a interacţiona cu succes din punct de vedere social. Pe scurt, inteligenţa socială ar fi capacitatea de a te înţelege (relaţiona) bine cu alţii şi de ai determina să coopereze cu tine. Goleman, un promotor iniţial al ideii de inteligenă emoţională cu o sferă de cuprindere mai largă, ce includea ambele categorii emoţională şi socială, a revenit şi a recunoscut că trebuie să fie făcută o distincţie între cele două aspecte[24]. Un individ cu o inteligenţă socială dezvoltată poate reduce conflictualitatea, poate crea condiţiile unei bune colaborări, înlocuind comportamentul extremist cu o atitudine înţelegătoare, poate mobiliza oamenii pentru atingerea unor scopuri comune.

Există multe ambiguităţi cu privire la definirea acestor concepte, astfel încât, se pot întâlni lucrări care descriu conceptul de inteligenţă emoţională folosind caracteristicile conştiinţei sociale şi invers. De aceea, este dificil de definit care sunt factorii predictivi pentru existenţa şi nivelul inteligenţei emoţionale sau sociale.

După Bar-On[25] ceea ce este caracteristic inteligenţei emoţionale, este capacitatea de a conştientiza, de a înţelege şi de a controla şi procesa atât propriile emoţii cât şi ale altora, în procesul relaţionării sociale. El consideră ca inteligenţa emoţională este *un indice al capacităţii generale a unei persoane de a se adapta la situaţii dificile*[26].

5. Ce ar trebui să facem pentru a maximiza performanţele analiştilor?

Un agent în acţiune, trebuie să fie mereu conectat la realitate, la momentul prezent, conştientizând astfel, evenimentele reale, nedistorsionate de propriile emoţii, fără a le aplica un filtru propriu. Acest comportament asigură obiectivitatea analizei, raportului. Lucrătorul în intelligence trebuie să fie un observator, calitate care îi permite să înregistreze în mod obiectiv, evenimentul aşa cum se desfăşoară, incluzând toate aspectele lui. Implicarea emoţională şi condiţionarea psihoemoţională[27] obturează anumite aspecte ale evenimentelor, reduc câmpul conştiinţei (figura nr. 3), diminuând capacitatea lucrătorului de intelligence de a înţelege întregul context al acţiunii, de a lua cele mai bune decizii.

Capacitatea de a fi observator este una care poate fi antrenată, exersată şi în acelaşi timp, poate fi refăcută dacă a fost obturată prin condiţionare emoţională[28]. Această capacitate, de observator, presupune existenţa unor abilităţi crescute în ce priveşte atenţia concentrată şi memoria, fără de care nu se poate vorbi de conştientizarea realităţii.

---

[24]Daniel GOLEMAN, *Inteligenţa socială*, editura Curtea Veche, 2007, p.11.
[25]Iulia FODOR, *Inteligenta emotionala si stilurile de conducere*. Editura Lumen, 2009, p.23.
[26]Claudia DANILIUC, *Perspectivă asupra cercetării inteligenţei emoţionale şi sociale în relaţie cu dezvoltarea mentală*, Psihologia aplicată în structurile de apărare, ordine publică şi siguranţă naţională, între standardizare şi creativitate- *PSIHOPOL II*, 2010, p. 62.
[27]Aliodor MANOLEA, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012, p. 69.
[28]*Ibidem.*

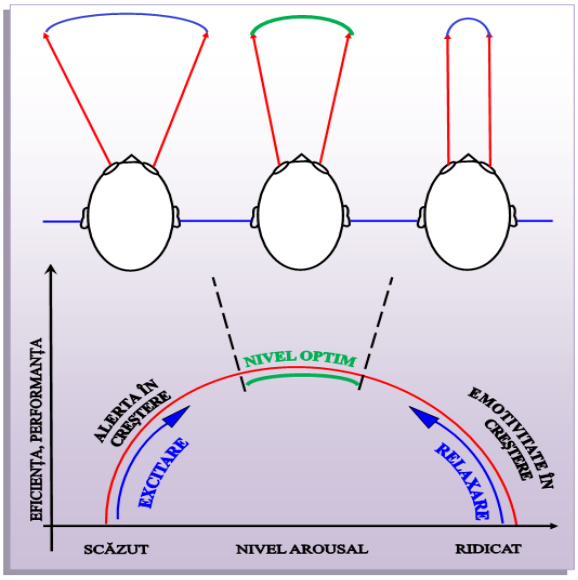


Figura nr. 3 Relaţionarea arousal-câmp al conştiinţei cu nivelul eficienţei şi al performanţei

(Sursa: Manolea, A.,Fundamente epistemice, metodologice şi acţionale privind investigarea experimentală a influenţei psihoinformaţionale distale în acţiunea de intelligence", Provocări şi strategii în ordinea şi siguranţa publică, coordonatori Mihai Bădescu, Veronica Stoica, Editura Universitară, Bucureşti, 2014, pp. 493-499)

Aceste două procese psihice pot fi considerate precursori ai conştientizării. Îmbunătăţirea lor implică un grad mai mare de conştientizare a evenimentelor realităţii sociale, când vorbim de activitatea de intelligence.

Concluzii

Aşa cum am arătat, conştientizarea este o caracteristică foarte importantă a inteligenţei emoţionale şi sociale, aflată în raport de proporţionalitate cu acestea. Cu alte cuvinte, conştientizarea crescută determină existenţa unei persoane cu inteligenţă emoţională şi socială, ridicate. Aceste două aspecte ale inteligenţei umane sunt corelate direct (pozitiv) cu nivelul performanţei umane în foarte multe domenii ale activităţii, inclusiv în cea de intelligence. Corelaţia performanţei în intelligence cu cele două faţete ale inteligenţei umane, rezultă din coincidenţa caracteristicilor lucrătorului în intelligence cu cele ce definesc inteligenţa emoţională şi cea socială.

Selecţia personalului pentru activitatea de intelligence ar trebui să se facă plecând, în primul rând, de la nivelul acestor două aspecte ale intelligenţei umane, folosind mai multe metode de evaluare ale acestora. Apoi, cei selectaţi, trebuie antrenaţi în ce priveşte nivelul conştientizării care, aşa cum am arătat, determină creşterea nivelului celor două faţete ale inteligenţei. Metodele ce ar putea fi utilizate, presupun modificarea anumitor comportamente prin unele tehnici ale psihologiei moderne (metode cognitiv-comportamentale, hipnoză, procese ale memoriei adânci (Deep Memory Process), metode psihocuantice[29], etc), metode ale căror rezultate au fost puse în evidenţă prin intermediul unor tehnici specifice neuroştiinţei. Acestea, au arătat cum se reconfigurează reţelele neuronale în timpul aplicării

[29]Aliodor MANOLEA, Emphasizing the Psycho-quantum Way of Psychotherapeutic Action: Quantum Deep Psychotherapy. *Procedia-Social and Behavioral Sciences*, vol. 127, 2014, pp.636-639.

unor metode de antrenament psihologic[30]. Meţinerea noilor configuraţii ale acestor reţele, prin antrenare susţinută, determină modificări comportamentale cu caracter permanent, astfel încât, este posibil să se amelioreze, de exemplu, conştientizarea, văzută ca o cunoaştere a realităţii. Antrenând memoria şi atenţia concentrată prin metode specifice, care să implice susţinerea în stare conectată a anumitor reţele neuronale, timp de cel puţin zece secunde[31], se poate obţine creşterea gradului de conştientizare. Această ameliorare a nivelului conştientizării, poate genera îmbunătăţirea inteligenţei emoţionale şi sociale, astfel încât, să se obţină o creştere semnificativă a performanţei umane, inclusiv în activitatea de intelligence.

BIBLIOGRAFIE:

1. BROOKFIELD Stephen D., *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting*, San Francisco, CA: Jossey–Bass Publishers, 1987.
2. DAMASIO Antonio, *Eroarea lui Descartes. Emoţiile,raţiunea şi creierul uman*, Ed. Humanitas,Bucureşti, 2005.
3. FACIONE Peter A., FACIONE Noreen C., GIANCARLO Carol A ., *Professional Judgment and the Disposition Toward Critical Thinking,* Milbrae, CA: California Academic Press, 2002.
4. FACIONE Peter A., FACIONE Noreen C., GIANCARLO Carol A., *The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill*, Informal Logic 20, no. 1 2000.
5. GARDNER Howard,.*Assessment of intellectual profiles: A perspective from multiple intelligences theory*. In D. Flanagan, C. Graham (Eds.), Contemporary intellectual assessment, New York, Guilford Press, 2011.
6. GOLEMAN Daniel, *Inteligenţa emoţională*, editura Curtea Veche, 2008.
7. GOLEMAN Daniel, *Inteligenţa socială*, editura Curtea Veche, 2007.
8. http://www.sri.ro/analiza-intelligence.html.
9. http://www.ziaristionline.ro/2012/12/05/george-maior-despre-analiza-de-intelligence.
10. MAIOR George Cristian, *Incertitudine. Gandire strategica şi relaţii internaţionale în secolul XXI*, Bucureşti, Editura RAO, 2009.
11. MANOLEA, Aliodor, *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie, Teza de doctorat, 2012.
12. MARRIN Stephen, *Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful*, în Intelligence and National Security, vol 27, nr. 3, 2012, pp. 398-422.
13. MOORE David, KRIZAN Lisa, *Intelligence Analysis: Does NSA Have What it Takes,* reprint NSA Center for Cryptologic History, Cryptologic Quarterly 20, nos. 1/2 , 2001.

[30]B. ECKER, B. TOOMEY, *Depotentiation of symptom-producing implicit memory în coherence therapy în Journal of Constructivist Psychology*, 21: DOI: 10.1080/10720530701853685, 2008, pp.87–150.
[31]*Ibidem*, p.95.

14. NOZAKI Y., KOYASU M., *The Relationship between Trait Emotional Intelligence and Interaction with Ostracized Others' Retaliation,* PLoS ONE 8(10).
15. PAUL Richard W., NOSICH Gerald, *Model for the National Assessment of Higher Order Thinking*, Dillon Beach, CA: Foundation for Critical Thinking, 2013.
16. PETRAŞ Lucian Ion, *Relaţionarea cu beneficiarii de intelligence în noua paradigmă - de la tirania hârtiei spre libertatea din wiki*, Intelligence, nr. 26, 2014.
17. PETRESCU Stan**,** *Despre Intelligence, spionaj si contraspionaj*, Bucuresti, Editura Militară,. 2007.
18. ZLATE Mielu, *Introducere In Psihologie*, Ed. Polirom, Bucureşti, 2007.

COMUNITATEA DE INFORMAŢII MODERNĂ ÎN SOCIETATEA CUNOAŞTERII

Petrişor BĂDICĂ
Doctorand în domeniul "Informaţii şi Securitate Naţională", Academia Naţională de Informaţii "MIHAI VITEAZUL", Bucureşti, e-mail petrisor_35@yahoo.com

Rezumat: *Dinamica mediului de securitate extinde nevoia expresă de adaptare structurală şi funcţională a CIM într-o nouă paradigmă ancorată la realitatea operaţională a secolului XXI în care elementele de apărare, securitate naţională, diplomaţie, cultură, economie, mediu etc. sunt interpătrunse activ, iar nevoia de colaborare, integrare, şi inovare reprezintă premise ale cunoaşterii avansate şi soluţia pentru interconectarea capabilităţilor acţionale ale entităţilor informative.*

Pe actualul registru al riscurilor şi ameninţărilor specifice mediului de securitate modern, caracterizat de o dinamică înaltă, varietate, neuniformitate şi de ambiguitatea cauză - efect, Comunitatea de Informaţii se structurează şi funcţionează în parametrii organizaţiei de intelligence reprezentând principalul furnizor al informaţiilor necesare adoptării infodeciziilor bazate pe intelligence şi asigurarea avantajului decizional în domeniile care vizează securitatea naţiunii, prin acţiune unificată şi realizarea unei abordări complexe, integratoare a acesteia. Efectul imediat al schimbării paradigmei de securitate în plan intern şi internaţional îl reprezintă transferul rolului şi ponderii intelligence-ului în infodecizie, acţiunea politică bazându-se din ce în ce mai mult pe calitatea produselor de intelligence.

Keywords*: the intelligence community, decision-making, informational revolution, Knowledge society, integrated system, sinergy and intelligence exchange.*

1. Comunitatea de informaţii modernă – valenţe teoretice şi operaţionale

În contextul cunoaşterii actuale a domeniului "intelligence", preocupările de definire şi implementare a conceptului "comunitate de informaţii" s-au dezvoltat mai ales în rîndul noilor democraţii create după sfârşitul Războiului Rece, fiind legate indisolubil de nevoia unui răspuns adecvat factorilor de risc şi insecuritate prezenţi în mediul operaţional al secolului XXI marcat de incertitudine, fragmentare, crize cu conotaţii multiple şi activarea unor vechi ameninţări, precum şi a unor noi forme de conflictualitate, între care evidenţiem confuntarea informaţională .

A devenit evidentă nevoia de sinergie la nivelul componentelor naţionale de intelligence, precum şi de participare la procesele strategice de adoptare a deciziilor aliate (la nivel NATO / UE) bazate pe intelligence – cu efort naţional, iar din această perspectivă, acţiunea şi efortul integrat aşează comunitatea de informaţii într-o nouă paradigmă, organizaţională şi funcţională, pe *baza unor priorităţi şi principii moderne, între care evidenţiem pe cele de integrare, colaborare, inovare*.

Valorile acestei noi construcţii ţin de de implicare, iniţiative, anticipare şi adaptare la provocări complexe, colaborare, iar una dintre caracteriticile sale primordiale este fiabilitatea[1].

[1] Karl Weick, cel care a introdus conceptul de *organizare de înaltă fiabilitate, scria în 1999: „Organizaţiile de înaltă fiabilitate se disting graţie propriilor eforturi de a organiza în moduri care sporesc calitatea de atenţie în întreaga organizaţie, sporind astfel vigilenta oamenilor şi conştientizarea la detalii, astfel încât acestea să poată detecta*

1.1. Consideraţii teoretice privind comunitatea de informaţii modernă

Comunitatea de informaţii (CIM) este specifică fiecărui stat suveran în funcţie de capacitatea şi de interesele acestuia, pe baza unor principii comune de organizare şi funcţionare, dar şi a unor caracteristici specifice, date de obiectivele pe care le urmăresc, de modalităţile de realizare a acestora, precum şi de caracterul imprimat procesului informaţional. Lipsa de echivalenţă a acestor comunităţi de informaţii este expresia raţionalităţii sociale cu care au fost îndrituite.

În accepţiunea noastră, actualmente, comunitatea de informaţii este o entitate cu responsabilităţi majore de coordonare, planificare şi gestiune a informaţiilor de securitate necesare apărării valorilor şi intereselor unei naţiuni, accentul căzând, în principal, pe evaluarea şi interpretarea analitică multisursă[2] a informaţiilor specifice acestui domeniu, precum şi pe transpunerea în practică a strategiilor generale şi operaţionale de securitate naţională.

Comunitatea de informaţii contribuie la acoperirea întregii problematici specifice domeniilor de realizare a securităţii naţionale, permite abordarea unitară a problemelor manageriale şi funcţionale ale structurilor de informaţii care o compun, implică evitarea paralelismelor şi suprapunerilor în managementul riscurilor, ameninţărilor şi vulnerabilităţilor care pot afecta valorile unei naţiuni.

Constituirea comunităţii de informaţii moderne vizează primordial îndeplinirea misiunii sale strategice[3]: *crearea avantajului decizional* prin integrarea capacităţilor informaţionale externe, interne şi militare, politici tehnologice şi de personal, priorităţi bugetare şi planuri de implementare.

Acest lucru evidenţiază o nouă paradigmă în ecuaţia îndeplinirii obiectivelor de securitate naţională şi furnizează o provocare pe linia generării unor procese de reformă a intelligence-ului la nivelul statelor democratice, serviciile de informaţii devenind constante sociale şi membre ale relaţiilor duale între acestea fără de care lumea modernă nu poate funcţiona în absenţa lor. *„... serviciile de informaţii trebuie să fie pe cât de eficiente, pe atât de flexibile şi inteligente în a putea analiza, anticipa şi prognoza în zone oricum obscure ale cunoaşterii"*[4].

Aşa cum am exprimat, rolul primordial al comunităţii de informaţii este de a furniza cunoaştere strategică, concept care în contextul evoluţiei informaţionale are tendinţa să-şi dilueze din consistenţă dar nu poate fi omis, tocmai datorită potenţialităţilor oferite de noile tehnologii pentru obiective punctuale, strategice.

Astăzi, decizia politică modernă nu mai este luată în absenţa informaţiei de securitate provenită de la comunitatea de informaţii, de aceea eşecurile sau erorile din intelligence pot fi dramatice. *„Un eşec în activitatea serviciilor de informaţii constă, în esenţă, în înţelegerea incorectă a unei situaţii, fapt ce determină un guvern (sau forţele sale militare) să întreprindă acţiuni inadecvate sau contraproductive din perspectiva intereselor sale"*[5].

Provocarea primordială a intelligence-ului este legată indisolubil de rolul comunităţilor de informaţii în procesele de definire a securităţii globale / regionale / naţionale, statele

---

moduri subtile, în contexte variate." (*Karl E. Weick and, Ted Putnam,* **Organizing for Mindfulness Eastern Wisdom and Western Knowledge** in Journal of Management Inquiry, Vol. 15 No. 3, , September 2006)

[2] Pentru intelligence, *conceptul de ansamblu al surselor în intelligence sau multisurse* se referă la toate produsele de intelligence şi procesele utilizate pentru producerea acestora. De asemenea, se referă la produsele de intelligence şi/sau organizaţiile pe care le încorporează în procesul informării, cel mai frecvent incluzând surse umane de intelligence-HUMINT, IMINT, MASINT, SIGINT şi OSINT în producerea şi elaborarea de produse de intelligence.

[3] *** - Viziunea 2015 a SUA - o organizaţie globală şi integrată de intelligence, trad., Bucureşti, 2008

[4] Maior, George-Cristian, *Serviciile de informaţii şi drepturile omului în era terorismului global* în Steve Tsang (coord.), *„Serviciile de informaţii şi drepturile omului în era terorismului global – Geopolitica Lumilor secolului XXI"*, Editura Univers Enciclopedic, Bucureşti, 2008, p. 10

[5] N. Abraham Shulski şi J. Gary Schmitt, *Războiul tăcut - Introducere în universul informaţiilor secrete,* Editura Polirom, Iaşi, 2008, p. 110

generând reconfigurări şi reconceptualizări profunde ale obiectivelor şi misiunilor instituţiilor de intelligence componente, precum şi redefiniri ale raporturilor de cooperare / colaborare la nivel aliat, partenerial sau a schimburilor de informaţii globale. Vizăm aici inclusiv aspectele interne ce ţin de stabilirea locului şi rolului serviciilor de informaţii în arhitecturile de intelligence naţionale, misiunile şi responsabilităţile acestora, strategiile şi obiectivele de reformă, respectiv de modernizare.

Pe aceste coordonate, considerăm că *obiectivul fundamental şi specificitatea funcţionării Comunităţii de Informaţii Moderne, integrată şi colaborativă, îl reprezintă nivelul şi relevanţa infodeciziei strategice*[6] *în* probleme ce ţin de activităţile politico-diplomatice, economice, ştiinţifice şi de altă natură care garantează independenţa şi suveranitatea naţională, integritatea teritorială, ordinea constituţională şi propriul sistem de valori, precum şi promovarea şi realizarea nestânjenită în cadrul comunităţii internaţionale a unor interese fundamentale, prin acţiuni conforme normelor de drept internaţional.

Prin prisma cercetării academice, putem afirma că definirea "*Comunităţii de informaţii – organizaţie de intelligence*" reprezintă unul dintre cei mai importanţi paşi în procesul de concretizare a eforturilor de reformare a întregului sistem al securităţii naţionale, un ansamblu funcţional sinergic şi o provocare privind asigurarea fluxurilor informaţionale de produse analitice necesare susţinerii infodeciziei strategice.

1.2. Comunitatea de Informaţii – organizaţie de intelligence integrată, colaborativă şi inovativă

Într-o viziune modernă, mediul de conflictualitate al societăţii viitorului cu influenţe asupra gândirii strategice va prezenta noi caracteristici[7], va fi guvernat de noi principii[8] şi va fi susţinut de un suport tehnologic diversificat.

Marea violenţă a secolului XXI, localizată la graniţa dintre starea convenţională de război şi starea convenţională de pace, generată preponderent de vulnerabilităţile şi ameninţările non-statale şi de noile tipuri de ameninţări specifice spaţiului cibernetic sau a utilizării înaltei tehnologii şi a tehnologiei informaţiei, va accentua un nou tip de confruntare, specifică societăţii cunoaşterii, asimetrică, de reţea, complexă şi dinamică într-un spaţiu multidimensional (politic, militar, economic, diplomatic, informaţional, cibernetic, psihologic, mediatic, cosmic, cultural, etc.), pe coordonatele asigurării controlului şi dominării spaţiului informaţional şi de comunicare publică, respectiv a controlului / gestionării activităţilor / acţiunilor pe aceste dimensiuni.

Tendinţele de reformă identificate pe timpul studiului şi aprofundării cadrului organizatoric şi funcţional al unor comunităţi de informaţii din spaţiul euro-atlantic şi nu numai, arată că intelligence-ul este considerat un element de putere naţională, iar în acest sens sunt acceptate şi menţionate noi competenţe în legislaţiile naţionale pentru noile riscuri atribuite pe agenda serviciilor de informaţii sau sunt generate organizări structurale adaptate acestora.

---

[6] Ca şi componentă a conducerii strategice, potrivit profesorului Onişor Constantin, constă în ansamblul de activităţi specifice atributelor conducerii derulate de componentele sistemului – previziune, planificare, organizare, comandă, coordonare şi control şi asigură pregătirea şi desfăşurarea acţiunilor de mare amploare prin care este îndeplinit scopul strategic (Onişor Constantin, Bălan Mihail, Prună Cristian, *Intelligence şi management strategic modern*, Ed. Academiei Oamnilor de Ştiinţă din România, Bucureşti, 2012, p.34)

[7] Cauzalitatea complexă, decalajele de dezvoltare tehnologică şi influenţa civilizaţiei hight-tech, permanenta ameninţare WMD, predominanţa strategiilor de alianţă şi de coaliţie, responsabilitatea internaţională; creşeterea rolului cooperării şi colaborării; implicarea unui nou tip de binom terorism-contraterorism; imprevizibilitatea; flexibilitatea

[8] Sunt avute în vedere, principiile higt-tech şi I.T., disproporţionalităţii, generării asimetrice, ripostei, surprinderii, rezonanţei, remanenţei şi dominoului.

Prin aceste provocări, comunitatea de informaţii se identifică în paradigma organizaţiei de intelligence care răspunde unei nevoi superioare de asigurare a securităţii naţionale / aliate, precum şi unor necesităţi legate de implementarea a patru obiective primordiale:

- nevoia de a acţiona în comun, pe fondul proceselor de integrare şi globalizare;
- lucru în echipe comune (la nivel inter-agenţii sau multinaţional) şi pe areale de cercetare cât mai mari, pentru aprofundarea şi înţelegerea mecanismelor şi fenomenelor de risc;
- nevoia de valorificare permanentă a informaţiilor de securitate prin schimburi de cunoaştere;
- prioritizarea şi selectivitatea activităţilor de securitate, prin generarea de proiecte comune, practici operaţionale şi bugetare adecvate.

Cu alte cuvinte, în plan operaţional, considerăm că o CIM este o construcţie activă, adaptabilă şi integrată, în măsură să asigure avantajul decizional şi realizarea următoarelor obiective de modernizare[9]:

- *dezvoltarea unor capacităţi integrate de intelligence* în măsură să asigure *infodecizia strategică* privind noile misiuni aflate în atenţia organizaţiei de intelligence (apărarea cibernetică, interdependenţa şi securitatea energetică, protecţia infrastructurilor critice, operaţiuni internaţionale de menţinere a păcii – care necesită sprijin de informaţii, proliferarea armelor de distrugere în masă, protejarea inovaţiilor ştiinţifice şi tehnologice, dezastrele financiare, competiţia economică, problemele legate de mediu, ameninţările transnaţionale şi a celor hibride[10], utilizarea nanotehnologiei, încălcarea drepturilor omului, participarea la gestionarea urmărilor dezastrelor, căutarea criminalilor de război etc.);

- *crearea unui model de acţiune în intelligence care să aibă în centrul atenţiei beneficiarul informaţiei de securitate naţională şi care să fie bazată pe unitatea de scop şi obiective între acesta şi organizaţia de intelligence*, prin construcţii de tip reţea având ca actori analiştii-beneficiarii-managerii şi care permit beneficiarilor să descopere, să acceseze şi să exploateze informaţiile de securitate, în manieră sigură şi ajustată nevoilor fiecăruia, fiind convinşi că produsele informaţionale reprezintă elemente de patrimoniu strategic prin care trebuie apărat şi promovat interesul naţional sau aliat;

- *dezvoltarea componentelor de „early-warning"* în măsură să anticipeze şi să prevină surprizele strategice sau să asigure oportunităţi pentru infodecizie privind prevenirea şi combaterea riscurilor şi ameninţărilor la adresa securităţii;

- *reconfigurarea arhitecturii comunităţii de intelligence prin integrarea capabilităţilor existente la nivelul entităţilor informative în reţele neuronale/ platforme colaborative* în măsură să asigure lucru facil, independent sau în cooperare, în timp aproape real, la disponibilităţile informaţionale ale actorilor implicaţi;

- *generarea unei doctrine operaţionale unitare în cadrul comunităţii***;**

- *dezvoltarea şi perfecţionarea cadrului de cooperare inter-agenţii,* în acord cu nevoile de securitate ale statului şi angajamentele asumate în plan internaţional;

- *înlăturarea barierelor organizaţionale ce limitează colaborarea internă şi externă* prin instituţionalizarea de practici comune în domeniul planificării strategice, analizei integrate,

---

[9] Reprezintă repere asumate şi reflectate la specificul naţional al căror izvor este Viziunea 2015 a Comunităţii de Informaţii a SUA.

[10] Hybrid threats – rezultat al activităţilor desfăşurate de adversari ce utilizează mijloacele convenţionale şi non-convenţionale pentru a-şi atinge obiectivele. Aceste ameninţări se materializează prin adâncirea instabilităţii în anumite regiuni şi se referă la acţiunile militare convenţionale, atacuri teroriste, criminalitate cibernetică, criminalitate economică. Apar pe fondul instabilităţii regionale (ce poate fi provocată de eşecul guvernării, lipsa resurselor, schimbările climatice, migraţia economică, dezastre, extremism) şi se pot extinde rapid, în contextul globalizării şi al facilităţilor moderne oferite de sistemele moderne de comunicaţii. (Potrivit General NATO Roy Hunstoie, www.colaborationjam.com, Seminar pe tema Ameninţărilor transnaţionale şi hibride – 19-23-03.2012)

managementului misiunilor, diseminării informaţiilor, politicilor de achiziţii, politicilor de management resurse umane şi de formare/training a personalului, securităţii organizaţionale, schimbului de informaţii, adoptării legislaţiei în intelligence şi a relaţionării cu beneficiarii informaţiilor de securitate;

- *generarea şi impunerea unei noi culturi organizaţionale* bazate pe încredere reciprocă, idealuri şi valori comune, mediu propice dezvoltării profesionale în condiţii de egalitate de şanse, transparenţă şi pregătire multilaterală, eficienţă şi eficacitate – în acord cu standardele de performanţă impuse de organizaţie.

În consecinţă**,** organizaţia de intelligence integrată[11] trebuie să fie construită pe o infrastructură robustă şi dinamică de informaţii, bazată pe o cultură a schimbului de informaţii şi susţinută de o serie de servicii şi facilităţi care să permită utilizatorului analitic final să transforme volumul mare de date în informaţii predictibile şi pe baza cărora să se poată acţiona. Comunitatea de informaţii se identifică ca organizaţie capabilă să răspundă ameninţărilor şi provocărilor societăţii cunoaşterii, are caracteriticile unui sistem deschis şi o deosebită capacitate de adaptabilitate la schimbările de mediu, o organizaţie robustă, puternică, cu niveluri ridicate de monitorizare şi control, cu activităţi direcţionate în acord cu următoarele principii de bază ale funcţionării sistemului:

- *sinergie* – prin integrarea elementelor separate ale sistemului şi asigurarea obţinerii de rezultate imposibil de atins dacă unităţile sunt autonome şi independente;
- *flexibilitate* – capacităţile organizaţionale sunt în limitele cadrului legal şi aplicarea de metode diferite care asigură îndeplinirea obiectivului principal: securitatea naţională ;
- *eficacitate* - obţinerea maximului de rezultate posibile cu resursele disponibile;
- *lucru integrat,* ca o echipă, într-un mediu operaţional care favorizează încrederea reciprocă, unitatea de efort şi acţiune, integrarea şi transparenţa, adaptabilitatea şi agilitatea mentală, precum şi apropierea de beneficiarii produselor informaţionale;
- *concentrarea capabilităţilor pe misiuni* pentru a atinge eficienţa la fiecare nivel (strategic, tactic, operaţional) incluzând centralizarea planificării cu descentralizarea implementării, restructurări adaptabile şi redirecţionarea resurselor pe priorităţi;
- *furnizare de expertiză, capabilităţi, precum şi prin consolidarea de parteneriate puternice* cu mediul academic, sectorul privat şi partenerii internaţionali;
- *aplicarea managementului performanţei* pentru a maximiza lucrul individual, în echipă sau performanţa organizaţională în scopul asigurării către beneficiari de servicii şi produse informaţionale relevante pentru nevoile acestora, responsabilizării personalului pentru acţiunile şi performanţa lor bazate pe rezultate măsurabile.

Aşa cum am prezentat, *obţinerea avantajului decizional reprezintă misiunea strategică a unei Comunităţi de Informaţii Moderne, iar adaptabilitatea, una din condiţiile de succes pentru funcţionarea optimă a acesteia*. Fiind supusă permanent unor evoluţii corespondente transformărilor din mediul de securitate, priorităţile de dezvoltare ale comunităţii de informaţii *"... sunt subsumate unor obiective strategice a căror realizare va asigura premisele adaptării la provocările şi oportunităţile erei informaţionale*[12]***":*** capacitatea operaţională în culegerea şi valorificarea informaţiilor; tehnologia ca avantaj competitiv în intelligence; noi perspective asupra serviciilor de securitate; investiţia în resursa umană; tehnologia ca facilitator al cooperării; cercetarea ştiinţifică şi dezvoltarea tehnologică; securitatea instituţională; comunicarea publică în era informaţională.

Aşadar, CIM se identifică şi se manifestă cu o formulă de acţiune în cadrul unor ansambluri funcţionale sinergice , în măsură să ofere valoare adăugată capacităţilor individuale şi un răspuns multiplicat şi eficient în procesele de răspuns la riscurile şi ameninţările de

---

[11] Ibidem

[12] *** - Viziunea 2011-2015 „*SRI în era informaţională*"

securitate. Astfel, *comunitatea de informaţii funcţionează pe principiile şi logica organizaţiei integrate de intelligence*.

2. Reforma comunităţii de informaţii – între necesitate şi oportunitate

În contextul actual marcat de evoluţii strategice complexe, obiectivul schimbării nu-l reprezintă justificarea acesteia ci mai degrabă "…*ce fel de schimbare trebuie să-şi asume un serviciu de informaţii, cum poate fi tratat acest proces tratat ca oportunitate, printr-o abordare pro-activă, în opoziţie cu una pasivă, reactivă*[13]".

În opinia specialiştilor din domeniu, modelarea şi edificarea unor arhitecturi de intelligence moderne nu ţine exclusiv de generarea unor restructurări de amploare ci de direcţionarea viitoare a transformării tuturor actorilor implicaţi în activitatea de intelligence, într-o nouă paradigmă, prin:

- asimilarea noilor tehnologii în activităţile operaţionale;
- identificarea mecanismelor de utilizare eficientă a resurselor informaţionale şi adoptarea culturii schimbului de informaţii;
- mai bună utilizare a fondurilor financiare pe proiecte de securitate comune şi priorităţi operaţionale;
- mai bună coordonare şi evaluare obiectivă a performanţelor, în context sistematizat şi standardizat.

Gradul de performanţă al sistemului integrat[14] va fi dependent de implementarea noilor tehnologii informaţionale şi de comunicaţii, precum şi de valorizarea practicilor operaţionale de lucru integrat, în reţea, în măsură să genereze plusvaloare şi vigilenţă operaţională în aport cu noile ameninţări şi provocări de securitate. Acest lucru se traduce prin concentrarea eforturilor în direcţiiile asigurării libertăţii asupra mijloacelor de informaţii, îmbunătăţirii vigilenţei informaţionale, reducerii timpului de culegere de informaţii pentru o analiză oportună, sporirea acurateţii culegerii de informaţii prin analiză, coordonare şi corelare, regândirii proceselor de evaluare a componentei culegerii de informaţii, definirii priorităţilor informaţionale, concentrării eforturilor operaţionale prin echipe inter / multi-agenţii, creşterii suportului şi calităţii componentei tehnologice în operaţiunile curente.

Transformarea intelligence trebuie gândită şi în domeniul cooperării între comunităţile de informaţii. Astăzi a devenit din ce în ce mai evident faptul că în definirea unor politici de securitate naţională sau regională, pentru gestionarea ameninţărilor vechi şi a noilor riscuri, „*... nici un servicu de informaţii nu poate fi eficient în absenţa unei cooperări strânse cu structuri naţionale similare sau cu partenerii externi*", sens în care, sunt necesare eforturi pentru[15]:

- creşterea interconectivităţii între serviciile de informaţii pentru identificarea zonelor de interferenţă şi vulnerabilităţilor existente la limita de demarcare a mai multor zone de cunoaştere în noile domenii aflate pe agenda acestora (infrastructuri critice de securitate, întreruperea furnizării de energie, pieţele financiare, schimbările climatice);
- construirea unei infrastructuri robuste de informaţii, bazată pe valorificarea noilor tehnologii informaţionale şi pe o cultură a schimbului de informaţii;

---

[13] Maior George Cristian, *Cuvânt înainte* în lucrarea *Ionel Niţu – Analiza de intelligence – o abordare din perspectiva teoriilor schimbării*, Editura RAO, 2012, pag. 13

[14] Onişor Constantin, *Intelligence performant - culegerea şi analiza de informaţii între adaptare şi adecvare*, articol, sesiunea de comunicări ştiinţifice cu participare internaţională organizată de Academia Naţională de Informaţii "Mihai Viteazul", 2011, existent în biblioteca digitală a instituţiei de învăţământ

[15] Abordare adaptată în urma evaluării problematicii potrivit articolului *Provocări privind definirea unui proiect naţional de intelligence* , în Revista Română de Studii de Intelligence nr. 8 / decembrie 2012, Ed. Academiei Naţionale de Informaţii „Mihai Viteazul", Bucureşti, p. 74

- trecerea accentului de la "*schimbul de informaţii*" la "*schimbul de cunoaştere*" prin: abordare strategică de schimb de cunoaştere şi management, operaţionalizarea de capacităţi de relaţionare robuste, servicii de colaborare permanente, soluţii integrate de e-learning, mijloace de vizualizare şi sisteme de management organizaţional;
- realizarea unor reţele secretizate virtuale între analiştii Comunităţii de Informaţii şi ai serviciilor de informaţii, cu acces la baze de date realizate pe probleme sau domenii.

Noile tehnologii produc mutaţii semnificative în zona misiunilor clasice ale serviciilor de informaţii, sens în care consolidarea şi dezvoltarea unei infrastructuri informatice comune, capabilă să susţină procesele de infodecizie, de cooperare în format intern şi conexiunea cu reţele partenere, precum şi interogarea rapidă şi eficientă a datelor necesare proceselor de analiză de informaţii reprezintă obiective asumate instituţional.

În opinia specialiştilor americani sunt importante două schimbări în mediu pentru a justifica nevoia de integrare[16] a CIM, precum şi crearea de oportunităţi puternice pentru realizarea integrării[17]:

- misiunile de astăzi sunt susţinute prin diviziune între actorii de informaţii de nivel strategic sau tactic (diplomatici, politici, economici, militari etc.), ci prin integrarea eforturilor lor. Componentele sistemului sunt strâns legate unele de altele;
- tehnologia informaţiei oferă oportunitatea unei mai strânse şi organice capabilităţi de intelligence, caracterizate prin unificarea valorilor, mai degrabă decât infrastructurilor individuale asociate în mod tradiţional cu fiecare disciplină de informaţii (tehnologia informaţiei permite managierea infrastructurilor disparate în mod uniform).

Pe acest fond, oficiali din cadrul IC a SUA au recunoscut necesitatea unei Comunităţi consolidate şi mai integrate. Integrarea inteligence-ului, poate conduce la noi şi colaborative procese capabile să asigure sprijinul decidenţilor / beneficiarilor, fiind posibilă datorită noii tehnologii. Impedimentele semnificative dau nu insurmontabile, pot fi abordate şi depăşite pentru a realiza această integrare.

Păstrarea unor standarde învechite în cultura CIM, iterează nevoia de dezvoltare culturală care trebuie să aibă loc, tocmai pentru a asigura succesul procesului de reformă. Noile generaţii de ofiţeri sunt deschise la tehnologiile inovatoare, fiind produsele unei societăţi informaţionale, dar la fel de mult sunt atrase de misterele activităţii de intelligence. Una din provocările revoluţionare a acestei culturi presupune trecerea uzualului „*ceea ce trebuie să ştie*" („*need to know*") la individuala „*resposabilitate de a oferi*" („*responsability to provide*"), în scopul de a colabora şi a-i ajuta mai mult pe cei care au nevoie de informaţii.

Abordarea dezvoltării culturale la nivelul IC presupune / vizează:

- iniţiative practice pe linia reformelor pentru a produce performanţa efectivă la nivelul comunităţii;
- resetarea relaţiilor dintre serviciile de informaţii, între aceştia şi decidenţii politici şi militari;
- diminuarea diferenţelor şi barierelor organizaţionale – culturi diferite, sisteme care nu au interoperabilitate, drepturile neclare de decizie şi regulile conflcituale de business etc.;
- consolidarea surselor de informare integrate, provocare care vine să limiteze o nouă diviziune între domeniile civil şi militar, intern şi extern.

[1616] Intelligence-ul integrat are ca arie de manifestare sfera conducerii strategice a statului şi înglobează elemente de decizie, de planificare şi acţionale.

[17] AFCEA International, *National Security and Horizontal Integration,* SUA , 2004

- Accesarea unui concept adaptat intelligence-ului modern în societatea cunoaşterii porneşte de la provocarea lansată de către Alianţa Nord-Atlantică legată de faptul că „*..împreună elementele sistemului pot realiza mai mult decât individual*", într-un context dominat de criza economică şi dorinţa NATO de a eficientiza operaţiunile.

Conceptul **„***Smart Defence***",** lansat cu ocazia Summit-ului NATO de la Chicago din mai 2012, reprezintă răspunsul Alianţei la provocarea de a utiliza cu maximă eficienţă resursele limitate, sens în care aşează ca principii de acţiune următoarele: *prioritizarea cheltuielilor; specializarea aliaţilor*; *cooperare între aliaţi.*

Credem că utilizarea unui astfel de concept trebuie să fie definit şi aplicat la nivelul arhitecturilor de intelligence naţionale, având în vedere unele realităţi de necontestat: structuri supradimenisionate, incoerenţa şi competiţia pentru investiţii, eforturi disipate, suprapuneri operaţionale şi generarea de structuri de suport cu mult peste necesar, competenţe care nu se înscriu pe agenda unui serviciu de informaţii modern, concepte lansate, greu înţelese şi neaplicate etc.

Pe fondul „războiului total împotriva terorismului", investiţiile în forţa specializată şi în crearea de capabilităţi informaţionale au crescut exponenţial, însă realităţile economice şi provocările globale de astăzi induc un nou mod de gândire şi acţiune la nivelul intelligence-ului, pe baza unor analize serioase privind cheltuielile asupra securităţii naţionale/aliate, cu păstrarea obiectivului de revine IC, precum şi determinarea de reduceri semnificative, fără a afecta eficienţa.

Capitalul uman trebuie văzut ca resursă strategică a CIM, iar activitatea pe această linie, ca un program investiţional în care deciziile luate se bazează pe eficacitatea strategiilor forţei de muncă şi a resurselor disponibile, precum şi pe dezvoltarea valorilor de performanţă, în special în zonele dezvoltate exponenţial în cadrul comunităţii.

O altă abordare vizează sistemul de performanţe al personalului. Pe fond, acest sistem poate permite îmbunătăţirea capacităţii CIM, inclusiv prin reducerea forţei de muncă şi reechilibrarea structurilor care au crescut excesiv pe o situaţie existentă la un moment dat. Aceste reduceri trebuie să stea în atenţia liderilor astfel încât la momentul oportun să poată oferi stimulente pentru păstrarea specialiştilor din domeniile cheie şi limitarea plecării acestora către zona privată. Nu trebuie omis faptul că orice reducere trebuie să fie realizată funcţie de priorităţile misiunilor ce revin CIM.

Având în vedere creşterea anuală a costurilor cu personalul din anul 1990 este din ce în ce mai probabil că, pe fondul crizei actuale, bugetele Comunităţii să se aplatizeze sau chiar să scadă. Acest lucru impune maximizarea forţei de muncă alocate pe priorităţi de misiuni, menţinerea nivelului adecvat de susţinere, păstrarea expertizei tehnice, provocările putând apare în zona efectivelor de personal, procesele de achiziţie, recrutarea, cercetarea şi dezvoltarea domeniului, dimensiunile structurilor de intelligence.

CIM trebuie să se adapteze noilor realităţi fiscale, sens în care este necesară o strategie cu un plan final prederminat şi un plan pentru genera reduceri de personal, cu păstrarea obiectivelor propuse şi fără a aduce atingere capabilităţilor de bază ale organizaţiei. O provocare este pe relaţia ofiţeri cu experienţă-tineri, aceşta din urmă deşi dezvoltă capacităţi adaptate realităţii informaţionale, le lipseşte experienţa ceea ce poate fi un risc în detrimentul misiunii.

În cele din urmă, IC trebuie să continue să dezvolte eficienţa forţei de muncă prin utilizarea mai bună şi exploatarea pe deplin integratelor capacităţi de OSINT (inclusiv prin recrutarea direcţionată spre aceste sectoare insuficient exploatate), a întăririi parteneriatelor cu sectoarele private care pot furniza eficienţă (zonele de nanotehnologie, software, hardware, tehnologie înaltă etc.) şi dezvoltarea schimbului de informaţii cu partenerii străini.

Putem afirma că, reducerile bugetare preconizate la nivelul CIM vor induce un nou tip de „intelligenţă" care va putea fi privită la o posibilitate de regândire / resetare a CIM, iar

leadership-ul are instrumentul de a redefini, realinia şi reorienta misiunile serviciilor de informaţii.

Concluzii

Actualele arhitecturi de intelligence sunt rezultatul unei realităţi geopolitice ce se încadrează între abordările tradiţionaliste legate de o anumită perioadă istorică şi tendinţele de reconfigurarere a relaţiilor de putere la nivel global. Comunitatea de informaţii a secolului XXI răspunde unor provocări şi niveluri ale riscurilor de securitate de o complexitate deosebită, interconectării acestora, pe o logică operaţională ce implică eficienţa activităţilor, parteneriate puternice cu societatea civilă şi centrele de cercetare/academice, cooperare/colaborare prin schimb de informaţii şi cunoaştere la nivel naţional şi internaţional.

Pe fondul provocărilor de reformă / transformare a intelligence-ului, considerăm oportune a fi evaluate şi aprofundate câteva direcţii de cercetare, între care amintim:

- studiul conceptului lansat în zona de cercetare legat de abordarea „comprehensivă bazată pe reţea[18]" (multinodality) a securităţii şi implicaţiile sale asupra CIM;
- crearea unui model de intelligence naţional în cadrul unui proiect care înglobează serviciile de informaţii intern, extern şi militar, alături de structuri de protecţie şi departamente de analiză create în domenii special indentificate de risc precum zona financiar-economică, vamală etc., cu definirea misiunilor şi responsabilităţilor acestora pentru acţiuni eficiente şi integrate;
- definirea mecanismelor instituţionale de coordonare strategică care să asigure nivelul de acceptabilitate optim pentru adoptarea infodeciziei în problemele urgente aflate pe agenda serviciilor de informaţii
- fundamentarea unor proceduri de evaluare a performanţelor la nivel individual, al serviciilor de informaţii şi al întregii comunităţi;
- dezvoltarea unui mecanism de „lecţii învăţate" care să dinamizeze componentele acţionale în procesele de manageriere a riscurilor, să ajute la identificarea oportunităţilor de dezvoltare organizaţională şi să furnizeze formule de validare a performanţei individuale şi colective sau pentru monitorizarea progresului.
- explorarea şi dezvoltarea conceptului că „oamenii sunt cea mai bună resursă pe care o pot avea organizaţiile de intelligence";
- definirea unor mecanisme de monitorizare şi control al proceselor organizaţionale care să asigure date privind modificarea parametrilor cheie ai CIM;
- inovare direcţionată spre creşterea capacităţilor tehnice şi tehnologice (cu efecte în formule colaborative, standarde şi procese, mediu comun pentru operaţiuni, integrarea practicilor de securitate, îmbunătăţirea integrării şi schimbului de informaţii, noi tehnologii şi procese moderne de achiziţii etc.);

Relevant pentru CIM este faptul că procesele de reformă au determinat o reînnoire a gândirii strategice, paradigma incluzând o nouă diviziune între domeniile militar şi civil, intern şi extern, precum şi o mai mare integrare a open-source.

Concluzia finală este că, pe actualul registru al riscurilor şi ameninţărilor, CIM se structurează şi funcţionează ca o organizaţie inteligentă de intelligence[19].

---

[18] Conceptul a fost lansat de Felix Artega, Senior Analyst la Real Instituto Elcano de Estudios Internacionales y Estrategios/Spania. În actualul context, principii noi precum pragmatismul, flexibilitatea şi eficienţa, trebuie să înlocuiască formalismul, normativismul şi legitimitatea, iar problemele de securitate nu mai sunt încastrate în seturi limitate de poli naţionali sai interguvernamentali, putând fi mai bine gestionate prin inermediul unor reţele de actori (noduri) ce lucrează pe nivele diferite (moduri);

[19] Potrivit Maior George Cristian în articolul „*Managing Change: The Romanian Intelligence Service în the 21 Century*", publicat în *International Journal of Intelligence and Counterintelligence din 29.03.2012*, conceptul

BIBLIOGRAFIE:

1. ***, - *Viziunea 2011 -2015, SRI în era informaţională*, Bucureşti;
2. Han Laurenţiu, *Intelligence şi management informaţional: provocări globale, informaţionale şi private*, Editura Academiei Naţionale de Informaţii ”Mihai Viteazul”, Bucureşti, 2011
3. Maior, George-Cristian (coord.) - *Un război al minţii, Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI*, Ed. RAO, Bucurepti, 2010;
4. Maior, George-Cristian, *Serviciile de informaţii şi drepturile omului în era terorismului global* în Steve Tsang (coord.), „*Serviciile de informaţii şi drepturile omului în era terorismului global – Geopolitica Lumilor secolului XXI*”, Editura Univers Enciclopedic, Bucureşti, 2008
5. *Viziunea 2015* a Comunităţii de Informaţii a SUA, Bucureşti, 2008.

Această lucrare este elaborată şi publicată sub auspiciile Institutului de Cercetare a Calităţii Vieţii, Academia Română ca parte din proiectul co-finanţat de Uniunea Europeană prin Programului Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013 în cadrul proiectului Pluri şi interdisciplinaritate în programe doctorale şi postdoctorale Cod ProiectPOSDRU/159/1.5/S/141086.

„*Smarter Intelligence*” vizează următoarele schimbări: reconceptualizarea misiunilor şi traducerea lor în eficienţă operaţională; consolidarea componentei analitice; accentuarea pregătirii unei resurse umane profesioniste şi competente; configurarea fluxurilor interne pe baze colaborative; maximizarea performanţei prin dezvoltare şi inovare tehnologică; intensificarea cooperării inter-agenţii şi cu partenerii externi; aprofundarea relaţiei cu beneficiarii legali; conectarea cu zona cercetării şi dezbaterilor din comunitatea academică şi societatea civilă.

SINERGIA SISTEMELOR INFORMAŢIONALE ÎN SOCIETATEA CUNOAŞTERII. IMPLICAŢII PENTRU ORGANIZAŢIA DE INTELLIGENCE

Petrişor BĂDICĂ
Doctorand în domeniul "Informaţii şi Securitate Naţională", Academia Naţională de Informaţii "MIHAI VITEAZUL", Bucureşti, e-mail petrisor_35@yahoo.com

Rezumat: Aprofundarea cunoaşterii şi abordării inteligente a fenomenelor de risc şi ameninţare specifice societăţii actuale şi viitoare este facilitată de adoptarea noilor tehnologii ca factori facilitatori de putere, precum şi de proiectarea unei arhitecturi moderne de intelligence în parametrii artei strategice şi al valorificăriii sinegiei organizaţionale şi funcţionale specifice organizaţiei bazate pe cunoaştere.

Înţelegerea şi redefinirea „sinergiei funcţionale şi acţionale" a Comunităţii de Informaţii Moderne, realizată prin studiul sistemelor informaţionale în general, precum şi al raţionalităţii şi gândirii proceselor de reformă, trebuie privită ca principiu al sistemelor informaţionale moderne menită să aducă valoare adăugată acţiunilor / operaţiunilor curente şi de perspectivă, în condiţii de eficienţă / eficacitate, o alocare şi utilizare adecvată a resurselor necesare îndeplinirii acestora, precum şi un grad de satisfacţie ridicat al beneficiarilor produselor informaţionale în raport cu aşteptările acestora. Sinergia capabilităţilor de culegere şi de analiză multidisciplinare a mediului de ameninţare este astfel în măsură să genereze viziune strategică şi fundamentele necesare adoptării infodeciziei de securitate, inclusiv în ceea ce priveşte promovarea şi susţinerea intereselor naţionale/aliate.

Cuvinte cheie*: the intelligence community, decision-making, strategical awareness, informational revolution, capabilities, integrated system; sharing*.

Introducere

Motto-ul prezentei abordări ştiinţifice aparţine lui Albert Eistein şi se prezintă astfel: „*Problemele mari cu care ne confruntăm nu pot fi rezolvate cu acelaşi nivel de gândire care le-a creat*."

Abordarea pragmatică a titlului propus se bazează pe asumarea caracteristicilor rafinate ale conceptului de sinergie[1] aşa cum rezultă din multitudinea de definiţii elaborate, pe reflectarea acestora în tipul de societate actuală şi previzionabilă, viitoare, precum şi pe interferenţa asupra sistemelor informaţionale specifice acestui tip de societate.

Schimbarea radicală şi într-un ritm alarmant a mediului de ameninţare reprezintă o realitate a secolului XXI, determinând deopotrivă reevaluarea modului corporativ – economic, a vieţii sociale şi a abordărilor politice, într-o paradigmă fluidă în care posibilele distrugeri pot fi provocate de arme aparţinând acestei lumi (arme financiare, cyber – în toate formele sale, concurenţa pentru resursele naturale, maladii, etc.) şi care pot fi invizibile, latente sau progresive. Vechile „dileme" ale cunoaşterii îşi schimbă semnificaţia, evoluţiile tehnologice, dinamica socială şi transformarea intelligence-ului reflectă nevoia de schimbare a proceselor, tehnicilor şi a abilităţilor analitice.

---

[1] Sinergia poate fi descrisă prin aforismul „unu plus unu este egal cu trei" şi se explicitează adesea în termeni de „energie multiplicată" şi „eficienţă". Etimologia cuvântului provine din limba greacă, fiind format din cuvântul „sin" – tradus prin „cu" sau „împreună cu" şi din cuvântul „ergon" – tradus prin „muncă" sau „a munci". În traducere literară, sinergia reprezintă „munca împreună" şi defineşte efectul sporit ce se poate obţine prin acţiunea simultană a mai multor elemente pentru un scop comun.

Ameninţările secolului XXI sunt interconectate, interdependente, virale, facilitate şi ale căror efecte sunt amplificate exponenţial de noile tehnologii, conştienţi fiind că uneori manifestarea acestora depăşeşte capacitatea noastră de a înţelege implicaţiile pe care acestea le au în planul securităţii şi de a genera strategiile de răspuns. Globalizarea şi revoluţia informaţională au schimbat centrul de interes analitic al comunităţilor de informaţii[2]. Fondul imprevizibil este susţinut şi de diversificarea tipologiei ameninţărilor de securitate şi extinderea arealului de manifestare a acestora.

Evoluţiile curente şi procesele viitoare de (re)aşezare a construcţiilor moderne de intelligence pornesc de la realitatea operaţională care identifică noi potenţialităţi de risc şi ameninţare, pe fondul discordanţei sistemelor actuale (politice, economice, sociale, militare etc.), ale noilor valenţe ale securităţii (naţionale, regionale, globale) generate de caracteristicile spectrului confruntării informaţionale moderne, precum şi ale provocărilor de securitate care depăşesc preocupările clasice ale serviciilor de informaţii. Pe fond, societatea umană se manifestă ca o entitate integrată, pare ca un singur sistem ce cuprinde întreg mapamondul şi în care nu mai există posibilitatea şi capacitatea unor mişcări singulare, fiind împinsă de o nouă lege, a interdependenţei, a unei conexiuni ce face parte dintr-un sistem integrat. Într-o lume interdependentă, naţiunea nu poate fi izolată şi trebuie să concure la securitatea internaţională doar în măsura în care acţiunile sale sunt recunoscute ca legitime[3].

În aceste condiţii, **„***sinergia funcţională şi acţională***”** trebuie privită ca principiu al sistemelor informaţionale moderne menită să aducă valoare adăugată acţiunilor sistemului / operaţiunilor de intelligence, în condiţii de performanţă, susţinute informaţional, tehnic - operaţional şi coordonate eficient prin organisme naţionale / aliate multidisciplinare, care să genereze fundamentarea oportună a info-deciziei naţionale de securitate şi câştigarea confruntării informaţionale.

Pe acest fond, aplicarea principiului sinergiei determină structuralitatea şi funcţionalitatea instituţiei de intelligence – centrată pe reţea, la nivel naţional, dar şi crearea mecanismelor necesare adoptării strategiilor de răspuns la riscurile emergente, atipice şi transnaţionale, în format bi- sau multilateral, în principal, cu partenerii din NATO şi UE sau la nivelul reprezentării în cluburile selecte de intelligence.

1. Sinergia sistemelor informaţionale în societatea cunoaşterii. abordare multidisciplinară

Adoptarea şi implementarea sistemelor informaţionale moderne, într-un mediu volatil şi interconectat de evoluţii integrate (economice, sociale, politice etc.) şi de ameninţare, emergent şi imprevizibil, ne conduce la a atribui societăţii cunoaşterii noi valenţe, aplicabile şi utile fundamental domeniului intelligence, ce pot fi definite şi înţelese din prisma sinergiei dintre procesele de cunoaştere şi cele de stimulare a creativităţii, cercetării şi inovării. În acest scop, capitalul intelectual cu valenţele sale inovative, relaţionale, motivaţionale, precum şi asigurarea unui cadru comun de cunoaştere care contribuie la valorificarea potenţialului tuturor actorilor implicaţi în ecuaţia asigurării securităţii naţionale / internaţionale reprezintă – din perspectiva intelligence-ului modern, nucleul societăţii cunoaşterii. De cunoaştere depinde infodecizia, iar acest lucru concură la implementarea politicilor aferente securităţii, bunăstării şi viitorului naţiunii. Găsirea unor răspunsuri la perspectiva adaptării instituţiei de

---

[2] W.J.Lahneman, *The Need for a New Intelligence Paradigm*, în International Journal of Intelligence and Counterintelligence, vol.23, 2010, p.212

[3] *** Carta Albă a Apărării şi Securităţii Naţionale a Franţei, 2013, accesată pe adresa de Internet http://fr.calameo.com/read/000331627d6f04ea4fe0e în data de 01.03.2015

intelligence moderne la cerinţele mediul de confuntare informaţională ne conduce indisolubil la abordarea a trei ipoteze fundamentale:

- vizualizarea locului şi rolului instituţiei din perspectiva parametrilor artei strategice adaptată nevoilor societăţii informaţionale şi a cunoaşterii şi integrată în politica comunităţii sociale pe care o apără şi promovează;
- reforma organizaţiei actuale în context şi condiţii de asigurare a performanţei organizaţionale, identificată ca un întreg – organizaţional şi operaţional şi nu ca o sumă de instituţii disparate – lucru ce implică implementarea principiului sinergiei, inclusiv generarea unei noi culturi organizaţionale;
- conexarea instituţiei de intelligence într-un angrenaj naţional modern, denumit „sistem naţional de management integrat al crizelor" şi a unei „comunităţi naţionale de securitate" cu locuri şi roluri bine definite pentru instituţiile naţionale cu responsabilităţi, capabilă să fundamenteze deciziile naţionale în materia securităţii naţionale şi să contribuie la aplicarea măsurilor NATO / UE de răspuns la crize, potrivit angajamentelor asumate.

1.1. Principiul sinergiei în sistemele informaţionale

Conceptul de sistem este în conexiune cu conceptul de sinergie – privit ca rezultat al combinării subsistemelor şi a resurselor sistemului şi în care sunt identificate comportări ale întregului care depăşesc "suma" posibilităţilor părţilor luate separat. Orice sistem dinamic şi oricât de complex funcţionează şi se dezvoltă numai datorită unei tensiuni dinamizatoare din interior, întreţinută de confruntarea, combinarea şi cooperarea elementelor componente.

Sinergia unui sistem, care se formează şi se dezvoltă prin mişcare şi organizare, fiind totodată o rezultantă a interacţiunilor reciproce între strategia şi cultura organizaţiei. *Sinergia presupune nu numai cooperarea şi / sau competiţia subsistemelor, ci şi:*

- *supradeterminarea sistemului faţă de subsisteme*, adică aservirea subsistemelor de către sistemul ierarhic adiacent;
- *generarea ordinii din dezordine* („haos determinat" - H.Haken), adică apariţia unei ordini etalate (manifeste) din ordinea implicată (ascunsă).

Pe aceste considerente, implementarea *conceptului 2.0*.[4] influenţează modul de evoluţie a societăţilor şi organizaţiilor de reţea, dinamice, adaptabile şi flexibile, generând o nouă arhitectură socială şi o nouă filosofie de diseminare a cunoştinţelor prin colaborare în scopul asigurării cunoaşterii colective.

Acest demers aduce în prim plan rolul sinergiilor în sistemele informaţionale bazate pe cunoaştere[5], având ca fundament faptul că „*... societatea informaţională este definită ca o societate a cunoaşterii şi, în acelaşi timp, ca o societate a organizaţiilor*" (Drucker, 1992) şi că în funcţionarea acestora, determinante sunt procesele desemnate generic prin sintagma

---

[4] Conceptul 2.0 este legat indisolubil de evoluţia emancipării domeniului Web şi a utilizări aplicaţiilor acestuia în toate zonele activităţii sociale: management, inovaţii, educaţie, relaţii internaţionale, planificare strategică, politică etc.

[5] *Conceptul de organizaţie bazată pe cunoaştere* s-a cristalizat în anii 1984-1988, Huber (1984) sesizând necesitatea unui model organizaţional propriu noului tip de societate ce îi succede celei industriale. Ideea de organizaţie bazată pe cunoaştere se regăseşte în cadrul a două abordări care îi explică determinismul, fie pornind de la factorii tehnologici, fie de la factorii organizaţionali. Promotorii tehnologiei informatice (Holsapple şi Whinston - 1987) definesc organizaţia bazată pe cunoaştere drept o „colectivitate de lucrători cu muncă de concepţie, interconectaţi printr-o infrastructură computerizată". Abordarea managerială (Drucker-1988), tratează organizaţia bazată pe informaţii ca reprezentând modelul organizaţional al secolului XXI şi îi preconizează principalele caracteritici: componenţa dominată de profesionişti, numărul redus al nivelurilor intermediare de conducere ierarhică, asigurarea coordonării prin mijloace de factură non-autoritară (standarde, norme, reguli de cooperare etc.).

celor „3I", respectiv *inovare* (creare de cunoştinţe noi), *învăţare* (asimilare de cunoştinţe noi) şi *interactivitate partenerială referitoare la cunoaştere*[6].

În acest context, edificarea conceptului de sinergie în sistemele informaţionale / intelligence şi nevoia de acţiuni sinergice în mediul volatil şi interconectat al secolului XXI, uzitează ipoteza că organizaţiile inteligente / bazate pe cunoaştere sunt actori colectivi inteligenţi ai societăţii actuale şi au un rol determinant în afirmarea acesteia ca societate a cunoaşterii din următoarele perspective:

- aparţin realităţii contemporane în calitate de mediu de activitate profesională şi managerială, obiect de cercetare ştiinţifică şi proiect strategic;
- marchează convergenţa între două fenomene definitorii pentru natura umană (cel al cunoaşterii şi cel al organizării), într-o construcţie socială emblematică pentru ideile de competenţă colectivă, acţiune inteligentă şi performanţă durabilă.

Evoluţiile tehnologice actuale şi dinamica socială, raportate la valenţele unei lumi globalizate şi interdependente, impun noi atribute şi responsabilităţi intelligence-ului guvernamental, conştienţi fiind că procesele, tehnicile şi abilităţile uzitate trebuiesc redefinite, iar noi concepte operaţionale trebuiesc împrumutate şi validate din mediul privat sau cel de cercetare / academic. Deopotrivă, unitatea de scopuri şi acţiune pentru gestionarea problemelor securităţii secolului XXI nu se poate realiza fără acţiunea unificată a tuturor actorilor care pot furniza cunoaştere, inclusiv prin exploatarea unor teorii / ideii încă nevalide, dar importante prin ipotezele lansate pentru procesele de cunoaştere (de ex. conceptul „knowmads[7]").

Sub impuls tehnologic, integrarea masivă a tehnologiilor înalte într-un spaţiu de confruntare integrat va domina perspectiva realizării unor obiective sistemice implicite, în care principalele provocări le reprezintă gradul de interoperabilitate în tehnologia informaţiei şi gradul de digitalizare a conducerii, lucru greu de atins într-un format partenerial în care cooperarea devine fundamentală pentru atingerea obiectivelor comune.

Plecând astfel de la identificarea rolurilor, misiunilor şi fluxurilor informaţionale în sectoarele organizaţiei, *abordarea sistemică a acesteia constituie punctul de plecare în identificarea şi definirea sinergiilor*. Actele de cooperare intra- şi interorganizaţională creează un mediu informaţional activ, caracterizat de parametri de intensitate şi integralitate dinamici, în care constatăm complexitatea efectelor sinergetice şi sinergia proceselor, rezultat al unui principiu derivat „*competitivitate prin cooperare*".

În activitatea practică a organizaţiei moderne se constată apariţia mai frecventă a sinergiilor pozitive în următoarele şase cazuri – fără a exclude şi alte posibilităţi[8]:

- coordonarea strategiilor componentelor organizaţiei;
- integrarea tuturor capacităţilor şi capabilităţilor prin coordonarea fluxurilor informaţionale, tehnice, logistice etc.;
- crearea de noi oportunităţi prin combinarea potenţialului existent;
- adiţionarea forţei de negociere;
- exploatarea în comun a resurselor tangibile;
- valorificarea în comun a know-how-ului.

Potrivit studiilor de specialitate, în dezvoltarea de sinergii organizaţionale şi funcţionale, vor fi abordate trei comportamente de sprijin progresiv:

---

[6] H.Dragomirescu, *Organizaţii bazate pe cunoaştere*, Studiu tematic elaborat în cadrul proiectului prioritar „*Societatea informaţională-societatea cunoaşterii*" al Academiei Române, Bucureşti, 2001

[7] **"***Conceptul „knowmads***"** – identifică acei lucrători de cunoaştere nomazi (extensie a conceptului „*knowledge workers*" lansat de Peter Drucker în anul 1992 în vol. „*Managing For The Future*"), respectiv indivizi creativi, inventivi şi inovativi care pot lucra cu oricine, oricând şi oriunde.

[8] Radu Popescu**,** *Sinergetica în sprijinul atingerii excelenţei firmelor industriale***,** în Revista Economia nr. 1/2004, p. 25-27

- *redundanţă* – „*mai multe organizaţii exercită activităţi similare având în vedere îndeplinirea aceloraşi obiective*" – care conduce la:
- *standardizare* – „*mai multe organizaţii exercită aceleaşi activităţi pentru a atinge aceleaşi obiective*" – conduce la:
- *sinergie – „o organizaţie, exercită o activitate specifică mai multor organizaţii similare şi realizează mai mult decât ar fi putut realiza toate aceste organizaţii dacă ar fi exercitat aceeaşi activitate".*

În fundamentarea răspunsurilor aşteptate, iterăm oportunitatea de valorificare a conceptului de „*reengineering*[9]" în practica şi cultura organizaţională a organizaţiei inteligente. Regândirea activităţii organizaţiei, inclusiv a celei cu responsabilităţi în asigurarea informaţiei de securitate, vine pe fondul acţiunilor conjugate a influenţelor unor *factori obiectivi ai societăţii actuale asupra întregului proces de cunoaştere* (globalizare, competiţie de nivel înalt, informaţia – resursă cheie, spaţiul virtual şi chiar derularea activităţilor în condiţii virtuale, comerţ electronic, existenţa personalului specializat în procesarea datelor şi analiză – knowledge worker, etc.), iar soluţiile necesare pot fi generate / găsite şi susţinute în noile soluţii IT&C.

1.2. Sinergii inter-sectoriale – fundamente ale performanţei sistemelor de informaţii

Sinergiile inter-sectoriale şi ideea interdependenţelor[10] în sistemele de informaţii reprezintă o transformare cuantică de mentalitate în care autoritatea de conducere, reprezentând nivelul vertical, se întrepătrunde cu acţiunile comune derulate cu partenerii implicaţi în realizarea scopurilor stabilite, proces în care un rol fundamental revine factorului uman..

Asigurarea integrării conducerii cu sinergiile domeniilor operaţionale sunt în măsură să genereze strategiile de răspuns în acord cu rapiditatea manifestării stărilor de insecuritate, iar acest lucru poate fi tradus astfel:

- *managementul activităţii / misiunii* - valorifică întregul potenţial la dispoziţie (informaţional, uman, tehnic etc) şi asigură stabilirea clară a misiunilor;
- *sinergia inter-sectorială* - valorifică capabilităţile proprii cu cele ale partenerilor / aliaţilor în scopul creşterii eficienţei generale.

Aşadar, din perspectiva sistemului integrat de informaţii sunt de valorificat 3 perspective majore:

- *consolidarea încrederii între entităţile comunităţii* – pe fondul derulării din ce în ce mai accentuat a unor proiecte comune şi a nevoii de acţiune unificată . Sunt de aşteptat rezultate în ceea ce priveşte autonomia organizaţională, sinergia operaţională şi eficacitatea activităţilor / operaţiunilor;
- *dezvoltarea abilităţii de acţiune a personalului*, tradusă prin iniţiative operaţionale racordate la tipul şi nivelul ameninţării;
- *întărirea rolului managementului şi stabilirea autorităţii activităţilor / misiunilor* – pe fondul necesităţii utilizării eficiente a capabilităţilor la dispoziţie, efortului de stabilire a autorităţii care să genereze sinergiile operaţionale aferente, modul de alocare a resurselor pe priorităţi şi să sincronizeze acţiunile, în acord cu tipul, nivelul

---

[9] *Conceptul de reengineering* desemnează regândirea fundamentală şi reproiectarea radicală a proceselor specifice activităţii organizaţiei pentru obţinerea de îmbunătăţiri substanţiale privind costurile, calitatea, viteza de reacţie a decidenţilor (Mihail Hammer)

[10] Interdependenţa aparţine de facto mediului inter-organizaţional şi presupune încredere în partenerii de misiune. În acelaşi timp, este necesară cunoaşterea riscurilor potenţiale determinate de accesul limitat la capacităţi şi de dezvoltare a eforturilor de limitare a riscurilor aflate în proximitatea sistemului.

şi rapiditatea propagării ameninţării. Cu alte cuvinte, agilitatea sinergiei de conducere / comandă[11].

Provocările unui astfel de demers în previzionarea sistemelor de informaţii ţin de:

- înţelegerea unei diversităţi de abordări existente la nivelul organizaţiilor performante, a celor ce ţin de autorităţi şi politici;
- elaborarea de orientări clare şi de intenţie, inclusiv în ceea ce priveşte evoluţia mediului de securitate;
- dinamica mediului informaţional şi a efectelor acestuia asupra activităţilor / operaţiunilor de intelligence, a deciziilor adoptate, precum şi vizibilitatea în timp real a acestora în media internaţională;
- numărul, diversitatea şi înţelegerea capabilităţilor organizaţiilor şi a partenerilor participanţi în proiectele comune de securitate;
- complexitatea şi posibilităţile informaţionale în context transfrontalier pentru proiectarea şi ducerea operaţiunilor de intelligence, de regulă în format aliat.

În context, conlucrarea şi combinarea capacităţilor interorganizaţionale specializate poate conduce la obţinerea unor efecte dincolo de domeniile de care aparţin cu relevanţă prin sporirea eficacităţii acestora şi compensarea vulnerabilităţilor în alte zone organizaţionale. Important este ca rezultatele sinergiilor rezultate să amplifice rezultatele misiunilor executate în parametri de performanţă operaţională.

Provocările privind atingerea sinergiilor intersectoriale sunt:

- *recunoaşterea realităţii şi a necesităţii interdependenţelor* – nimeni nu va avea asigurat luxul alocării resurselor necesare îndeplinirii obiectivelor / misiunilor, lucru care evidenţiază importanţa interdependenţelor / parteneriatelor, a „lecţiilor învăţate" din operaţiuni, ideea de acţiune unificată şi capacitatea de a atinge obiectivul strategic;
- *câştigarea sinergiilor şi armonizărilor* - cu alte organizaţii naţionale / aliate sau cu alţi parteneri internaţionali, bazate pe relaţii de încredere şi decizii adaptate pentru rezolvarea împreună a unor sarcini critice, tocmai pe fondul nevoii de reacţie unitară asupra unor riscuri interdependente. Deşi, în acest domeniu, este nevoie de a transforma un deziderat în realitate, totuşi sunt eforturi conştiente pentru a asigura un grad ridicat de înţelegere, de coeziune, pentru a atenua problemele şi riscurile plecând de la relaţiile personale, utilizarea elementelor de legătură şi decizii conştiente privind gradul de dependenţă al partenerilor pentru responsabilităţile critice.

Provocările generate de noul mediu operaţional se reflectă în nevoia realizării unor noi sinergii inter-sectoriale prin[12] :

- *cunoaşterea mediului operaţional şi nevoia de interdependenţe;*
- *obţinerea sinergiei şi încrederii*, în special cu alte sisteme şi entităţi multinaţionale;
- *înţelegerea limitelor de autoritate, a competenţelor şi capacităţilor celorlalte sisteme participante* (pe zona operativă, cyber, spaţială, contrateroristă, etc.);
- *valorizarea practicii conducerii integrate şi coordonării acţiunilor diverselor sisteme*;
- *interoperabilitatea reţelelor şi sistemelor de conducere*;
- *concentrarea asupra unităţii de efort*.

---

[11] Vizează conducerea misiunilor integrate, în relaţionare cu partenerii / aliaţii, ca bază pentru eficienţa sinergiilor între domeniile operaţionale şi a obţinerii unui avantaj decisiv.

[12] Gary Luck (Gl.ret.) and the JS J7 Deployable Training Division (Martie 2013), *Mission Command and Cross -Domain Synergy*, accesibil pe Joint Staff J7 Joint Training Intelink (CAC enabled):https:// intelshare.intelink.gov/ sites/jcw/jt/default.aspx

2. Implementarea principiului sinergiei în practica comunităţii de intelligence

Evoluţiile în teoria şi practica organizaţională specifice mediului secolului XXI dominat de implementarea tehnologiilor informaţionale şi de comunicaţii în activităţile curente, conduce la orientarea preocupărilor noastre de cercetare către modelul „organizaţiei inteligente", flexibilă şi competitivă, precum şi la identificarea factorilor facilitatori de schimbare, într-un context de corelare optimă a proiecţiilor structurale ale acesteia - facilitatoare de comportament inteligent, cu nivelul tehnologic necesar asigurării avantajului competitiv.

Organizaţia actuală este deplin angajată să implementeze noile tehnologii informaţionale şi să valorizeze puterea informaţiei generate de acţiunile tip reţea – ca bază de organizare şi funcţionare modernă, corespunzător unor viziuni strategice multianuale care să asigure perspective de dezvoltare şi competitivitate într-un mediu concurenţial dinamic şi a unor noi directive / principii care să eficientizeze lucrul în reţea: consolidarea reţelei; conştientizarea şi îmbunătăţirea colaborării – cu efecte privind calitatea informaţiei diseminate; auto-sincronizare. Acest lucru se răsfrânge într-o emancipare a politicilor privind accesul la informaţii pe toate nivelurile, precum şi printr-o redefinire a relaţiilor interne sau externe organizaţiei.

O primă ipoteză: în societatea viitorului, *organizaţia inteligentă* se redefineşte conceptual având ca fundamente schimbarea, sinergia şi leadership-ul, un nou mod de gândire şi performanţa prin inovaţie, precum şi utilizarea eficientă a acestora în orientarea direcţiilor de dezvoltare, elaborarea viziunii şi în îndeplinirea standardelor de performanţă de către grupuri / echipe şi „comunităţi de practicieni". Acest lucru se traduce prin nevoia de adaptare rapidă a organizaţiei la transformările mediului operaţional şi de flexibilizare organizaţional – funcţional a structurilor, coordonare eficientă a acţiunilor de către un management performant care promovează abordarea prospectivă, conectivistă şi inovativă a fenomenelor de risc şi ameninţare şi, desigur, prin interconectarea tuturor senzorilor de cunoaştere din societate în cadrul unor parteneriate de cooperare sau prin cooperare (multidisciplinare, interdisciplinare, zone specifice de expertiză).

Aplatizarea nivelurilor intermediare între leadership şi membrii organizaţiei, implică generarea unui nou model pentru instituţiile de intelligence, bazate pe informaţii. Rolul comunităţilor de informaţii a devenit primordial după evenimentele din 11 septembrie 2001, în special în modelarea mediului, teoriei şi practicii operative de intelligence, iar implicaţiile profunde şi extinse la nivelul global. Astfel, *noua comunitate de intelligence tinde să devină „furnizor de cunoaştere"***.**

Nu trebuie să omitem că întregul demers de cercetare se realizează într-un context în care sunt din ce în ce mai relevante antinomiile cunoaşterii prevăzute de P.Bobbit şi care sunt create de actualele modele de securitate. Pe acest fond, „*... serviciile de informaţii se confruntă cu o lume a incertitudinilor, a frontierelor tot mai vagi şi sinuoase dintre război şi pace, o lume in care eşecul poate fi o sursă a viitoarelor succese numai dacă este înţeles şi procesat ca o necesitate a schimbării modului clasic de a gândi al analiştilor*[13]".

Aplicarea unor concepte moderne, între care îl menţionăm pe cel al sinergiei, trebuie să genereze puternice modificări structurale ale actualelor construcţii de intelligence în vederea edificării unor Organizaţii de tip reţea, mult mai dinamice, flexibile şi competitive, specifice exigenţelor şi provocărilor actuale ale mediului de securitate. Apariţia de resurse specifice dezvoltate în cadrul intelligence („ -INT-uri"), strâns legate şi condiţionate de evoluţia tehnologică, pe de-o parte, şi de emergenţa riscurilor non-tradiţionale şi asimetrice, pe de altă parte, reclamă importanţa găsirii resorturilor sinergice de structuralitate şi funcţionalitate a sistemelor informaţionale moderne, a instituţiei de intelligence în mod special, pentru performanţă operaţională necesară obţinerii avantajului decizional, în opinia noastră, misiunea strategică a acesteia.

---

[13] P.Bobbitt, *Terror and Consent. The Wars for the Twenty-First Century*, Penguin Books, Londra, p.290

Utilizarea de software şi tehnologii inteligente în aplicaţiile profesionale poate conduce la creşterea capacităţii de procesare şi de rafinare a informaţiei utile, la edificarea şi consolidarea lucrului în reţea, precum şi la constituirea, consolidarea şi valorificarea avantajelor competitive determinate de interconexiunile cu alte sisteme similare a căror funcţionalitate se bazează pe intelligence competitiv şi de cooperare. Pe aceste considerente, redefinirea instituţiei de intelligence aşează din perspectivă sinergetică, ca fundamente, *o serie de obiective, între care amintim*[14]*:*

- compatibilizarea conceptuală şi acţională cu structurile de intelligence şi securitate din spaţiul euro-atlantic;
- delimitarea clară a competenţelor structurilor componente ale comunităţii, eliminarea suprapunerilor şi paralelismelor structurale şi operaţionale;
- analiza strategică unitară a informaţiilor privind securitatea naţională;
- organizarea proceselor de cunoaştere prin elaborarea unei strategii naţionale de intelligence;
- asigurarea unitară a coordonării activităţilor ce vizează securitatea naţională, în zonele de competenţă ale structurilor desemnate ca autorităţi naţionale, precum prevenirea şi combaterea terorismului, domeniile CYBERINT, IMINT, GEOINT, SIGINT, PROTINT, OSINT – scurtând astfel ciclul de decizie operativă şi promovând astfel în numele organizaţiei parteneriate public-privat;
- inducerea ideii de creare a unei noi culturi organizaţionale;
- asigurarea de acţiuni eficiente şi comunicaţii aliniate pentru energizarea serviciilor, componente ale noii organizaţii de intelligence;
- creşterea gradului de interoperabilitate internă în domeniul intelligence-ului şi eliminarea concurenţei neproductive între structurile comunităţii;
- asigurarea feed-back-ului operaţional cu beneficiarii legali ai produselor de intelligence, îmbunătăţirea ciclului de informare şi implicarea acestora în definirea unei culturi operaţionale în acest domeniu;
- optimizarea şi coordonarea Diplomaţiei intelligence-ului;
- operaţionalizarea Centrelor de Excelenţă în Intelligence şi abordarea unitară a proceselor de formare, training, cercetare şi valorificare a intelligence-ului;
- relaţionarea cu structuri private de intelligence, în special pe zona de analiză de risc, precum şi promovarea, în numele organizaţiei a legislaţiei în domeniul intelligence.

Un nou model operaţional trebuie *definit şi operaţionalizat în concordanţă cu* cele *4 principii de intelligence (management integrat al misiunilor; culegere adaptată de informaţii; analiză coroborată; parteneriat strategic)*, să fie centrat pe misiune, agil, dinamic, suficient şi flexibil, capabil să adapteze rolurile serviciilor de informaţii la noi provocări, să încorporeze noi tehnologii şi procese, să se dezvolte pe domeniile integrării şi colaborării, fără contrângerile legilor organizaţionale sau canalelor funcţionale.

Abordarea unui asemenea model complex implică analize multiple, sens în care sunt necesare a fi analizate rezultatele unui *studiu privind provocările întâmpinate asupra companiilor private moderne, cele mai competitive* (din domeniul farmaceutic, electronic, comercial, chimic), formulate în legătură cu desfăşurarea procesului de intelligence şi a managementului cunoaşterii, *principalele concluzii fiind*[15]*:*

- *misiunea de intelligence s-a modificat* – de la un mijloc pasiv de obţinere de informaţii, aflat sub comanda unor decidenţi, la un agent intern activ (poziţia

---

[14] Bădică P., Ştefan R.(2008), *Provocări privind definirea unui proiect naţional de intelligence*, în Revista Română de Studii de Intelligence nr. 8 / 2012, pp.61-62

[15] *Journal of Studies in Business* – Magnus Hope – *The Intelligence Worker as a Knowledge activist – an alternative view on intelligence by the use of Bukes pentad*/march 2013

ierarhică nu determină procesul sau produsul, nevoile informaţionale aflate la fiecare subunitate a unei organizaţii asigură input-ul necesar. Intelligence-ul dobândeşte 2 dimensiuni: analistul este agentul individual cu o reţea personală; produsul este adaptat la indivizi şi la situaţia specifică);

- *intelligence-ul este dispersat*, există atât în structurile centrale ale unei organizaţii, cît şi în filiale sau în echipe de proiect care, la rândul lor, cooperează cu grupuri similare, însă în baza intereselor comune, nu sub coordonarea unui manager central special desemnat;
- *ciclul de intelligence tradiţional* – în care planificarea este prerogativ a decidentului, iar celelalte componente (culegere,analiză, diseminare) sunt sarcini ale echipei de lucru este din punct de vedere conceptual corect, însă descrie procesul de intelligence la un nivel organizaţionals implificat, nu la unul individual complex;
- *practicienii sunt implicaţi în alte activităţi decât cele aflate în strânsă legătură cu procesul decizional* cum ar fi: organizarea / participarea la „conversaţii" analitice; actualizarea analizei standard; ordonarea informaţiilor şi profilurilor competitorilor;
- *intelligence-ul este creat pentru a îmbunătăţi afacerile şi a sprijini procesul decizional*.

În acest sens**,** rolul practicienilor se redefineşte în domeniile iniţierii de cunoaştere, reducerii timpului şi costurilor necesare creării cunoaşterii, popularizării iniţiativelor în cadrul organizaţiei şi ghidării creării de cunoaştere. Pe aceste coordonate, edificarea sinergică a organizaţiei de intelligence va fi ghidată şi de aceste provocări de cunoaştere.

Edificator pentru finalul acestui demers de cercetare este discursul lui John C. Gannon[16] care atrage atenţia că „*... fuzionarea intelligence-ului, sinergia oamenilor bine pregătiţi şi a tehnologiilor avansate şi munca în echipe mixte interagenţii sunt la cel mai înalt nivel atins vreodată ... deşi este întotdeauna loc de mai bine în activitatea de intelligence, performanţa puternică, colaborativă a agenţiilor noastre ... la ora actuală este fără precedent – şi o sursă de mândrie justificată pentru IC*".

BIBLIOGRAFIE:

1. ***, *Intelligence Overview of US Intelligence Community*, SUA, 2011;
2. ***, *Viziunea 2011 – 2015 „SRI în era informaţională"*, Bucureşti, 2011;
3. ***, *Viziunea 2015 a SUA - o organizaţie globală şi integrată de intelligence*, trad., Bucureşti, 2008;
4. David S. Alberts (2002), Information Age Transformation, DoD Command and Control Research Program – accesat pe adresa web http://www.dodccrp.org/files/ Alberts_IAT.pdf, in 10.02.2015
5. Fingar, Thomas, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, Stanford University, octombrie 2009
6. Lahneman, William J., *The Need for a New Intelligence Paradigm*, în „International Journal of Intelligence and CounterIntelligence", vol. 23, nr. 2, 25 februarie 2010
7. Maior George Cristian, *Incertitudine, gandire strategică şi relaţii internationale în secolul XXI*, Editura RAO Bucuresti, 2009

[16] *Ten Years After 9/11: Is Intelligence Reforme Working?*, Opening Statementof John C.Gannon to the US Senate Homeland Security and Government Affairs Committee Hearing, May 12, 2011, pp.1-6

8. Maior, George Cristian, (coord.), *Un război al minţii, Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI*, Ed. RAO, Bucureşti, 2010;
9. Maior, George Cristian, Konoplyov Sergei (coord.) – *Cunoaştere strategică în zona extinsă a Mării Negre*, Ed. RAO, Bucureşti, 2011;
10. Matei, Florina Cristiana, *Romania's Intelligence Comunity: From an Instrument of Dictatorship to Serving Democracy*, în International Journal of Intelligence and Counterintelligence, nr. 4/2007;
11. Mihaela, Muresan- *Sinergia dintre cunoastere, creativitate, cercetare, inovare si educaţie*, accesat pe adresa http://euromentor.ucdc.ro/dec2011/ro/sinergiadintre cunoastere creativitatecercetaremihaelamuresan_9.pdf
12. Niţu, Ionel, *Analiza de intelligence. O abordare din perspectiva teoriilor schimbării*, Ed. RAO, Bucureşti, 2012.
13. Pallaris, Chris, *Open Source Intelligence:A Strategic Enabler of National Security*, CSS Analyses in Security Policy, vol.3, no.32, 2008

Această lucrare este elaborată şi publicată sub auspiciile Institutului de Cercetare a Calităţii Vieţii, Academia Română ca parte din proiectul co-finanţat de Uniunea Europeană prin Programului Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013 în cadrul proiectului Pluri şi interdisciplinaritate în programe doctorale şi postdoctorale Cod ProiectPOSDRU/159/1.5/S/141086.

CERCETAREA EXPERIMENTALĂ A INFLUENŢEI PSIHOINFORMAŢIONALE DISTALE[1]

Dr. Aliodor MANOLEA
Doctor în Psihologie (PhD), Universitatea din Bucureşti.
Doctor în Ştiinţe - Medicină Complementară (DSc),Colombo, Sri Lanka.
Doctorand în Ştiinţe Militare, Universitatea Naţională de Apărare "Carol I", Bucureşti.
Email: aliodor@glide.ro

Rezumat: *Demonstrarea experimentală a transmiterii de informaţii, între subiecţi izolaţi spaţial şi senzorial, aparent fără sprijin material, în operaţiuni de război, este posibilă prin înregistrarea pattern-lui EEG al activităţii cerebrale produsă de expunerea la stimulii vizuali afectogeni. Fenomenul de conectivitate cerebrală, în timpul a ceea ce am numit Influenţă Psihoinformaţională Distală, este demonstrat prin determinarea coerenţei semnalelor EEG, folosind clasificatorul neuroscientific ERD/ERS.*

Cuvinte cheie: *psihoinformaţional, distal, subliminal, coerenţă, sincronizare.*

Sintagma Influenţă Psihoinformaţională Distală (IPsiD) este un concept integrator ce cuprinde o extensie a comunicării şi influenţei subliminale în domeniul cinetic al acţiunii[2]. Scopul folosirii influenţei psihoinformaţionale distale, în toate etapele acţiunii beligene, este acela de a altera capacităţile psihoemoţionale ale inamicului, care îi sunt necesare ducerii acţiunilor de luptă, de reducere a capacităţilor sale de luare a deciziilor, la toate nivelurile, de la comandanţi până la trupă, de a slăbi voinţa combativă a inamicului.

Montajul experimental

Experimentul a constat în expunerea simultană a subiecţilor inductori la stimuli vizuali cu semnificaţie afectogenă şi măsurarea efectului presupusei transmiteri psihoinformaţionale distale la subiecţii receptori.

Activitatea cerebrală a ambelor categorii de subiecţi a fost monitorizată cu ajutorul unor căşti EEG wirelless cu câte un canal, care au comunicat cu un sistem de achiziţie a datelor dotat cu trei calculatoare portabile, cu sincronizarea timpului asigurată prin internet, pe care a rulat sistemul de operare LINUX. Pe calculatorul master a rulat un program PSYCHOPY[3], care a gestionat desfăşurarea temporală a experimentului (figura nr. 2), în ceea ce priveşte expunerea la stimulii vizuali cu conţinut afectogen.

Electrodul fiecarei căşti EEG a fost plasat în zona lobului frontal al fiecarui subiect, în punctul Fp1 din schema „10-20" de amplasare pe scalp a electrozilor EEG.

S-au efectuat trei experimente, negintenţional şi intenţional cu câte 16 subiecţi neexperimentaţi (fără pregătire specifică psihoinformaţională) şi încă unul intenţional cu 16 subiecţi, din care opt subiecţi au avut o pregătire specifică psihoinformaţională (activarea

---

[1]Manolea, A. *Acţiunea beligenă şi influenţarea psihoinformaţională distală,* referat Scoala Doctorală Ştiinţe Militare şi Informaţii, UNAp, Bucureşti, pp.4-65.

[2]Manolea, A. "Influenţa psihoinformaţională distală ca parte a influenţei informaţionale de intelligence". *Academia Nationala de Informatii "Mihai Viteazul" International conference „Intelligence in the knowledge society"* Bucharest, Romania, October 19th 2012. Biblioteca electronica a Academiei Nationale de Informatii (ANI), Colectia "ANI - Mihai Viteazul", ISBN 978-606-532-062-3.

[3]Peirce J.W., „Generating stimuli for neuroscience using PsychoPy". *Frontiere Neuroinform*. 2:10. doi:10.3389/neuro. 11.010.2008.

potenţialului propriu prin tehnica neutrală). În total au fost 48 de subiecţi participanţi la aceste experimente, din care 40 au fost studenţi ai Facultăţii de Psihologie a Universităţii Bucureşti iar opt aparţinând unui grup cu pregătire specifică psihoinformaţională. Toate trei experimentele au avut aceeaşi desfăşurare temporală. Fiecare experiment a avut câte 25 de sesiuni de lucru la care au participat grupuri de subiecţi distribuiţi după şirul lui Fibonacci[4].

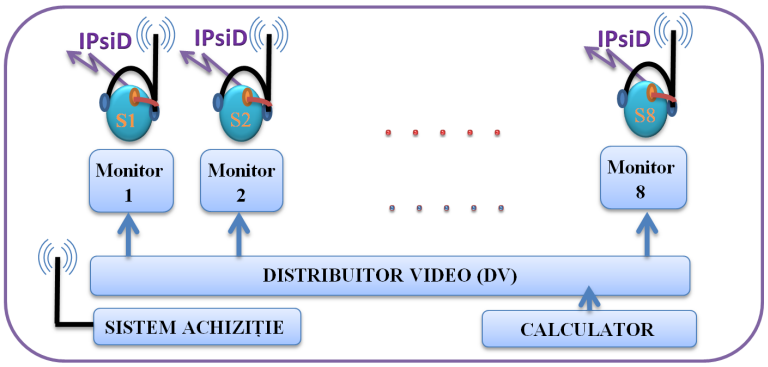


Figura nr. 1. Montaj experimental pentru subiecţii din sala 1 (Manolea, A., 2014)

Fiecare sesiune a fiecarui experiment a avut câte nouă imagini cu durata de câte şase secunde precedate de o pauză de atenţionare de 3 secunde, unele cu conţinut afectogen pozitiv, altele cu conţinut afectogen negativ şi altele neutre din punct de vedere emoţional.

Sesiunile cu număr de ordine fără soţ (1, 3, 5... 25) au avut ca inductori subiecţii din sala 1 (fig. 1), iar pentru cele cu număr de ordine par subiecţii inductori au fost cei din sala 2. Au fost opt subiecţi în sala 1 şi alţi opt în sala 2, izolaţi spaţial prin intermediul unui perete de beton armat.

Am măsurat, sincronizat în timp, activitatea cerebrală a subiecţilor inductori şi a celor receptori, iar datele obţinute le-am prelucrat cu mai multe pachete de programe pentru analiza semnalelor: EXCEL, MATLAB, EEGLAB, ASAEEG, pentru extragerea informaţiilor împachetate în structura EEG.

Toate canalele EEG individuale au fost reunite într-o structură unitară corespunzatoare schemei EEG 10-20, cu maxim 19 canale, din care am activat tehnic numai 15 canale.

Am echivalat înregistrarea EEG corespunzătoare fiecărui subiect cu câte un canal specific înregistrării unei EEG cu sistemul de electrozi 10-20. Corespondenţa a fost: S1-Fp1, S2-Fp2, S3-F7, S4-Fz, S5-F8, S6-T3, S7-Cz, S8-T4, S9-O1, S10-O2, S11-T5, S12-P3, S13-Pz, S14-P4, S15-T6, şi S16-Oz, în care Si sunt cei 16 subiecţi. Procedând astfel am putut utiliza facilităţile analitice ale programelor de analiza a EEG, care tratează toate semnalele simultan, astfel încât rezultatele au fost obţinute unitar, prin aplicarea aceloraşi proceduri de prelucrare, având aceleaşi valori pentru parametrii specifici. Astfel, electrozii EEG corespunzători jumătăţii din faţă a scalpului model au fost în corespondenţă cu înregistrările EEG ale subiecţilor din sala 1 iar cele dinspre ceafă au corespuns cu înregistrările EEG ale subiecţilor din sala 2.

Metode de studiere a sincronizării activităţii cerebrale

Ipoteza, care se află în spatele oricarei analize EEG, este că anumite modele ale activitaţii cerebrale corespund întotdeauna aceloraşi evenimente declanşatoare şi invers, cu

[4]Manolea, A., „Fundamente epistemice ale influenţei psihoinformaţionale distale”, *Buletinul UNAP* nr.1/2013, pp. 378-382.

alte cuvinte există o relaţie biunivocă între evenimentele declanşatoare şi tiparul activităţii cerebrale. În cazul nostru evenimentele declanşatoare au fost emoţiile generate de expunerea subiecţilor inductori la imagini cu conţinut afectogen, iar presupunerea a fost că printr-un mecanism care nu este încă elucidat, aceste emoţii se transmit distal şi altor subiecţi, fără ca aceştia sa fie în contact de orice fel şi fără conştientizare. De fapt am urmărit să măsor ce se întamplă, cum şi dacă se transmite vreo informaţie de la subiecţii inductori la cei receptori, atunci când există şi atunci când nu există o intenţie. La nivelul prelucrării datelor, acest fapt este echivalent cu existenţa unor modele comune ale activitaţii cerebrale, atât subiecţilor inductori cât şi celor receptori.

Această analiză se bazează pe presupunerea că activitatea cerebrală este specifică fiecărei interacţiuni a fiinţei umane cu mediul, oricare ar fi el, sau cu alte cuvinte, adaptat cazului nostru, fiecare emoţie determină apariţia unui tipar specific al activităţii cerebrale.

Dacă descoperim structuri în domeniul timp sau frecvenţă care sunt asemănătoare putem spune că există un grad mare de similitudine între evenimentele (emoţiile) care au determinat acea structură a activităţii cerebrale la subiecţii inductori.

ERS/ERD – Event Related Synchronization/Event Related Desynchronization

Un mod comun de a analiza EEG este medierea datelor pentru a descoperi anumite structuri, tipare care apar la anumite momente de timp fixate, legate de evenimente specifice (de exemplu stimuli sau răspunsuri la stimuli) – aşa numitele ERP (Event Related Potential). Prin mediere, raportul semnal-zgomot este îmbunătăţit dramatic, astfel încât apare vizibilă o anumită structură comună.

Dar, în multe cazuri (aşa cum este şi acesta), nu există momente de timp bine determinate, la care să apară activitate cerebrală legată de un anumit eveniment, pentru că nu ştim cum şi când o imagine cu conţinut afectogen generează o emoţie în mintea subiectului inductor.

Activitatea electrică a creierului subiectului inductor, generată de emoţii, poate fi determinată de amintirile acestuia sau de un mecanism inconştient legat de reacţiile instinctive gen luptă sau fugi, astfel încât există o nedeterminare cu privire la momentul apariţiei unui tipar al activităţii electrice cerebrale (EEG).

Nedeterminarea, în ceea ce priveşte momentul la care se petrece transmiterea informaţiei, este specifică influenţei psihoinformaţionale distale (IPsiD), astfel încât dacă utilizăm metoda determinării ERP, informaţia va fi distrusă prin mediere pentru că ea nu apare la aceleaşi intervale faţă de evenimentul declanşator, pentru toate sesiunile experimentului. Acest lucru poate fi evitat prin aplicarea metodei analizei sincronizării/ desincronizării (ERS/ERD – Event Related Synchronisation/Event Related Desynchronisation) activităţii cerebrale determinate de apariţia unor evenimente la momente oarecum aleatoare în timp.

ERS reprezintă o creştere în amplitudine a puterii undelor cerebrale dintr-o banda de frecvenţe specifică, de scurtă durată şi bine localizate spaţial, în timp ce ERD reprezintă o scădere a amplitudinii. Aceste creşteri/descreşteri în amplitudine nu sunt corelate în faza cu un anumit eveniment şi sunt foarte specifice anumitor benzi de frecvenţa (alfa, beta, gama, delta, teta), adică pot să apară în unele benzi de frecvenţă în timp ce în altele nu.

Din acest motiv înregistrările EEG brute arată ca un semnal haotic, aleator, ce nu pare a conţine tipare foarte clare ale activităţii cerebrale, decât în cazuri bine cunoscute. De aceea calcularea ERS şi ERD este folosită pentru a ne oferi o imagine a dinamicii reţelelor neuronale, în cazul nostru a dinamicii legăturilor dintre activităţile cerebrale ale subiecţilor inductori şi receptori.

O formulă care descrie ERD/ERS este:

$$ERD\ (t) = [R - A\ (t)] / R \times 100$$

unde:

R= puterea medie a semnalului într-un interval de referinţă şi pentru o anumită bandă de frecvenţă.

A (t)= puterea medie a semnalului în intervalul de timp şi în banda de frecvenţă de interes.

Atunci când valoarea acestui raport este mai mare decât zero, se spune că are loc o desincronizare a activităţii cerebrale (ERD), în timp ce atunci când valoarea este negativă are loc o sincronizare a activităţii cerebrale (ERS).

Analiza coerenţei semnalelor EEG

O altă metodă utilizată pentru a arăta că există o similitudine între două semnale EEG este calcularea coerenţei dintre acestea. Coerenţa este similară cu corelaţia temporală dintre două semnale, dar este un estimator al similarităţii (ne dă o imagine a cuplării semnalelor) în domeniul frecvenţă. Coerenţa ne poate arăta că există modele de activitate cerebrală comune în anumite benzi de frecvenţă, în timp ce corelaţia temporală maschează aceste paternuri.

Coerenţa este o funcţie complexă a cărei amplitudine variază între 0 şi 1, 0 indicând lipsa similarităţii dintre semnale iar valori apropiate de 1, o mare similaritate.

Rezultate parţiale

Nu trebuie să uităm că imaginea activităţii cerebrale, aşa cum arăt aici, este de fapt o simulare a activităţii cerebrale a tuturor subiecţilor experimentului, fiecare semnal EEG fiind corespunzător câte unui subiect.

Aşadar, o imagine a scalpului standard conţine până la 15 electrozi virtuali corespunzători fiecărui subiect. Înregistrările EEG au fost făcute cu aparate EEG cu câte un electrod situat în zona frontală, corespunzătoare punctului Fp1 din sistemul 10-20 de aplicare a electrozilor EEG pe scalpul uman.

Am ales această reprezentare pentru că este foarte sugestivă şi în acelaşi timp intuitivă, dar şi pentru că pachetele software pentru prelucrarea datelor EEG utilizează acest mod de vizualizare a rezultatelor obţinute.

În cazul sesiunilor cu număr impar ale experimentului, grupul de electrozi Fp1, Fp2, F7, Fz, F8, T3, Cz şi T4 reprezintă subiecţii inductori, iar grupul de electrozi O1, O2, T5, P3, Pz, P4 şi T6 subiecţii receptori, rolurile inversându-se pentru sesiunile cu număr par.

Testarea ipotezelor

Ipoteza nr.1 *Demonstrarea existenţei sincronizării temporale a modelelor (tiparelor) de activitate cerebrală comune atat subiecţilor inductori cat şi celor receptori.*

Rezultatele prezentate în continuare au fost obţinute cu pachetul de programe pentru interpretarea înregistrărilor EEG, EEGLAB[5] un proiect coordonat de Swartz Center for Computational Neuroscience (SCCN) al Institute for Neural Computation care aparţine de University of California San Diego.

---

[5] A. Delorme, S. Makeig „EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics". *Journal of Neuroscience Methods* 134:9-21, 2004, http://sccn.ucsd.edu/eeglab/index.html, accesat aprilie 2014.

In fig.2 se observă cum variază intensitatea conexiunii dintre activităţile cerebrale a doi subiecţi în timpul unei sesiuni experimentale de influenţare distală. Cea mai mare energie, comună celor doi subiecţi, este în domeniul de frecvenţe teta (1-6Hz) al undelor cerebrale. Acesta este domeniul de frecvenţe care caracterizează activitatea subconştientului, domeniul percepţiilor subliminale. De asemenea, se observă variaţia ritmică a intensităţii conexiunii activităţilor cerebrale ale celor doi subiecţi, variaţie care are, în cea mai mare parte o puternică corelaţie (maximele graficului sunt în intervalele 1-2s, 3-4s, 6-7s, 7-8s, 8-9s) cu momentul apariţiei imaginilor cu conţinut afectogen. Imaginile cu efect afectogen au apărut la 14s, 24s, 34s...94s, adică la intervale de 10 secunde, având o durată de şase secunde. Acest fapt s-a înregistrat în majoritatea sesiunilor experimentale cu o frecvenţă mai mare sau mai mică, în funcţie de patru factori.

Primul factor a fost capacitatea de concentrare şi de păstrare a acesteia un timp suficient de lung, pentru a se putea spune că energia undelor cerebrale a fost suficient de mare pentru a putea genera asemenea efecte.

Al doilea factor ţine de atenţia concentrată pe care o poate manifesta un subiect, factor cu o mare variabilitate mai ales atunci când este vorba despre menţinerea lui un timp îndelungat, în cazul nostru aproape 100 secunde. În general, un subiect neantrenat nu-şi poate menţine atenţia concentrată, asupra unui singur obiectiv mental, mai mult de câteva secunde.

Un al treilea factor este, în mod evident, antrenamentul pe care l-au avut subiecţii participanţi. Din cei 48 de subiecţi participanţi, numai opt au avut un antrenament specific pentru îmbunătăţirea capacităţii de menţinere a atenţiei şi concentrării, ceilalţi încadrându-se în profilul normalităţii.

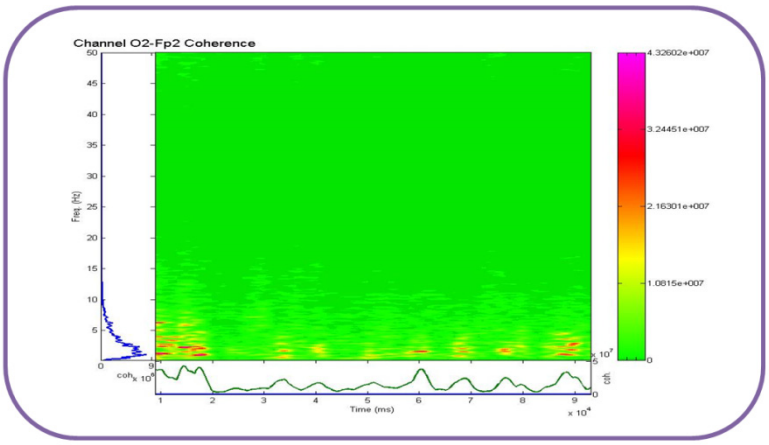


Figura nr. 2 Interacţiunea dintre activităţile cerebrale a doi subiecţi (S2 şi S10) reprezentată în domeniul frecvenţă (graficul din stânga) din şi în domeniul timp (graficul de jos), Graficul din centru arată conexiunea celor doi subiecţi atât în frecvenţă cât şi în timp
(Manolea, A., 2014)

Al patrulea factor a fost activarea potenţialului propriu într-un mod specific, activare care este parte a programului de antrenare, şi de care au beneficiat aceeaşi opt subiecţi.

De asemenea dacă studiem conexiunea dintre subiecţi prin intermediul metodei determinării ERS/ERD (fig.3) observăm, de data aceasta la scară globală (pentru toţi subiecţii odată), cum se produc alternanţe între momentele de cuplare (sincronizare-ERS) şi decuplare (desincronizare-ERD).

Momentele de sincronizare corespund unei creşteri a puterii undelor cerebrale, iar cele de desincronizare unei scaderi a acestei puteri[6]. De asemenea se observă cum diferiţi subiecţi devin conectaţi (sincronizaţi) pe rând sau împreună, aceasta fiind o caracteristică pe care o relevă acest tip de analiză[7]. Deci, se poate spune că un subiect poate fi conectat cu mai mulţi subiecţi.

Se observă că există intervale scurte (sub 0,5 secunde) în care activitatea cerebrală a subiecţilor implicaţi ia o pauză, devine desincronizată, decuplată, momente în care reţelele neuronale ale subiectului receptor îşi manifestă maximum de disponibilitate[8] la influenţarea distală.

Prin urmare acţiunea de influenţare pare a se petrece în impulsuri, fapt ce poate fi explicat prin aceea că o energie mai mare poate fi disponibilă numai pentru scurte perioade de timp, printre altele şi datorită posibilităţii subiecţilor de a păstra atenţia şi concentrarea, fixate un interval mai lung sau mai scurt.

Astfel, putem spune că există o corelaţie temporală ritmică între tiparele activităţii cerebrale a subiecţilor participanţi la acest experiment.

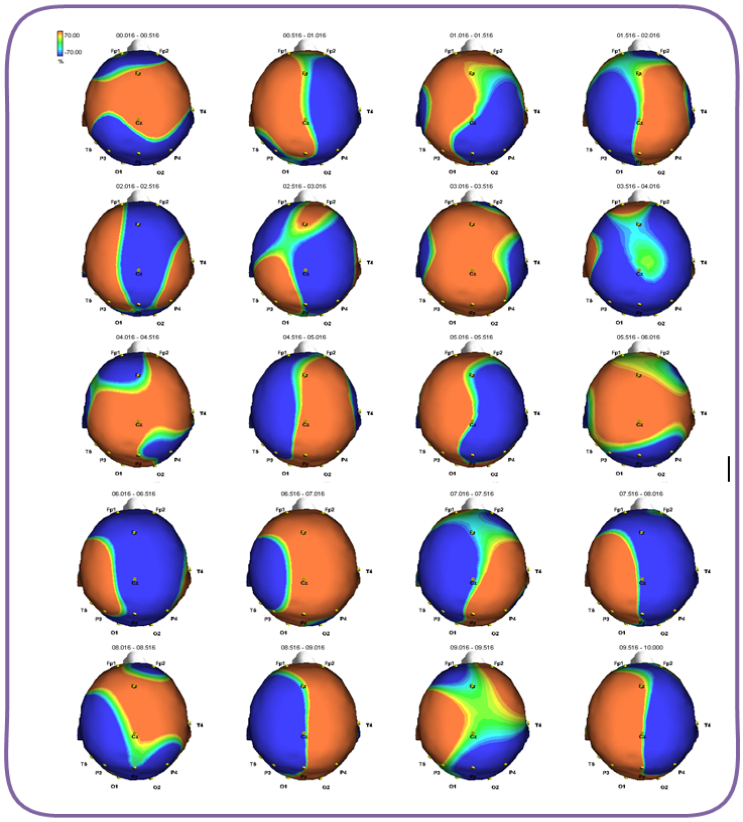


Figura nr. 3 Dinamica ERD/ERS (sincronizare-desincronizare a activităţii cerebrale) în intervalul 10-20 secunde (din 0,5s în 0,5s) al unei sesiuni experimentale şi în banda

[6] Durka, P. J., Zygierewicz, J., Klekowicz, H., Ginter, J., & Blinowska, K. J. "On the statistical significance of event-related EEG desynchronization and synchronization in the time-frequency plane". *Biomedical Engineering, IEEE Transactions on*, 51(7), 1167-1175, 2004.

[7] Brazdău, O. "Constiinta si misterele fizicii cuantice" *Buletinul psihologiei transpersonale*, Numărul 7-8/2003, http://www.arpt.ro/RO/TPBuletin/7-8-2003.htm, accesat 11.11.2012.

[8] Pfurtscheller , G., Lopes da Silva, F. H. , "Event-related EEG/MEG synchronization and desynchronization: basic principles". *Clinical neurophysiology*, Vol. 110, No. 11. (November 1999), pp. 1842-1857.

teta (2-4Hz). Sincronizarea activităţii cerebrale este redată cu roşu iar desincronizarea cu albastru. (Manolea, A., 2014)

Ipoteza 2. *Subiecţii ale caror potenţe proprii au fost activate au fost mai puţin influenţaţi decât cei care nu au trecut printr-un astfel de proces*

O altă modalitate de a arăta conectivitatea dintre două sisteme este evidenţierea funcţiei coerenţă. Aceasta funcţie este un estimator al corelaţiei dintre două sisteme în domeniul frecvenţă. Imaginile prezentate în continuare, arată amplitudinea coerenţei dintre toţi cei 15 subiecţi participanţi la două sesiuni experimentale de tipul opt inductori şi şapte receptori, schimbând rolurile pe rând. Cei opt subiecţi din sala 1 sunt cei care au avut un program de antrenament şi care au beneficiat de activarea potenţelor proprii prin tehnica neutrală. Ce se observă?

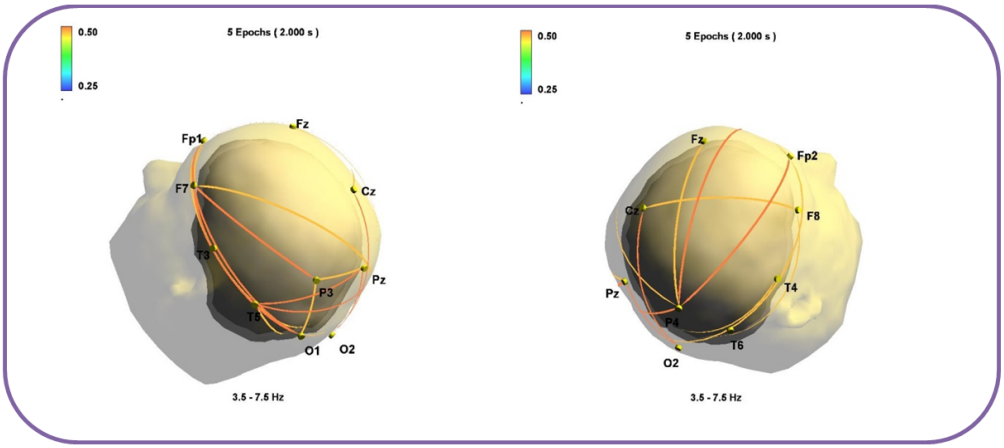


Figura nr. 4 Amplitudinea coerenţei (intervalul 0,25-0,50) pentru sesiunea în care subiecţii antrenaţi au fost inductori (12 conexiuni cu receptorii) (Manolea, A., 2014)

În fig.4 observăm că inductorii antrenaţi au reuşit să stabilească 12 conexiuni cu cei şapte subiecţi receptori, conexiuni a căror valoare a coerenţei se află în intervalul 0,25-0,5, o valoare semnificativă, având în vedere că este vorba de creiere diferite[9].

Din fig.5, rezultă că subiecţii fără pregătire specifică au reuşit să stabilească numai 5 conexiuni cu receptorii, ceea ce ne arată că au avut o eficienţă mai scăzută.

[9] D.E, Amos, L.H., Koopmans, Tables of the distribution of the coefficient of coherence for stationary bivariate Gaussian processes. Monograph SCR-483, Sandia Corp., Alburquerque, New Mexico, 1963, p. 56

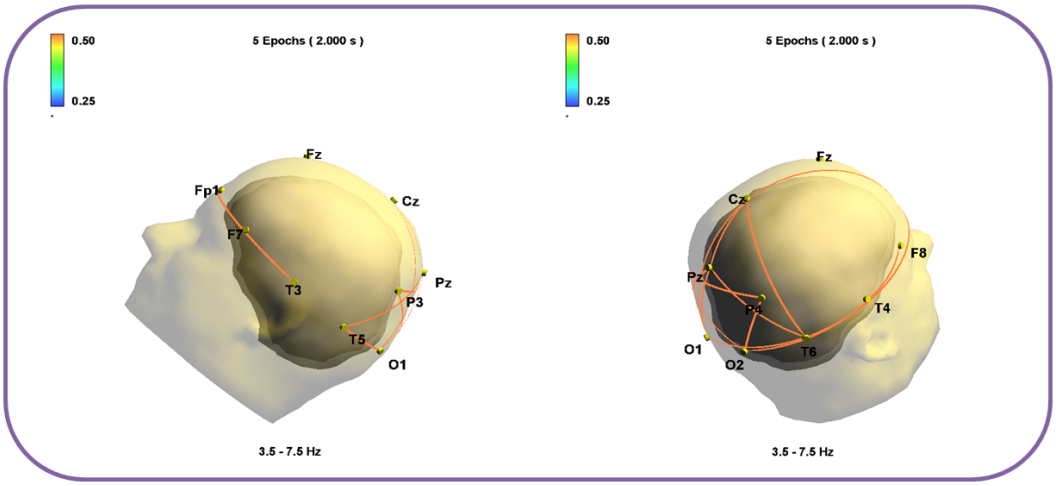


Figura nr. 5 Amplitudinea coerenţei (intervalul 0,25-0,50) pentru sesiunea în care subiecţii neantrenaţi au fost inductori (5 conexiuni cu receptorii) (Manolea, A., 2014)

Acest fapt ar putea să însemne că pregătirea specifică a subiecţilor antrenaţi poate să determine o mai mare eficienţă în influenţarea psihoinformaţională distală, şi, în acelaşi timp, protecţie mai mare la influenţele exterioare de orice tip ar fi acestea.

Concluzii

Înregistrările EEG pot fi un instrument util, viabil şi sigur pentru a pune în evidenţă influenţa psihoinformaţională distală. Extragerea informaţiei împachetate în structura înregistrărilor EEG este o activitate foarte laborioasă care, în acelaşi timp, cere o înţelegere aprofundată a dinamicii reţelelor neuronale implicate în transferul subliminal al informaţiei. Acest transfer poate fi efectuat de către orice subiect normal sănătos, dar cei mai eficienţi se dovedesc a fi cei care au o pregătire specifică. Influenţa psihoinformaţională distală poate avea loc cu sau fără intenţie, mediatorul acesteia fiind emoţia manipulată într-un mod specific. Prin urmare, se poate afirma că există posibilitatea de a modula comportamentul oricărui subiect ţintă astfel încât acesta să fie în imposibilitatea de a-şi atinge obiectivele stabilite. De altfel şi reciproca este adevărată (pare a fi şi mai etic) subiectul ţintă poate fi susţinut pentru a atinge obiectivul stabilit folosindu-şi potenţialul la maximum.

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului POSDRU/159/1.5/S/138822, cu titulul „Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile “Ştiinţe Militare”, “Securitate şi Informaţii” şi “Ordine Publică şi Siguranţă Naţională” - Program de Formare Continuă a Cercetătorilor de Elită –“ SmartSPODAS”.”Proiect cofinanţat din Fondul Social European prin Programul Operaţional Sectorial pentru Dezvoltarea Resurselor Umane 2007-2013 „Investeşte în OAMENI”

BIBLIOGRAFIE:

1. ***, *Strategia de securitate naţională a României*, Bucureşti, 2001.
2. Aniţei, M. *Psihologie experimentală*, Ed. Polirom, Iaşi**,** 2007.
3. Brazdău, O. "Constiinta si misterele fizicii cuantice" *Buletinul psihologiei transpersonale*, Numărul 7-8/2003, http://www.arpt.ro/RO/TPBuletin/7-8-2003.htm, accesat 11.11.2012.
4. Durka, P. J., Zygierewicz, J., Klekowicz, H., Ginter, J., & Blinowska, K. J. "On the statistical significance of event-related EEG desynchronization and synchronization in the time-frequency plane". *Biomedical Engineering, IEEE Transactions on*, 51(7), 1167-1175, 2004.

a. http://sccn.ucsd.edu/eeglab/index.html, accessed April 2014.
b. http://sccn.ucsd.edu/eeglab/index.html, accessed Aprilie 2014.

5. Manolea Aliodor "Considerations on distant psycho –informational influence in warfare". *International Conference „STRATEGIES XXI"* „Carol I" National Defence University, Bucharest, Romania. April 18 – 19, 2013-03-29,ISSN 2285-8415, ISSN-L 2285-8318, (2013):577.
6. Manolea Aliodor "Items required to elaborate experiments on distal psycho-informational influence". *International Conference „STRATEGIES XXI"* „Carol I" National Defence University, Bucharest, Romania. April 18 – 19, 2013-03-29, ISSN 2285-8415, ISSN-L 2285-8318, (2013):585.
7. Manolea, A. "Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă", *Bucharest University, Doctoral School of Psychology and Education Sciencies.* Psychology Department, Doctoral Thesis, 2012.
8. Manolea, A. "Influenţa psihoinformaţională distală ca parte a influenţei informaţionale de intelligence". *Academia Națională de Informații "Mihai Viteazul" International conference „Intelligence in the knowledge society" Bucharest, Romania, October 19th 2012. Biblioteca electronică a Academiei Naţionale de Informaţii (ANI), Colecţia "ANI - Mihai Viteazul", ISBN 978-606-532-062-3.*
9. Manolea, A. "The cibernetics'subtle energy of the human being. Fundaments of the neutral theory referring to the living beings' system". Doctoral Thesis in Sciencies, Complementary Medicine, *The Open University for the Complementary Medicines*, Colombo, SriLanka, 2000.
10. Manolea, A. „Fundamente epistemice ale influenţei psihoinformaţionale distale". *Buletinul UNAP nr.1/2013, pp. 378-382.*
11. Manolea, A. *Acţiunea beligenă şi influenţarea psihoinformaţională distală,* referat Scoala Doctorală Ştiinţe Militare şi Informaţii, UNAp, Bucureşti, 2013, pp.4-65.
12. Manolea, A. *Condiţionarea psihosomatică. Psihodiagnoză şi intervenţie psihoterapeutică folosind stările modificate de conştiinţă*, Universitatea Bucureşti, Scoala doctorală de Psihologie şi Ştiinţe ale Educaţiei, Departamentul Psihologie,Teza de doctorat, 2012.
13. Manolea, D.E, Manolea, A. *Influenţa distală - Teoria şi practica vindecării la distanţă*. Aldomar Extrasenzorial Publishing House, Bucharest, 1997.
14. Pfurtscheller, G., Lopes da Silva, F. H. , "Event-related EEG/MEG synchronization and desynchronization: basic principles". *Clinical neurophysiology*, Vol. 110, No. 11. (November 1999), pp. 1842-1857.

SECURITATE CIBERNETICĂ ŞI DREPTURILE CETĂŢENILOR ÎN MEDIUL VIRTUAL

Alexandru ION
Doctorand la Facultatea de Ştiinţe Politice, Universitatea din Bucureşti, România,
ion.alexandru@fspub.unibuc.ro

Rezumat: *Lucrarea se va concentra pe ameninţările de pe internet şi cum acestea au un impact direct asupra noastră şi a relaţiilor internaţionale actuale. Mediul online este disponibil astăzi milioanelor de persoane din întreaga lume prin intermediul calculatorului şi al telefonului. Potenţialul acestui serviciu fiind nelimitat, de la simpla navigare până la terorismul cibernetic. Este necesară o mai bună securizare a internetului, dar în acelaşi timp şi respectarea intimităţii civililor, apare astfel următoarea întrebare: "Cum putem combate terorismul cibernetic, şi în acelaşi timp, respecta confidenţialitatea şi libertatea indivizilor în mediul online, având în vedere că instituţiile acreditate pot face abuz de informaţiile particulare?" Răspunsul acestei întrebări îl vom afla atunci când vom identifica statul/statele capabile de a satisface ambele criterii.*

Cuvinte cheie: *confruntare, cibernetică, vulnerabilităţi, cyberterrorism, conflicte, internet.*

Introducere

Forma conflictelor în cadrul relaţiilor internaţionale s-a modificat în secolul al XXI-lea, datorită inovaţiilor tehnologice, dar şi implicării mai active a cetăţeanului de rând în viaţa politică. Interesele sunt variate, ca şi suportul financiar şi al resurselor umane, depind de fiecare actor politic internaţional[1]. Nu este de mirare, faptul că internetul, dintr-un mijloc de comunicare şi transfer al datelor inofensiv, a devenit pe parcursul anilor o metodă eficientă de a servii intereselor statelor în probleme conflictuale. Modul prin care internetul a fost transformat într-o armă ofensiva/defensivă diferă de la caz la caz. Numeroase state s-au confruntat cu probleme în războiul cibernetic internaţional, ajungând astfel victime în faţa statele experimentate în acesta arie. Ţările precum: China, Rusia, SUA, Marea Britanie, au descoperit în internet, o cale prin care îşi pot marii influenţă la nivel internaţional, iar în acelaşi timp atacându-şi rivalii prin orice mijloace[2]. Din moment ce oricine are acces la internet, un atac cibernetic este posibil din partea oricărei persoane şi îndreptat împotriva: propriei tari, a unei ţări aliate, unei ţări rivale sau a unei simple persoane.

Domeniul confruntărilor cibernetice reprezintă o arie enormă a studiilor de securitate, unde subiectele pe această temă sunt numeroase, cu toate acestea am ales în cadrul lucrării mele să abordez două teme importante: legislaţia privind pe drepturile şi libertăţile omului şi războiului cibernetic în relaţiile internaţionale. Conflictele interstatale au directe consecinţe asupra fiecăruia dintre noi, iar în această manieră se recurge la încălcarea drepturilor la intimitate pe internet, din necesitatea de accesare a mai multor informaţii. Voi folosi ca studiu de caz în lucrare SUA, China şi Uniunea Europeană dorind să aflu care dintre acestea vizează un echilibru între respectarea drepturilor individuale şi promovarea unui sistem de apărare cibernetic eficient. Voi încerca să utilizez bibliografia limitată pentru a trata acest subiect într-

[1] Athina KARATZOGIANNI, *Cyber conflict and global politics*, Routledge, New York, 2008, p. 27
[2]Ronald DEIBERT, *Access controlled: The shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, Massachusetts, 2010, p. 4

o manieră cât mai explicită şi să formulez o lucrare de cercetare capabilă să aducă o contribuţie importantă.

Reprezentarea drepturilor individuale pe internet şi reducerea metodelor de control de către guvernele ce doresc invadarea intimităţii a devenit o prioritate pentru ONU, a organizaţiilor internaţionale ce urmăresc respectarea drepturilor umane, dar şi a grupurilor precum Anonymus. Pornind de la iniţiativa ONU de protecţie, promovare şi garantare a libertăţii pe internet, voi urmării în cadrul proiectului meu de cercetare impactul pe care l-a produs în cadrul relaţiilor internaţionale[3]. Pornind de la ipoteza: unui sistem cibernetic de apărare ideal şi evitarea intruziunii în domeniul privat. Întrebarea de cercetare este: Cum putem combate terorismul cibernetic, şi în acelaşi timp, respecta confidenţialitatea şi libertatea indivizilor în mediul online, având în vedere că instituţiile acreditate pot face abuz de informaţiile particulare?Maniera în care statele au reacţionat la această iniţiativă este un subiect interesant pe care îl voi trata în primul capitol, o analiză atentă a schimbărilor survenite şi beneficiile asupra guvernanţi cât şi guvernaţilor, folosind legislaţia în vigoare. În cel de-al doilea capitol vom avem în centrul atenţiei modificările dintre actorilor internaţionali, dar şi efectele pozitive şi negative, cercetând ce teorie a relaţiilor internaţionale se confirma în diplomaţie. La final, în cadrul concluziilor voi restrânge informaţiile esenţiale ale cercetării mele asupra domeniului.

1. Viziunea asupra problematicii drepturilor

Voi începe acest capitol printr-o scurtă prezentare a hotărârii ONU cu privire la drepturile şi libertăţile umane pe internet. După ani în care s-a discutat intens pe tema aceasta, la finalul tratativelor a fost adoptată fără vot Rezoluţia 20/8 din data 05.07.2012. Dupa cum urmează:

"Promovarea, protecția și exercitarea drepturilor omului pe internet

Consiliul pentru Drepturile Omului,

Ghidat de Carta Națiunilor Unite,

Reafirmând drepturile omului și libertățile fundamentale înscrise în Declarația Universală a Drepturilor Omului și a tratatelor internaționale în materie de drepturile omului, inclusiv Pactul internațional cu privire la drepturile civile și politice și Pactul internațional cu privire la drepturile economice, sociale și culturale,

Reamintind toate rezoluțiile relevante ale Comisiei pentru Drepturile Omului și Consiliul pentru Drepturile Omului privind dreptul la libertatea de opinie și de exprimare, în special Rezoluția Consiliului 12/16 din 2 octombrie 2009, și reamintind, de asemenea, Rezoluția Adunării Generale 66/184 din 22 decembrie 2011 .

Constatând că exercitarea drepturilor omului, în special a dreptului la libertatea de exprimare, pe Internet este o problemă de interes tot mai mare şi importantă că ritmul rapid de dezvoltare tehnologică permite persoanelor din întreaga lume de a utiliza noi tehnologii ale informației și comunicațiilor,

Luând act de rapoartele raportorului special privind promovarea şi protejarea dreptului la libertatea de opinie și de exprimare, prezentate Consiliului pentru Drepturile Omului în cadrul sesiunii sale XVII-lea, precum și Adunării Generale în sesiunea 66, cu privire la libertatea de expresie pe internet,

1. afirmă că aceleași drepturi pe care le au oamenii deconectat trebuie să fie de asemenea protejate on-line, în special libertatea de exprimare, care se aplică indiferent de

[3]http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, Rezolutia privind drepturile omului pe internet, A/HRC/17/27, 2011, accesat la data de: 20.03.2015

frontiere și prin orice mijloace, la alegerea cuiva, în conformitate cu articolele 19 din Declarația Universală a Drepturilor Omului și a Pactul internațional cu privire la drepturile civile și politice;

2. recunoaște caracterul global și deschis al internetului ca o forță motrice în accelerarea progresului către dezvoltarea în diversele sale forme;

3. invită toate statele să promoveze și să faciliteze accesul la Internet și cooperarea internațională în vederea dezvoltării mass-media și informații și mijloace în toate țările;

4. încurajează proceduri speciale pentru a lua aceste aspecte în considerare în cadrul mandatului lor existenţe, după caz;

5. decide să continue examinarea de promovare, protecția și exercitarea drepturilor omului, inclusiv dreptul la libertatea de exprimare, pe internet și în alte tehnologii, precum și a modului în care Internetul poate fi un instrument important pentru dezvoltare și pentru exercitarea drepturilor omului, în conformitate cu programul său de lucru."[4].

Având în vedere adoptarea rezoluţiei ONU, deducem faptul că statele au obligaţia de a respecta drepturile civile pe internet, cu toate acestea nu în toate cazurile avem acelaşi rezultat. Cel mai bun exemplu pe care îl voi folosi, este China, care deşi este un stat modern şi competitiv cu alte democraţii mondiale, deţine un control puternic asupra internetului naţional[5]. Cenzura impusă de guvernul de la Beijing în privinţa internetului fiind foarte dură începând cu anul 2000, fenomenul fiind cunoscut drept "Great Firewall of China"[6]. Între metodele cunoscute privind sancţiunile din China a cetăţenilor se numără: arestarea, reeducarea, amendarea spre menţinerea ordinii[7]. Deşi la prima vedere am considera impunerea cenzurii un afront la adresa drepturilor umane, totuşi stabilitatea guvernamentală, reducerea incitărilor la revoltă, banarea materialelordestinate adulţilor şi un control mai dur asupra informaţiilor destinate cetăţenilor reprezintă un avantaj important al unui regim comunist. Astfel se restrâng drepturile individuale în favoarea unei mai bune securităţi naţionale. Cu toate acestea în ultima perioadă de timp, China se confrunta cu un număr în creştere al breşelor în sistemul de cenzură naţional, acest fapt demonstrează că se doreşte libertatea internetului atât din interiorul statului, cât şi din afara acestuia prin intermediul tinerilor[8].

Discutând cazul Chinei, observăm schimbări cu paşi mărunţi, în continuare vom discuta despre un stat aflat la polul opus, Statele Unite ale Americii, unde sunt garantate libertăţile pe internet[9]. Cu toate acestea chiar şi statele capitaliste precum SUA, s-au dovedit mai interesante de securitatea naţională în ciuda încălcării drepturilor cetăţeneşti, oferind ca exemplu NSA[10]. Supravegherea constant pe internet a cetăţenilor săi este o încălcare a drepturilor la viaţa privată şi confidenţialitate[11]. Mai multe organizaţii pentru drepturi umane au protestat împotriva guvernului de la Casa Alba după incidental cu Edward Snowden, surclasând ţară din topul mondial al celor mai democrate state. În schimb interesele SUA nu

[4]http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, Rezolutia privind drepturile omului pe internet, accesat la data de: 20.03.2015

[5]https://freedomhouse.org/country/china#.VIiPmXuPVoM, Freedom House accesat la data de: 21.03.2015

[6]Pippa NORRIS, *Public Santinel: News Media & Government reform*, The World Bank, Washingston, 2010, p. 360

[7]http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?_r=0, China toughens restrictions on internet use, accesat la data de: 21.03.2015

[8]http://www.huffingtonpost.com/2012/02/29/china-firewall-breach_n_1308836.html?, China firewall breach, accesat la data de: 21.03.2015

[9]https://freedomhouse.org/country/united-states#.VRaVH-G1doM, Freedomhouse, accesat la data de: 21.03.2015

[10]http://www.spiegel.de/international/topic/nsa_spying_scandal/, NSA spying scandal, accesat la data de: 21.03.2015

[11]http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, NSA tools collect everything a user does on the internet, accesat la data de: 25.04.2015

s-au limitat doar la problemele de interes naţional, acestea au intrat şi în sfera private, iar aici vom încadra iniţiativele: SOPA (Stop Online Piracy Act) şi ACTA (Anti-Counterfeiting Trade Agreement). Despre aceste programe pot adăuga că urmăresc protejarea intereselor marilor companii americane ce au pierderi datorită pirateriei pe internet, acestea cauzând daune de mii de dolari anual.

Văzând acestea în momentul în care aducem în discuţie libertăţile individuale pe internet cea mai reprezentativă zona pentru această idee sunt ţările Uniunii Europene, oferind o libertate mult mai mare a cetăţenilor pe internet, spre deosebire de SUA. De menţionat este şi Factsheet on the "Right to be forgotten" ruling (c-131/12), European Commission, 2012[12], document prin care fiecare cetăţean european ce se simte ofensat de anumite materiale pe internet legate de persoana acestuia, poate cere retragerea lor. Dar mai important de atât este "Codul UE al drepturilor în mediul online", în care Secţiunea 1, Capitolul 4(1), prevede: "Orice persoană fizică are dreptul la protecţia adecvată a datelor sale cu caracter personal.[13]" şi de asemenea paragraful 2: "Persoanele fizice au dreptul să primească de la persoanele şi întreprinderile care deţin o parte din datele lor cu caracter personal în evidente cum ar fi site-uri web, baze de date, furnizori de servicii, etc, precum şi să corecteze sau să şteargă datele respective dacă sunt incomplete sau inexacte"[14]. Prin urmare serviciile secrete ale statelor membre joacă un rol esenţial în menţinerea unui echilibru între drepturile cetăţeneşti şi menţinerea securităţii naţionale şi protejarea intereselor guvernamentale[15]. Ameninţările cibernetice fiind mai numeroase pe fiecare zi, din acest motiv se urmăreşte dezvoltarea unui sistem cât mai bun şi destinat să satisfacă necesităţile naţionale şi individuale.

În afară de viziunea generală asupra nerespectării drepturilor online de către autorităţile naţionale, doresc să aduc în discuţie şi problema hackerilor ce reprezintă o ameninţare pentru informaţiile personale, cât şi celor financiare. Doar pentru anul 2014 una dintre cele mai reprezentative ameninţări era virusul "Heartbleed", cunoscut pentru infiltrarea în site-urile de socializare, precum: Facebook, Instagram, Pinterest, Tumblr, Google şi Yahoo[16]. Recomandarea acestor companii după atac a fost de a ne schimba cât mai urgent parolele conturilor noastre şi nu s-au oprit doar la atât, au luat iniţiativa formării unui program comun de apărare împotriva viitoarelor ameninţări, fiecare alocând o sumă de 100000 $ anual[17].

Rezultatul cercetării analizând cazurile expuse mai sus am ajuns la trei rezultate distincte în care voi încadra statele după politica naţională faţă de libertatea pe care o oferă pe internet: internet liber, internet semi-liber şi internet cenzurat. Doresc să fac o observaţia asupra primei categorii, a internetului liber, care nu numai că este garantat de legislaţie, dar se şi promovează în mod activ această idee. Discutând mai departe despre internetul semi-liber, unde Guvernul intervine şi supraveghează intens activitatea cetăţenilor săi, sfidând drepturile umane. Internetul cu libertate limitată sau cenzurat, defineşte statele cu o politică naţională autoritară, caracterizată prin controlul total al accesului la internet, unde drepturile la

[12]http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Factsheet data protection, accesat la data de: 21.03.2015

[13]https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20RO%20final.pdf, Codul UE al drepturilor in mediul online, accesat la data de: 24.04.2015

[14]https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20RO%20final.pdf, Codul UE al drepturilor in mediul online, accesat la data de: 24.04.2015

[15]Tom DYSON, Theodore KONSTADINIDES, *Europe Defense Cooperation in EU law and IR theory*, Palgrave Macmillan, Hampshire, 2013, p. 19

[16]Office of the Privacy Commissioner of Canada, *Privacy and Cybersecurity: Emphasizing privacy protection in cyber security activities*, 2015, p. 1

[17] http://mashable.com/2014/04/24/facebook-google-microsoft-join-forces-to-prevent-another-heartbleed/, Facebook, Google, Microsoft Join Forces to Prevent Another Heartbleed, accesat la data de: 23.04.2015

confidenţialitate online nu există. Am încadrat în prima categorie a internetului liber statele Uniunii Europene, de asemenea Statele Unite ale Americii le-am catalogat în cea de-a doua categorie a internetului semi-liber, iar China face parte din a treia categorie a internetului cenzurat.

2. Războiul cibernetic

Termenului "Război cibernetic" nu-i putem oferi o definiţie concretă, fiind foarte controversat la nivelul comunităţii internaţionale. Resursa principală a acestui război este însuşi informaţia, iar prin specularea atentă a acesteia daunele obţinute sunt variate, de la manipularea populaţiei şi împingerea spre revolta până la daune de milioane de dolari. La acest capitol doresc să amintesc şi conceptele de "cyber spionaj" şi "cyber terrorism". Definim termenul de spionaj cibernetic pătrunderea în mod fraudulos în bazele de informaţiilor private sau guvernamentale şi transferul acestora fără acordul proprietarului. Al doilea concept al terorismului cibernetic se referă la atacurile asupra aparaturii hardware şi software prin intermediul internetului având ca scop provocarea daunelor ireparabile.

În continuare vom cerceta modificările relaţiilor bilaterale şi multilaterale dintre state ca urmare a intensificării războiului cibernetic. Încă din 27 aprilie 2007, moment în care Rusia a atacat site-urile oficiale ale Estoniei, producând mari pagube pentru guvernul de la Tallinn, demonstrând astfel forţelor NATO existenţa unei noi arme în relaţiile internaţionale[18]. De menţionat este şi războiul ruso-georgian, moment în care Rusia a atacat toate site-urile Georgiei arătându-i incapacitatea de apărare cibernetică. Fiecare stat al lumii îşi ia propriile măsuri pentru pregătirea unei apărării cibernetice ce va corespunde mediului politic intern. Dintre cele mai relevante exemple în acest sens este Marea Britanie, care anunţa public că ameninţările prin intermediul internetului sunt unele reale. O măsura luată de către Guvernul conservator, este lansarea unei campanii de recrutare a experţilor în IT, pentru crearea unei echipe de combatere a ameninţărilor iniţiate de Ministerul Apărării[19]. Letonia este un alt stat european ce a observat că securitatea mediului virtual este foarte importantă, motiv pentru care a început recrutarea unei echipe de contracarare a ameninţărilor internaţionale[20]. Experţii explică faptul că spre deosebire de un adversar real, în mediul online adversarul poate venii de oriunde din lume, chiar şi din interiorul statului, din partea unui stat aliat sau inamic. Austria, primul stat ce nu este membru NATO, a luat decizia de a se alătura Alianţei Centrului de Excelentă a Securităţii Cibernetice[21]. Ministerul Apărării din Japonia, a luat iniţiativa înfiinţări unei echipe de de aproximativ 90 de persoane, sub denumirea de Unitatea de Securitate Cibernetică, pentru protejarea intereselor naţionale în mediul virtual[22]. Sub conducerea lui Obama, bugetul pentru apărare cibernetică a SUA a crescut de-a lungul timpului, dorind o focalizare mai mare pe combaterea atacurilor cu care se confrunta ţară.

Situaţia internaţională actuală de ne demonstrează un singur lucru: tendinţa de multipolaritate, spre deosebire de secolul trecut, unde lumea era împărţită în sfere de influenţa bipolare. După cum observăm, este abordata o perspectivă diferită, dar toate acestea au în comun un singur lucru: combaterea ameninţărilor de către Guvern prin recrutarea personalului

[18]http://www.theguardian.com/world/2007/may/17/topstories3.russia, Russia accused of unleashing cyberwar to disable Estonia, accesat la data de: 21.03.2015
[19]http://www.bbc.com/news/uk-24321717, UK creates a new cyber defense force, accesat la data de: 21.03.2015
[20]http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936, Latvia launches cyber defense unit to beef up online security, accesat la data de: 21.03.2015
[21]http://www.defensenews.com/article/20140512/DEFREG01/305120014/Austria-First-non-NATO-Nation-Join-Alliance-Cyber-Defence-Centre-Excellence, Austria first non-NATO nation join Alliance cyber defense center, accesat la data de: 21.03.2015
[22]http://www.janes.com/article/35956/japan-establishes-cyber-defence-unit, Japan establishes cyber defense unit, accesat la data de: 21.03.2015

specializat al unui nou tip de război. Tratatele multilaterale, pe baza compromisurilor au potenţialul de a da naştere unor proiecte eficiente în securitatea cibernetică, cum am amintit mai sus despre Alianţa Centrului de Excelentă a Securităţii Cibernetice.

Raportul financiar al World Economic Forum din 2014 demonstrează clar şi dă un semnal de alarmă asupra problemei de eficientă a unui sistem de apărare cibernetic eficient va aduce pierderi internaţionale de aproximativ 3 miliarde până în anul 2020[23]. Descendenţa din ce în ce mai mare de datele obţinute pe cale digitală le transformă în ţinte vitale pentru agresori ce doresc să interfereze cu sistemele guvernamentale şi internaţionale. De aici putem deduce, că ţintele vizate de către agresori cu cât au un sistem de apărare mai slab, cu atât sunt mai uşor de atacat. După cum aminteşte şi James B. Comey în discursul sau de Conferinţă Internaţională pe Cyberdefence de la Forham University din New York, 2015: "viaţa noastră s-a schimbat radical datorită internetului, iar tot ce reprezintă o ameninţare a evoluat"[24].

Consecinţele unui sistem de apărare cibernetic statal ineficient, pot fi închiderea site-urilor, furtul de informaţii, spionaj, însă între numeroasele ameninţări cu care se confrunta cetăţenii, precum şi instituţiile publice în fiecare zi pe internet, putem amintii de viruşi, iar cel mai cunoscut dintre aceştia este Stuxnet, preconceput pentru a distruge sistemele industriale. Prezenţa sa a fost confirmată atât în SUA, Europa, cât şi Asia, în Iran atacând sistemele unei centrale nucleare, provocând daune uriaşe[25]. Cel de-al doilea caz este al virusului rusesc Rocra, cel ce ani de zile a furat informaţii guvernamentale de la statele ce nu l-au detectat[26]. Sesizările zilnice asupra ameninţărilor în acest domeniu, sunt disponibile în raportul de date ale Centrului Strategic şi Studiilor Internaţionale, urmărindu-se criminalitatea online cu mare atenţie[27]. Observăm din aceste exemple de ce este necesară şi prioritara adaptarea unei strategii de apărare cibernetică.

Tendinţa individualistă a statelor faţă de problema conflictului cibernetic ne demonstrează metoda compromisului naţional între sfera publică şi cea privată pentru obţinerea celor mai bune rezultate în materie de securitate. Că observaţie asupra diplomaţiei între state, în opinia noastră acestea confirma teoria realismului în cadrul relaţiilor internaţionale, unde statele acţionează în scopul atingerii intereselor statale. Vulnerabilităţile sistemului de apărare duce la compromiterea informaţiilor aflate în patrimoniu, pagubele rezultate fiind uriaşe. Ameninţările cibernetice sunt din ce în ce mai numeroase cu fiecare zi, din acest motiv bugetul alocat de către statele lumii pentru îmbunătăţirea securităţii cibernetice este în creştere de la an la an, direct proporţional cu ameninţările cu care se confruntă.

Concluzii

Am urmărit cu atenţie efectele implicării tot mai activă a individului în viaţa politică şi observam schimbările pe care le-au adus într-un timp atât de scurt într-un domeniu atât de nou. Am parcurs cele două capitole ale lucrării căutând răspunsul la întrebarea de cercetare: "Cum putem combate terorismul cibernetic, şi în acelaşi timp, respecta confidenţialitatea şi libertatea indivizilor în mediul online, având în vedere că instituţiile acreditate pot face abuz de informaţiile particulare?". Am observat cum fiecare stat şi-a adaptat propria politică cu

[23]World Economic Forum, *Risk and responsibility in a Hyperconnected world*, 2014

[24]http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, International Conference on Cyber Security, Fordham University, accesat la data de: 23.04.2015

[25]http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, Stuxnet was far more dangerous than previous thought, accesat la data de: 21.03.2015

[26]http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html, Red October malware discovered after years of stealing data in the wild, accesat la data de: 21.03.2015

[27]http://csis.org/program/significant-cyber-events, Significant Cyber Events, accesat la data de: 23.04.2015

privire la subiectul aflat în discuţie, metoda fiind determinată de istoria şi experienţele internaţionale. În timp ce Rusia prefera o abordare agresivă în privinţa securităţii cibernetice, China urmăreşte impunerea cenzurii pentru un control cât mai mare asupra ameninţaţilor din interior şi exterior. Statele Unite ale Americii au o abordare intrusive în viaţa privată a cetăţenilor, pentru a avea un sistem cibernetic eficient. În schimb statele membre ale Uniunii Europene au avut o abordare asupra situaţiei într-un mod cât mai echilibrat, dorind să satisfacă ambele părţi.

Organizaţia Naţiunilor Unite joacă un rol important în definirea în viitorul apropiat a relaţiilor bilaterale şi a respectării drepturilor individuale pe internet, prin iniţiativă să. Cu toate acestea nu este suficient, este necesară o implicare mai mare a statelor puternice, cât şi a altor organizaţii internaţionale. Din studierea bibliografiei primare constituită de: tratate, legislaţie şi interviuri, am răspuns la întrebarea cercetării concluzionând că statele Uniunii Europene îndeplineşte ambele criterii atât al securităţii cibernetice cât şi al respectării drepturilor online. În cazul acesta se afirma ipoteza cercetării mele demonstrând existenţa unei zone a compromisului, simple şi eficiente. După rezultatele cercetării, în Capitolul 1 am catalogat statele în funcţie de drepturile cetăţeneşti oferite pe internet, Uniunea Europeană intrând în prima categorie, a internetului liber, SUA în categoria internetului semi-liber şi China ca făcând parte din a treia categorie, a internetului cenzurat. Colaborarea statelor şi a organizaţiilor internaţionale pentru dezvoltarea acestei strategii limitată, dar este interesantă de urmărit în prezent[28]. Iar motivul pentru care spun acest lucru este că posibilitatea declanşării unui război real prin intermediul internetului este o ameninţare ce trebuie luată în calcul. O altă perspectivă asupra domeniului acesta o conferă organizaţiile internaţionale de protecţie a drepturilor omului, care au criticat în nenumărate rânduri spionajul virtual[29]. Astfel subiectul poate avea mai multe moduri de interpretare în funcţie de actorul politic la nivel internaţional şi de interesele sale. Teoria realismului ne este confirmată din cercetarea efectuată în Capitolul 2, din care deducem necesitatea de adaptare fata de schimbările actuale prin acţiunile de creştere a securităţii, în detrimentul idealurilor internaţionale. Cu toate acestea, este necesară adaptarea societăţii noastre având în vedere schimbările ce se produc spre a contracara ameninţările iminente şi pentru a ne urmării interesele noastre în timp ce ne bucurăm de protecţia drepturilor fără să abuzăm de această libertate[30].

Domeniul securităţii cibernetice reprezintă pentru noi o nouă lume de explorare a diferitelor posibilităţi ce în urmă cu câţiva ani păreau imposibile de creat. Este necesară studierea domeniului aflat în discuţie, deoarece are un impact direct asupra noastră, a modului în care obţinem informaţii, cum învăţăm, modul de a comunica, etc. Noi metode sunt dezvoltate zilnic de fiecare actor politic internaţional, în scopul obţinerii unui avantaj fata de competitori. Informarea noastră este esenţială în cazul de faţă, iar realizarea articolelor şi conferinţelor pe această temă trebuie să fie prioritatea numărul unu.

[28]Daniel VENTRE, *Cyber Conflict: competing national perspectives*, ISTE Ltd, London, 2012 , p. 182
[29]Tom DYSON, Theodore KONSTADINIDES, *Europe Defence Cooperation in EU law and IR thory*, Palgrave Macmillan, Hampshire, 2013, p. 19
[30]Myriam Dunn CAVELTY, *Cyber-Security and threat politics: US efforts to secure the information age*, Routledge, New York, 2008, p. 27

BIBLIOGRAFIE:

1. ANDRESS, Janson, Steve WINTERFELD, *Cyber warfare: Techniques, Tactics and tools for security practitioners*, SYNGRESS, 2013

2. BAYLON Caroline, *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Chatham House, 2014

3. CAVELTY, Myriam Dunn, *Cyber-Security and threat politics: US efforts to secure the information age*, Routledge, New York, 2008

4. DEIBERT, Ronald, *Access controlled: The shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, Massachusetts, 2010

5. DYSON Tom, Theodore KONSTADINIDES, *Europe Defense Cooperation in EU law and IR theory*, Palgrave Macmillan, Hampshire, 2013

6. European Commission, Factsheet on the "Right to be forgotten" ruling (c-131/12), Bruxelles, 2012

7. KARATZOGIANNI, Athina, *Cyber conflict and global politics*, Routledge, New York, 2008

8. KLIMBURG, Alexander, *Naţional Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012

9. NORRIS Pippa, *Public Santinel: News Media & Government reform*, The World Bank, Washingston, 2010

10. Office of the Privacy Commissioner of Canada, *Privacy and Cybersecurity: Emphasizing privacy protection in cyber security activities*, 2015

11. SHACKELFORD, Scott J, *Managing Cyber Attacks in International Law, Business, and Relations: In search for cyber peace*, Cambridge University Press, Cambridge, 2014

12. VENTRE Daniel, Cyber Conflict: competing national perspectives, ISTE Ltd, London, 2012

13. World Economic Forum, Risk and responsibility in a Hyperconnected world, 2014

14. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280, Rezolutia privind drepturile omului pe internet, A/HRC/17/27, 2011

15. https://freedomhouse.org/country/china#.VIiPmXuPVoM, Freedom House China

16. http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?_r=0, China toughens restrictions on internet use

17. http://www.huffingtonpost.com/2012/02/29/china-firewall-breach_n_1308836.html?, China firewall breach

18. https://freedomhouse.org/country/united-states#.VRaVH-G1doM, Freedomhouse SUA

19. http://www.spiegel.de/international/topic/nsa_spying_scandal/, NSA spying scandal

20. http://www.theguardian.com/world/2007/may/17/topstories3.russia, Russia accused of unleashing cyberwar to disable Estonia

21. http://www.bbc.com/news/uk-24321717, UK creates a new cyber defense force

22. http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936, Latvia launches cyber defense unit to beef up online security

23. http://www.defensenews.com/article/20140512/DEFREG01/305120014/Austria-First-non-NATO-Nation-Join-Alliance-Cyber-Defence-Centre-Excellence, Austria first non-NATO nation join Alliance cyber defense center

24. http://www.janes.com/article/35956/japan-establishes-cyber-defence-unit, Japan establishes cyber defense unit

25. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, Stuxnet was far more dangerous than previous thought
26. http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, International Conference on Cyber Security, Fordham University
27. http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html, Red October malware discovered after years of stealing data in the wild
28. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Factsheet data protection

SUNT FORŢELE AERIENE ALE ROMÂNIEI PREGĂTITE PENTRU A RĂSPUNDE AMENINŢĂRILOR VIITORULUI?

Cosmin Liviu COSMA
Căpitan comandor, Doctorand, Universitatea Naţională de Apărare "CAROL I",
e-mail: airspider@yahoo.com

Rezumat: *Alături de fragmentare, impredictibilitate, asimetrii multiple, crimă organizată şi terorism, provocările recente la adresa securităţii impun a reevaluare atentă a naturii ameninţărilor, implicaţiile fiind multiple în modul în care viitoarele forţe militare ale Alianţei vor fi obligate să se pregătească şi să acţioneze.*

În acest context, ca parte integrantă a Alianţei, România şi implicit forţele sale aeriene – pentru îndeplinirea unor obiective ca asigurarea securităţii României şi a spaţiului nord atlantic, respectarea angajamentelor asumate în cadrul organizaţiilor de securitate etc. – sunt obligate să continue procesele de modernizare, impunându-se o continuă şi de substanţă transformare la nivel conceptual, organizaţional-structural şi în cel al infrastructurii şi înzestrării.

Pornind de la aceste considerente, lucrarea de faţă îşi propune identificarea caracteristicilor contextului în care forţele aeriene vor fi nevoite să acţioneze, respectiv a implicaţiilor asociate, pentru ca pe baza acestora să poată fi stabilite capacităţile şi atributele operaţionale care trebuie generate pentru a permite instrumentului aerian să răspundă ameninţărilor prezente şi celor prefigurate. În vederea formulării unor concluzii a fost utilizată metoda deductivă, iar în încercarea de extrapolare a experienţei trecute în cea viitoare s-a recurs la metoda inductivă. Pentru stabilirea unei legături sistemice între explicaţii, cadre conceptuale şi predicţii a fost utilizată o combinaţie între sistemele teoretice şi toxonomii, respectiv teoriile axiomatice pentru prezentarea raporturilor de cauzalitate între factorii externi şi organizaţia militară (forţele aeriene).

Cuvinte cheie: *transformare, forţele aeriene române, ameninţări viitoare, NATO*

1. Evoluţia forţelor aeriene române după sfârşitul Războiului Rece

Încheierea Războiului Rece şi respectiv desfiinţarea Tratatului de la Varşovia în iulie 1991 au determinat profunde schimbări asupra arhitecturii mediului de securitate, determinând adoptarea de către România a unei politici de securitate bazate pe teoria apărării circulare, acoperirea şi protejarea frontierelor. Forţele aeriene, parte integrantă de bază a Armatei României, odată cu schimbarea paradigmei de securitate vor intra într-un proces consistent de reformare, restructurare pentru a răspunde noii realităţi geostrategice. Doctrina *războiului întregului popor* care fundamenta strategiile de apărare militară până în 1991 este uitată, fiind stabilit ca *obiectiv general* al transformării Armatei României *"realizarea unei structuri moderne, complet profesionalizate, cu grad sporit de mobilitate, eficientă, flexibilă, cu capacitate de dislocare mărită, sustenabilă, având capacitatea de a acţiona întrunit şi a fi angajată într-un larg spectru de misiuni, atât pe teritoriul naţional, cât şi în afara acestuia"*[1].

Acest obiectiv formulat imediat după desfiinţarea Tratatului de la Varşovia poate părea destul de ambiţios, considerând situaţia concretă a forţelor aeriene române existentă

[1] Mihail E. Ionescu, *Etapele reformei armate în perioada post-Război Rece* (1990-2008), în *Reforma Militară şi societatea în România (1878-2008)*, Editura Militară, Bucureşti, 2009, p.325.

înainte de 1990. Acestea aveau un efectiv de 32,000 oameni, din care mai puţin de o treime era personal angajat civil, deţinând un număr de aproximativ 512 avioane de luptă al căror rol principal era de a spijini şi proteja forţele terestre şi navale prin executarea unor misiuni de acoperire aeriană, bombardament, recunoaştere şi transport aerian. Structura acestora era construită în jurul a trei divizii tactice, fiecare având în compunere două regimente cu câte trei escadrile de vânătoare-interceptare şi una de atac la sol.

Avioanele de luptă din înzestrare erau preponderant de provenienţă sovietică (MiG-21, MiG-23), dar şi un număr semnificativ de IAR-93 construite în România. Începând cu decembrie 1989 ajung în ţară primele MiG-29 Fulcrum, la Baza 57 Aeriană de la Mihail Kogălniceanu, zborul de instrucţie începând din martie 1990 (iniţial au fost livrate 14 MiG-29A simplă comandă şi 4 MiG-29UB dublă comandă, iar apoi alte 2 MiG-29A, respectiv 1 MiG-29C în 1992 de la Forţele aeriene ale Republicii Moldova). Avioanele MiG-29 au rămas în dotarea forţelor aeriene până la începutul anului 2003, când au fost retrase din activitate.

Alături de aceste demersuri, se iau măsuri privind punerea în aplicare a prevederilor Tratatului de la Paris cu privire la Forţele Armate Convenţionale în Europa semnat de ţările Tratatului de la Varşovia şi NATO la 19 noiembrie 1990, intrat în vigoare la 9 noiembrie 1992. Astfel, armata română a redus efectivele de tehnică militară, atât la nivelul forţelor terestre (tancuri, vehicule blindate, piese de artilerie), cât şi la cel al aviaţiei militare (avioane de luptă – de la 512 la 430). Este declanşat şi un proces de reducere a efectivelor de personal, urmărindu-se ajungerea la un efectiv de 70,000 militari şi 10,000 civili la nivelul Armatei României. Au loc şi reorganizări la nivelul structurii de forţe, înfiinţându-se Statul Major General (în locul Marelui Stat Major), respectiv statele majore ale categoriilor de forţe, renunţându-se la eşaloanele tip divizie şi regiment, în favoarea structurilor de tip corp de armată şi regiment, şi reducând numărul de armate de la patru la trei.[2] La nivelul forţelor aeriene, în 1993 este înfiinţat *Statul Major al Aviaţiei Militare*, prin unificarea dintre *Comandamentul Aviaţiei Militare şi Comandamentul Apărării Antiaeriene a Teritoritoriului*, noua structură de comandă reunind astfel *aviaţia, artileria, rachetele antiaeriene* şi *radiolocaţia* (începând cu 1 iunie 2000, va fi folosită denumirea actuală, *Statul Major al Forţelor Aeriene*). În 1995 sistemul regimental de tip communist este schimbat într-unul bazat pe o structură constituită din baze aeriene, grupuri şi escadrile.

Această primă etapă de reformare a forţelor armate române şi implicit a forţelor aeriene este caracterizată de un ritm redus, *"desfăşurată într-o concepţie inerţială doctrinar, centrată pe apărarea teritorială"*[3]. Astfel, procesele de adaptare din cadrul forţelor aeriene sunt aliniate direcţiei generale *de acoperire a teritoriului* din punct de vedere militar şi dislocarea precumpănitor spre frontiere. Această adoptare de poziţie este justificată de un complex de factori cu implicaţii directe în situaţia geostrategică regională din imediata vecinătate a României (disoluţia URSS, dezintegrarea Iugoslaviei şi războiul de pe Nistru din 1992, indecizia NATO privind extinderea către est, răbufnirile naţionaliste din exterior etc.).

La nivelul înzestrării, în prima parte a anilor 1990 se iau o serie de decizii în vederea modernizării unor platforme şi sisteme de arme aflate în inventarul forţelor aeriene, respectiv derularea unor programe de achiziţii. Astfel, în 1992, în urma unui concurs privind selecţia unei companii care să modernizeze avionul MiG-21, este aleasă firma israeliană Elbit, cu care este semnat un contract în valoare de 300 mil.USD, reprezentând contravaloarea conversiei unui număr de aproximativ 110 avioane MiG-21 (UM, M şi MF) în 75 LanceR-A aer-sol (livrate 71 la final), 25 Lancer-C aer-aer (livrate 26 în final) şi 10 Lancer-B dublă comandă (într-un final sunt livrate 14 LanceR-B). Prototipul MiG-21 LanceR-A zboară pentru prima

---

[2] Călin Hentea, *Armata şi luptele românilor din Antichitate până la intrarea în NATO, Breviar de istorie militară*, Editura Nemira, Bucureşti, 2002, p.257.

[3] Mihail E. Ionescu, *Etapele reformei armate în perioada post-Război Rece* (1990-2008), p. 327.

data în 22 august 1995, LanceR-B în 6 mai 1996, iar prototipul versiunii aer-aer, LanceR-C în data de 6 noiembrie 1996. Programul presupune integrarea pe structura existenă a avionului MiG-21 un număr de sisteme de avionică, navigaţie, comunicaţii, radiolocaţie şi armament, iar la sol a unor sisteme de pregătire/ analiză a misiunii etc, care să permită executarea unor misiuni de natură nouă, într-o manieră diferită. Toate sistemele nou integrate sunt la nivelul standardelor NATO, ceea ce va permite în perioada imediat următoare executarea unui număr semnificativ de exerciţii în comun cu partenerii internaţionali şi culminând cu executarea primei misiuni de luptă (pe timp de pace) după cel de-al doilea Război Mondial de către forţele aeriene române, *Baltica 2007* (misiune de poliţie aeriană în Lituania, Letonia şi Estonia, executată de către piloţii Bazei 71 Aeriană Câmpia Turzii).

Alte programe de modernizare sunt derulate pentru avionul IAR-99 şi elicopterul IAR-330, în vederea integrării unor sisteme avansate de avionică, navigaţie, comunicaţii şi armament etc, pentru atingerea unui grad de compatibilitate (ca şi în cazul MiG-21) şi a unor performanţe care să le ofere interoperabilitatea necesară desfăşurării operaţiilor în comun cu partenerii NATO.

În 23 octombrie 1996 intră în dotarea Bazei 90 Aeriană Otopeni primele două avioane C-130B Hercules (următoarele două în 16 februarie 1997), iar în 14 februarie 2007, ultimul Hercules, un C-130H (cumpărat de la Forţele Aeriene Italiene în iunie 2004 şi apoi trimis pentru executarea unor lucrări de mentenanţă şi modernizare la Centrul Logistic Lockheed Martin din Greenville, Carolina de Sud). Achiziţia acestor aeronave a permis forţelor aeriene române dezvoltarea unei capacităţi de transport aerian strategic, reprezentând o contribuţie importantă a României la efortul NATO în diferitele teatre de operaţii.

Un alt program major de înzestrare a forţelor aeriene ale României este demarat prin semnarea în decembrie 2007 a unui acord între Ministerul Apărării Naţionale şi compania italiană Alenia Aeronautica SpA privind achiziţia unui număr de şapte aeronave C-27J Spartan. Primele aeronave sunt livrate începând cu 2010, iar în ianuarie 2015 aterizează la Baza Aeriană de la Otopeni cel de-al şaptelea şi ultimul C-27J Spartan contractat. Prin achiziţia avioanelor C-27J Spartan, forţele aeriene române devin posesoarele unor platforme de ultimă generaţie, destinate transportului aerien tactic direct în teatru, în cadrul operaţiilor de menţinere a păcii sau a celor umanitare, indiferent de condiţiile meteorologice, ziua şi noaptea.

Începând cu anul 2000, o serie de programe de restructurare sunt desfăşurate la nivelul forţelor aeriene, pentru ca în 2004 România să deţină doar cinci baze aeriene active, dispuse la Câmpia Turzii, Borcea-Feteşti, Bucureşti-Otopeni, Bacău şi Boboc, plus alte două baze de rezervă destinate elicopterelor (Mihail Kogălniceanu şi Timişoara-Giarmata). Au fost desfiinţate Baza Aeriană 91 de la Caracal-Deveselu la începutul anului 2002, Baza Aeriană 93 de la Timişoara-Giarmata în august 2004, Baza Aeriană 61 Titu-Boteni în octombrie 2004, Baza 57 Aeriană Mihail Kogălniceanu.

La nivelul celorlalte categorii de forţe din cadrul forţelor aeriene – *radiolocaţia şi apărarea antiaeriană* –, în vederea aderării la structurile Alianţei Nord-Atlantice, în perioada 1998-2003, au loc procese similare de reformă şi restructurare. Astfel, în 1998 sunt desfiinţate cele două brigăzi radiotehnice (Brigada Radiotehnică 46 de la Ploieşti şi Brigada 41 Radiotehnică de la Timişoara, înfiinţate în 1965, respectiv în 1966 cea de a doua), fiind implementată o nouă structură – Centrul de Radiolocaţie – similară regimentului organizat pe batalioane şi companii de radiolocaţie. Scopul acestei reorganizări a vizat *"creşterea operativităţii, supleţei şi eficienţei actului de decizie, optimizarea fluxului informational despre situaţia aeriană şi crearea condiţiilor pentru realizarea sistemului integrat military şi*

civil de gestionare a spaţiului aerian"[4]. Structura organizaţională nou creată – pentru a atinge gradul de compatibilitate necesar operării în cadrul *Sistemului Integrat de Apărare Aeriană şi Antirachetă al NATO – NATINAMDS (NATO Integrated Air and Missile Defense System)* – a cunoscut transformări majore şi la nivelul înzestrării, prin introducerea în dotarea subunităţilor de radiolocaţie a sistemelor radar modulare tridimensionale (3D) cu rază lungă de acţiune *FPS/117E(T)* şi a celor cu rază mica de acţiune *Gap Filler*, respectiv prin operaţionalizarea *Centrului de Operaţii pentru Suveranitate Aeriană (ASOC).*

Parte integrantă a sistemului de apărare antiaeriană, unităţile de rachete sol aer cunosc şi acestea restructurări şi transformări privind achiziţiile şi înzestrarea. În 1995 – în cadrul Comandamentul Apărării Antiaeriene a Teritoriului –, Brigada 1 Rachete Antiaeriene, prin luarea în subordine a 4 Divizioane de rachete antiaeriene şi a unui Divizion Tehnic Neva, devine Brigada 1 Rachete Antiaeriene Mixtă, subordonată Corpului 1 Aviaţie şi Apărare Antiaeriană. La 1 septemebrie 2001 va primi denumirea de Brigada 1 Rachete Sol-Aer, iar la 1 mai 2006 se înfiinţează în cadrul acesteia *Batalionul Hawk*, aceasta constituind prima unitate de rachete sol-aer din Statul Major al Forţelor Aeriene înzestrată cu tehnică de luptă compatibilă cu sitemele de rachete sol-aer NATO. *Sistemul Hawk* este destinat asigurării apărării aeriene cu baza la sol a unor obiective importante împotriva atacurilor cu avioane pilotate şi fără pilot, a atacului cu rachete de croazieră şi alte vehicule aeriene ce evoluează la înălţimi mici şi medii.

Pe fondul unor deziderate clar expuse de aderare la structurile euro-atlantice, imediat după 1990, sunt demarate procese ample pentru crearea un nou cadru legislativ în vederea realizării structurii organizatorice şi a cadrului normativ care să răspundă principiilor de funcţionare ale armatei într-un stat democrat, cu influenţă directă asupra tuturor categoriilor de forţe şi servicii. Astfel, în direcţia compatibilizării dispoziţiilor Constituţiei României din anul 1991 cu prevederile Articolului 5 din Tratatul Atlanticului de Nord, s-a urmărit amendarea Constituţiei în sensul consacrării constituţionale a aderării României la NATO şi asigurarea unui cadru constituţional pentru modificările viitoare ale legislaţiei privind apărarea naţională.

În această direcţie, prin republicarea Constituţiei României în 2003, este creat cadrul adoptării *Legii nr. 22/2004* pentru aderarea României la Tratatul Atlanticului de Nord, semnat la 4 aprilie 1949. Modificări suferă şi *Legea nr. 80/1995* privind statutul cadrelor militare, respectiv *Legea nr. 384/2006* privind statutul soldaţilor şi gradaţilor profesionişti. Pentru definirea, îndeplinirea obiectivelor securităţii naţionale a României în domeniul apărării este adoptată *Legea nr. 473/2004* privind planificarea apărării, în conformitate cu prevederile acesteia fiind elaborate documentele de planificare a apărării: *(1) Strategia Naţională de apărare; (2) Programul de guvernare; (3) Carta albă a apărării; (4) Strategia militară; (5) Directiva de planificare a apărării; şi (6) Programele majore şi Planurile operaţionale de întrebuinţare a forţelor.*[5]

În 1993 România îşi depune oficial canditatura în vederea aderării la NATO, iar un an mai târziu devine primul stat care răspunde invitaţiei de a participa *la Parteneriatul pentru Pace (PfP),* fiind primul stat din Europa Centrală şi de Est care aderă la PfP. În vederea admiterii de noi membri, NATO lansează în aprilie 1999 *Planul de Acţiune (MAP – Membership Action Plan),* care stabilea obiective, măsuri şi termene de realizare în vederea aderării la Alianţa Nord-Atlantică. Respectând prevederile acestuia, România pregăteşte şi prezintă propriul Plan Naţional de pregătire pentru Aderare.

---

[4] Aurelian Halus, *75 ani de radiolocaţie în Armata română* în *Observatorul Militar* nr.8 (1254), 26 februarie – 4 martie 2014, p. 16.

[5] Ministerul Apărării Naţionale, *România-NATO, Primii zece ani*, Bucureşti, 2014, p.4.

La 21 noiembrie 2002, în cadrul Summit-ului de la Praga – pe baza evaluării progreselor înregistrate de statele candidate, şefii de state şi de guverne ai ţărilor membre NATO au decis invitarea României să înceapă convorbirile în vederea aderării la Alianţa Nord-Atlantică. Alături de România mai sunt invitate la discuţii Bulgaria, Estonia, Letonia, Lituania, Slovacia şi Slovenia.

Protocolul de aderare este semnat la Bruxelles la 26 martie 2003, iar la 29 martie 2004 România devine stat membru cu drepturi depline al NATO, în urma depunerii instrumentelor de ratificare la Departamentul de Stat al SUA, ceea ce va constitui iniţierea unui proces susţinut de transformare al Armatei României în vederea *"lărgirii gamei de obiective şi procese pentru a include structurarea şi pregătirea forţelor pentru participarea la apărarea colectivă, îmbunătăţirea capacităţilor pentru întreaga gamă de operaţii de management al crizelor şi a celor pentru operaţii multinaţionale de combatere a terorismului"*[6].

Implicaţiile transformării la adresa forţelor aeriene române vor fi multiple – fiind vizate nivelul conceptual, organizaţional, precum şi cel funcţional-acţional şi al infrastructurii –, cu manifestări directe asupra doctrinelor, structurii de forţe, instrucţiei şi operaţiilor, respectiv tehnologiilor şi armamentelor.

2. Aspecte privind transformarea forţelor aeriene române în contextul noii paradigme de securitate

De la sfârşitul Războiului Rece, cu preponderenţă în perioada parcursă de la acceptarea ca membru al Alianţei Nord-Atlantice a României, forţele aeriene – alături de celelalte categorii de arme ale Armatei – au fost supuse unor procese de substanţă în vederea transformării acestora în structuri de forţe moderne, de dimensiuni reduse, foarte specializate, echipate adecvat, cu capacitate mărită de dislocare şi proiecţie în teatru, interoperabile, cu capacitate de autosusţinere şi de protecţie multidimensională, cu o conducere flexibilă[7], pentru a a-şi putea îndeplini responsabilităţile privind apărarea naţională, dar şi pentru a fi în măsură să răspundă într-o manieră întrunită şi multinaţională în cadrul Alianţei ameninţărilor actuale şi viitoare specifice unui mediu de securitate deosebit de complex, *"cu o evoluţie dificil de estimat şi gestionat datorită volumului mare de date şi a gradului ridicat de impredictibilitate"*[8].

Corelaţia transformării Armatei României cu procesul de transformare al Alianţei a oferit cadrul de manifestare al acestei metamorfozări, ca urmare a reconsiderării modalităţilor de răspuns de către NATO, de la unele specifice unei organizaţii rigide, aflată într-o postură pur defensivă, la cele ale organizaţiei de astăzi, implicată în operaţiuni militare desfăşurate în afara zonei de responsabilitate tradiţională, oriunde interesele Alianţei solicită acest lucru. În acest context, noile orientări strategice şi de transformare a NATO direcţionează procesul de transformare al viitoarelor structuri de forţe ale României, urmărindu-se generarea acelor capacităţi militare care să le permită să acţioneze atât împotriva ameninţărilor convenţionale cât şi a celor asimetrice, prin executarea întregii game de misiuni, de la prevenirea crizelor până la operaţii umanitare şi războiul de mare intensitate.

Transformarea la nivelul conceptelor presupune dezvoltarea şi experimentarea unor abordări noi privind modul de desfăşurare a războiului, a capacităţilor şi conceptelor operaţionale, respectiv a construcţiilor organizaţionale prin intermediul simulărilor şi exerciţiilor desfăşurate într-o manieră concepută pe baza provocărilor şi oportunităţilor emergente. Rezultatele acestui proces de evaluare prin simulare sunt destinate rafinării şi

---

[6] Ministerul Apărării Naţionale, *Strategia de transformare a Armatei României*, Bucureşti, 2007, p.3.
[7] Ibidem.
[8] Mihail Orzeaţă, *Războiul Continuu*, Editura Militară, Bucureşti, 2011, p.25.

ajustării noilor concepte, pentru ca apoi, prin utilizarea unor mecanisme puternice de implementare, să poată fi implementate în dezvoltarea capacităţilor operaţionale militare *transformaţionale* vizate.[9]

Astfel, o serie de teorii au fost dezvoltate – având la bază factorii de natură internă ai organizaţiei militare, factorii contextuali ai mediului de securitate, respectiv rolul integrării noilor tehnologii –, menite să ofere cadrul necesar dezvoltării unor capacităţi militare adecvate şi relevante contextului actual şi viitor de securitate. Generarea capacităţilor este un proces construit în jurul unor funcţiuni distincte, aflate în interdependenţă, alături de *concepte* aflându-se *factorul uman, mijloacele materiale şi instrucţia*[10]. Importanţa transformării la nivelul conceptual rezidă din rolul determinant manifestat în generarea capacităţilor operaţionale, actualizarea conceptelor actuale, respectiv dezvoltarea unor noi concepte impunându-se din perspectiva funcţiilor combative, înţelese ca o fuziune a factorului uman, armamentului, sistemelor de arme şi muniţiei, infrastructurii, ideilor, abilităţilor şi a echipamentului.

Conform teoriilor Departamentului Apărării al SUA privind procesul transformării militare, dezvoltarea unor concepte novatoare – care să satisfacă cerinţele strategiilor de transformare – reprezintă facilitatorul cel mai important pentru construirea capacităţilor militare transformaţionale (implicând tehnologia, procesele, organizaţia şi factorul uman[11]).

Din perspectiva transformării conceptuale a forţelor aeriene ale României, în vederea oferirii orientărilor cadru necesare planificării şi conducerii operaţiilor aeriene, în 2000 este elaborată *Doctrina forţelor aeriene*, iar apoi în 2005 revizuită şi redenumită *Doctrina pentru Operaţii a forţelor aeriene (DOFA)*. Menită să stabilească ansamblul principiilor care orientează întrebuinţarea forţelor aeriene în toate tipurile de operaţii executate pentru îndeplinirea obiectivelor ce le revin în timp de pace, în situaţii de criză şi la război, DOFA este un document ce are la bază studiul doctrinelor naţionale de ordin superior şi al doctrinelor NATO, respectiv ale unor ţări membre NATO, precum şi analiza experienţei rezultate din desfăşurarea exerciţiilor naţionale şi multinaţionale şi a acţiunilor militare ale forţelor aeriene ale statelor care au participat la diferite conflicte în ultimele decenii.

Ca urmare a diversificării şi amplificării riscurilor de natură asimetrică, a manifestării unor fenomene de instabilitate şi criză, respectiv a menţinerii unor focare de tensiune tradiţionale şi a exprimării unor tendinţe de reproiectare geopolitică a unor zone (Asia Centrală, Zona Caucaziano-Caspică, Orientul Mijlociu Extins, Africa etc.[12]) – pe fondul sporirii rolului comunităţii internaţionale şi a unor organizaţii specializate în soluţionarea şi gestionarea crizelor – în cadrul NATO sunt derulate procese pentru *"creşterea capacităţii de intervenţie în situaţii de criză şi a posibilităţilor de proiectare a forţei în spaţiile de interes, concomitent cu continuarea procesului de transformare a mecanismelor, structurilor şi a procedurilor de luare a deciziilor"*[13].

Adoptarea acestei *abordări cuprinzătoare* de către Alianţa Nord-Atlantică a determinat alinierea conceptuală a Armatei României în vederea construirii cadrului necesar dezvoltării unor structuri de forţe apte să participe la întreaga gama de misiuni, de la cele de prevenire a crizelor până la operaţiile umanitare şi conflictele de mare intensitate. În acest context, în 2007 este elaborată *Strategia de transformare a Armatei României*, reprezentând viziunea militară consolidată asupra viitoarelor structuri de forţe şi capacităţi operaţionale, necesare

---

[9] US DoD, Office of the Secretary of Defense, *Military Transformation – A Strategic Approach*, Director, Force Transformation, Pentagon, Washington, US p.3.

[10] Christopher Ankersen, *Capabilities and Capacities* în *Transforming National Defense Administration,* School of Policy Studies, Queen's University Kingston, Ontario, Canada, 2005, p.13.

[11] Ibidem.

[12] MApN, *Strategia de transformare a Armatei României*, p.3.

[13] Ibidem.

îndeplinirii misiunilor într-o formă întrunită şi multinaţională în cadrul NATO sau a unor alianţe cu partenerii. Practic, este momentul în care în lexiconul militar asociat fenomenelor de reformare, restructurare, înnoire, modernizare etc. a Armatei României apare şi conceptul de *transformare militară*, cu toate implicaţiile terminologice şi procesuale aferente, determinând o mai bună permeabilizare a cadrului conceptual al Alianţei (din care s-a dezvoltat şi evoluat cel al României şi al altor state membre), respectiv facilitând transferul de idei, precepte etc.

Strategia de transformare a Armatei României, în contextul nivelului de ambiţie, subliniază importanţa capacităţilor pe care forţele aeriene române (alături de celelalte categorii de forţe) le generează în vederea îndeplinirii sarcinilor şi rolurilor pentru apărarea teritoriului statului român pe de o parte şi în vederea respectării angajamentelor asumate faţă de NATO, UE şi alte organizaţii regionale pe de altă parte, conturând de asemenea atributele viitoarelor structuri de forţe aeriene, acestea urmând să fie *"moderne, complet profesionalizate, cu grad sporit de mobilitate, eficiente, flexibile, sustenabile, apte de luptă, adaptate misiunii, dislocabile la distanţe mari sau chiar la nivel global, care să poată răspunde rapid situaţiilor de criză şi să participe la operaţii întrunite şi/sau multinaţionale"*[14]. De asemenea, este completat cadrul conceptual oferit de DOFA prin introducerea, chiar dacă sumar, a unor concepte emergente (operaţii/capacităţi orientate către generarea de efecte şi operaţiile desfăşurate în reţea), respectiv a conceptelor asociate dezvoltării capacităţilor operaţionale care să permită desfăşurarea operaţiilor aeriene în afara zonei tradiţionale de responsabilitate a Alianţei, într-o manieră expediţionară.

Procesele asociate *transformării forţelor aeriene la nivelul organizational-structural* trebuie analizate atât în contextul mai larg al organizaţiei militare, ca parte a acesteia, dar şi în cel particular, specific instrumentului aerian, caracterizat de atribute distincte de diferenţiere faţă de celelalte categorii de arme, servicii etc. Organizaţia militară este caracterizată pe de o parte de cutume interne proprii şi de repetitivitate, considerată inerţială prin raportare la acţiunea proceselor de transformare, dar şi de particularităţi unice pe de altă parte, precum specializarea ridicată, stabilitatea, autoritatea şi ierarhia bine definite, orientate către atingerea obiectivelor şi îndeplinirea misiunii.

Unele teorii consideră organismul militar *"o mare birocraţie, construită astfel încât să producă rutină şi acţiune ordonată, preferând continuitatea şi nu schimbarea"*[15]. Pentru a-şi menţine relevanţa, acesta este obligat să-şi reevalueze şi reconfigureze structurile organice pe baza unor analize a factorilor şi surselor care impun schimbarea organizaţional-structurală (politica şi strategia, normele cultural-organizaţionale, noile tehnologii etc.). O astfel de analiză centrată în jurul obiectivelor şi strategiei ar trebui să ofere informaţii despre performanţa organizaţiei militare – având aplicabilitate directă şi în cazul forţelor aeriene – prin identificarea răspunsurilor la următorul set de întrebări privind principiile de bază ale structurii organizaţionale: (1) Reuşesc structura şi arhitectura organizaţiei să îndeplinească solicitările atingerii scopurilor şi strategiei acesteia? (2) Reprezintă structura şi arhitectura organizaţiei un vehicul care să sprijine sau să permită schimbarea culturii interne? (3) Este structura astfel proiectată încât să creeze flexibilitatea necesară proceselor prin care resursele pot fi transferate şi utilizate în conformitate cu noile priorităţi? (4) Este structura astfel gândită încât să poată fi susţinută financiar?

În vederea atingerii capacităţii de luptă, gradului sporit de interoperabilitate şi a capacităţilor radical transformate, prefigurate în Strategia de transformare a Armatei României, procesele de proiectare ale viitoarelor forţe aeriene ale României vor trebui centrate în jurul unui set de cerinţe şi principii constând în: (1) *eficienţă şi eficacitate;* (2)

---

[14] Ibidem, p.28

[15] Stephen Peter Posen, *Winning the Next War: Innovation*, Ithaca: Cornell University Press, US, 1991, p.2.

standardizarea proceselor interne în cadrul organizaţiei; (3) *cooperare/ interoperabilitate;* (4) *partajarea informaţiei şi asigurarea feedback-ului;* (5) *oportunităţile privind promovarea în carieră;* (6) *componenţa structurilor de conducere;* (7) *aspectul legislativ-normativ;* (8) *satisfacţia şi motivaţia profesională;* (9) *evaluarea şi reevaluarea continuă a relevanţei organizaţiei.*

Devine astfel crucială înţelegerea factorilor care afectează proiectarea unor structuri în cadrul organizaţiei militare care să îndeplinească roluri şi funcţiuni precise, ajustate să ofere efectele urmărite în teatru. În aceste procese de construcţie structurală, la nivelul organizaţional se impune de asemenea considerarea raporturilor dintre *structură şi strategie, structură şi dimensiune, structură şi tehnologie*, dar şi a celor ce stau la baza interacţiunii aflate între *structură şi un mediu de securitate* deosebit de complex şi dinamic. Alte aspecte care trebuie considerate sunt referitoare la partea relaţional-funcţională care trebuie satisfăcută (funcţiuni, sarcini, forme de organizare a personalului şi de manifestare/ transferare a autorităţii – linii de comandă, comunicaţii şi proceduri etc.).

Chiar dacă aceste principii îşi au originea în sfera managementului tradiţional şi al teoriei organizaţionale clasice, se regăsesc într-o formă clar conturată, caracterizând şi unele dintre conceptele transformării militare *(Revoluţia în problemele militare*). Prin aplicarea acestora în procesele de modelare organizaţional-structurală a viitoarelor forţe aeriene ale României, ar trebui să rezulte *"forţe pentru secolul XXI, de dimensiuni reduse, mult mai specializate funcţional, destinate atât apărării teritoriale, cât şi împotriva ameninţărilor specifice conflictelor de intensitate redusă (SSC)"*[16], definite de caracteristici distincte: *(1) flexibilitate în domeniul doctrinar; (2) mobilitate strategică; (3) configurabilitate şi modularitate; (4) posibilitatea de a acţiona întrunit şi în mod conectat într-un mediu internaţional; şi (5) versatilitatea de a funcţiona într-un conflict şi Operaţii militare altele decât războiul (MOOTW)*.[17]

Aceeaşi Strategie de transformare a Armatei României din 2007, mai subliniază, atât din perspectiva organizational-structurală, cât şi *din perspectiva funcţional-acţională*, necesitatea metamorfozării forţelor aeriene române dintr-o structură statică într-o forţă puternică, cu potenţial expediţionar şi viteză mare de reacţie, capabilă să acţioneze întrunit pentru a fi în măsură să răspundă provocărilor viitoare ale mediului de securitate. Principiile enumerate anterior îşi găsesc aplicabilitate în procesele de proiectare a unor pachete care să funcţioneze integrat în cadrul unor grupări expediţionare de forţe.

În ultimele două decenii, forţele aeriene ale statelor membre NATO au fost dislocate în variate construcţii, configurate în pachete de forţe alături de unităţi ale forţelor terestre sau navale, sau de alte categorii similare multinaţionale, pentru a executa misiuni în diferite teatre de operaţii, precum Bosnia, Irak, Afganistan, Libia etc., rezultând din această experienţă o serie de lecţii învăţate, care sunt deja teoretizate în principii şi modele de constituire şi proiectare a forţei în teatre de operaţii aflate la distanţe mari, dincolo de ariile de responsabilitate tradiţionale.

În dezvoltarea viitoarelor forţe aeriene române, utilizarea unor teorii, precum cea a modularităţii, ar trebui să ofere cadrul conceptual necesar dezvoltării capacităţii de dislocare prin derularea proceselor de constituire/asamblare a componentei aeriene în vederea integrării acesteia în cadrul unor grupări operaţionale de forţe expediţionare (ca forme temporare de organizare). Constructele rezultate vor fi structuri având la bază funcţiuni precise, escadrilele

---

[16] Kevin D.Stringer, *Military Organizations for Homeland Defense and Smaller-scale Contingencies: A Comparative Approach*, Library of Congress, Praeger Security International, US, 2006, p.3.

[17] Thomas Barnett, *Blueprint for Action: A Future Worth Creating*, 2005 în Ivan Dinev Ivanov, *Transforming NATO – New Allies, Missions and Capabilities*, Ed. Lexington Books, Plymouth, UK, 2011, p.47.

de sprijin constând în elemente funcţionale, precum controlul traficului aerian, mentenanţa, reparaţii, logistica etc, destinate deservirii escadrilelor de luptă pentru îndeplinirea rolului operaţional.

Conform aceleaşi teorii privind modularitatea organizaţiilor, respectiv cea a sistemelor militare, din moment ce majoritatea structurilor de forţe sunt caracterizate într-o oarecare măsură de capacitatea de grupare, conectare prin intermediul capacităţilor (mecanismelor interne) deţinute de categoriile de forţe, aproape toate elementele existente ale forţelor sunt într-o anumită măsură modulare. Unele dintre sistemele organizaţionale militare deţin o capacitate mult mărită din această perspectivă a modularităţii, *"putând fi descompuse într-un număr de elemente care pot fi mixate şi potrivite/ recombinate într-o varietate de grupări operaţionale (temporare), fără a pierde din funcţionalitate"* [18].

Este şi cazul forţelor aeriene, care, beneficiare ale unor atribute native în această direcţie, deţin o arhitectură compusă din unităţi care pot fi despărţite, conectate şi mixate în configuraţii diverse, cu păstrarea funcţiilor de bază, continuând să interacţioneze,*"să permită schimbul de resurse (materiale sau sub forma informaţiilor), prin aderarea la proceduri comune de operare, sau prin alte tehnologii comune de coordonare"*[19]. Forţele aeriene vor deveni mult mai modulare prin creşterea compatibilităţii şi standardizarea elementelor din organică, crescând astfel numărul configuraţiilor posibile.

3. Concluzii şi propuneri

Modificările survenite în noul mediu de securitate – creat de evenimentele desfăşurate după sfârşitul Războiului Rece – au determinat schimbarea strategiilor la nivelul organizaţiilor militare, prin identificarea unor noi provocări şi ameninţări, diferite de cele anterioare, fapt ce a implicat conturarea unor obiective noi. Pentru membrii Alianţei Nord-Atlantice, această schimbare a strategiei a impus reconfigurarea structurilor şi realinierea rolurilor şi funcţiunilor la noile obiective, impunându-se astfel derularea unor procese complexe de transformare a categoriilor de arme ale instituţiei militare.

După accederea în NATO şi acceptarea ca membru cu drepturi depline, România – alături de majoritatea ţărilor europene membre ale Alianţei – a urmat calea proceselor de transformare militară, utilizând cadrul conceptual dezvoltat şi oferit de NATO. Astfel, începând din 2005, odată cu iniţierea procesului de integrare în NATO a Armatei României, derulat în baza *Planului de accedere şi integrare al Comandamentului Forţei Întrunite pentru Bulgaria, România şi Slovenia (2004),* sunt iniţiate o serie de măsuri în vederea operaţionalizării, înzestrării forţelor şi dezvoltării capacităţilor operaţionale asumate în cadrul Alianţei. Până în anul 2014 sunt certificate şi afirmate 80 structuri ale Armatei României (o parte dintre acestea fiind reprezentată de cele ale forţelor aeriene), parte a pachetului de forţe prevăzut de *Obiectivele Forţei 2008*.[20]

Transformarea forţelor aeriene ale României se impune a fi înţeleasă din perspectiva generării acelor capacităţi operaţionale transformaţionale, care implică aspecte de ordin tehnologic, procesual, organizaţional şi aspecte asociate factorului uman. La baza acestora se află concepte novatoare, dezvoltate atât pe baza experienţei cumulate ca urmare a participării NATO în diferite operaţii şi conflicte în ultimele două decenii, cât şi pe baza teoriilor şi rezultatelor oferite de programele de cercetare şi dezvoltare specifice erei informaţionale.

---

[18] Melissa A.Schilling şi Christopher Paparone, *Modularity: An Application of General Systems Theory to Military*
force Development, în *Defense Acquisition Review Journal*, US, 2005, p.284.
[19] Ibidem.
[20] Ministerul Apărării Naţionale, *România-NATO, Primii zece ani*, Bucureşti, 2014, p.4.

Astfel, pentru obţinerea acelor capacităţi operaţionale care să permită generarea efectelor urmărite necesare combaterii adversarilor de mâine, se impun transformări semnificative la nivelul organizaţional, al structurii de forţe, platformelor, echipamentului si misiunii – *"care trebuie să evolueze continuu pentru a răspunde pozitiv cerinţelor şi pentru a exploata toate oportunităţile ivite; în ce priveşte schimbarea... se impune luarea unor decizii privind care dintre actualele capacităţi operaţionale trebuie menţinute sau reţinute şi modificate, care trebuie dezvoltate şi care dintre cele vechi trebuie îndepărtate"*[21].

Privite din perspectiva adaptabilităţii, la nivel organizational, forţele aeriene trebuie să deţină acea arhitectură care să le permită o reconfigurare a capacităţilor deţinute, într-un număr suficient de alternative, pentru a executa misiuni specifice într-un mediu întrunit şi multinaţional. Modularitatea noilor structuri de forţe este considerată un atribut indispensabil în noul context de securitate, facilitând *"mixarea şi ajustarea unităţilor în structuri integrate în grupări expediţionare de forţe"*.[22]

În domeniul functional-acţional, noile misiuni şi roluri prefigurate pentru viitor vor necesita în continuare deţinerea de către forţele aeriene ale NATO a unor capacităţi care – din perspectivă spaţială – să permită mai întâi proiectarea forţei iar apoi accesul în regiuni greu accesibile, cu infrastructură limitată sau fără existenţa acesteia, dispuse la distanţe mari şi foarte mari de locaţiile de bază, iar – din perspectivă temporală – capacitate mare de reacţie şi intervenţie (în cazul opririi unor genocide, similar celui actual, din Siria şi nordul Irakului unde grupul terorist Statul Islamic comite atrocităţi de nedescris), respectiv capacitatea de susţinere a unor operaţii pe perioade lungi de timp.

Implicaţiile întrebuinţării forţelor aeriene în MOOTW, respectiv în viitoarele operaţii desfăşurate în sprijinul Naţiunilor Unite, sunt mai puţin de natură structurală, impunându-se transformări mai ales de natură organizaţională. Astfel chiar dacă implicarea în misiunile specifice desfăşurate în sprijinul UN – de la furnizarea unor structuri specializate de comandă şi control, comunicaţii şi computere (C4), ISR, până la executarea unor misiuni de căutare şi salvare – *"nu impun schimbări radicale la nivelul structurii de forţe, dar impun schimbări la nivelul: (1) Atitudinii şi raportării faţă de acest tip de misiuni; (2) Antrenamentului şi instrucţiei; şi (3) Doctrinei şi procedurilor de planificare"*[s23].

Pentru gestionarea acestor provocări prin oferirea de soluţii la nivelul de implicare al forţelor, concepte de nivel înalt, referitoare la noile misiuni (non-Articol V), precum păstrarea şi impunerea păcii, respectiv construirea şi menţinerea păcii, au fost translatate şi aliniate cu conceptele strategice şi operaţionale. Această abordare permite organizaţiei militare să gestioneze un număr mare de roluri şi misiuni într-un spectru violent foarte complex, *"oferind în acelaşi timp – prin transferarea în zona conceptuală practică la nivelul organizaţiei – o direcţie clară privind modul în care organizaţia consideră, reconsideră şi integrează capacităţile la nivelul structurii de forţe pentru a genera valoare eterogenă"*[24].

Transformarea forţelor aeriene ale României trebuie să vizeze toate cele trei componenete ale puterii aeriene (morală, conceptuală şi fizică), urmărindu-se astfel alinierea doctrinelor, strategiilor, principiilor, standardelor şi procedurilor operaţionale proprii cu cele ale Alianţei, dar şi demararea şi/sau continuarea proceselor de achiziţie şi înzestrare a forţelor cu noi tehnologii care să permită obţinerea interoperabilităţii cu aliaţii în cadrul NATO. Dezvoltarea capacităţilor operaţionale necesare forţelor aeriene pentru a răspunde efectiv

---

[21] Kevin D.Stringer, *Military Organizations for Homeland Defense*, p.4.

[22] Erik J.de Waard, Eric-Hans Kramer, *Tailored task forces: Temporary organizations and modularity*, Netherlands Defense Academy, Department of Management, 20 May 2008, p.1.

[23] Steven Metz, *The Air Force Role in United Nations Peacekeeping*, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj93/win93/metzzz.htm, pagină accesată la 07.05.2014.

[24] Joseph Soeters Paul C. van Fenema, *Military Organizations's Capabilities for Heterogeneous Value Creation* în *Managing Military Organizations. Theory and Practice*, Routledge, US, 2010, p.494.

provocărilor actuale şi viitoare ale mediului de securitate, vizează următoarele arii: (1) informaţiile; (2) supravegherea aeriană, achiziţia şi neutralizarea ţintelor; (3) supravegherea spaţiului terestru; (4) capacităţile de atac cu armament de înaltă precizie şi de neutralizare a apărării aeriene a inamicului; (5) transportul aerian strategic şi realimentarea în aer; şi (6) sistemele de comandă, control şi comunicaţii dislocabile.

Importanţa acestor domenii este susţinută de atenţia acordată programelor de modernizare, achiziţii şi înzestrare, prin concentrarea asupra tehnologiilor care să permită obţinerea şi dezvoltarea capacităţilor operaţionale vizate. Dezvoltarea acestor capacităţi noi va contribui atât la consolidarea capacităţii de răspuns a Alianţei în întreg spectrul de misiuni – de la cele specifice securităţii colective, respectiv apărării teritoriale, la cele de stabilitate – cât şi la întărirea credibilităţii puterii aeriene a României în cadrul NATO.

Începând din 2016 (şi preconizat până în 2025), prin intrarea în ultima etapă a procesului de transformare (cum este prevăzută de *Strategia de Transformare a Armatei României*), urmează să fie îndeplinite obiectivele pe termen lung care vizează: *"(1) continuarea modernizării înzestrării cu echipamente noi şi realizarea interoperabilităţii depline cu armatele ţărilor membre NATO şi ale Uniunii Europene; (2) concentrarea eforurilor şi resurselor financiare şi umane în vederea realizării capacităţilor prevăzute în Obiectivele de Capacităţi şi îndeplinirii responsabilităţilor în cadrul NATO şi Uniunii Europene; şi (3) concentrarea activităţilor de evaluare sistemică şi structural pe domeniul procesului de înzestrare şi modernizare cu tehnică şi echipamente"*[25].

Pentru forţele aeriene ale României, atât implicaţiile cât şi provocările sunt majore, atingerea acestor obiective fiind posibilă doar în situaţia în care o bugetare corespunzătoare va permite continuarea proceselor de transformare în domeniile conceptual, organizaţional, acţional-funcţional şi în cel al infrastructurii. Din această perspectivă, se impune atât îmbunătăţirea cadrului normativ prin actualizarea, respectiv elaborarea unor concepţii şi doctrine noi, cât şi crearea unui context complet diferit de manifestare a proceselor la nivelul organizaţiei *"(prin schimbarea mentalităţii, atitudinilor şi a înţelegerii/raportării la valoare, educaţie etc.), care să faciliteze trecerea de la exprimări reactive către cele proactive"*[26], într-un final fiind vizate cele transformaţionale.

Astfel, măsura în care forţele aeriene ale României sunt pregătite să răspundă ameninţărilor viitoare este aceea în care vor reuşi să genereze capacităţi operaţionale rezultate din înţelegerea şi implementarea la nivelul forţei a conceptelor de ultimă oră dezvoltate în cadrul Alianţei (fiind incluse şi cele referitoare la *Operaţiile bazate pe efecte,* respectiv *Războiul în reţea*), susţinute de procese de achiziţie şi înzestrare cu tehnologie modernă la nivelul tuturor categoriilor de arme din cadrul forţelor aeriene (aviaţia, apărarea antiaeriană şi radiolocaţia), rezultatul final urmărit fiind atât obţinerea unor structuri expediţionare, flexibile, cu un nivel ridicat de pregătire, cu capacitate de dislocare într-un timp foarte scurt, capabile să acţioneze întrunit şi multinaţional în întreg spectrul de misiuni, cât şi a unui sistem integrat de apărare aeriană a României şi spaţiului aerian integrat al Alianţei (NATINAMDS), prin implicarea sinergică a tuturor capacităţilor operaţionale deţinute.

---

[25] MApN, *Strategia de transformare a Armatei României*, p.7.
[26] Mihail Orzeaţă, *Globalization, Crises and World Security*, LAP LAMBERT, Academic Publishing, Germany, 2013, p.126

BIBLIOGRAFIE:

1. Ankersen, Christopher, *Capabilities and Capacities* în *Transforming National Defense Administration,* School of Policy Studies, Queen's University Kingston, Ontario, Canada, 2005
2. Barnett, Thomas, *Blueprint for Action: A Future Worth Creating*, 2005 în Ivan Dinev Ivanov, *Transforming NATO – New Allies, Missions and Capabilities*, Ed. Lexington Books, Plymouth, UK, 2011
3. Halus, Adrian, *75 ani de radiolocaţie în Armata română* în *Observatorul militar nr.8* din 26 februarie-4 martie 2014
4. Hentea, Călin, *Armata şi luptele românilor din Antichitate până la intrarea în NATO, Breviar de istorie militară*, Editura Nemira, Bucureşti, 2002
5. Ionescu, Mihail E., *Etapele reformei armate în perioada post-Război Rece* (1990-2008), în *Reforma Militară şi societatea în România (1878-2008)*, Editura Militară, Bucureşti, 2009
6. Metz, Steven, *The Air Force Role in United Nations Peacekeeping*, http://www.airpower. maxwell. af.mil/ airchronicles/apj/apj93/win93/metzzz.htm.
7. Ministerul Apărării Naţionale, *România – NATO, Primii zece ani*, 2014
8. Ministerul Apărării Naţionale, *Strategia de transformare a Armatei României*, Bucureşti, 2007
9. Orzeaţă, Mihail, *Războiul Continuu*, Editura Militară, Bucureşti, 2011
10. Orzeaţă, Mihail, *Globalization, Crises and World Security*, LAP LAMBERT, Academic Publishing, Germany, 2013
11. Posen, Stephen Peter, *Winning the Next War: Innovation*, Ithaca: Cornell University Press, US, 1991
12. Schilling, Melissa A. şi Paparone, Christopher, *Modularity: An Application of General Systems Theory to Military force Development*, în *Defense Acquisition Review Journal*, US, 2005
13. Soeters, Joseph şi van Fenema, Paul C., *Military Organizations's Capabilities for Heterogeneous Value Creation* în *Managing Military Organizations. Theory and Practice*, Routledge, US, 2010
14. Stringer, Kevin D, *Military Organizations for Homeland Defense and Smaller-scale Contingencies: A Comparative Approach*, Library of Congress, Praeger Security International, US, 2006
15. US DoD, Office of the Secretary of Defense, *Military Transformation – A Strategic Approach*, Director, Force Transformation, Pentagon, Washington, US
16. Waard, Erik J.de şi Kramer, Eric-Hans, *Tailored task forces: Temporary organizations and modularity*, Netherlands Defense Academy, Department of Management, 20 May 2008
17. www.nato.int

CERINŢE OPERAŢIONALE IMPUSE AERONAVELOR ŞI INFRASTRUCTURII VIITOARELOR FORŢE AERIENE ROMÂNE

Cosmin Liviu COSMA
Căpitan comandor, Doctorand, Universitatea Naţională de Apărare "CAROL I",
e-mail: airspider@yahoo.com

Rezumat: *Forţele aeriene, prin atributele unice deţinute – viteza, puterea de foc, flexibilitatea, capacitatea de proiecţie a puterii la scară globală, dominaţia informaţională etc. – vor reprezinta şi în viitor elementul esenţial în soluţionarea conflictelor militare, la orice nivel, indiferent de construcţiile şi formele de implicare propuse de factorii de decizie militari şi politici. Utilizarea eficace a instrumentului aerian este însă condiţionată de o serie de factori, o parte dintre aceştia fiind reprezentaţi atât de atributele aeronavelor şi sistemelor de arme, cât şi de către cele ale infrastructurii bazelor aeriene.*

Scopul principal al lucrării de faţă este – ca pe baza unei analize calitative, prin utilizarea metodei deductive, a teoriilor axiomatice şi a taxonomiilor – să stabilească atributele pe care avioanele şi infrastructura forţelor aeriene ale României trebuie să le deţină pentru a fi în măsură să răspundă viitoarelor provocări şi ameninţări la adresa securităţii României şi a NATO. Pentru atingerea acestui obiectiv, iniţial au fost identificate raporturile de supervenienţă (relaţiile de cauzalitate) dintre misiuni/ roluri şi cerinţe/ atribute ale platformelor aeriene, respectiv ale infrastructurii.

Cuvinte cheie: *forţele aeriene române, avioane de luptă, infrastructură, achiziţii, înzestrare, interoperabilitate, NATO*

1. Aspecte privind înzestrarea şi infrastructura forţelor aeriene române în noul context creat după sfârşitul Războiului Rece

Situaţia nou creată după sfârşitul Războiului Rece – caracterizată de manifestarea în imediata proximitate a României a unor conflicte separatiste, interetnice, religioase, a traficului ilegal de arme, droguri, persoane, respectiv a altor forme de criminalitate transfrontalieră[1], iar mai recent cea generată de anexarea Crimeei de către Rusia – au determinat, dintr-o perspectivă militară, definirea unor obiective naţionale de securitate care vizează asigurarea unor capacităţi de apărare necesare atât garantării intereselor naţionale, cât şi respectării obligaţiilor asumate în calitate de membru al NATO şi al Uniunii Europene[2].

În acest context, în vederea adaptării capacităţilor militare la exigenţele mediului de securitate nou creat, imediat după 1990, forţele aeriene, alături de celelalte categorii de forţe ale Armatei României au fost supuse unor reforme la nivelul structurilor de forţe, doctrinelor, conceptelor, pregătirii, echipamentelor, dar şi infrastructurii, proces ce a căpătat substanţă şi o abordare unitară şi consistentă în special după accederea României în structurile NATO în 2004.

Din perspectiva proceselor de înzestrare şi a celor asociate infrastructurii, programele de achiziţii derulate după 1990 au vizat: (1) retragerea echipamentului perimat, aflat în dotare din timpul Războiului Rece şi înlocuirea acestuia cu sisteme moderne, care să permită

[1] Ministerul Apărării Naţionale, *Carta Albă a Apărării*, Bucureşti, 2011, p.7.
[2] Ibidem.

operarea în reţea; (2) modernizarea aeronavelor existente atât pentru creşterea performanţelor combative, cât şi pentru obţinerea compatibilităţii tehnice cu platformele aliate în cadrul Alianţei; (3) Achiziţia unor platforme aeriene destinate transportului trupelor şi echipamentului în teatru sau în sprijinul unor misiuni de menţinere a păcii; (4) realizarea unui sistem integrat pentru controlul traficului aerian; şi (5) dezvoltarea unui sistem de identificare amic-inamic, compatibil NATO.

Aceste programe au constat în: (1) modernizarea aeronavelor MiG-21, IAR-99 şi elicopterelor IAR-330 PUMA, fiind integrate la bodul acestora sisteme moderne de avionică, navigaţie, armament, radar şi comunicaţii. Pe lângă performanţele mărite de descoperire şi combatere a ameninţărilor aeriene şi terestre s-a obţinut şi un grad ridicat de interoperabilitate cu platformele şi sistemele aliaţilor din NATO; (2) modernizarea sistemului de supraveghere prin achiziţia radarului tridimensional AN/FPS-117, destinat atât asigurării cu date în timp real despre fiecare ţintă aeriană aflată în volumul cercetat (descoperire, urmărire şi identificare a mijloacelor aeriene ce evoluează la distanţe de până la 450 km), cât şi controlului spaţiului aerian, dirijării avioanelor proprii la interceptare; Introducerea acesui sistem a permis obţinerea compatibilităţii tehnice şi operaţionale la standardele NATO, prin asigurarea supravegherii aeriene şi conectarea cu sistemul integrat NATO de apărare aeriană; (3) achiziţionarea sistemului aerian pilotat de la distanţă (**UAV**) **SHADOW 600**, care a permis creşterea capacităţii de culegere şi partajare a informaţiilor în timp real la nivelul teatrului de luptă, respectiv integrarea unor astfel de sisteme, compatibile cu sistemele aliate, la nivelul structurilor de comandă control şi informaţii (C2I); (4) modernizarea şi asigurarea asistării la aterizare a aeronavelor la standarde NATO prin achiziţionarea *sistemului de asistenţa tehnică la aterizare pentru navigaţie aeriană (Technical Land Assistance System for Air Navigation)* pentru patru aerodromuri şi heliporturi ale forţelor aeriene române; (5) Iniţierea şi dezvoltarea *Centrului Operaţional pentru Suveranitatea Aeriană (ASOC)* în vederea obţinerii capacităţii de conducere centralizată a acţiunilor de asigurare a suveranităţii aeriene, prin integrarea datelor furnizate la nivel naţional atât de radarele militare, cât şi de cele civile; şi (6) dezvoltarea *sistemului amic-inamic (IFF) DIALOG*, compatibil cu sistemele NATO similare, destinat identificării tuturor platformelor de luptă care evoluează în interiorul spaţiului aerian al României.

Pentru atingerea obiectivelor generale ale Ministerului Apărării Naţionale, pe baza priorităţilor definite în baza prevederilor *Strategiei naţionale de apărare*, a liniilor directoare ale politicii de apărare stabilite prin *Programul de guvernare* şi în *conformitate cu prevederile Conceptului strategic al NATO şi a Directivei ministeriale a NATO* – se impune continuarea reformelor în domeniul resurselor de apărare, dar şi modificarea cadrului legislativ, astfel încât să corespundă noilor realităţi instituţionale, mediului de securitate intern şi internaţional, precum şi experienţei acumulate în teatrele de operaţii.[3] Prin eficientizarea proceselor, respectiv prin asigurarea coerenţei tuturor disciplinelor de planificare a apărării şi a coordonării acestora în mod unitar (în conformitate cu prevederile *Liniilor generale pentru procesul de planificare a apărării în NATO (Outline Model for a NATO Defence Planning Process),* prezentat în cadrul Summit-ului de la Strasbourg-Kehl, 3-4 aprilie 2009) este urmărită dezvoltarea unor capacităţi operaţionale de apărare pe termen mediu şi lung. Pentru aceasta, este prevăzut ca planificarea şi programarea resurselor să fie realizate pe baza unor programe majore.

Conform *Legii nr. 473/2004 privind planificarea apărării*, aceste programe majore reprezintă *"totalitatea acţiunilor şi a măsurilor concrete desfăşurate pentru constituirea, modernizarea, înzestrarea, instruirea, întreţinerea la pace şi pregătirea pentru situaţii de*

---

[3] Ministerul Apărării Naţionale, *Planul Strategic al Ministerului Apărării Naţionale 2010-2013*, Bucureşti, 2010, p.8.

criză şi război a unităţilor militare, asigurarea condiţiilor optime de viaţă pentru personal, asigurarea sprijinului logistic şi a rezervelor pentru mobilizare şi război, crearea şi întreţinerea infrastructurii pentru acţiuni militare în cadrul apărării comune a NATO, participarea la acţiuni de cooperare internaţională cu alte state, precum şi resursele necesare anuale pentru realizarea acestora".[4]

La nivelul forţelor aeriene au fost dezvoltate capacităţi, care prin avantajele oferite la nivel operational şi strategic, au ajuns să fie apreciate şi în cadrul NATO: (1) capacităţi de transport aerian strategic (participare la *Capacitatea de Transport Aerian Strategic*) şi tactic; (2) elicoptere: SOCAT, de transport (NATO şi de evacuare medicală – MEDEVAC), navalizat, iar începând cu 2010, elicoptere destinate *Căutării şi Salvării prin lup***tă** (CSAR); (3) supraveghere aeriană, prin participarea la NATINAMDS (*NATO Integrated Air and Missile Defense System*); şi (4) modernizarea aerodromurilor militare la standarde NATO cu sisteme de radionavigaţie, dirijare la aterizare şi balizaj.

Alte programe de modernizare, înnoire a echipamentelor şi infrastructurii au fost *"concretizate în sprijinul forţelor dislocate în teatrele de operaţii, în domeniul mişcare şi transport, în cel al sprijinului naţiunii gazdă şi în cadrul programului NATO de investiţii în infrastructura de securitate (NSIP)"*[5].

În ceea ce priveşte programul NATO de investiţii în securitate (NSIP), dezvoltat după admiterea României în NATO, se derulează în prezent un număr total de 50 proiecte, care fac parte din 10 pachete de capacităţi operaţionale, având o valoare financiară totală de 128,029 mil. Euro, din care fonduri NATO NSIP în valoare de 104,106 mil. Euro (aproximativ 81%).[6]

Forţele aeriene române sunt beneficiarele unui procent considerabil din numărul proiectelor cuprinse în cele 10 pachete de capacităţi operaţionale care conţin proiecte NSIP, prin faptul că acestea vizează în special facilităţi operaţionale, îndeosebi în domeniul infrastructurii de aerodrom, asigurarea şi întreţinerea capacităţilor incluse în Sistemul Integrat NATO de Apărare Antiaeriană şi Împotriva Rachetelor (NATINAMDS), respectiv îmbunătăţirea sistemelor de comunicaţii în reţea, de interes major la nivelul NATO.

Odată cu izbucnirea crizei din Ucraina în 2014, are loc schimbarea priorităţilor pentru Alianţa Nord-Atlantică, ceea ce determină la nivelul Ministerului Apărării Naţionale punerea accentului pe creşterea capacităţii operaţionale, fapt oglindit şi în deciziile luate în domeniul înzestrării. Acestea s-au concentrat pe următoarele priorităţi: programul strategic *Avion multirol al Forţelor Aeriene*, programul *Avion mediu-scurt curier C-27 Spartan*, sistemul de rachete sol-aer cu bătaie medie *Hawk*, programul *Elicopter IAR 330 Puma Naval*, programul *Transportor blindat 8x8 Piranha.*[7]

În perioada următoare, în vederea realizării unei structuri de forţe cu un grad ridicat de susţinere şi interoperabilitate, flexibile, mobile, desfăşurabile în teatre de operaţii, capabile să participe atât la întreaga gamă de misiuni NATO şi UE, cât şi la misiuni de tip **coaliţie** – aşa cum reiese din *Planul Strategic al Ministerului Apărării Naţionale* – vor continua procesele de achiziţii în domeniul înzestrării, în corelare cu resursele puse la dispoziţie, a sistemelor de armamente ce înglobează tehnologii moderne, adecvate, în scopul satisfacerii cerinţelor categoriilor de forţe ale armatei şi asigurării interoperabilităţii cu forţele NATO.

---

[4] Ibidem.
[5] Ministerul Apărării Naţionale, *România-NATO. Primii zece ani*, Bucureşti, 2014, p.5.
[6] Ibidem.
[7] Mircea Duşa, *Bilanţul MApN pe 2014,* Ministerul Apărării Naţionale, Bucureşti, 10 martie 2015, TVRNEWS.

2. Cerinţe impuse bazelor şi elementelor de infrastructură ale forţelor aeriene române în contextual viitoarelor ameninţări

Analiza caracteristicilor infrastructurii din înzestrarea forţele aeriene se impune a fi realizată din perspectiva rolurilor şi misiunilor pe care aceste structuri de forţe trebuie să le îndeplinească, abordare justificată printr-o *relaţie de supervenienţă* de tipul *mijloace - procese sau infrastructură - roluri/ misiuni.* Această relaţie asimetrică de dependenţă între cele două categorii de proprietăţi – *fizice (infrastructura, bazele) şi procesuale (rolurile, misiunile)* – presupune transferarea efectelor din prima categorie către cea de a doua, ca urmare a schimbărilor sau transformărilor efectuate.

Se impune mai întâi o definire a conceptelor referitoare infrastructurii, bazelor aeriene, respectiv sistemului logistic, proceselor şi programelor asociate acestora. Astfel, în accepţiunea NATO, infrastructura reprezintă *"construcţiile statice şi instalaţiile permanente destinate sprijinului forţelor militare"*[8], sau *"mijloacele statice ale investiţiilor de capital care sunt destinate sprijinului material pentru planurile operaţionale necesare în vederea facilitării funcţionării eşaloanelor superioare (comandamentelor) şi diferitelor categorii de forţe într-o manieră eficientă".*[9] Conform documentelor doctrinare ale SUA, infrastructura reprezintă *"furnizarea serviciilor, proceselor, facilităţilor şi sprijinul asociat pentru dezvoltarea, generarea, susţinerea, mentenanţa şi refacerea puterii aeriene. Infrastructura, de asemenea, este o colecţie de elemente fizice, precum clădirile în care îşi desfăşoară activitatea escadrilele, respectiv procesele, reprezentate de operaţiile de zbor executate de către personalul militar"*[10].

Infrastructura, în final, sprijină operaţiile în întreg spectrul conflictului, atât în garnizoane, cât şi în mediul expediţionar, incluzând: (1) instalaţiile; (2) logistica; (3) serviciile pentru personal; (4) sprijinul serviciilor privind sănătatea; (5) cartierele generale (comandamentele) şi funcţiile de sprijin ale acestora; (6) programele privind ştiinţa şi tehnologia; (7) facilităţile de testare şi evaluare, precum şi poligoanele; (8) frecvenţele electromagnetice; (9) instrucţia alta decât cea pentru unităţi; (10) facilitarea/ sprijinul serviciilor de achiziţie, contractare şi financiare; (11) sistemele de comandă, control, comunicaţii, computere şi informaţii (C4I); (12) funcţiile de sprijin al instalaţiilor; (13) funcţiile de sprijin al comunităţii; (14) spaţiile destinate proceselor de mentenanţă (ateliere); şi (15) sisteme de sprijin asociate componentei aeriene.[11]

Bazele aeriene reprezintă locaţiile de unde operaţiile sunt generate şi sprijinite, putând fi definite ca instalaţii care conţin facilităţile şi infrastructura. *Infrastructura*, cum s-a subliniat anterior, se referă la toate instalaţiile/ mijloacele fixe şi expediţionare, la construcţii şi facilităţi, precum şi la procesele care sprijină şi asigură controlul forţelor militare. Prin *facilitate* se înţelege o entitate reală, constând într-una sau mai multe clădiri, structuri (aici fiind incluse şi structurile temporare – corturi etc.), sisteme de utilităţi, terenuri etc. Funcţiile principale ale bazelor aeriene includ furnizarea energiei, combustibililor, muniţiilor, apei, lucrărilor civile, serviciilor, asistenţei medicale, precum şi a comenzii şi controlului.

Dincolo de serviciile oferite de bazele aeriene, acestea pot fi categorisite pe baza funcţiunilor şi a intensităţii cu care sunt desfăşurate/ generate operaţiile aeriene. Identificăm astfel: (a) *Baze principale de operare (Main Operations Bases)* – caracterizate de deţinerea

---

[8] NATO Infrastructure Commitee, *50 Years of Infrastructure – NATO Security Investment Programme is the Sharing of Roles, Risks, Responsibilities, Costs and Benefits,* 15 may 2001, p.18.
[9] Ibidem.
[10] US Air Force, *Air Force Doctrine Document 2-4.4 – Bases, Infrastrastructure and Facilities ,* 13 November 1999, p.7.
[11] Ibidem.

unei infrastructuri dezvoltate şi a unor servicii de sprijin care pot satisface totalitatea proceselor destinate sprijinului/generării operaţiilor aeriene în întreg spectrul; (b) *Baze colocate de operare (Collocated Operations Bases)* – acestea sunt de regulă deţinute şi operate de o forţă aliată; infrastructura, starea de operativitate şi activitatea de sprijin ale acestora se pot prezenta în diferite grade de disponibilitate, fiind de regulă utilizate de structuri ale forţelor aeriene de tipul celor aflate în rezervă; şi (c) *Baze de operare înaintate (Forward Operations Bases)* – infrastructura acestora poate varia de la una austeră la una dezvoltată, fiind de regulă baze care au rol de sprijin pentru aeronavele care evoluează pe rute către/ din teatrul de operaţii, baze dispuse în punctele cele mai apropiate de teatrele de operaţii, sau baze înaintate pentru înarmare şi realimentare.

Experienţa conflictelor desfăşurate de la terminarea Războiului Rece până în prezent – cea mai recentă fiind cea rezultată din *Operaţiunea Unified Protector* din 2011 din Libia – au conturat trăsăturile necesare bazelor aeriene şi infrastructurii forţelor aeriene ale statelor membre NATO, pentru a fi în măsură să desfăşoare misiuni în întreg spectrul conflictului într-un mediu întrunit şi multinaţional.

Misiunile pe care forţele armate ale României vor trebui să le îndeplinească în noul context de securitate înglobează un spectru larg, pornind de la apărarea teritoriului naţional şi până la cele aferente participării în cadrul angajamentelor multinaţionale derulate sub egida NATO şi UE, organizaţiilor precum ONU şi OSCE sau în cadrul coaliţiilor de voinţă.[12]

Astfel, caracteristicile bazelor aeriene şi infrastructurii deţinute de forţele aeriene române trebuie înţelese din perspectiva generării şi sprijinului unor operaţii aeriene distincte (pentru apărarea naţională şi pentru cea colectivă în cadrul NATO), alături de aliaţi, atât în zona de responsabilitate, cât şi în afara acesteia, în cadrul unor operaţii expediţionare. Alt aspect ce trebuie luat în considerare – asociat operaţiilor expediţionare – din perspectiva caracteristicilor/ condiţiilor infrastructurii se referă la *sprijinul naţiunii-gazdă (HNS)*.

Viitoarele baze aeriene şi infrastructura aferentă acestora – destinate deservirii activităţii structurilor combatante şi de comandă din forţele aeriene române, sau a celor aliate dislocate pe teritoriul României (din perspectiva contribuţiei la HNS) – trebuie astfel configurate şi înzestrate încât să permită generarea misiunilor de luptă prin asigurarea: (1) suprafeţelor de operare a aeronavelor sau operarea aeronavelor la sol (necesitatea îndeplinirii unor condiţii ce ţin de starea şi caracteristicile tehnice ale suprafeţelor de rulare, dimensiunile acestora, astfel încât să permită atât operarea avioanelor de lovire, cât şi a celor de transport de dimensiuni mari (airlift and cargo), de tipul C-17 Globemaster, C-5 Galaxy etc.); (2) suprafeţelor şi spaţiilor tehnice necesare inspecţiilor, mentenanţei, testării şi evaluării, respectiv reparaţiilor aeronavelor şi a echipamentelor asociate; (3) zonelor destinate sprijinului logistic pentru depozitarea şi distribuirea materialelor, echipamentului, consumabilelor (petrol, ulei şi lubrifinaţi), respectiv a celor necesare operării vehiculelor la sol, mentenaţa şi repararea acestora; (4) facilităţilor administrative şi a celor destinate comandamentelor destinate sprijinului elementelor C2 şi personalului; (5) sprijinului sistemelor de comunicaţii şi informaţii; (6) facilităţilor de hrănire a personalului; (7) facilităţilor şi zonelor tehnice destinate sistemelor de utilităţi; (8) facilităţi medicale; (9) facilităţi destinate protecţiei şi protecţiei împotriva incendiilor; şi (10) spaţiilor de cazare a personalului şi a familiilor acestora.[13]

Dintr-o perspectivă operaţională, infrastructura bazelor aeriene va trebui să permită desfăşurarea unor activităţi distincte, raportate la sistemul de arme deservit sau la natura activităţilor de sprijin, conform principiului specializării. Raportându-ne la acest criteriu,

---

[12] Ministerul Apărării Naţionale, *Carta Albă a Apărării*, Bucureşti, 2011, p.9.
[13] US Air Force, *Air Force Doctrine Document 2-4.4 – Bases, Infrastrastructure and Facilities,* 13 November 1999, p.14.

bazele aeriene vor fi destinate: (a) *generării misiunilor de luptă independente* sau executate în cadrul unor operaţii aeriene de anvergură; (b) *generării unor operaţii ofensive şi defensive de război electronic* şi furnizării sprijinului de informaţii, respectiv a funcţiilor asociate C2; (c) *furnizării unui sprijin tehnic înalt specializat*, necesar activităţii de mentenanţă, reparaţii, cercetării şi dezvoltării; (d) *furnizării sprijinului medical*, prin utilizarea unor capacităţi deţinute, de tipul evacuării aeromedicale; (e) *sprijinului proceselor de instruire, antrenament în zbor şi a celor educaţionale; (f) testării şi evaluării platformelor aeriene*, armelor şi sistemelor de arme.

Astfel, bazele aeriene şi infrastructura vor constitui mijloacele prin care forţele aeriene ale României vor genera puterea de luptă, prin facilitarea executării misiunilor pentru combaterea forţelor ostile, dar şi prin controlul exercitat asupra resurselor. Dependenţa astfel creată între misiuni şi infrastructură determină considerarea acesteia de către adversari ca fiind un centru de greutate care trebuie neutralizat, ceea ce impune dezvoltarea unor planuri încă din timp de pace privind protecţia. Însă, nu este suficient ca bazele şi infrastructura să fie doar în măsură să reziste unor atacuri aeriene sau terestre. Acestea trebuie să fie în măsură să asigure misiuni de luptă prelungite şi concentrate împotriva inamicului.

Situaţia unor conflicte precum cel din Libia din 2011 (*Unified Protector*) – chiar dacă nu a fost de o anvergură foarte mare – a demonstrat neajunsurile pe care le provoacă executarea unor operaţii aeriene executate de pe baze aeriene dispuse la distanţe mari de zona de conflict. Devine însă obligatorie prezenţa acestora atât în cazul unor campanii îndelungate, pentru satisfacerea cerinţelor operaţionale pe care o astfel de campanie le presupune (tempo-ul operaţiilor, disponibilitatea platformelor aeriene de vânătoare, de atac la sol, transport şi de realimentare în aer, asigurarea operaţiilor de mentenanţă, asigurarea serviciului de căutare-salvare etc.), cât şi în cazul în care operaţia militară presupune participarea forţelor terestre, ceea ce implică un set diferit de activităţi (începând cu transportul forţei şi a echipamentului în teatru şi terminând cu asigurarea logistică, medicală etc.).

Din aceeaşi perspectivă a forţelor expediţionare, pentru funcţionarea acestor baze în condiţiile optime generării capacităţilor de lovire necesare în teatru, se impune dislocarea/ redislocarea şi realizarea facilităţilor necesare susţinerii forţelor într-un timp foarte scurt. Aceasta presupune existenţa unor proceduri şi acorduri stabilite în prealabil: *"puncte stabilite de intrare şi plecare, autorizări de survol, autorizări privind utilizarea frecvenţelor radio, controlul traficului aerian, aprobări diplomatice, drepturi privind funcţionarea bazelor, acorduri privind facilităţile de acces, proceduri de contractare ale Coaliţiei, conectivitate, protecţia forţei, examinarea/ inspecţia locaţiei, manipularea şi depozitarea explozibililor, muniţiei şi armamentului etc."*[14].

Acestea din urmă trebuie înţelese din perspectiva proceselor şi standardelor care odată îndeplinite, să permită desfăşurarea unor operaţii militare într-un mediu întrunit şi multinaţional, fiecare armă, platformă aeriană sau echipament de la sol, capacitate operaţională a Alianţei să poată fi conectată la un hub sau reţea comună, permiţând astfel sinergia acţională a forţelor statelor membre NATO, indiferent de condiţiile teatrului de luptă. Este vizată astfel obţinerea interoperabilităţii, care poate fi asigurată prin standarde şi proceduri comune, din perspectivă organizaţională şi prin compatibilitatea sistemelor.

[14] Michael W.Lamb, *Operations Allied Force – Golden Nuggets for Future Campaigns*, BiblioScholars, 2012, pag.17.

3. Cerinţe operaţionale impuse aeronavelor şi sistemelor de arme din dotarea viitoarelor forţe aeriene ale României

Pentru stabilirea cerinţelor operaţionale ale aeronavelor care vor înzestra viitoarele structuri de forţe aeriene ale României, se impune utilizarea aceleaşi *abordări de analiză a raporturilor de supervenienţă dintre proprietăţile fizice şi cele operaţionale*, asociate misiunii.

Din perspectiva exprimării acţionale, forţele aeriene, prin atributele lor unice, vor rămâne şi în viitor singura categorie de forţe care poate acoperi întreg spectrul de misiuni, de la cele tradiţionale ofensive şi defensive de aplicare a forţei – în operaţii de apărare a spaţiului naţional sau al celui integrat al NATO – până la cele expediţionare, respectiv cele executate în sprijinul activităţii unor organizaţii precum Naţiunile Unite, OSCE etc, destinate menţinerii şi impunerii păcii, asistenţei umanitare sau impunerii de sancţiuni.

Dezvoltarea unor concepte novatoare în cadrul Alianţei, precum şi experienţa implicării militare a NATO în conflictele ultimelor două decenii ar trebui să constituie fundamentul proceselor de înzestrare şi integrare a noilor platforme aeriene şi sisteme de arme în inventarul de arme al forţelor aeriene române. Pentru a permite executarea întregii game de misiuni (amintite anterior), este necesar ca forţele aeriene să deţină un inventar variat de platforme aeriene (avioane de vânătoare, vânatoare-bombardament, avioane destinate transportului forţelor şi materialelor în teatrele de operaţii, avioane cisternă pentru alimentarea în aer, avioane-şcoală destinate instruirii în zbor, elicoptere de atac, elicoptere pentru evacuare medicală, căutare şi salvare, căutare şi salvare prin luptă (MEDEVAC, CSAR etc.).

Un astfel de inventar ar permite punerea în practică a unor concepte noi la nivelul forţelor aeriene române, precum *operarea în reţea şi desfăşurarea operaţiilor din perspectiva efectelor generate* asupra obiectivelor desemnate. Reorientarea conceptuală la nivelul factorilor de decizie NATO privind planificarea operaţiilor, de la cele centrate în jurul ameninţării şi a platformelor, către cele centrate în jurul unor capacităţi adaptative şi a obţinerii de efecte ar fi astfel validată, prin punerea la dispoziţia comandanţilor a unui arsenal complet de platforme aeriene, arme şi sisteme de arme, din care să le poată selecta pe cele care pot furniza efectele urmărite în teatru.

Raportat la *platformele aeriene destinate furnizării de efecte cinetice* asupra inamicilor – campaniile aeriene desfăşurate de la sfârşitul Războiului Rece până în prezent au demonstrat necesitatea deţinerii unor platforme aeriene care să fie apte să acţioneze în condiţiile tot mai complexe şi restrictive ale teatrelor de luptă actuale, aspect ce implică deţinerea unor caracteristici care să le permită atât descoperirea şi combaterea adversarilor, cât şi protecţia proprie în faţa unor ameninţări multiple din aer şi de la sol. Pe de altă parte, limitările impuse de regulile de angajare, respectiv de necesitatea desfăşurării unor operaţii de eliminare a unor adversari aflaţi în zonele urbane, în imediata proximitate a populaţiei civile necombatante etc. determină includerea în arsenalul propriu a unor aeronave posesoare ale unor caracteristici distincte (viteză, autonomie, costuri de achiziţie şi întreţinere, dar şi posibilitatea integrării muniţiilor inteligente letale şi neletale, capacitatea de funcţionare în reţea în vederea utilizării unor funcţii care să permită identificarea şi selectarea ţintelor în cel mai scurt timp posibil etc.) care pot furniza efectele urmărite în teatru, fără producerea unor pagube şi distrugeri colaterale.

Teatrele de operaţii în care platformele aeriene vor evolua în viitor se prefigurează că vor cunoaşte infuzia masivă a unor sisteme de arme de ultimă generaţie, posesoare ale unor caracteristici mult îmbunătăţite, privind atât autoprotejarea şi supravieţuirea, cât şi capacităţile de executare a unor lovituri letale. Integrarea unor senzori deosebit de performanţi va contribui la permeabilizarea şi asigurarea transparenţei mediului operaţional. Această realitate prefigurată impune dezvoltarea unor sisteme care, odată integrate la bordul aeronavelor, să

permită acestora supravieţuirea şi executarea unor misiuni de neutralizare a apărării aeriene inamice (SEAD).

Datorită ameninţărilor multiple din teatru, este impusă integrarea unor sisteme de armament şi avionică la bordul aeronavelor care să permită pe timpul unei singure misiuni executarea unor acţiuni multiple, constând în lovirea unor obiective şi ţinte distincte, în medii de operare diferite prin lansarea armamentului şi muniţiei potrivite. Pentru aceasta sunt de asemenea necesare, alături de posibilitatea acroşării unui armament variat (aer-aer, aer-sol, destinat loviturilor împotriva navelor de suprafaţă, radarelor etc.), şi posibilitatea acroşării unor echipamente (tip *pod)* deţinătoare ale unor funcţiuni distincte, care să permită *lansarea armamentului de precizie, discriminarea exactă a unor ţinte prioritare, executarea zborului în condiţii de vizibilitate redusă ziua sau noaptea prin urmărirea terenului* etc.

Din perspectiva utilizării *armamentului şi muniţiei*, se impune o standardizare şi compatibilizare, atât la nivelul tehnic al aeronavelor privind posibilităţile de acroşare, cât şi la cel referitor la încărcătura de luptă ce urmează să fie acroşată (rachete, bombe, lovituri de tun etc.), aspect deosebit de important în contextul operaţiilor aeriene, prin reducerea timpilor de înarmare, evitarea desfăşurării unor procese separate şi paralele privind asamblarea rachetelor, bombelor etc. Acest aspect determină atât păstrarea unui tempo ridicat al acţiunilor de luptă, cât şi eficientizarea proceselor.

Alte cerinţe impun integrarea unor echipamente (sisteme de comunicaţii rezistente la bruiaj, sisteme de identificare etc) care să permită obţinerea interoperabilităţii cu forţele militare ale aliaţilor NATO. Prin dispunerea la bordul platformelor aeriene de luptă a echipamentului *Link-16* – o reţea destinată schimbului de date militare la nivel tactic (a military tactical data exchange network), utilizată de SUA şi NATO, dar şi de alte state precum Suedia şi Japonia – este facilitat schimbul de date referitoare la câmpul de luptă (dispunerea aeronavelor inamice şi a celor aliate, a navelor şi unităţilor forţelor terestre etc.) în timp real, în mod automat şi la distanţe foarte mari, cu platformele aliate care au integrate la bord această capacitate (majoritatea platformelor aeriene ale statelor membre NATO, incluzând şi platformele AWACS, o parte dintre portavioanele şi navele Alianţei, sistemele de apărare împotriva rachetelor, elementele de comandă şi control etc.).

Însumând cerinţele prezentate anterior, avem astfel conturat profilul operaţional al viitoarelor avioane de luptă ale forţelor aeriene române, caracteristic unor avioane multirol, moderne, de generaţia a 4-a, compatibile cu platformele statelor membre NATO, apte să execute misiuni într-un mediu complex, impredictibil, caracterizat de riscuri şi asimetrii multiple.

Sintetizat, aceste cerinţe constau în: (1) *eficacitate maximă* în condiţiile câmpului de luptă modern; (2) *capacitate mărită de supravieţuire* în medii ostile, în condiţiile războiului electronic; (3) *flexibilitate în executarea întregii game de misiuni*, cu posibilitatea reconfigurării/ schimbării misiunii în timpul zborului; (4) *asigurarea unui număr mare de ieşiri-avion* în unitatea de timp, prin reducerea timpilor necesari refacerii capacităţii de zbor şi a celei de luptă; (5) *cost de operare şi mentenanţă scăzut* pe durata vieţii; (6) *autonomie mare de zbor***,** realizat prin consum redus de combustibil; (7) *capacitatea acroşării unor arme şi muniţii multiple* (aer-aer, aer-sol, anti-navă, sisteme de bruiaj etc.), într-o cantitate mare; (8) *arhitectură deschisă*, care să ofere posibilităţi de modernizare ulterioară, calităţi de zbor şi manevriere deosebite (exprimate prin viteze supersonice la orice altitudine, calităţi manevriere foarte bune, exploatare la sol şi în zbor fără restricţii, sistem de realimentare în zbor, reducerea sarcinilor pilotului, consumul eficient al resursei avionului, caracteristici bune la decolare/aterizare etc); (9) integrarea unor *sisteme şi echipamente compatibile* cu cele ale aliaţilor.

Pentru executarea unor misiuni expediţionare, forţele aeriene vor trebui să deţină *platforme aeriene de transport*, considerate capacităţi critice pentru spijinul operaţiilor aeriene

prin transportul pe calea aerului a trupelor, echipamentului, sistemelor de arme etc. în locaţii optime în interiorul ariei de responsabilitate NATO, sau în afara acesteia. Momentan, forţele militare ale Alianţei utilizează aeronavele destinate transportului strategic C-17 şi C-5 (Marea Britanie deţine 8 C-17, Canada 4 C-17, iar 10 state membre NATO au acces la un grup separate de trei C-17, cunoscut sub numele de *Capacitate Strategică de Transport Aerian (Strategic Airlift Capability – SAC*)**.**

La fel ca în cazul aeronavelor de luptă, acestea trebuie să satisfacă un set de cerinţe operaţionale referitoare la: (1) *eficacitate*, în condiţiile unor medii de operare complexe; (2) *eficienţă* prin raportare la costuri de operare, mentenanţă etc.; (3) *capacitatea de supravieţuire în* medii ostile; (4) *autonomie mare de zbor*; (5) *capacitate de încărcare mare*; (6) integrarea la bord a *echipamentelor de navigaţie, radionavigaţie moderne* care să permită zborul în toate condiţiile meteo ziua şi noaptea; (7) *capacitatea de a decola şi ateriza de pe/pe piste austere*, de dimensiuni reduse; (8) *arhitectură deschisă*, care să permită modernizări ulterioare; şi (9) sisteme compatibile cu platformele aeriene ale aliaţilor.

Referitor la *sistemele de apărare antiaeriană cu baza la sol* ale forţelor aeriene ale statelor membre NATO (GBAD), importanţa acestora este cu atât mai mare în viitor cu cât, în condiţiile ameninţărilor anterior conturate, capacităţile de lovire ale potenţialilor adversari vor cunoaşte o evoluţie semnificativă. Dezvoltarea acestora pentru a fi ajustate necesităţilor operaţionale vor constitui un important element de combatere, dar şi de descurajare a agresiunii la adresa securităţii spaţiului aerian al Alianţei.

Concluzii

Noile misiuni asumate de Alianţă, la care România ia parte, aflate într-o permanentă redefinire şi adaptare datorită factorilor externi, au determinat apariţia unui set de parametri asociaţi atât structurilor operaţionale, cât şi infrastructurii şi platformelor aeriene din dotare, înţelese din perspectiva satisfacerii scopurile urmărite (misiuni, roluri).

Satisfacerea acestor cerinţe implică – alături de aspectele referitoare doctrinelor, generării de forţe, instrucţiei şi pregătirii – şi aspecte tehnice asociate echipamentelor, armamentului şi muniţiei, sistemelor de arme, elementelor de infrastructură, respectiv proceselor asociate (achiziţii, înzestrare şi echipare). Astfel, fiecare dintre capacităţile operaţionale presupune existenţa unor elemente de infrastructură specializate care să permită derularea activităţii şi proceselor pentru exercitarea rolurilor şi executarea misiunilor.

Este cu atât mai importantă proiectarea şi integrarea în sistemul de apărare colectivă a unei infrastructuri ajustate corespunzător necesităţilor operaţionale, cu atât mai mult cu cât gradul de complexitate al mediului de securitate este într-o continuă schimbare, determinând apariţia unor ameninţări hibride noi ca exprimare, greu de anticipat şi combătut. Nu este suficientă doar deţinerea unor sisteme de arme moderne de ultimă generaţie, posesoare a celor mai noi tehnologii şi echipamente, dacă acestea nu sunt susţinute de un sistem adecvat de C2 de la sol pe de o parte, respectiv de o infrastructură logistică care să asigure atât operarea, cât şi mentenanţa acestora în mod eficient şi eficace.

Chiar dacă dezvoltarea unor platforme aeriene capabile să proiecteze puterea prin executarea misiunilor la nivel global reprezintă un process continuu, reducând necesitatea existenţei unui sistem de baze aeriene înaintate de operare, campaniile aeriene contemporane au subliniat importanţa existenţei unor astfel de baze, *"reprezentând o cerinţă fundamentală pentru obţinerea succesului în operaţiile forţelor expediţionare"*[15]. Lipsa bazelor sau un număr insuficient al acestora crează presiune nu numai pe echipaje (datorită creşterii gradului de complexitate prin executarea unor zboruri foarte lungi, necesitatea executării unui număr

[15] Ibidem.

mare de realimentări în aer, pentru ca apoi să execute atacul la obiectiv etc.), ci şi pe factorii de planificare şi pe sistemul logistic.

România deţine o infrastructură şi facilităţi valoroase – acestea fiind puse la dispoziţia Alianţei încă din perioada pre-aderare – constând, alături de aeroporturi, în porturi, terminale, căi ferate, depozite, respectiv facilităţi medicale, de mentenanţă, logistice şi de comunicaţii. În ceea ce priveşte gradul de funcţionalitate şi dezvoltare al acestora, este continuată derularea proceselor de modernizare pentru atingerea standardelor impuse la nivelul Alianţei Nord-Atlantice.

Alături de cerinţele de ordin cantitativ cu privire la existenţa fizică a unui număr suficient de baze de operare, trebuie îndeplinite cerinţe de ordin calitativ, care să permită executarea/ generarea operaţiilor aeriene din perspectiva operaţiilor de sprijin, precum refacerea capacităţii de luptă, asigurarea logistică necesară executării mentenanţei aeronavelor şi tehnicii, protecţia tehnicii şi a personalului, asigurarea medicală, de hrănire a personalului etc.

Conflictele viitoare vor implica participarea diferiţilor actori organizaţi în diferite alianţe, *"naţiunile fiind înclinate să desfăşoare atât operaţii unilaterale, dar şi altele sub forma unor coaliţii formate dintr-o mare varietate de parteneri cu capacităţi diferite"*[16], ceea ce implică la nivelul infrastructurii un nou nivel de înţelegere al compatibilităţii sistemelor, care nu este suficient să satisfacă doar echipamentele şi sistemele de arme ale forţelor militare ale NATO, ci şi pe cele ale potenţialilor parteneri de coaliţie.

Asumarea în viitor a unei game variate de misiuni şi roluri de tip nou, executate alături de aliaţi, precum cele desfăşurate în sprijinul UN şi a altor organizaţii, presupune echiparea forţelor aeriene cu un inventar care să răspundă acestui nivel de implicare, constituit din platforme aeriene variate, specializate, începând cu cele destinate loviturilor şi aplicării puterii în maniera clasică şi continuând cu cele destinate asigurării mobilităţii globale şi sprijinului, căutării-salvării, evacuării etc. Caracteristicile acestora trebuie să le permită evoluţia şi supravieţuirea în teatre de operaţii complexe, operarea de pe baze aeriene precare, cu piste de aterizare/ decolare rudimentare, de dimensiuni reduse etc. Dintr-o altă perspectivă, datorită caracterului întrunit şi multinaţional privind desfăşurarea operaţiilor militare ale Alianţei, platformele aeriene ale statelor membre NATO trebuie să deţină sisteme de comunicaţii, de identificare etc. compatibile, în vederea obţinerii interopera-bilităţii, operând astfel într-o manieră eficace, eficientă, dar şi sigură.

BIBLIOGRAFIE:

1. Duşa, Mircea, *Bilanţul MapN pe 2014,* Ministerul Apărării Naţionale, Bucureşti, 10 martie 2015, TVRNEWS.
2. Greanleaf, Jason R, *The Air War in Libya*, în *Air & Space Power Journal*, martie-aprilie 2013
3. Lamb, Michael W., *Operations Allied Force – Golden Nuggets for Future Campaigns*, BiblioScholar, US, 11 September 2012
4. Ministerul Apărării Naţionale, *Carta Albă a Apărării*, Bucureşti, 2011
5. Ministerul Apărării Naţionale, *Planul Strategic al Ministerului Apărării Naţionale 2010-2013*, Bucureşti, 2010
6. Ministerul Apărării Naţionale, *România – NATO, Primii zece ani*, 2014

[16] Jason R.Greenleaf, *The Air War in Libya*, în *Air & Space Power Journal*, martie-aprilie 2013, pag.44.

7. Ministerul Apărării Naţionale, *Strategia de transformare a Armatei României*, Bucureşti, 2007
8. NATO Infrastructure Committee, *50 Years of Infrastructure – NATO Security Investment Programme is the Sharing of Roles, Risks, Responsibilities, Costs and Benefits,* 2001
9. Orzeaţă, Mihail, *Globalization, Crises and World Security*, LAP LAMBERT, Academic Publishing, Germany, 2013
10. US Air Force, *Air Force Doctrine Document 2-4.4 – Bases, Infrastrastructure and Facilities,* 13 November 1999
11. www.nato.int

TENDINŢE ŞI CONCEPTE ÎN MODERNIZAREA FORŢELOR TERESTRE

Cristinel Dumitru COLIBABA
Doctorand, Batalionul 280 Infanterie Mecanizată
e-mail: cristicolibaba@yahoo.com

Abstract: *Pentru a fi competitive şi a putea acţiona eficient în faţa noilor riscuri şi ameninţări generate de evoluţia mediului operaţional contemporan, forţele terestre trebuie să se adapteze continuu. Capacitatea de adaptare rezidă în implementarea unui plan de modernizare şi transformare care să ofere pe termen lung o viziune care să sprijine efortul de dezvoltare a capabilităţilor şi forţelor pentru a avea succes în spaţiu de luptă întrunit.*

Cuvinte cheie: *adaptare, forţe terestre, mediu operaţional, transformare, sistem*

Introducere

Istoria ne-a arătat în permanenţă că armatele care sunt dispuse să se adapteze continuu au succes în luptă, fapt valabil mai ales în zilele noastre, când este posibil să ne confruntăm cu adversari neconvenţionali, care beneficiază de o capacitate mai mare de adaptare, nefiind restricţionaţi de procesul birocratic sau constrângeri de ordin moral.

Pentru a evita adoptarea unei atitudini reactive în faţa unui adversar aflat mereu cu un pas înaintea noastră este necesară implementarea unui plan de transformare pe termen lung a forţelor armate care să conţină schimbările şi capabilităţile cerute de evoluţia contextului operaţional viitor. Acest plan trebuie să reprezinte centrul de greutate al procesului de modernizare şi transformare a Armatei României şi să ofere o viziune clară a viitorului forţelor terestre care să sprijine eforturile de dezvoltare a forţelor şi capabilităţilor.

Prin acest plan se asigură elementele constitutive, oameni, echipamente şi tehnologii, care vor permite forţelor terestre să obţină victoria în spaţiul de luptă întrunit al viitorului şi de asemenea, se pot identifica aspectele care necesită o mai profundă investigare, experimentare şi analiză.

Demersul propus trebuie să aibă punctul de plecare în descrierea mediului operaţional şi stabilirea principiilor care trebuie respectate în generarea viitoarei structuri de forţe, ulterior identificarea conceptelor şi cerinţelor tactice necesare gestionării eficiente a viitoarelor conflicte.

1. Contextul operaţional

Chiar dacă viitorul nu poate fi prezis cu exactitate şi incertitudinea va fi caracteristica dominantă a mediului operaţional în care vor opera forţele terestre, se pot determina anumite tendinţe relativ stabile care pot ghida cu suficientă claritate eforturile de modernizare.

Un punct de plecare îl reprezintă misiunea fundamentală a Armatei României, care constă în „*apărarea intereselor naţionale ale României, în condiţiile democraţiei constituţionale şi ale controlului democratic şi civil asupra forţelor armate. Armata trebuie să fie pregătită să prevină, să descurajeze şi să contracareze o eventuală agresiune armată*

împotriva României şi aliaţilor săi"[1], precum şi misiunile generale, stipulate în *Carta albă a apărării*, respectiv:

- contribuţia la securitatea României pe timp de pace;
- apărarea suveranităţii şi integrităţii teritoriale a României;
- participarea la apărarea aliaţilor săi, în cadrul NATO şi UE;
- promovarea stabilităţii regionale şi globale, inclusiv prin utilizarea diplomaţiei apărării;
- sprijinul autorităţilor publice centrale şi locale, în situaţii de urgenţă, pentru acordarea de asistenţă populaţiei şi managementul consecinţelor dezastrelor.

Pentru realizarea acestor misiuni este necesară utilizarea unor concepte moderne de planificare operaţională, unul dintre acestea fiind acela de „campanie adaptabilă" care conţine cinci linii de operaţii independente, dar care se pot completa reciproc: Lupta Terestră Întrunită, Protecţia Populaţiei, Operaţii Informaţionale, Sprijinul Populaţiei şi Dezvoltarea Capabilităţilor Locale. Forţele terestre viitoare trebuie să fie optimizate pentru prima linie de operaţie, cu toate că vor deţine capacitatea de a participa, la nevoie, şi în cadrul celorlalte linii de operaţii, pentru că ducerea luptei şi siguranţa pe care o oferă, reprezintă o condiţie esenţială pentru executarea celorlalte linii de operaţii.

Luând în considerare complexitatea mediului operaţional, cheia succesului forţelor terestre va fi gestionarea eficientă a eforului în cadrul celor cinci linii de operaţii, în locul potrivit şi la momentul potrivit, cu respectarea următoarelor principii:

1. Flexibilitea – abilitatea de a menţine eficienţa de-a lungul întregii game de misiuni, situaţii şi condiţii, în cadrul unei linii de operaţie;

2. Agilitatea – abilitatea de a gestiona dinamic, în timp şi spaţiu, capacitatea de efort de-a lungul tuturor liniilor de operaţii;

3. Rezistenţa – capacitatea de a suporta pierderi, deteriorări şi întârzieri cu menţinerea nivelurilor esenţiale de capabilitate a funcţiunilor cheie;

4. Capacitatea de răspuns – abilitatea de a identifica rapid şi, ulterior, de a reacţiona eficient la noi ameninţări şi oportunităţi din cadrul unei linii de operaţie;

5. Robusteţe – abilitatea de a genera şi susţine un nivel optim al forţelor în funcţie de densitatea populaţiei şi capabilităţile adversarilor, obţinându-se astfel un control suficient al mediului operaţional pentru a gestiona incertitudinea şi a acţiona de-a lungul celor cinci linii de operaţii.

Un alt aspect de care trebuie să se ţină cont în proiectarea viitoarei structuri de forţe îl reprezintă capacitatea de a acţiona în mediu urban, incluzând aici operaţii de asistenţă umanitară şi reconstrucţie, dar şi operaţii în care adversarul adoptă în mod deliberat tactica de „ascundere printre populaţie". În îndeplinirea tuturor misiunilor şi sarcinilor, soldaţii din forţele terestre a viitorului vor trebui să fie capabili să angajeze eficient populaţia locală pentru a putea influenţa percepţia şi comportamentul acestora.

Tehnologia este un alt element care va avea o influenţă deosebită asupra mediului operaţional şi cu toate că avantajul tehnologic va rămâne o componentă de bază a eficacităţii militare, impactul său va depinde în mare măsură de modalitatea în care este folosit şi de deprinderile celor care îl utilizează.

Din punct de vedere al potenţialelor ameninţări cu care se vor confrunta forţele terestre este de menţionat că natura adversarului poate varia de la unul major, chiar dacă la momentul actual, conform *Strategiei de apărare naţională*, posibilitatea unui conflict interstatal tradiţional pare fie minimă pentru România, la o serie de forţe neregulate constituite ad-hoc care pot executa acţiuni în cadrul întregului spectru al conflictului. Adversarii cu care este posibil să se confrunte forţele terestre în viitor vor fi adaptabili şi vor schimba abordarea

[1] Ministerul Apărării Naţionale, *Carta albă a apărării*, Bucureşti, 2013, p. 25.

operaţională în funcţie de experienţa dobândită, cel mai periculos curs de acţiune fiind un adversar care ar avea posibilitatea să coordoneze executarea unei campanii multi-dimensionale, atacând simultan în plan fizic, informaţional şi moral.

Având în vedere natura viitorului tip de conflict, este probabil ca o gamă variată de activităţi din cadrul spaţiului de luptă să se desfăşoară simultan, multe dintre acestea aflându-se la graniţa dintre responsabilităţile tradiţionale militare şi cele civile, incluzând aici aplicarea legii, acţiuni în caz de dezastre şi dezvoltarea capabilităţilor locale. Astfel, puţine provocări de securitate viitoare vor fi rezolvate cu succes doar prin aplicarea forţei militare şi mai mult decât atât, luând în considerare impactul globalizării şi creşterea interconectivităţii dintre state, forţele terestre vor acţiona foarte probabil ca parte a unei forţe întrunite, interagenţii, interguvernamentale sau multinaţionale.

Dimensiunea umană este un alt aspect care trebuie luat serios în considerare pentru că, aşa cum a fost întotdeauna, succesul forţelor terestre v-a depinde de abilităţile militarilor săi, cu specificaţia că în operaţiile viitoare acţiunile tactice ale fiecărui soldat şi consecinţele lor pot avea importanţă strategică. Având în vedere posibilitatea ridicată a unei examinări minuţioase din partea mass-media şi a publicului în general, transparenţa va deveni un imperativ operaţional şi aderarea la cele mai înalte valori etice va fi esenţială. Mai mult decât atât deprinderile complexe de luare a deciziilor vor fi critice pentru militarii de toate nivelurile.

2. Consideraţii de nivel tactic

Viitoarea forţă terestră va fi reprezentată de un sistem de sisteme, care va cuprinde diferite tipuri de forţe, cu diferite niveluri de pregătire, formare, echipare şi personal care se integrează pentru a realiza eficacitatea operaţională. Fiecare element al sistemului are diferite caracteristici şi capabilităţi, astfel că pentru a sprijini dezvoltarea corectă a acestor elemente este necesară utilizarea unui concept nou, evoluat din sistemele de operare pe câmpul de luptă şi ulterior din funcţiunile de luptă, denumit Sisteme primare terestre integrate. Diferenţa dintre cele două concepte constă în faptul că în timp ce funcţiunile de luptă sunt concentrate pe orchestrarea efectelor, sistemele primare terestre integrate reprezintă o abordare mai cuprinzătoare care pune accent pe dezvoltarea şi integrarea capabilităţilor care permit folosirea efectelor pe câmpul de luptă şi cuprinde următoarele sisteme:

- soldatul ca sistem;
- sistemul de luptă;
- sistemul de operaţii speciale;
- sistemul de sprijin de luptă;
- sistemul de sprijin logistic
- sistemul de comandă, control şi comunicaţii (C3).

Soldatul ca sistem. Un prim sistem primar este „soldatul ca sistem”, conceptul neavând intenţia de a dezumaniza soldatul, ci să pună accentul pe importanţa individului în următoarea structură de forţe terestre. Considerând soldatul ca pe un sistem distinct, se asigură faptul că soldaţii şi tot ceea ce învaţă, fiecare acţiune pe care o execută, tot ceea ce întrebuinţează, transportă şi consumă funcţionează împreună ca un sistem integrat. Din punctul de vedere al dimensiunii umane este nevoie ca indivizii să fie pregătiţi pentru executarea operaţiilor specifice forţelor terestre prin dezvoltarea componentelor fizice, psihologice, sociale, intelectuale şi morale ale soldatului.

Sistemul de luptă va fi solicitat să stabilească şi să menţină securitatea în medii caracterizate de violenţă, incertitudine, complexitate şi haos şi este format din luptători şi platforme mobile de luptă terestră, elemente care asigură capacitatea de a luptă, ca parte a

unei grupări interarme, în contact cu adversarul indiferent de teren şi în toate tipurile de acţiuni tactice ale spectrului conflictului.

Sistemul de operaţii speciale conţine forţe capabile să execute operaţii specializate de către indivizi şi echipe atent selecţionate, instruite şi pregătite şi care beneficiază de o atitudine creativă capabilă să producă soluţii dincolo de abordările convenţionale. Principalul atu al acestui sistem este abilitatea de a executa întregul spectru de operaţii bazându-se pe capabilitatea de a rezolva probleme unicat prin care să se obţină efecte la nivel operaţional şi strategic.

Sistemul de sprijin de luptă reprezintă un ansamblu de sub-sisteme critice pentru obţinerea şi menţinerea libertăţii de acţiune, precum şi pentru asigurarea unei capacităţi de luptă multiplicată prin acţiuni de sprijin, respectiv: protecţia forţei, cunoaşterea spaţiului de luptă, operaţiile informaţionale, mobilitatea, focul întrunit, apărarea antiaeriană şi antirachetă, sprijinul manevrei, protecţia împotriva dispozitivelor explozive improvizate şi apărarea CBRN.

Protecţia forţelor implică măsuri coordonate în timp şi spaţiu pentru contracararea şi limitarea riscurilor şi ameninţărilor, cu scopul de a asigura un mediu operaţional în care comandanţii să aibă libertatea de manevră. Pentru asigurarea protecţiei viitoarelor forţe terestre este necesar un ansamblu echilibrat de măsurile active, pasive şi de recuperare care să ofere flexibilitatea şi agilitatea de a răspunde eficient la noi circumstanţe în acelaşi timp cu menţinerea abilităţii de a executa misiunile încredinţate.

Cunoaşterea spaţiului de luptă asigură elaborarea unor estimări relevante, corecte, cuprinzătoare şi în timp scurt care să permită aplicarea cu succes a puterii de luptă, să asigure protecţia forţei şi îndeplinirea misiunii şi cuprinde la rândul său sub-sistemul Informaţii, Supraveghere, Achiziţia ţintelor şi Cercetare (ISTAR)[2] şi sub-sistemul război electronic[3].

Operaţiile informaţionale vor reprezenta o activitate importantă în viitor având în vedere că mediul informaţional[4] va afecta semnificativ executarea operaţiilor viitoare datorită expansiunii rapide a organizaţiilor şi reţelelor globale de vehiculare a informaţiilor. De aceea, acest sub-sistem trebuie să se asigure că informaţiile deţinute de forţele terestre oferă un avantaj în faţa adversarilor prin exploatarea tuturor mijloacelor la dispoziţie, inclusiv angajarea comunităţilor, forurilor internaţionale şi mass-media.

Mobilitatea este o altă caracteristică esenţială a viitoarelor forţe terestre şi are drept scop principal dislocarea elementelor luptătoare în apropierea obiectivului unde vor putea debarca în relativă siguranţă şi vor executa asaltul. Acest sub-sistem cuprinde un ansamblu optimizat de putere de foc, mobilitate şi protecţie şi este capabil să susţină operaţii de amploare în timp şi spaţiu.

Pentru executarea eficientă a sprijinului prin foc întrunit este fundamentală abilitatea acestui sub-sistem de a planifica, coordona, prioritiza şi controla obţinerea efectelor precise şi pe arii extinse în sprijinul forţelor terestre. Scopul lui este de a angaja ameninţările în acelaşi timp cu luarea tuturor măsurilor pentru evitarea fratricidului şi a daunelor colaterale şi va asigura abilitatea de a fi integrat la cel mai mic nivel cu aliaţii pentru obţinerea efectelor întrunite în cadrul coaliţiilor multinaţionale.

Sub-sistemul de apărare antiaeriană şi antirachetă va fi compus din sisteme de armament sol-aer care vor fi complementare cu componente ale supravegherii aeriene

---

[2] Sistemul ISTAR trebuie să fie în măsură să îndeplinească următoarele funcţiuni: prioritizarea cerinţelor critice de informaţii ale comandantului, managementul misiunii, colectarea datelor, analiza datelor, exploatarea datelor, diseminare, achiziţia ţintelor.

[3] Sistemul război electronic contribuie la obţinerea unei game largi de efecte în câmpul de luptă şi include: sprijinul electronic, atacul electronic şi protecţia electronic.

[4] Mediul informaţional este constituit din ansamblul de indivizi, organizaţii cu modelele lor sociale şi culturale, precum şi din sistemele care colectează, procesează, diseminează sau acţionează în baza informaţiilor deţinute.

asigurând astfel un nivel optim de protecţie împotriva unei game largi de posibile ameninţări, cum ar fi: avioane şi elicoptere, sisteme aeriene fără pilot, sisteme de armament de artilerie şi rachete balistice.

Sub-sistemul de sprijin al manevrei va încorpora două concepte principale:

- *mobilitatea asaltului*, care constă în executarea de acţiuni de trecere şi înlăturare a obstacolelor şi executarea breşelor pentru a crea condiţii favorabile forţelor luptătoare în executarea manevrei în orice fel de teren, înainte, pe timpul şi după realizarea contactului cu adversarul.
- *reducerea riscurilor*, care constă în capabilităţi specializate de minimizare a pericolelor spaţiului de luptă viitor, incluzând aici şi atacurile asimetrice cu substanţe explozive şi CBRN.

Apărarea împotriva atacurilor cu dispozitive explozive improvizate se bazează pe o abordare multi-disciplinară, eforturile fiind concentrate la început pe atacarea reţelelor pentru prevenirea amplasării unor astfel de dispozitive, iar în situaţia în care acest lucru nu are succes se va trece la neutralizarea dispozitivului.

Apărarea CBRN se va concentra pe asigurarea protecţiei atât împotriva ameninţărilor convenţionale, cât şi a celor improvizate. Pentru a contracara ameninţările convenţionale acest sub-sistem va continua să se bazeze pe colectarea de date şi informaţii pentru avertizare şi angajare, pe sprijinul de foc întrunit pentru executarea de atacuri şi de sprijinul de geniu pentru neutralizarea dispozitivelor, în timp ce în cazul ameninţărilor neconvenţionale se va folosi o procedură similară apărării CIED.

Sistemul de sprijin logistic este un element cheie în cadrul demersului de modernizare a forţelor terestre şi trebuie să fie capabil să asigure resurse şi servicii esenţiale într-o manieră proactivă, prin utilizarea eficientă a reţelelor şi personalului avut la dispoziţie. Este compus la rândul său dintr-o serie de sub-sisteme esenţiale, respectiv:

- sub-sistemul de mentenanţă;
- sub-sistemul de sănătate;
- sub-sistemul de servicii de campanie.

Sistemul de comandă, control şi comunicaţii este un alt factor decisiv pentru asigurarea succesului forţelor terestre în spaţiul de luptă viitor şi va trebui să fie capabil să se adapteze la mediul de operare în acelaşi timp cu exploatarea eficientă a capabilităţilor avute la dispoziţie. Acesta este un nou concept, denumit „sistem de comandă, control şi comunicaţii adaptabil" care conţine oameni (comandanţi şi personal de stat major), organizaţii şi reţele, toate având ca principală caracteristică capacitatea de adaptare.

Concluzii

Sistemul militar evoluează, iar componentele acestuia devin din ce în ce mai integrate şi interconectate, astfel că este esenţial a se identifica acele capabilităţi care trebuie să fie păstrate, cele la care trebuie să renunţăm şi cele care se pot redistribui către alte elemente ale sistemului de apărare.

În urma realizării demersului de faţă se pot stabili câteva linii directoare a procesului de modernizare şi transformare a armatei, respectiv:

- ducerea luptei împotriva unui adversar credibil rămâne fundamentul pe care trebuie să se planifice structura de forţe;
- dezvoltarea echilibrată a unor structuri de manevră şi sprijin care să fie capabile să contribuie la apărarea ţării şi a intereselor naţionale;
- implementarea unor concepte strategice, operaţionale şi tactice noi, care să crească eficienţa planificării şi executării întregii game de misiuni;

- dezvoltarea capacităţii forţelor terestre de a acţiona în cadru întrunit şi multinaţional;
- dezvoltarea unei forţe care să fie adepta filosofiei eficienţei şi eficacităţii prin exploatarea tehnologiilor nou apărute.

Această lucrare a fost realizată cu sprijinul finanţării obţinute în cadrul proiectului de studii doctorale şi postdoctorale: „Studii doctorale şi postdoctorale Orizont 2020: promovarea interesului naţional prin excelenţă, competitivitate şi responsabilitate în cercetarea ştiinţifică fundamentală şi aplicată românească" Contract POSDRU/159/1.5/S/140106.

BIBLIOGRAFIE:

1. AUS Departement of Defence, *Campania adaptativă. Conceptul viitor de operare a forţelor terestre*, Canberra, 2009;
2. Carta albă a apărării, Bucureşti, 2013;
3. Land warfare development centre, *The Army Objective Force 2030*, 2011;
4. Strategia naţională de apărare a ţării, Bucureşti, 2008;
5. US JFCOM, *Mediul operaţional întrunit. Lumea până în 2030 şi mai departe*, 2006.

RISCURI CIBERNETICE ŞI VULNERABILITĂŢI, UN PERICOL CLAR ŞI ACTUAL

Emanoel MATEI
Facultatea de Ştiinte Politice, Universitatea Bucureşti, student masterand, Bucureşti, Romania,
e-mail: f117@astrospot.ro

Ioana Corina JULAN
Facultatea de Ştiinte Politice, Universitatea Bucureşti, student, Bucureşti, Romania,
e-mail: julan.ioan-corina@fspub.unibuc.ro

Abstract*: Lucrarea de faţă explorează pe scurt unele dintre principalele riscuri, ameninţări şi vulnerabilităţi din zona spaţiului cibernetic. Folosind în mod extensiv diferite surse deschise vom analiza atacurie cibernetice cele mai importante care au avut loc pe parcursul ultimului an, cum ar fi atacul Sony spre sfârşitul anului 2014 şi explorarea vulnerabilităţilor cibernetice, a riscurilor*

şi ameninţărilor atât la nivel naţional cât şi la nivele mai mici precum şi impactul având ca suport dispozitivele de securitate mobile. Vom încerca să clasificăm riscurile de expunere şi vom încerca să prezentăm, să descriem şi să analizăm pe scurt cele mai importante vulnerabilităţi majore care sunt prezent în acest moment în spaţiul cibernetic. Lucrarea nu are pretenţiea de exhaustivitate şi se bazează pe studiul extins a diverse surse deschise şi a unor lucrări importante în domeniul Ştiinţelor Politice, Studiilor Strategice şi Studiilor Puterii Cibernetice.

Cuvinte cheie: *atac cibernetic, Cyber risc, Cyber vulnerabilitate, atac Sony, Atingerea securitate.*

Această lucrare nu îşi propune să ofere cititorilor o serie de fapte generale despre întreaga zonă a ameninţărilor cibernetice. Are un scop cu totul diferit, acela de a oferi o perspectivă nouă asupra cazurilor de ameininţări cibernetice care au avut loc pe parcursul ultimului an. La începutul acestei lucrări vom încerca să explicăm conceptele de bază folosite, în scopul de a facilita o mai bună înţelegere a cititorului asupra faptelor prezentate în secţiunile următoare.

Spaţiul cibernetic este definit ca fiind "un domeniu funcţional, definit prin utilizarea de electronice în scopul (...) de a exploata informaţiile prin intermediul sistemelor interconectate şi infrastructurii asociate cu aceasta"[1]. În plus faţă de această definiţie prezentă într-o lucrare de ştiinţe politice, există definiţii mai tehnice care definesc spaţiul cibernetic ca fiind "un domeniu global în mediul informaţional care constă în infrastructura interdependentă a reţelelor IT si TIC, inclusiv Internetul, reţelele de telecomunicaţii, sistemele informatice şi procesoarele şi controlerele aferente"[2].

[1] Robert O. KEOHANE and Joseph S. NYE, "Power and Interdependence: World Politics in Transition", Little Brown, Boston, 1977, p.

[2] U.S. Department of Energy, "Electricity Subsector Cybersecurity", p.67, accessed on March 25, 2015 at the Internet address
http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

Pentru Daniel Kuehl, profesor de Managementul Sistemelor la Departamentul de Operaţiuni Informatice şi Asigurare la Colegiul de Managementul Resurselor Informatice a Universităţii Naţionale de Apărare de la Ft. McNair, Virginia, spaţiul cibernetic este "un domeniu operaţional încadrat de folosirea mijloacelor electronice şi a spectrului electromagnetic pentru a crea, stoca, modifica, schimba, precum şi pentru exploatarea de informaţii prin intermediul sistemelor informatice interconectate şi conectate la internet şi infrastructurile asociate acestora"[3].

Atacurile cibernetice - hacking de diferite tipuri – au devenit parte a vieţii cotidiene. De-a lungul timpului au existat o multitudine de actori de stat acuzaţi de a fi luat parte la atacuri cibernetice îndreptate împotriva altor state, companii sau cetăţeni cu diverse locuri de muncă şi responsabilităţi. Există, de asemenea indivizi sau grupuri de indivizi bine pregătiţi, care îşi desfăşoară activitatea în comun, în scopul de a obţine acces la diverse informaţii care nu sunt publice şi care ulterior sunt folosite într-o formă sau alta. Mii de astfel intruziuni sunt detectate în fiecare zi, dar există unele care rămân nedetectate pentru o perioadă lungă de timp, continuând cu înregistrarea informaţiilor şi oferind atacatorilor acces continuu la sistemul compromis sau la reţea. Exista temeri asupra faptului că atacurile pot fi utilizate în scopuri geo-strategice, pentru a colecta informaţii sensibile, a testa puterea de securitate a statului vizat şi capacitatea sa de reacţie a descuraja, împiedica astfel de atacuri.

Puterea cibernetică - reprezintă capacitatea de a folosi un număr bine definit de resurse ale spaţiului virtual pentru a crea avantaje şi pârghii în toate celelalte medii operaţionale combinate cu instrumente de putere.[4]

Ameninţările cibernetice - acest tip de ameninţări are un impact enorm asupra vieţii noastre de zi cu zi, a afacerilor sau a unor instituţii şi servicii sociale esenţiale. Cel mai recent exemplu de ameninţare cibernetică a avut loc la lansarea filmului Sony Pictures "Interviu", atunci când atacatorii avut acces la nume, adrese, numere de securitate socială şi alte informaţii financiare ale unui număr mare de angajaţi, lansând ameninţări concrete, fizice, atât împotriva lor cât şi a membrilor familiilor lor.

Terorismul cibernetic - este convergenţa terorismului şi a spaţiului virtual, cu atacuri împotriva computerelor şi reţelelor cu scopul de a intimida sau de a constrânge un guvern sau o naţiune în promovarea unor obiective politice sau sociale.

Conceptul *Cyber* se referă la un loc în care datele pot fi schimbate între diferite sisteme interconectate, routere şi alte dispozitive electronice, utilizând acelaşi protocol de comunicare şi ascultă de aceleaşi reguli de reţea. În prezent, aceasta este una dintre cele mai importante simple şi uşoare modalităţi de a obţine influenţă, un mod disponibil pentru orice entitate, mare sau mică, publică sau privată: companii, organizaţii, persoane fizice, terorişti. Dacă spaţiul virtual este un domeniu comparabil cu alte domenii "obişnuite", cum ar fi spaţiul terestru, maritim, aerian şi spaţiul analizat în contexte tradiţionale geopolitice, este un subiect care merită o discuţie mai amplă.[5]

Hacking-ul, în general, desemnează operaţiuni care exploatează calculatoare sau trec peste sisteme de securitate cu ajutorul unui software special creat (şi malware).

Hackerii sunt persoane cu cunoştinţe tehnice avansate care petrec ore nesfarsite finisându-şi abilităţile. Cei mai mulţi dintre ei sunt motivaţi de curiozitate şi se provoacă în scopul de a vedea dacă pot perturba sistemul informatic. Nu ar trebui să considerăm curiozitatea în acest caz un act terorist însă trebuie să luăm în considerare faptul că astfel de abilităţi pot fi folosite în activităţi teroriste.

[3] Department of Defense, "2006 Quadrennial Defense Review Report", Washington, DC: Department of Defense, February 6, 2006, accessed on March 25, 2015 at the Internet address http://www.defense.gov/qdr/report/Report20060203.pdf

[4] *Ibidem*

[5] *Ibidem*

Trebuie să înţelegem că lumea noastră, fie că ne place sau nu, devine din ce în ce mai interconectată. Spaţiul cibernetic se extinde de la calculatoarele noastre obişnuite la tot mai multe elemente obişnuite ale vieţii domestice: cuptoare cu microunde, frigidere, aparate de aer condiţionat, televizoare, oferindu-ne un loc mai bun de a trăi şi un control mai bun asupra confortului şi stilului nostru de viaţă. Spaţiul cibernetic devine tot mai 'real' pe măsura ce noi devenim inevitabil mai 'virtuali'. Noţiunea militară veche de primă linie a frontului, continuă şi uşor de recunoscut devine depăşită cu fiecare zi care trece, noi toţi devenind acum "prima linie" a luptei prin gradul de expunere tot mai ridicat. Pentru a câştiga bătălia avem nevoie să dezvoltăm un set de instrumente cibernetice şi o atitudine pozitivă faţă de grupurile mari de populaţie. Dar este foarte clar că aceste tipuri diferite de atacuri care au loc în spaţiul cibernetic pot influenţa rezultatul unor evenimente majore care au loc pe scena internaţională.

1. Cazul ISIL – Terorismul cibernetic şi Reţelele sociale

Statul Islamic din Irak şi Levant (ISIL) a fost prima organizatie care a utilizat masiv şi într-adevăr sistematic social media pentru a răspândi frica. Filmele lor provocă scandaluri la nivel global, ceea ce face ISIL mai cunoscut decât orice altă organizaţie teroristă sau structură anterioară. Folosind *Twitter, Facebook, LiveLeak, YouTube* şi alte site-uri bine-cunoscute, au vizat un număr masiv de oameni pentru a răspândi zvonuri cu privire la propria lor existenţă şi programul lor public. ISIL a aplicat aceleaşi vectori de publicitate ca orice agent economic occidental. Societatea noastra absoarbe în mod regulat o mulţime de ştiri de ultimă oră, iar reţelele sociale media sunt terenul perfect pentru propagarea unor astfel de ştiri. Atunci când informaţiile îşi ating ţintele acestea se transformă la rândul lor în transmiţători diseminând informaţiile in mod spectaculor. Chiar dacă motivaţia este una complet diferită, cu fiecare individ care raspandeşte ştirea mai departe, mesajul este din ce în ce mai sonor şi astfel se ajunge la captarea unui public neaşteptat de mare. Scopul de propagandă este astfel îndeplinit. Descrierea unui astfel de model a fost relatată de *Time* la data de 11 septembrie 2014: "teroriştii iubesc Twitter. Aceasta include Statul Islamic din Irak şi Levant (ISIL), extremiştii musulmani sunniţi pe care SUA ii vizează într-o campanie militară extinsă. ISIL devine grupul cel mai sofisticat care utilizează acest serviciu pentru a-şi răspândi mesajul însetat de sânge."[6]

Nu avem posibilitatea de a contracara rapid mesajul iar, pe termen lung, aceste mesaje pot afecta moralul unei populaţii mari. Utilizatorii social media sunt în multe ocazii dornici de a vedea orice fel de contra-acţiune din partea autorităţilor, astfel încât filmele anti-propagandă sau chiar o lovitură armată împotriva organizaţiei teroriste este de cele mai multe ori binevenită.

O altă problemă este cea a recrutării. Acest tip de propagandă poate face un număr mare de persoane să îşi dorească să înceapă o aventură periculoasă pentru o cauză virtuală. Numărul de "voluntari" este în creştere şi site-urile sunt un instrument puternic pentru organizaţiile extremiste de tot felul. Potrivit unei surse deschise "în ultimii ani, recrutorii online au câştigat cu succes în faţa occidentalilor, inclusiv a americanilor"[7], a declarat Rita Katz, director şi co-fondator al SITE Intelligence Group[8], care a studiat, urmărit, şi analizat teroriştii internaţionali, reţeale jihadiste globale şi surse ale finanţării terorismului pentru mai mult de un deceniu.

[6] Alex ALTMAN, "Why Terrorists Love Twitter", Time, September 13, 2014, accessed on March 25, 2015 at the Internet address http://time.com/3319278/isis-isil-twitter/?xid=newsletter-brief

[7] Maria VULTAGGIO, "ISIS Online Recruitment: 3 Colorado Teenage Girls A Textbook Case", Ibi Times, November 11, 2014, accessed on March 25, 2015 at the Internet address http://www.ibtimes.com/isis-online-recruitment-3-colorado-teenage-girls-textbook-case-1722155

[8] SITE Intelligence Group is a for-profit Bethesda, Maryland-based company that tracks online activity of White supremacist and Jihadi organizations.

Organizaţiile teroriste pot trece cu uşurinţă la oricând următorul nivel - finanţarea socială sau apelul la grupurile pe care le abordează online în acest scop şi astfel începe colectarea de bani de la mai mulţi susţinători. Ei pot folosi diverse tipuri de monede virtuale pentru a obţine bani reali de la aceştia, direct de la donatori. Acest lucru poate mobiliza susţinătorii să joace un rol activ şi să sprijine cauza. La 29 ianuarie 2015 o sursă deschisă a relatat că "un analist de la Tel Aviv care lucrează pentru o companie de *cyber intelligence* din Singapore a descoperit dovezi concrete că o celulă teroristă, care are legături cu Statul Islamic şi care operează în America, a solicitat *Bitcoins*, ca parte a eforturilor sale de strângere de fonduri."[9]

Internetul este un loc sigur pentru terorişti. Ei nu au nevoie să călătorească şi sunt pe deplin capabili să rămână anonimi. Teroriştii pot ascunde, de asemenea, mesajele lor folosind internetul ca un "dispozitiv de transport" pentru comunicarea criptată.

2. Atacul Sony de la sfârşitul anului 2014

La sfârşitul anului 2014, Sony Pictures a fost lovit de un atac major. În acest caz particular, putem spune cu siguranţă că atacul a avut mai mulţi vectori. Este un exemplu care evocă diferenţele semnificative dintre puterea unui actor statal şi a capacităţilor de putere ale unei mari companii.

Atacul a fost, în măsura în care ştim, bazat pe o *vulnerabilitate ziua zero*, (o vulnerabilitate descoperită după folosirea aceluiaşi sistem de operare sau serviciu de către cineva care cauta aceste tipuri de gauri de securitate), precum şi cartografierea întregii reţele *Sony Pictures* până când topologia internă a reţelei lor a fost expusă atacatorului. În a doua fază de atac, hackerii au început să extragă date din reţea, inclusiv e-mailuri interne ale companiei, datele cu caracter personal şi datele financiare ale angajaţilor.

Atacul a fost revendicat de un grup necunoscut care se autointitulează *Gardienii Păcii*. Atacatorii au fost hackeri din Coreea de Nord şi care în acea noapte au operat, în măsura în care ştim, de la un hotel din Thailanda.[10]

Acest atac a forţat *Sony* să amâne premiera filmului care era programată la acea dată iar imaginea publică a companiei *Sony* a avut de suferit foarte mult. *Sony* a cumparat de fapt, timp pentru a evalua întreaga reţea şi a verifica fiecare sistem şi calea de intruziune. Cu ajutorul NSA şi FBI, *Sony* a fost capabilă să identifice calea de intruziune şi alte informaţii relevante care leagă Coreea de Nord de atac. Angajaţii au fost forţaţi să renunţe la echipamentele electronice şi să îşi desfăşoare munca, folosind stilou, hârtie şi faxuri după hack.

Hackerii au furat, de asemenea, cinci filme *Sony* nelansate până la acea dată, şi le-a făcut publice pe reţelele de file-sharing, cauzând o pierdere financiară uriaşă a companiei. Ei au expus, de asemenea, multe conversaţii private din e-mailurile top managementului.

Astfel de atacuri sunt dificil de evitat şi de asemenea este greu de conceput o reţea absolut impenetrabilă.Coreea de Nord şi-a dezvoltat propriul sistem de operare, din motive evidente ce ţin de anumite temeri legate de spionaj, denumit "Red Star OS".

Lipsa de securitate internă a Sony a condus la această furt masiv de date. Lipsa straturilor şi nivelurilor interne de securitate combinate cu un sistem care nu dispune de proceduri de detectare a intruziunilor (un calculator sau un software care poate monitoriza

[9] Donna HARMAN, "U.S.-based ISIS cell fundraising on the dark web, new evidence suggests", Haaretz, January 29, 2015, accessed on March 25, 2015 at the Internet address http://www.haaretz.com/news/middle-east/.premium-1.639542

[10] Cheryl K. CHUMLEY, "Guardians of Peace hackers thank Sony for scrubbing 'The Interview'", Washington Times, December 19, 2014, accessed on March 25, 2015 at the Internet address http://www.washingtontimes.com /news/2014/dec/19/guardians-of-peace-hackers-thank-sony-for-scrubbin/

activitate suspectă, încălcarea politicilor şi notificarea conducerii sau a administratorilor de sistem) au stat la baza a ceea ce s-a întâmplat.

3. Atacurile împotriva NATO

Aşa cum am menţionat anterior, hackerii de obicei preiau controlul asupra sistemelor de calcul utilizând bug-uri nedescoperite. În octombrie 2014, hackerii ruşi au exploatat un bug gasit (şi care nu a fost raportat) în Microsoft Windows pentru a spiona calculatoarele mai multor structuri NATO, a Uniunii Europene, şi calculatoare din Ucraina şi din societăţile active în domeniul telecom şi al energiei.[11] *Atacurile au fost total diferite de orice alt tip de astfel de acţiuni prezentate până acum*. Atacatorii au utilizat, printre altele, o tehnica numita "Inginerie socială": atunci când utilizatorii primesc un e-mail care pare să vină de la o sursă legitimă, sunt înşelaţi să pornească un software ataşat unui e-mail iar hackerii obţin acces la sistemul de afectat. De obicei, aceste tipuri de atacuri dezactivează fără notificări protecţia calculatorului, inclusiv firewallul sistemului de operare şi protecţia împotriva viruşilor.

Dacă analizăm tipul de informaţii care pot fi obţinute în urma infestării unor astfel de sisteme putem concluziona faptul că hackerii au fost fie sponsorizaţi de către un stat sau angajaţi ca şi contractori însă este greu de identificat statul cu exactitate, chiar dacă putem specula.

Un studiu recent care include şi recomandări pentru generarea unor politici, precizează că "atacurile cibernetice pot varia de la atacuri mici, care produc pagube minore la atacuri foarte mari, care pot provoca daune masive. Este dificil de indicat un prag clar sub limita căruia un atac poate fi considerat minor dar peste care ar trebui să se declanşeze preocupări serioase în scopul descurajarii şi posibilitatea de a raăspunde cu represalii. Scala de escaladare conţine multe trepte de provocări crescânde şi daune, fiecare dintre ele meritând un raspuns, o creştere a intensităţii. O strategie de descurajaree cibernetică în SUA ar trebui modelată mai degrabă pentru a identifica răspunsuri decisive, proporţionale pentru fiecare nivel al scalei, decât încercarea de a specifica un singur prag care desparte acţiunile care nu necesită un răspuns de cele care au nevoie de răspunsuri puternice."[12]

Răspunsul la tentativă de spargere a protecţiei sistemelor de calcul ale NATO sau perturbarea comunicaţiilor electronice, trebuie analizat şi dimensionat corespunzător. Se poate intervenii local, prin oprirea atacatorului folosind mijloace clasice în cazul în care atacul este uşor de îndepărtat (filtru firewall) sau la nivel de nod reţelistic continental pentru atacurile susţinute sau de o complexitate mai mare.

4. Noi provocări ale spaţiului cibernetic

"Reflectând asupra manierei in care toate conflictele internaţionale au acum o anumită componentă digitală, NATO şi-a actualizat politica de apărare cibernetică pentru a clarifica faptul că că un atac cibernetic pot fi tratate ca echivalent al unui atac cu arme convenţionale"[13], menţionează surse deschise.

[11] Jim FINKLE, "Russian hackers target NATO, Ukraine and others: iSight", *Reuters*, October 14, 2014, accessed on March 25, 2015 at the Internet address http://www.reuters.com/article/2014/10/14/us-russia-hackers-idUSKCN0I308F20141014

[12] Franklin D. KRAMER, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", March 2014, accessed on March 25, 2015 at the Internet address http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-01.pdf

[13] Steve RANGER, "NATO updates cyber defence policy as digital attacks become a standard part of conflict", ZDNet, June 30, 2014, accessed on March 25, 2015 at the Internet address http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/

La 5 septembrie 2014, Sorin Ducaru, secretar general adjunct al NATO pentru riscurile de securitate emergente, a declarat că "articolul 5 din tratat se extinde şi asupra dezinformării, subversiunii şi atacurilor cibernetice."[14] Clauza prevede că un atac împotriva unui membru al NATO "trebuie să fie considerat un atac împotriva tuturor"[15].

Potrivit unei declaraţii a lui Jamie Shea, oficialul responsabil cu ameninţările de securitate emergente, a declarat că "recunoaşterea sabotajului spaţiului cibernetic ca fiind un act de război este doar jumătate din calea spre o politică coerentă", şi a adăugat că "noi nu spunem exact ce circumstanţe sau care este pragul la care un atac v a declanşa un răspuns colectiv NATO şi care ar trebui să fie acest răspuns". Iar o atitudine de genul "'vom şti când vom vedea'", nu este o strategie". În acelaşi articol, James G. Stavridis, decanul Şcolii Fletcher de Drept şi Diplomaţie de la Tufts şi fostul Şef al Comandamentului Suprem Aliat din Europa şi Dave Weinstein (un fost planificator strategic la US Cyber Command) au subliniat două probleme majore : că efectele "atacurilor cibernetice care ameninţă cu pierderi de vieţi omeneşti sau provoca daune fizice la infrastructură" trebuie "să fie luate în considerare în mod cumulativ, pe perioade de timp şi nu doar de la caz la caz", iar în al doilea rând, trebuie stabilit momentului exact când articolul 5 trebuie să fie invocat, deoarece există un număr mare de diferite atacuri cibernetice "care sunt inofensive fizic, dar pot provoca pagube economice severe"[16].

Tehnologia modernă permite relaţionarea socială peste spaţii imense. Graniţele nu mai contează. Oamenii dintr-o "zonă îndepărtată" pot interacţiona şi influenţa oamenii din alte zone. Pe măsură ce transformările în domeniul comunicării sunt accelerate şi mult mai ieftine, avem nevoie să remodelăm tiparele de control social, inclusiv colectarea şi interpretarea datelor. Necesitatea de a contracara riscul potenţial a răspândirii daunelor la scară largă generată de un atac cibernetic terorist masiv obligă autorităţile să conceapă şi să pună în aplicare strategii care vizează dezvoltarea unor sisteme de informaţii precise şi noi măsuri de cooperare. Prin Autoritatea de Aparare şi Management Ciberneti (CDMA), NATO are autoritatea de a răspunde rapid la atacurile cibernetice asupra membrilor săi şi de a trimite echipe de sprijin, dar acest tip de intervenţie poate fi filtrat până la nivel naţional în viitor.

Potrivit paginii oficiale a NATO "pe fondul creşterii dependenţei tot mai mare de tehnologie Şi de internet, Alianţa avansează în eforturile sale de a se confrunta cu o gamă largă de ameninţări cibernetice care vizează reţelele de NATO zilniuc. Creşterea complexităţii a atacurilor cibernetice determină ca protecţia comunicaţiilor Alianţei şi a sistemelor informatice (CIS) să fie o sarcină urgentă. Acest obiectiv a fost recunoscută ca o prioritate în Conceptul Strategic al NATO Şi a fost reiterat în declaraţiile ultimelor două Summit-uri, precum şi la reuniunile ministeriale ale NATO."[17]

O altă problemă este cea a spionajului cibernetic, în cea mai mare parte de către campaniile de hacking sponsorizate de state. Anul trecut, în noiembrie, un raport publicat de *Kaspersky*, un grup de securitate software cu mai mult de 300 de milioane de utilizatori şi 250.000 de clienţi corporativi din întreaga lume (în aproximativ 200 de ţări), a analizat într-un mod detaliat un nou tip de atac cibernetic care poate fi uşor considerat spionaj. "În ultimii

[14] Ioana Corina JULAN, "News Alert No.15: NATO Summit in Wales: CyberAttacks, integrated in Article V", Morgenthau Center, September 5, 2014, accessed on March 25, 2015 at the Internet address http://morgenthaucenter.org/news-alert-no-15-nato-summit-in-wales-cyberattacks-integrated-in-article-v/

[15] "The North Atlantic Treaty" at the Internet address http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[16] James G. STAVRIDIS and Dave WEINSTEIN, "NATO needs strong policy against cyber threats", *Boston Globe*, August 22, 2014, accessed on March 25, 2015 at the Internet address http://www.bostonglobe.com/opinion/ 2014/08/22/nato-needs-strong-policy-against-cyber-threats/cetoHkprGGZHMUAjfOhjHJ/story.html

[17] "Defending against cyber attacks", *North Atlantic Treaty Organization*, October 9, 2012, at the Internet address http://www.nato.int/cps/en/natohq/75747.htm

şapte ani, un actor puternic numit Darkhotel cunoscut de asemenea sub numele Tapaoux, a efectuat o serie de atacuri reuşite împotriva unei game largi de victime din întreaga lume. Implică folosirea de metode Şi tehnici care depăşesc cu mult comportament tipic cyber criminal. [..] Orientarea spre ţinte de genul directorilor de top de la diverse companii mari din întreaga lume în timpul şederii lor la anumite 'Dark Hotels' este unul dintre cele mai interesante aspecte ale acestei operaţiuni"[18], menţionează raportul. "Aşa cum am afirmat într-un scurt articol publicat la acea vreme "din cauza naturii atacurilor - care au ţinte exacte - episoadele despre care vorbim ar putea fi indicatorul unui actor politic puternic, cu interese globale."[19]

Ca şi exemplu, distribuţia ţintelor în decembrie 2014, la vârful listei se află siteurile industriale, guvernamentale şi educative. (Figura nr.1)

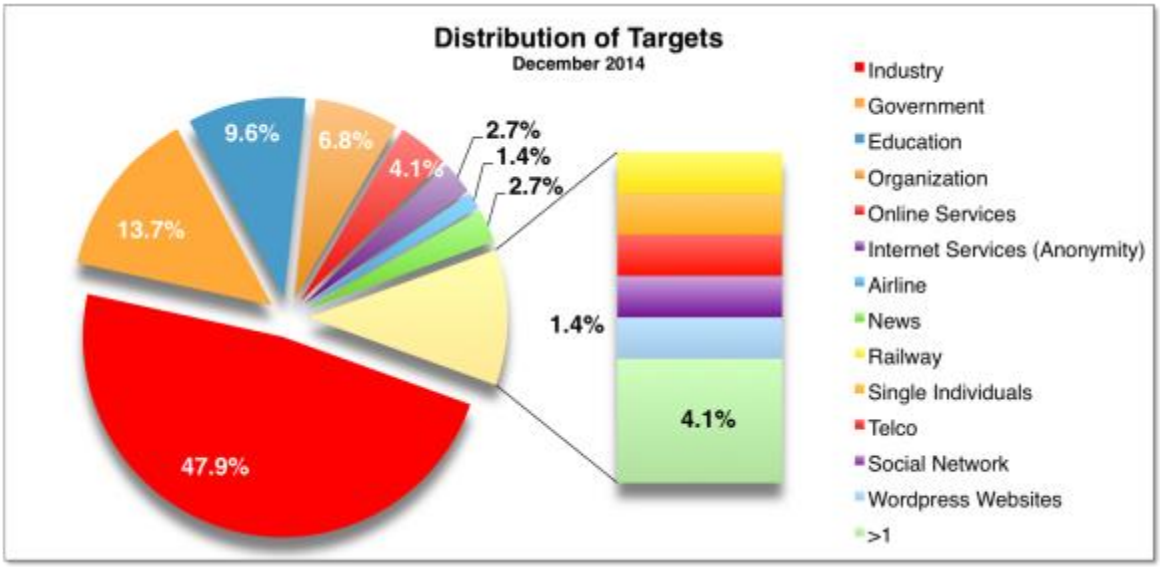


Figure no.1 Distribuţia ţintelor în Decembrie 2014[20]

Deoarece ameninţările sunt tot mai vizibile, lumea cibernetică se remodelează proiectând o oglindă a realităţilor fizice şi tangibile. Recunoaşterea sabotajului în spaţiul virtual direcţionat împotriva NATO ca Şi act de agresiune, alianţele cibernetice deja în curs de desfăşurare între Rusia Şi China[21], investiţiile mari în securitate cibernetică ale Israelului[22], o creştere a cheltuielilor în domeniul cibernetic de douăsprezece ori (o creştere de 1.200%!) în cazul Iranului[23] şi multe alte exemple sunt semne foarte clare dintre ale importanţei din ce în ce mai mari a acestui nou domeniu - apărarea cibernetică care vizează

[18] The DarkHotel Apt - A Story of Unusual Hospitality", Kaspersky, November 2014, accessed on March 25, 2015 at the Internet address https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

[19] Ioana Corina JULAN, "News Alert No.90: A cyber-threat with precise targets", Morgenthau Center, November 14, 2014 at the Internet address http://morgenthaucenter.org/news-alert-no-90-a-cyber-threat-with-precise-targets/

[20]"December 2014 Cyber Attacks Statistics", *Open Sources Info* accessed on March 25, 2015 at the Internet address http://opensourcesinfo.org/december-2014-cyber-attacks-statistics/

[21] Ioana Corina JULAN, "News Alert No.72: A potentially dangerous cyber-alliance: China and Russia", *Morgentahu Center*, October 22, 2014, accessed on March 25, 2015 at the Internet address http://morgenthaucenter.org/news-alert-no-72-a-potentially-dangerous-cyber-alliance-china-and-russia/

[22] Jason HINER, "How Israel is rewriting the future of cybersecurity and creating the next Silicon Valley", *Tech Republic*, accessed at March 28, 2014 at the Internet address http://www.techrepublic.com/article/how-israel-is-rewriting-the-future-of-cybersecurity-and-creating-the-next-silicon-valley/

[23] Cory BENNETT, "Iran has boosted cyber spending twelvefold", *The Hill*, March 23, 2015 at the Internet address http://thehill.com/policy/cybersecurity/236627-iranian-leader-has-boosted-cyber-spending-12-fold

descurajarea, oprirea şi "înfrângerea" ameninţărilor cibernetice şi a atacurilor cibernetice - atât pentru prezentul cât şi pentru viitorul securităţii naţionale în cele mai multe state.

BIBLIOGRAFIE:

1. AWAN, Imran and BLAKEMORE, Brian, "Policing Cyber Hate, Cyber Threats and Cyber Terrorism", Ashgate Publishing, 2012
2. CARR, Jeffrey, "Inside Cyber Warfare: Mapping the Cyber Underworld", O'Reilly Media, 2009
3. CLANCY Mark and LEIBROCK Michael, "Cyber Risk – A Global Systemic Threat", October 2014 at the Internet address http://www.dtcc.com/
4. CLARKE, Richard A., "Cyber War", Harper Collins e-books, 2010
5. Department of Defense, "2006 Quadrennial Defense Review Report", Washington, DC: Department of Defense, February 6, 2006, accessed on March 25, 2015 at the Internet address http://www.defense.gov/qdr/report/Report20060203.pdf
6. KEOHANE, Robert O. and NYE, Joseph S., "Power and Interdependence: World Politics in Transition", Little Brown, Boston, 1977
7. KRAMER, Franklin D., STARR H., WENTZ, Larry, "Cyberpower and National Security", National Defense University, Potomac Books Inc., 2009
8. STAVRIDIS, James G. and WEINSTEIN, Dave, "NATO needs strong policy against cyber threats", Boston Globe, August 22, 2014, accessed on March 25, 2015 at the Internet address http://www.bostonglobe.com/opinion/2014/08/22/nato-needs-strong-policy-against-cyber-threats/cetoHkprGGZHMUAjfOhjHJ/story.html
9. The DarkHotel Apt - A Story of Unusual Hospitality", Kaspersky, November 2014, at the Internet address https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf
10. U.S. Department of Energy, "Electricity Subsector Cybersecurity", accessed on March 25, 2015 at the Internet address
11. http://energy.gov/sites/prod/files/Cybersecurity%20Ris
12. k%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

ANALIZA CORELATĂ A MĂSURILOR DE SECURITATE FIZICĂ ŞI CIBERNETICĂ PENTRU OBIECTIVE NUCLEARE

Tudor RĂDULESCU
Doctorand, Universitatea Naţonală de Apărare "Carol I", Bucureşti, România,
e-mail: t.radulescu@gmail.com

Abstract: *Sistemele de protecţie fizică pentru obiectivele nucleare sunt proiectate, în majoritatea situaţilor, în baza Ameninţării Bază de Proiect, urmând o abordare cantitativă. Evaluarea măsurilor de protecţie fizică se poate face pornind de la numărul atacatorilor şi capabilităţile lor, probabilitate de detecţie, rata alarmelor false şi sensibilitatea la factorii de mediu pentru senzori, precum şi timpii de întârziere ai barierelor fizice.*

Sistemele informatice folosite în obiectivele nucleare (DCS/SCADA, reţea de business, sisteme de informaţii clasificate şi sisteme digitale de protecţie fizică) sunt proiectate în principal pentru funcţionalitate , mai puţin pentru securitate intrinsecă, măsurile şi sistemele de securitate cibernetică fiind implementate ca extensii. Ameninţarea bază de proiect (DBT) cibernetică este deseori definită în termeni generali şi nu poate cuantifica atacul credibil, în situaţia în care capabilităţile criminalilor cibernetici evoluează mai repede decât actualizările DBT.

În această lucrare examinăm diversele abordări pentru analiza măsurilor de protecţie fizică şi securitate cibernetică, evaluând asemănările şi evidenţiind necesitatea unei analize corelate de securitate fizică-cibernetică.

Cuvinte cheie: *analiză de securitate, securitate fizică, securitate cibernetică, nuclear, ameninţare bază de proiect*

1 Introducere

De mai bine de 40 ani, specialişti din domeniile militar, informaţii, poliţie şi companii private de inginerie pentru securitate, au contribuit la definirea unui mediu bine reglementat pentru proiectarea, operarea şi evaluarea sistemelor de protecţie fizică. Primul ghid internaţional important privind protecţia fizică a obiectivelor nucleare a fost publicat de către Agenţia Internaţională pentru Energie Atomică (AIEA) în 1972, cu titlul „Recomandări pentru protecţia fizică a materialului nuclear", care a fost denumită „INFCIRC/225" în 1975.

În România, CNCAN a publicat „Normele de protecţie fizică în domeniul nuclear (NPF-01)"[1] in 2001.

Preocuparea pentru securitate cibernetică în industria nucleară a luat amploare mult mai târziu. Primul eveniment de securitate cibernetică mediatizat pe larg a avut loc în 2003 loc la Centrala Nucleară Davis Besse, când virusul Slammer a infectat computerele de proces ale centralei, în urma căruia „Sistemele de Afişare a Parametrilor de Siguranţă şi Computerele de Proces ale centralei au fost dezafectate timp de mai multe ore"[2].

[1] "*Normele de Protecţie fizică în Domeniul Nuclear*", accesat 14.03.2015, la http://www.cncan.ro/assets/NPF/npf01.pdf

[2] Miller, Bill, Dale Rowe, "*A survey of SCADA and critical infrastructure incidents*", Proceedings of the 1st Annual conference on Research in information technology, ACM, 2012, p. 53

Reglementările de securitate cibernetică în sectorul nuclear au apărut mai târziu, când NRC a publicat primul său ghid în 2009, ca Titlul 10, Codul Federal de Reglementări, Partea 73, „Protecţia sistemelor digitale de calcul, de comunicaţii şi reţele”[3].

Există un decalaj de maturitate între cele două domenii, protecţia fizică şi securitatea cibernetică, care se reflectă în felul în care cele două domenii sunt reglementate şi în modul în care sunt evaluate măsurile.

2. Evaluarea Sistemelor de Protecţie Fizică

Proiectarea măsurilor de protecţie fizică pentru obiectivele nucleare se bazează, în cele mai multe cazuri, pe ameninţarea bază de proiect (DBT), care cuantifică caracteristicile atacatorului.

Potrivit ghidului „Dezvoltarea, utilizarea şi întreţinerea Ameninţării Bază de Proiect" publicat de AIEA, „DBT reprezintă descrierea făcută de Stat pentru un set reprezentativ de atribute şi caracteristici ale adversarilor, pe baza (dar nu neapărat limitat la) unei evaluări a ameninţărilor, pe care Statul a decis să o folosească ca bază pentru proiectarea şi evaluarea unui sistem de protecţie fizică.”[4]

Această abordare permite specialiştilor să prezică, să controleze şi să cuantifice performanţa sistemelor de protecţie fizică.

Conceptul DBT a fost introdus în 1979 de către US NRC (Comisia de Reglementare în domeniul Nuclear din SUA). În Capitolul 10, Codul Reglementărilor Federale, Partea 73, există o descriere standard a ameninţării bază de proiect, care acoperă: „Un atac extern hotărât, violent [...] şi [...] O ameninţare internă; şi [...] Un atac cu bombă într-un vehicul terestru [...] şi [...] Un atac cu bombă într-o ambarcaţiune [...] şi [...] Un atac cibernetic”[5].

Descrierile publice ale conceptului DBT sunt furnizate numai ca referinţă, descrierea cantitativă a DBT fiind clasificată. Un exemplu de descriere detaliată este disponibilă în materialele de curs oferite la atelierele DBT AIEA: „Tentativa de furt a unei cantităţi semnificative de MN (de exemplu, 10 kg de Pu), de către un grup de 6 atacatori externi echipaţi cu 10 kg de exploziv TNT, arme automate (inclusiv armament uşor de infanterie) şi instrumente specifice pentru pătrundere prin efracţie disponibile pe piaţă. Atacatorii au cunoştinţe bogate despre obiectiv şi măsurile de PF asociate. Sunt dispuşi să moară sau să ucidă. Nu au colaborator din interior.”[6]

Pe baza acestor informaţii cantitative, măsurile de protecţie fizică pot fi proiectate în aşa fel încât:

- ţintele protejate (zonele vitale) includ orice locaţie care conţine material nuclear (plutoniu) în cantităţi semnificative;
- sistemele de detecţie a intruziunilor sunt adecvate pentru a detecta intruşi cu pregătire militară, cu mobilitate mare / echipaţi bagaje uşoare (câteva kg de explozibil şi armament de infanterie), cu cunoştinţe cuprinzătoare despre obiectiv şi vulnerabilităţile sistemelor de detecţie şi ale barierelor fizice, şi cu instrumente de sabotaj a sistemului de detecţie intruziuni;

[3] “*Title 10, Code of Federal Regulations, Part 73.54, Protection of digital computer and communication systems and networks*”, accesat 15.03.2015, la http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

[4] “*Development, Use and Maintenance of the Design Basis Threat*”, accesat 15.03.2015, la http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf, p. 8

[5] “*Title 10, Code of Federal Regulations, Part 73.1*”, accesat 15.03.2015, la http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html

[6] “*Design Basis Threat (DBT) Workshop, Session 7, What Could a DBT Look Like?*”, DBT Workshop, IAEA, Bucharest, Romania, 2012

- barierele fizice pe orice căi posibile de pătrundere ale adversarului pot rezista atacurilor cu explozibili în cantităţi cumulate de 10 kg;
- barierele fizice oferă întârzieri semnificative împotriva instrumentelor de intruziune disponibile pe piaţă, astfel încât întârzierea este mai mare decât timpul necesar forţei de reacţie pentru a intercepta atacatorii;
- forţa de reacţie este dimensionată în aşa manieră încât are o probabilitate de neutralizare mai mare de 90% împotriva unei echipe de 6 atacatori înarmaţi cu armament uşor de infanterie şi dispuşi să le fie ucişi până la 5 membri ai echipei pentru a îşi atinge scopul misiunii.
- Există critici împotriva abordării DBT, care declară că aceasta ”nu încearcă să ţină cont de natura strategică a teroriştilor, decât în privinţa preferinţei lor pentru diverse ţinte”[7]. Articolul citat propune trei alternative la abordarea DBT:
- Niveluri de ameninţare diferenţiate – o alternativă care specifică trei niveluri DBT; nu considerăm această abordare diferită de abordarea clasică a DBT pentru evaluarea performanţelor măsurilor de securitate;
- Cultura de securitate - este doar un instrument complementar pentru DBT şi nu adaugă elemente care contribuie la evaluare;
- Teoria jocurilor – o abordare bazată pe ideea că “răsplata aşteptată de terorist în urma atacului este în realitate o funcţie de trei factori: posibilitatea că atacul respectiv va reuşi, consecinţele în cazul în care atacul reuşeşte, şi valoarea consecinţelor pentru terorist”[8]. Aceasta abordare combină elemente din procesul de Identificare a Zonelor Vitale („Accesibilitate, Atac de la Distanţă, Detectabilitatea, Atractivitatea ţintei”[9]) cu elemente de probabilitate de succes a atacului, care este inversa probabilităţii de neutralizare, pentru care “nu există o metodologie standardizată acceptabilă”[10].

Proiectarea protecţiei fizice ia în considerare principiile de bază ale ”Apărării în adâncime, consecinţe minime ale defectării componentelor, protecţie echilibrată şi protecţie gradată în conformitate cu semnificaţia sau potenţialele consecinţe radiologice.”[11] Principalele aspecte considerate în proiectare sunt detecţia, întârzierea, răspunsul şi măsurile de descurajare şi atenuare a participării celor din interior.

Senzorii de protecţie fizică pot fi caracterizaţi prin prisma probabilităţii detecţiei, ratei alarmelor false, precum şi sensibilităţii la efecte adverse ale factorilor de mediu, în timp ce barierele fizice pot fi caracterizate în termeni de întârziere, în funcţie de capacităţile instrumentelor adversarului. Proiectantul poate prescrie exact inelele de detecţie şi întârziere, pentru a permite forţei de reacţie să întrerupă şi să neutralizeze adversarul.

Evaluarea unui sistem de protecţie fizică începe cu o analiză a proiectului şi o vizită în locaţie pentru a evalua implementarea efectivă a sistemului. Pe baza documentaţiei de

[7] Kuperman, Alan J., Kirkham, Lara, “*Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current “Design Basis Threat” Approach*”, prepared for INMM 54th Annual Meeting, Palm Desert, CA, 2013, accesat 15.03.2015, la http://sites.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf, p. 5

[8] Kuperman, Alan J., Kirkham, Lara, “*Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current “Design Basis Threat” Approach*”, prepared for INMM 54th Annual Meeting, Palm Desert, CA, 2013, accesat 15.03.2015, la http://sites.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf, p. 6

[9] Malachova, Tereza, Malach, Jindrich, Vintr, Zdenek, "*Threat characterization in vital area identification process*", Proceedings of the 47th International Carnahan Conference on Security Technology (ICCST), vol., no., pp.1,6, 2013

[10] Whitehead, Donnie, Potter, Claude, O’Connor, Sharon, “*Nuclear Power Plant Security Assessment Technical Manual*”, Sandia Report SAND2007-5591, 2007, accesat 15.03.2015, la http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf, p. 39

[11] “*Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities,IAEA-TECDOC-967 (Rev.1)*”, IAEA, 2000, accesat 15.02.2015, la http://www-pub.iaea.org/MTCD/publications/PDF/te_967rev1_prn.pdf, p. 4

proiectare, se poate dezvolta modelul locaţiei. Cea mai utilizată metodă de analiză a eficienţei măsurilor este Analiza Căilor de Pătrundere. Această analiză "implică identificarea şi analizarea căilor (printr-un obiectiv), pe care un adversar le poate urma în timpul tentativei de furt sau sabotaj [...]. O cale a adversarului este o serie ordonată de acţiuni împotriva unei ţinte care, dacă au fost realizate, au ca rezultat reuşita furtului sau a sabotajului."[12]

Folosind această abordare, locaţia este modelată prin determinarea, pentru fiecare zona vitală, a unui set complet de căi ale adversarului credibile, constând din zone, acţiuni, elemente de detecţie şi bariere fizice, rezultând astfel diagrama de secvenţă a adversarului - ASD (a se vedea Figura nr. 1).

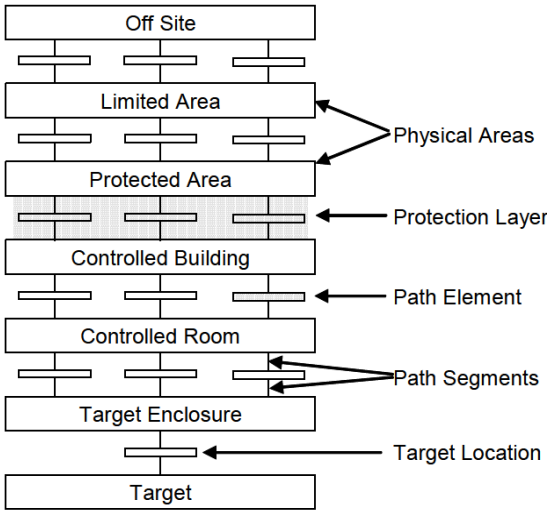


Figura nr. 1 Diagrama de bază a secvenţei a adversarului[13]

Fiecare element este caracterizat de proprietăţi specifice:

- dimensiuni (pentru a caracteriza întârzierea pe zonele traversate)
- caracteristicile barierei fizice (pentru a furniza informaţii privind timpii de întârziere pe baza instrumentelor disponibile atacatorilor – instrumente mecanice si electrice, explozivi)
- elemente de detecţie cu probabilităţi asociate şi avantaje ale tehnologiilor complementare (asigurând imunitate la atac disimulat)
- elementul uman (ca factor de detecţie şi factor de întârziere, dacă este înarmat)
- Pe baza ASD pot fi evaluate Punctul Critic de Detecţie (CDP) şi Probabilitatea de Întrerupere (P_I). CDP este ultimul punct pe calea adversarului în care elementele de detecţie încă mai contează, ceea ce înseamnă că forţa de reacţie mai are suficient timp pentru a întrerupe pătrunderea. Orice element de detecţie după acest punct este inutil pentru scopul sistemului de protecţie fizică. P_I este probabilitatea cumulativă ca atacatorii să fie detectaţi până la CDP. Calea cu cel mai mic P_I este numită Calea Critică.

Modelarea obiectivului şi calculele ulterioare pot fi realizate cu instrumente software specializate, cum ar fi EASI (Estimate of Adversary Sequence Interruption)[14], SAVI

[12] Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accesat 15.03.2015, la http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf, p. 31

[13] Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accesat 15.03.2015, la http://prod.sandia.gov/techlib/access-control.cgi/2007/075591.pdf, p. 37

[14] Garcia, Mary Lynn, "*The Design and Evaluation of Physical Protection Systems*", 2nd ed. Burlington, MA, Elsevier Butterworth–Heinemann, 2008

(Systematic Analysis of Vulnerability to Intrusion)[15], Analytic System and Software for Evaluating Safeguards and Security (ASSESS)[16] şi Systematic Analysis of Physical Protection Effectiveness (SAPE)[17].

Datele utilizate în simulările numerice pot fi extrase din baze de date generate în teste de laborator (unele din instrumentele enumerate mai sus deja dispun de date de performanţă generice incluse în pachetul software), sau pot fi determinate prin teste ale unor elemente similare în laborator.

Următoarea fază a evaluării este determinarea Probabilităţii de Neutralizare (P_N). P_N este determinată folosind modele software bazate pe Lanţuri Markov. Probabilitatea este determinată pe baza numărului de atacatori, a puterii lor de foc şi a inelelor succesive de apărători, caracterizaţi prin număr şi putere de foc.

Calcule mai complexe ale P_N pot fi realizare cu instrumente de simulare a conflictelor armate (jocuri de război), cum ar fi JCATS (Joint Conflict and Tactical Simulation). Programul JCATS „simulează în mod normal o luptă între două forţe opuse (adesea denumite echipele roşie şi albastră), dar poate simula până la 10 facţiuni cu relaţii de tip amic, inamic, neutru”[18].

Analiza măsurilor de protecţie fizică se reduce la calculul probabilităţii de eficacitate a sistemului P_E, care este: $P_E = P_I * P_N$.

În afara simulărilor numerice teoretice, bazate pe proiectul propriu-zis, rezultatele sunt validate utilizând analize de scenarii, exerciţii de simulare tactică şi exerciţii de luptă.

3. Evaluarea Sistemelor de Securitate Cibernetică

Sistemele cibernetice din obiectivele nucleare au fost implementate dinaintea utilizării termenului de securitate cibernetică. Prima utilizare a termenului „securitate cibernetică” nu este menţionată în bibliografia consultată, dar este în general legată de consacrarea termenului „spaţiu cibernetic” de către William Gibson, într-o nuvelă publicată în 1982[19], apoi în romanul „Neuromantul” în 1984.

Prima reglementare pentru securitatea cibernetică a obiectivelor nucleare a fost publicată în 2009, când NRC a publicat Titlul 10, Codul Federal de Reglementări, Partea 73, „Protecţia sistemelor digitale de calcul, de comunicaţii şi reţele”[20]. Acesta stabileşte responsabilităţi generale şi nu oferă îndrumări tehnice pentru implementare.

În „Norma privind protecţia instalaţiilor nucleare împotriva ameninţărilor cibernetice” publicată de CNCAN este folosită aceeaşi abordare de a defini roluri şi responsabilităţi. Cu toate acestea, documentul stabileşte categoriile de sisteme, componente şi echipamente (SCE)

[15] "*SAVI: Systematic Analysis of vulnerability to Intrusion*", Volume 1 of 2, SAND89-0926/1 Sandia National Laboratories, Albuquerque, New Mexico, 1989

[16] Al-Ayat, R.A., Cousins, T.D., Hoover, E.R., "*ASSESS (Analytic System and Software for Evaluating Safeguards and Security) update: Current status and future developments*", Institute of nuclear materials management conference, Los Angeles, CA (USA), 1990

[17] Jang, Sung Soon, Kwak, Sung-Woo, Yoo, Hosik, Kim, Jung-Soo, Yoon, Wan Ki, "*Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)*", Nuclear Engineering and Technology, Vol. 41 No.5, 2009, accesat 15.03.2015, la http://www.kns.org/jknsfile/v41/JK0410747.pdf

[18] Heller, Arnie, "*Simulating Warfare Is No Video Game*", Science & Technology Review, Lawrence Livermore National Laboratory, January/February 2000, accesat 15.03.2015, la https://str.llnl.gov/str/pdfs/01_00.1.pdf

[19] Gilles, Martin, "*Defending the digital frontier*", The Economist, 12 July 2014, accesat 15.03.2015, la http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals

[20] "*Title 10, Code of Federal Regulations, Part 73.54, Protection of digital computer and communication systems and networks*", accesat 15.03.2015, la http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

care trebuie protejate împotriva ameninţărilor cibernetice: „SCE cu funcţii de securitate nucleară; SCE care fac parte din sistemul de protecţie fizică; SCE care fac parte din sistemul de control de garanţii nucleare; SCE cu funcţii în răspunsul la situaţii de urgenţă, inclusiv sistemele de comunicaţi utilizate în situaţii de urgenţă."[21]

În mediul cibernetic, schimbările sunt dinamice. Evoluţa metodelor de atac şi a nivelului de cunoştinţe al atacatorilor sunt prezentare în graficul din Figura nr. 2.

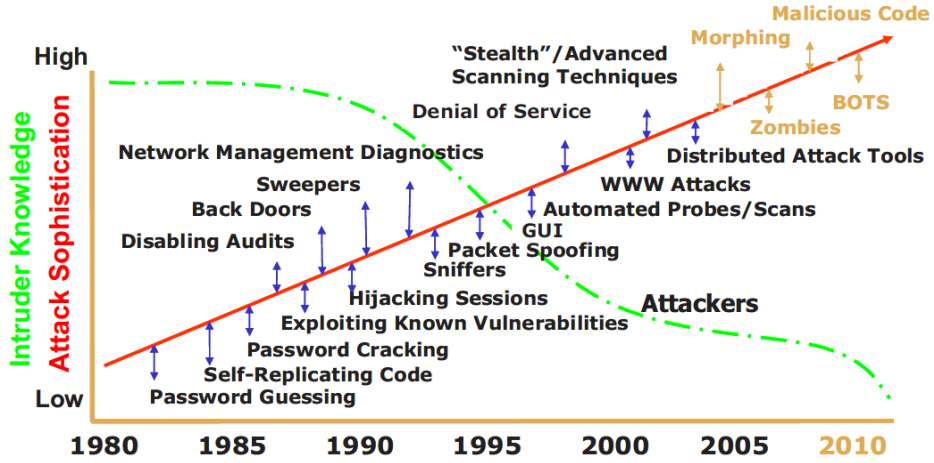


Figura nr. 2 Complexitatea în creştere a ameninţărilor odată cu proliferarea atacatorilor[22]

Cu toate acestea, tendinţele ameninţărilor cibernetice, ale instrumentelor disponibile pentru atac şi ale vulnerabilităţilor evoluează la o rată comparabilă cu cele mai optimiste aşteptări de revizie a Ameninţării Bază de Proiect. Raportul anual ENISA[23] arată cum ameninţările se modifică de la an la an, cum apar noi concepte.

Evaluarea măsurilor de securitate cibernetică, sau a controalelor, este descrisă în bibliografie ca o combinaţie de verificări ale conformităţi cu o listă de prescripţii procedurale şi, uneori, tehnice, şi evaluări structurate / cantitative.

În timp ce securitatea cibernetică este definită în contextul sistemelor cibernetice, care sunt sisteme tehnice, „există o lipsă a cercetării pentru metrici de securitate tehnice, pentru măsurarea controalelor tehnice de securitate din ansamblul de 133 de controale de securitate din standardul ISO/IEC 27001" [24]. Măsurile tehnice răspund unor ameninţări şi vulnerabilităţi specifice, despre care am văzut că evoluează rapid. Considerăm că aceasta limitează modelarea sistemelor cibernetice pentru scopuri de securitate cibernetică, întrucât orice model ar necesita o actualizare în timp real pe baza noilor metode de atac şi a vulnerabilităţilor nou identificate.

Un grup de cercetători de la Laboratoarele Naţionale Idaho propune o metodologie de evaluare pentru reducerea riscurilor „bazată pe presupunerea că riscul este legat de timpul necesar pentru finalizarea unui atac"[25]. Abordarea consideră ca un prim pas construirea unui

[21] "*Norme privind protecţia instalaţiilor nucleare împotriva ameninţărilor cibernetice*", accesat 15.03.2015, la http://www.cncan.ro/assets/NSC/Ordinul-181-norme-amenintari-cibernetice.pdf

[22] "*Computer Security at Nuclear Facilities*", NSS-17, International Atomic Energy Agency, 2011, p38

[23] "*ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats*", ENISA, 2014, accesat 15.03.2015, la https://www.enisa.europa.eu

[24] Azuwa, M.P., Ahmad, Rabiah, Sahib, Shahrin, Shamsuddin, Solahuddin, "*Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard*", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 280-288, 2012, p. 280

[25] McQueen, Miles, Boyer, Wayne, Flynn, Mark, Beitel, George, "*Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System*", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, accesat 15.03.2015, la http://www5vip.inl.gov/technicalpublications/Documents/3303778.pdf

model al obiectivului din punct de vedere al elementelor cibernetice, cu interconectări care reprezintă căile către elementele protejate (SCE vitale).

Pentru fiecare element, sunt determinate vulnerabilităţi şi acestea sunt caracterizate pe baza consecinţelor (starea elementului din sistem, care devine un nod în reprezentarea tip graf) şi tipului de acţiune (care devine o ramură a grafului). Fiecare acţiune are un cost asociat, care depinde de timpul necesar pentru compromiterea elementului.

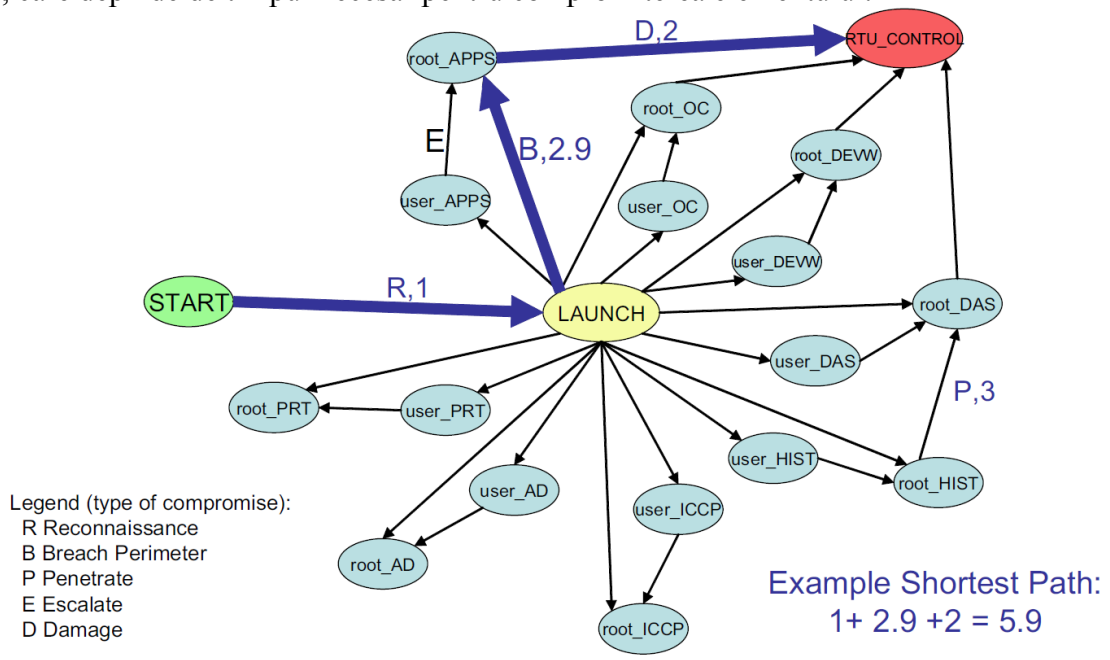


Figura nr. 3 Graful parţal de compromitere[26]

O altă abordare pentru evaluarea sistemelor de securitate cibernetică o reprezintă metoda Arborilor de Atac. Această metodă este atribuită lui Bruce Schneier. „Un arbore de atac este un arbore în care nodurile reprezintă atacurile. Nodul rădăcină este scopul final al atacatorului. Nodurile copil sunt rafinări ale acestui scop, iar frunzele reprezintă atacuri care nu mai pot fi rafinate.”[27]

[26] McQueen, Miles, Boyer, Wayne, Flynn, Mark, Beitel, George, “*Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System*”, Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, accesat 15.03.2015, la http://www5vip.inl.gov/technicalpublications/Documents/3303778.pdf, p. 5

[27] Mauw, Sjouke, Oostdijk, Martijn, “*Foundations of Attack Trees*”, Information Security and Cryptology - ICISC 2005, accesat 15.03.2015, la http://web.cs.du.edu/~ramki/papers/attackGraphs/foundations.pdf, p. 1

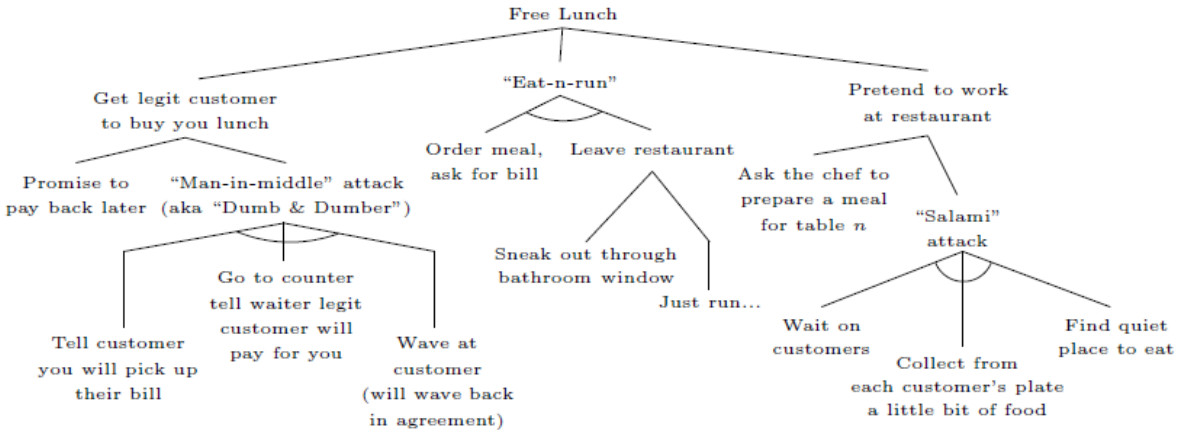


Figura nr. 4 Exemplu de arbore de atac[28]

Fiecare frunză a arborelui reprezintă acţuni care pot fi caracterizate folosind metrici cuantificabile. O dezvoltare ulterioară a acestui model, care reprezintă o separare a caracteristicilor de atac şi de apărare, este „arborele de atac-apărare" [29].

Concluzii

Deşi în acest moment există o separare între protecţia fizică şi securitatea cibernetică, atât în modele, cât şi în responsabilităţile organizaţionale, bibliografia[30] ia in considerare pentru analiză atacurile combinate: atac fizic, atac fizic cu sprijin cibernetic, atac cibernetic pur şi atac cibernetic cu sprijin fizic.

Observăm similarităţi între simularea de tip arbore de defectare pentru protecţie fizică şi modelele pentru securitate cibernetică care folosesc arbori de atac sau graful de compromitere, în principal pentru că permit modelarea atacului într-un mod secvenţial, cuantificabil.

Cu toate acestea, aspectul de timp real al ameninţărilor şi vulnerabilităţilor cibernetice nu permit o evaluare de vulnerabilitate combinată care să furnizeze rezultate cuantificabile, utilizabile pentru planificarea măsurilor pe termen lung. Mai degrabă vedem rezultatele unui instrument de evaluare combinat de securitate fizică-cibernetică sub forma unui instrument dinamic, permiţând detecţia şi ajustarea posturii de securitate în mod continuu.

Vedem potenţial în dezvoltarea unei platforme unice de modelare, evaluare şi management a securităţi pentru obiective nucleare, care să cuprindă protecţia fizică şi securitatea cibernetică. Eforturile noastre viitoare se vor concentra pe dezvoltarea unui model care să acopere aspectele tehnice, organizaţionale şi operaţionale ale managementului securităţi pentru obiectivele nucleare, în întreaga lor complexitate.

[28] Mauw, Sjouke, Oostdijk, Martijn, "*Foundations of Attack Trees*", Information Security and Cryptology - ICISC 2005, accesat 15.03.2015, la http://web.cs.du.edu/~ramki/papers/attackGraphs/foundations.pdf, p. 2
[29] Kordy, Barbara, Mauw, Sjouke, Radomirović, Saša, Schweitzer, Patrick, "*Foundations of Attack–Defense Trees*", Proceedings of the 7th international Workshop on Formal Aspects in Security and Trust (FAST 2010), volume 6561 of LNCS, pages 80-95. Springer-Verlag, 2011, accesat 15.03.2015, la http://satoss.uni.lu/members/barbara/papers/adt.pdf
[30] DePoy, Jennifer, Phelan, James, Sholander, Peter, Smith, Bryan J., Varnado, G. Bruce, Wyss, Gregory D., Darby, John, Walter, Andrew, "*Critical Infrastructure Systems of Systems Assessment Methodology*", Report SAND2006-6399, Sandia National Laboratories, 2006, p.14

BIBLIOGRAFIE:

1. "*SAVI: Systematic Analysis of vulnerability to Intrusion*", Volume 1 of 2, SAND89-0926/1 Sandia National Laboratories, Albuquerque, New Mexico, 1989
2. "*Computer Security at Nuclear Facilities*", NSS-17, International Atomic Energy Agency, 2011
3. "*Design Basis Threat (DBT) Workshop, Session 7, What Could a DBT Look Like?*", DBT Workshop, IAEA, Bucharest, Romania, 2012
4. "*Development, Use and Maintenance of the Design Basis Threat*", accesat 15.03.2015, la http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf
5. "*ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats*", ENISA, 2014, accesat 15.03.2015, la https://www.enisa.europa.eu
6. "*Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities,IAEA-TECDOC-967 (Rev.1)*", IAEA, 2000, accesat 15.02.2015, la http://www-pub.iaea.org/MTCD/publications/PDF/te_967rev1_prn.pdf
7. "*Norme privind protecţia instalaţilor nucleare împotriva ameninţărilor cibernetice*", accesat 15.03.2015, la http://www.cncan.ro/assets/NSC/Ordinul-181-norme-amenintari-cibernetice.pdf
8. "*Normele de Protecţie fizică în Domeniul Nuclear*", accesat 14.03.2015, la http://www.cncan.ro/assets/NPF/npf01.pdf
9. "*Title 10, Code of Federal Regulations, Part 73.1*", accesat 15.03.2015, la http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html
10. "*Title 10, Code of Federal Regulations, Part 73.54, Protection of digital computer and communication systems and networks*", accesat 15.03.2015, la http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
11. Al-Ayat, R.A., Cousins, T.D., Hoover, E.R., "*ASSESS (Analytic System and Software for Evaluating Safeguards and Security) update: Current status and future developments*", Institute of nuclear materials management conference, Los Angeles, CA (USA), 1990
12. Azuwa, M.P., Ahmad, Rabiah, Sahib, Shahrin, Shamsuddin, Solahuddin, "*Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard*", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 280-288, 2012
13. DePoy, Jennifer, Phelan, James, Sholander, Peter, Smith, Bryan J., Varnado, G. Bruce, Wyss, Gregory D., Darby, John, Walter, Andrew, "*Critical Infrastructure Systems of Systems Assessment Methodology*", Report SAND2006-6399, Sandia National Laboratories, 2006
14. Garcia, Mary Lynn, "*The Design and Evaluation of Physical Protection Systems*", 2nd ed. Burlington, MA, Elsevier Butterworth–Heinemann, 2008
15. Gilles, Martin, "*Defending the digital frontier*", The Economist, 12 July 2014, accesat 15.03.2015, la http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals
16. Heller, Arnie, "*Simulating Warfare Is No Video Game*", Science & Technology Review, Lawrence Livermore National Laboratory, January/February 2000, accesat 15.03.2015, la https://str.llnl.gov/str/pdfs/01_00.1.pdf
17. Jang, Sung Soon, Kwak, Sung-Woo, Yoo, Hosik, Kim, Jung-Soo, Yoon, Wan Ki, "*Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)*", Nuclear

Engineering and Technology, Vol. 41 No.5, 2009, accesat 15.03.2015, la http://www.kns.org/jknsfile/v41/JK0410747.pdf
18. Kordy, Barbara, Mauw, Sjouke, Radomirović, Saša, Schweitzer, Patrick, "*Foundations of Attack–Defense Trees*", Proceedings of the 7th international Workshop on Formal Aspects in Security and Trust (FAST 2010), volume 6561 of LNCS, pages 80-95. Springer-Verlag, 2011, accesat 15.03.2015, la http://satoss.uni.lu/ members/barbara/papers/adt.pdf
19. Kuperman, Alan J., Kirkham, Lara, "*Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current "Design Basis Threat" Approach*", prepared for INMM 54th Annual Meeting, Palm Desert, CA, 2013, accesat 15.03.2015, la http://sites.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf
20. Malachova, Tereza, Malach, Jindrich, Vintr, Zdenek, "*Threat characterization in vital area identification process*", Proceedings of the 47th International Carnahan Conference on Security Technology (ICCST), vol., no., pp.1,6, 2013
21. Mauw, Sjouke, Oostdijk, Martijn, "*Foundations of Attack Trees*", Information Security and Cryptology - ICISC 2005, accesat 15.03.2015, la http://web.cs.du.edu/ ~ramki/ papers/attackGraphs/foundations.pdf
22. McQueen, Miles, Boyer, Wayne, Flynn, Mark, Beitel, George, "*Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System*", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, accesat 15.03.2015, la http://www5vip.inl.gov/technicalpublications/Documents/ 3303778.pdf
23. Miller, Bill, Dale Rowe, "*A survey of SCADA and critical infrastructure incidents*", Proceedings of the 1st Annual conference on Research in information technology, ACM, 2012
24. Whitehead, Donnie, Potter, Claude, O'Connor, Sharon, "*Nuclear Power Plant Security Assessment Technical Manual*", Sandia Report SAND2007-5591, 2007, accesat 15.03.2015, la http://prod.sandia.gov/techlib/access-control.cgi/2007/075591. pdf

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului POSDRU/159/1.5/S/138822, cu titlul „Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile "Ştiinţe Militare", "Securitate şi Informaţii" şi "Ordine Publică şi Siguranţă Naţională" - Program de Formare Continuă a Cercetătorilor de Elită - "SmartSPODAS"."

ASPECTE GENERALE PRIVIND MANAGEMENTUL RISCULUI ÎN MEDIILE INFORMATICE

Dănuţ NECHITA
Doctorand în domeniul Ordine Publică şi Securitate Naţională, instructor de criminalistică în cadrul Academiei de Poliţie „Alexandru Ioan Cuza" Bucureşti, România,
e-mail: danut_nec@yahoo.com

Dr. Georgică PANFIL
Doctor în domeniul Ordine Publică şi Securitate Naţională, lector în cadrul Academiei de Poliţie „Alexandru Ioan Cuza" Bucureşti, România, panfil.george@gmail.com

Rezumat*: Articolul prezintă principalele aspecte privind procesele eficiente specifice managementului riscului în mediile informatice. Autorii abordează etapele succesive ale procesului analizei de risc, măsurării riscurilor şi caracterizării riscurilor. Cu atât mai mult, concluziile sunt centrate pe idea unor bune practici şi metode de reducere a riscurilor, centrate pe specificul unor instituţii publice care conţin informaţii şi date sensibile.*

Cuvinte cheie*: managementul riscului, securitate, reducere, risc.*

La nivelul oricărei instituţii, mediile informatice au rol bine definit şi totodată sensibil. În prezent, în orice instituţie se poate identifica una sau mai multe legături între obiectivele sale şi unul sau mai multe sisteme informatice. Din punctul nostru de vedere, orice manager trebuie să fie conştient de provocările principalelor categorii de risc cu origini în mediile informatice, în special datorită faptului că aceste tipuri de medii pot reprezenta sursă de ameninţare sau a vulnerabilităţii de nivel intern.

1.Fundamente ale managementului riscului

Fiecare organizaţie are obiective specifice prestabilite. Cu toate acestea, uneori, unele incertitudini pot intra în consonanţă directă cu posibilităţile de a atinge obiectivele, indiferent de tipul lor. Odată apărute aceste incertitudini, este evident, că eficienţa este serios pusă sub semnul întrebării. Astfel, în situaţia mai sus descrisă putem vorbi despre un risc. Putem prezenta diferite definiţii ale conceptului de risc, dar una dintre cele mai acceptate dintre ele descrie riscul ca fiind probabilitatea unei ameninţări cu un prejudiciu cuantificabil să fie materializată de o vulnerabilitate internă sau o ameninţarea externă. În opinia Organizaţiei Internaţionale de Standardizare, riscul este definit ca "efectul unor incertitudini asupra obiectivelor", sau ca "probabilitatea unor evenimente viitoare incerte" (colecţia de standarde ISO 31000 – Risk vocabulary)[1]. Indiferent de abordarea definiţiei, putem concluziona că riscul are următoarele componente:

- O *vulnerabilitate* internă a organizaţiei;
- O *ameninţarea* externă;
- Un *efect* cuantificabil asupra bunurilor;
- *Probabilitatea* unui eveniment de a se manifesta (fie din punct de vedere al vulnerabilităţii, a ameninţării sau amândouă).

Vulnerabilitatea este definită drept componentă a riscului şi constă într-o stare de fapt, proces, persoană sau fenomen din interiorul unei organizaţii care poate diminua capacitatea de reacţie împotriva riscurilor potenţiale sau existe sau care favorizează apariţia sau dezvoltarea

[1] Standardul ISO 73:2009, Vocabularul Managementului Riscurilor www.iso.org şi www.iso-standards.org.

unui risc. Cu alte cuvinte, vulnerabilitatea reprezintă orice componentă a unui sistem ce poate fi atacată cu uşurinţă, care are componente sensibile. Indiferent de definiţia abordată, vulnerabilitatea reprezintă elementul intern al riscului.

Ameninţarea reprezintă acţiunea, inacţiunea, fenomenul, procesul sau individul capabil să cauzeze o pierdere sau un impact negativ organizaţiei. Ameninţările au de obicei o sursă externă şi nu trebuie confundate cu conceptul de vulnerabilitatea.

Din punct de vedere al cercetării în domeniul managementului riscului, combinaţia dintre ameninţare şi vulnerabilitate produce mediul de risc şi parametrii apariţiei riscului. Dacă una dintre componentele menţionate are probabilitatea de apariţie aproape de zero, atunci şi riscul este aproape inexistent. cu atât mai mult, când o instituţie este în prezenţa unei ameninţări, dar aceasta nu are nici o vulnerabilitate de exploatat, nu este nici un impact. Astfel, riscul potenţial este inexistent (spre exemplu să ne imaginăm situaţia în care există un virus sau o ameninţare informatică, dar nu avem în organizaţie nici un computer – astfel nu avem nimic expus).

Când un risc apare, managerul trebuie să ia o decizie, să transfere riscul, să îl respingă, să îl reducă sau să îl accepte. Oricare dintre aceste opţiuni are diferite implicaţii, cum ar fi luarea unui set de măsuri (eliminarea vulnerabilităţii sau sursei ameninţării, creşte măsurilor generale de prevenţie, neluarea niciunei decizii în unele cazuri etc.) Cu toate acestea, pentru a avea posibilitatea concretă de a înţelege cu ce avem de a face este necesară realizarea unei evaluări/analize de risc (procesul de caracterizare a riscului, din punct de vedere a componentelor, arhitectura, variabilele – vulnerabilităţile exploatate, sursa ameninţării, probabilitatea – din punct de vedere matematic şi statistic etc., toate aceste aspecte cu elementele teoretice şi descriptive). Trebuie spus că această sarcină trebuie realizată de un analist de risc, care, de obicei, nu este aceeaşi persoană cu managerul. Ca urmare a celor expuse mai sus, realizarea unui profil al riscului organizaţiei şi determinarea gradului de expunere la risc trebuie să fie o continuă preocupare a oricărui manager.

Pentru a concluziona cele expuse mai sus, putem să oferim o definiţie a managementului riscului. Astfel, managementul riscului reprezintă totalitatea procedurilor, deciziilor şi măsurile luate de către manager în vederea identificării vulnerabilităţilor, ameninţărilor, riscurilor, a celor mai bune metode de contracarare a riscurilor, a celor mai bune opţiuni de prevenire a acestora sau cel puţin de reducere a impactului riscurilor. Procesul sau procesele asociate managementului riscurilor poate fi desfăşurat de o persoană sau mai multe, în persoana managerului sau a echipei de management dedicată acestui domeniu. Ar trebui ca procesul specific managementul riscurilor să fie realizat de un analist, iar echipa de management sau managerul să fie implicat doar în luarea deciziilor.

Principalele caracteristici ale procesului de management a riscurilor sunt evidenţiate de conceptele exprimate de Organizaţia Internaţională de Standardizare (ISO), în conţinutul standardelor din familia 31000[2], astfel:

- creează beneficii, bazat pe principiu conform căruia costurile specifice managementului riscurilor ar trebui să fie mai mici decât impactul unui risc nesupravegheat;
- managementul riscurilor este direct integrat în toate procesele desfăşurate la nivelul organizaţiei;
- este o componentă importantă a procesului de luare a deciziei;
- Abordează în mod explicit concepte nesigure, cum ar fi probabilitatea şi posibilitatea;
- este un proces structurat pe nivele şi etape;
- procesul managementului riscurilor trebuie sprijinită pe o documentaţie foarte bine structurată;

[2] Organizaţia Internaţională de Standardizare, Colecţia ISO 31000 – www.iso.org.

- procesul managementului strategic trebuie calibrat pe nevoile organizaţiei;
- se bazează pe evaluarea şi acţiunea factorilor umani;
- este un proces transparent, cel puţin din anumite puncte de vedere;
- trebuie să fie un proces adaptabil;
- trebuie să permită o readaptare permanentă[3].

2. Evaluarea riscurilor pentru sistemele IT – un pas esenţial al managementului riscurilor

Primul pas în asigurarea unui flux de lucru eficient a managementului riscurilor dedicat mediilor informatice constă în evaluarea riscurilor. De obicei, această fază este realizată pentru a oferi o imagine a dimensiunii ameninţării şi a caracteristicilor acesteia. Acestea din urmă vor fi exploatate în fazele următoare pentru diminuarea sau eliminarea riscului.

Evaluarea riscurilor este compusă din nouă segmente fundamentale, astfel:

- Descrierea şi caracterizarea mediului;
- Identificarea ameninţării;
- Identificarea vulnerabilităţii;
- Analiza metodelor de control şi prevenţie;
- Determinarea posibilităţilor şi probabilităţilor;
- Analiza impactului;
- Determinarea riscului;
- Elaborarea propunerilor pentru controale viitoare;
- Documentarea rezultatelor.

Trebuie reţinut că ordinea activităţilor menţionate mai sus nu este obligatorie, unele dintre ele, precum identificarea ameninţării/vulnerabilităţii şi analiza controlului pot fi realizate simultan, în timp ce caracterizarea sistemului şi documentarea rezultatelor sunt activităţi iniţiale şi respectiv finale.

2.1. Caracterizarea sistemului

Evaluarea unui sistem informatic este bazată pe înţelegerea modului de lucru, cunoaşterea fluxului de lucru şi funcţiilor sistemului. Astfel, componentele fundamentale şi resursele sistemului trebuie identificate[4], precum şi datele conţinute de sistem.

Unul dintre cele mai importante aspecte legate de caracterizarea sistemului este legat de strângerea datelor. Pentru asta, trebuie luate în consideraţie următoarele tipuri de date:

- elemente legate de hardware şi software (caracteristici ale sistemului, dezvoltatori, versiunea software-ului, politici de update etc.);
- conexiuni interne şi externe ale sistemului;
- liste ale conturilor ce au acces şi tipul de acces al fiecărui utilizator;
- principalul scop al sistemului;
- valoarea sistemului;
- nivelul de protecţie necesar pentru menţinerea integrităţii sistemului, disponibilităţii şi confidenţialităţii;
- alte date precum politici de securitate, diagrama reţelelor, fluxuri de lucru, securitate fizica etc.

[3] Standardul NIST SP 800-30, 800-37 şi 800-39 – www.crc.nist.gov.
[4] Standardul NIST 800-37 (www.crc.nist.gov) Ghidul de aplicare a cadrului de management a riscurilor.

2.2. Identificarea vulnerabilităţii

Cum am afirmat şi înainte, vulnerabilităţile sunt slăbiciuni în securitatea sistemului. Pentru a obţine o listă viabilă a vulnerabilităţilor ce pot fi exploatate de ameninţările externe, este recomandat accesarea unor diferite surse de informare, testarea sistemului şi verificarea unor date rezultate în urma caracterizării sistemului.

Sursele vulnerabilităţilor pot fi abordate diferit, în funcţie de starea sistemului[5]:

- în cazul unui sistem operaţional, identificarea vulnerabilităţilor se va concentra pe analiza efectivă a sistemului, precum şi a măsurilor deja în vigoare menite să protejeze sistemul;
- pentru sistemele deja proiectate, fiind în faza de implementare, căutarea de vulnerabilităţi va fi concentrată pe politicile legate de punerea în aplicare şi pe schema existentă, împreună cu certificările existente şi testele anterioare[6];
- pentru sistemele aflate în faza de proiectare, căutarea vulnerabilităţilor se va realiza prin concentrarea pe politicile generale ale instituţiei, procedurile, regulamentele, analizele anterioare şi, dacă este cazul, pe caracteristicile tehnice ale sistemului.

Unele avantaje legate de identificarea vulnerabilităţilor pot fi obţinute din testarea sistemului, prin folosirea unor metode de testare, precum scanarea automată a vulnerabilităţilor, prin teste de securitate sau teste de penetrare (scanarea port-urilor, scanarea bazelor de date, simulări etc.).

2.3. Identificarea ameninţării

În cadrul acestei etape, activităţile sunt concentrate pe posibilele surse ce exploatează defectele sistemului informatic, pe stabilirea motivaţiei sau, dacă este cazul, pe manifestarea efectivă a unor asemenea surse. Direct legat de subiectul acestui articol, o ameninţare a sistemului IT poate orice circumstanţă sau eveniment cu potenţial de afectare a sistemului. Cele mai comune ameninţări pot avea origine umană, naturală sau de mediu. Este evident că factorul uman este cel mai important a fi luat în considerare, dar totuşi nu trebuie neglijate nici celelalte – furtuni, cutremure, furtuni electrice, poluare etc.

Din punct de vedere a motivaţiei ameninţării, este evident că aceasta poate abordată doar făcând referire doar la factorul uman – drept urmare, oamenii sunt cea mai gravă sursă de ameninţare. Este o necesitate de a separa eventualele persoanelor cu intenţii de a face rău utilizând taxonomii legate de mediul din care provin, scopul lor etc. Nu trebuie să neglijăm personalul anterioare care au lucrat anterior în cadrul instituţiei (datorită cunoştinţelor legate de sistemul în sine), eventualii teroriştii cibernetici, infractorii cibernetici obişnuiţi, precum şi hackeri simpli, motivate doar de dorinţa de a ocoli-un firewall sau pentru a obţine glorie de la preluarea controlului a unui website guvernamental.

2.4. Analiza măsurilor de control şi prevenire

Scopul acestei etape este eliminarea defectelor implementate anterior în sistem. Pe de altă parte, nu trebuie să se neglijeze măsurile preventive care sunt prognozate a fi implementat la un anumit moment viitor. Dacă nu există astfel de măsuri aplicate, necesitatea aplicării trebuie să fie subliniată şi adusă în atenţia forului de management. Măsurile preventive pot fi fie cele tehnice (încorporate în hardware, software sau firmware) sau cele procedurale / operaţionale (politicile de securitate, procedurile de operare, reglementările interne etc.).

---

[5] Georgică Panfil, *Managementul riscurilor associate securităţii informatice*, editura Estfalia, Bucureşti, Romania, 2013, pp. 27.

[6] Urs E. Gattiker,– *Securitatea informatică, strategii pentru înţelegerea şi reducerea riscurilor,* editura Wiley & Sons, 2005, pp.87.

2.5. Determinarea probabilităţii

În cadrul acestei faze scopul principal este de a obţine o estimare a posibilităţii ca o anumită vulnerabilitate să fi exploatată de o anumită ameninţare. Ca atare, următorii factori vor fi luaţi în considerare:

- motivaţia şi capacitatea sursei ameninţării de a fi periculoasă pentru sistem IT / organizaţie;
- natura şi caracteristicile vulnerabilităţii;
- existenţă şi eficienţa măsurilor de prevenire / control.

Concluziile acestei faze vor fi prezentate la o scară calitativă, cu posibilitatea de a fi mare, moderată sau scăzută, direct legate de gradul de motivare a ameninţării şi a măsurilor deja puse în aplicare.

2.6. Analiza impactului potenţial

Este foarte important să înţelegem cât de mult daune pot fi provocate de anumite incidente. Ca atare, ar trebui să se ia în considerare aspecte legate de importanţa sistemului informatic pentru instituţie, destinaţia sistemului şi proceselor şi, de asemenea, de sensibilitatea sistemului (nivelul de protecţie necesar pentru sistem în vederea menţinerii trinomului sale CIA). Prin urmare, analiza va evalua sistemul din următoarele puncte de vedere: pierderea integrităţii (modificărilor neautorizate), pierderea de disponibilitate (în cazul în care sistemul este esenţial pentru obiectivele organizaţiei, pierzând posibilitatea de a-l accesa înseamnă a pune în pericol scopul fundamental al organizaţiei) şi pierderea de confidenţialitate (eşecul de a proteja datele împotriva accesului neautorizat).

Impactul potenţial ar trebui să fie caracterizat după cum urmează:

-mare (afectează grav însăşi instituţia cu obiectivele sale, resursele umane şi valorile);

-mediu (se creează un mare prejudiciu financiar şi poate induce, de asemenea, daune pentru resurselor umane);

-mic (creează unele pierderi financiare şi pierderi minore pentru organizaţie în sine).

2.7. Determinarea nivelului riscului

Această sarcină se bazează pe datele anterior colectate în cadrul altor segmente ale evaluării şi are menirea de a reflecta nivelul de risc asociat sistemului informatic[7]. Determinarea riscului pentru o pereche vulnerabilitate - ameninţare este strâns legată de:

- posibilitatea ca o anumită sursă a ameninţării să exploateze o anumită vulnerabilitate;
- dimensiunea şi efectele impactului sunt consecinţă a exploatarea cu succes a unei vulnerabilităţi de către o ameninţare;
- eficienţa estimată a prevenţiei sau cel puţin a mecanismelor de detecţie implementate pentru reducerea sau eliminarea riscurilor.

Pentru a măsura riscul, pot fi utilizate diferite instrumente, precum matricea riscului, urmată de scala riscului.

2.8. Recomandări cu privire la măsurile antirisc

Urmărind etapele prezentate până în acest punct, măsuri capabile să diminueze sau chiar să elimine riscurile identificate pot fi elaborate. Scopul acestora este de a reduce riscul pentru sistemul informatic şi datele conţinute la un nivel acceptabil[8]. Cu toate acestea, ar trebui să se ia în considerare următoarele aspecte legate de aceste măsuri:

- compatibilitate cu sau realităţile organizaţiei sau sistemului;
- legea sau limitări de reglementare;

[7] Standardul NIST 800-39, Managementul riscurilor securităţii informatice, - www.crc.nist.gov.

[8] Doug Howard, – *Securitate în 2020, reducerea riscurilor acestui deceniu,* Editura Wiley, 2010, pp. 112.

- politicile organizaţiei;
- impactul operaţional;
- siguranţă / securitate asigurată de măsurile propuse.

Trebuie spus că, din punctul nostru de vedere, faza de recomandare a măsurilor este una dintre cele mai importante rezultate ale evaluării riscurilor (apreciere) şi este menită să ofere o bază solidă pentru procesul de diminuare a riscurilor, în cursul căreia recomandările procedurale, precum şi măsurile de securitate sunt evaluate, prioritizate şi puse în aplicare.

2.9. Documentarea rezultatelor

Documentarea rezultatelor reprezintă faza finală a evaluării riscurilor şi este legată de raportul care conţine rezultatele şi observaţiile constatate. Scopul raportului este de a oferi un sprijin durabil pentru stratul decizional în implementarea schimbărilor operaţionale, financiare, procedurale şi de reglementare. Acest tip de raport nu este legat de forma unui raport de audit, care uneori tinde să conţină obiective destul de dure-, ci mai degrabă este de o manieră mai sistematică şi analitică ce furnizează stratului de gestionare un instrument pentru o mai bună înţelegere a evaluării procesului decizional.

Raportul va conţine următoarele aspecte[9]:

- partea introductivă (scopul evaluării, obiective descrierea sistemului, descrierea componentelor, utilizatorii, locaţii, infrastructură etc.);
- prezentarea scurtă a metodologiei de lucru, participanţii, tehnicile utilizate pentru evaluare, tipuri de matrice etc.
- caracterizarea sistemului din punct de vedere a hardware-ului, software-ului, interfeţelor, datelor, utilizatorilor, politicilor, diagrame, grafice etc.
- descrierea vulnerabilităţilor şi riscurilor;
- prezentarea rezultatelor evaluării, evaluarea riscurilor, a măsurilor recomandate, tipul de impact şi amplitudine etc.
- concluzii.

3. Concluzii

Prezentul articol este concentrat pe problemele legate de managementul riscurilor şi axat pe evaluarea riscurilor privind un sistem de tehnologie a informaţiei, fie calculator sau reţea există sau alte active informaţionale. Considerăm că fiecare manager trebuie să fie conştient de principalele faze legate de evaluarea riscurilor şi cele mai bune practici de urmat. Este evident că, în contextul actual, fiecare organizaţie trebuie să acorde o atenţie sporită riscurilor care tind să o ameninţe, şi în special celor legate de siguranţa componentelor cibernetice.

Eliminarea sau diminuarea riscurilor legate de mediile informatice este un pas important în realizarea obiectivelor organizaţiei. Astfel, o politică de management care să gestioneze corespunzător riscurilor aduce numeroase beneficii, atât de ordin economic cât şi la nivelul mediului de lucru.

[9] Standardul NIST 800-37 (www.crc.nist.gov) – Ghidul de Aplicare a Cadrului Managementului Riscurilor.

REFERINŢE BIBLIOGRAFICE:

1. Georgică Panfil, Managementul riscurilor asociate securităţii informatice, editura Estfalia, Bucureşti, Romania, 2013.
2. Georgică, Panfil – Fundamentele managementului riscurilor, în European Journal of Public Order and National Security, numărul 3/2014.
3. Doug, Howard – *Securitate în 2020, reducerea riscurilor acestui deceniu,* Editura Wiley, 2010.
4. Urs .E., Gattiker – Securitatea informatică, strategii pentru înţelegerea şi reducerea riscurilor, editura Wiley & Sons, 2005.
5. Standardele ISO/IEC 27000 (www.iso.org) – Tehnologia Informaţiei — Tehnici de Securitate — Sisteme de management al securităţii informaţionale — Prezentare generală şi vocabular.
6. ISO 31000:2009 Standard (www.iso.org) - Principii şi Direcţii de Implementare.
7. Standardul ISO/IEC 31010:2009 (www.iso.org) – Managementul Riscurilor – Tehnici de Evaluare a Riscurilor.
8. Standardul ISO 73:2009, Vocabularul Managementului Riscurilor www.iso.org şi www.iso-standards.org.
9. NIST Standard 800-30 (www.crc.nist.gov) – Ghidul de Management al riscurilor pentru Sistemele Informatice
10. Standardul NIST 800-37 (www.crc.nist.gov) – Ghidul de Aplicare a Cadrului Managementului Riscurilor.
11. Standardul NIST 800-39, Managementul riscurilor securităţii informatice, - www.crc.nist.gov.

COMUNICAREA TERORII ÎN SPAŢIUL VIRTUAL

Dragoş Claudiu FULEA
Serviciul Român de Informaţii, dfulea870@dcti.ro

Cătălin MIRCEA
Serviciul Român de Informaţii, cmircea870@dcti.ro

Marius Ciprian CORBU
Serviciul Român de Informaţii, mcorbu870@dcti.ro

Abstract: *Din punct de vedere al facilităţilor tehnologice oferite, WEB 2.0 constituie un spaţiu ideal de manifestare pentru organizaţiile teroriste în scopul coordonării operaţiunilor, revendicării atentatelor sau promovării ideologiei proprii. Recent, în cazuri precum cel al aşa-zisului Stat Islamic din Irak şi Siria (ISIS) se observă o mutaţie în registrul comunicării, prin translatarea mesajului către o formă explicită şi ilustrativă de teroare. Din această perspectivă, nu trebuie omis nici riscul ca dependenţa crescută în rândul segmentului de tineret, chiar şi cel având un nivel ridicat de instruire din ţările occidentale tintă, faţă de emoţiile puternice generate de mesaje cu nivel crescut de violenţă, vehiculate de produsele mediatice cu audienţă globală, să favorizeze un efect de popularizare a „producţiilor" ISIS. Pe de altă parte, forţa colosală de comunicare specifică erei New Media poate fi în măsură să dinamizeze procesul de auto-îndoctrinare online, intenţionat de către terorişti.*

Lucrarea îşi propune să exploreze evoluţia şi impactul mesajului terorist în spaţiul cibernetic, constituindu-se, totodată, într-o pledoarie pentru obţinerea unei superiorităţi tehnologice de către serviciile de intelligence care, concomitent cu instruirea resursei umane proprii, să conducă la o sporire a eficienţei de reacţie faţă de ameninţarea teroristă.

Cuvinte-cheie: Terorism WEB, New Media, IT&C, servicii de intelligence, WEB 2.0.

Introducere

Opinia publică mondială este în continuare asaltată de către operatorii media, cu clişee stereotipe ale teroriştilor proveniţi din Orientul Mijlociu de genul: alienaţi mintali violenţi marcaţi de o viaţă pauperă, dotaţi cu mijloace rudimentare de comunicare şi de luptă.

De asemenea, cvasi-inexistenţa unui demers analitic integrat în procesul de elaborare a mesajului mediatic diseminat la nivel global a sporit percepţia schematică, confuză, cu conotaţii negative la adresa acestei regiuni geografice considerată drept o lume tradiţionalistă, interiorizată, care respinge valorile contemporane. Astfel, gruparea extremistă Stat Islamic din Irak şi Siria (ISIS) a devenit noua etichetă mediatică a Orientului Mijlociu.

Incontestabil, realitatea din ţările musulmane din regiune este traversată de diverse orientări fundamentaliste violente, iar unul dintre motivele esenţiale ale implantării geografice ale ISIS rezidă în slăbiciunea sau chiar epuizarea unor ţări aflate la limita eşuării, marcate de conflicte militare externe (Irak) sau interne (Siria, Libia).

În cazul Statului Islamic din din Irak şi ash-Sham, o succintă analiză a profilului organizaţional relevă o realitate alternativă surprinzătoare, precum:

- existenţa unei profunde motivaţii politice suficient de elaborate pentru a fi în măsură să deformeze idealuri religioase şi să uziteze cu cinism, în scopuri violente, devoţiunea şi fervoarea specifice unei religii milenare;

- caracter social eterogen, compus din segmente diverse de populaţie;
- caracter multinaţional regional cu risc concret de difuzare la nivel internaţional;
- capabilităţi IT&C importante, angrenate într-un demers minuţios elaborat de propagare online a unei forme ilustrative şi explicite de teroare;
- pregătire în domeniul militar - deţinerea unor cunoştinţe solide, atât din punct de vedere teoretic, cât şi practic, în tactica militară, în special lupta de gherilă în mediul urban.

În acest context, devine evidentă preocuparea ţărilor musulmane din Orientul Mijlociu de a sigila efectul de contagiune fundamentalist-teroristă, la nivelul teritoriului ocupat în prezent de ISIS.

Lucrarea îşi propune să exploreze evoluţia şi impactul mesajului terorist în spaţiul cibernetic, constituindu-se, totodată, într-o pledoarie pentru obţinerea unei superiorităţi tehnologice de către serviciile de intelligence care, concomitent cu instruirea resursei umane proprii, să conducă la o sporire a eficienţei de reacţie faţă de ameninţarea teroristă.

1. Comunicarea în spaţiul cibernetic

Internetul oferă posibilitatea de desfăşurare a unei comunicări interactive, emiţătorul putând să dirijeze mult mai bine fluxul comunicaţional şi să-l îndrepte spre receptorul vizat. Fiecare utilizator de Internet este capabil să transmită mesaje mai multor receptori care, la rândul lor, pot emite mesaje în timp ce recepţionează. Concluzia este că fiecare participant la comunicarea de masă de pe Internet este atât emiţător, cât şi receptor.

Totodată, utilizarea intensivă şi evoluţia continuă a platformelor tehnologice oferite de Internet a amplificat profunzimea procesului de comunicare în masă cu elemente noi precum feedback-ul instantaneu şi posibilitatea de a răspunde folosind acelaşi canal precum emiţătorul, dar şi prin utilizarea simultană a unor canale suplimentare.

În acest context, se poate afirma că deşi trinomul comunicaţional fundamental a rămas neschimbat (emiţător-canal de comunicare-receptor), revoluţia tehnologică a canalului de transmitere a mesajului a determinat evoluţia de la modelul clasic liniar la un model molecular al comunicării.

Definirea conceptuală a etapei actuale a procesului de comunicare online, respectiv fenomenul New Media, este dificilă întrucât se referă la un domeniu de referinţe vast, fluid, aflat în permanentă evoluţie. Un înţeles particularizat al termenului, util acestei lucrări, se referă la multitudinea formelor de comunicare electronică care sunt posibile datorită existenţei platformei tehnologice numite WEB 2.0.

Social media este cel mai reuşit exponent al interactivităţii sociale din mediul on-line şi, totodată, componentă principală a filozofiei New Media.

Elementele din spaţiul cibernetic reprezentative pentru ceea ce numim New Media se referă la:

- *Bloguri;*
- *Forumuri, camere de chat;*
- *Reţele de socializare;*
- *Aplicaţii gen messenger;*
- *Lumile realităţii virtuale;*
- *Integrarea telefoniei mobile în spaţiul digital.*

Amplitudinea propagandei diseminate prin intermediul instrumentelor informaţionale şi de comunicare New Media nu trebuie subestimată iar un exemplu concludent este rolul social media în declanşarea şi evoluţia „Primăverii Arabe” sau a diseminării mesajului violent al ISIS.

Dacă ar mai exista o urmă de scepticism faţă de această afirmaţie, ar fi suficientă consultarea paginilor de Facebook *We are all Hamza Akhateeb*, care prezintă abuzurile grave comise de regimul de la Damasc la adresa populaţiei civile şi un feedback constant asupra evenimentelor din Siria sau a celor aparţinând organizaţiei Statul Islamic din Irak şi ash-Sham.

2. Terorismul „WEB 2.0"

WEB 2.0 constituie un spaţiu ideal de manifestare pentru grupările teroriste din mai multe motive, dintre care se pot enumera:

- accesul rapid;
- interactivitatea sporită;
- audienţe vaste formate din indivizi de pe tot cuprinsul globului;
- anonimatul comunicării pe perioade scurte de timp;
- accesul la un flux rapid de informaţii;
- resurse financiare reduse;
- posibilităţi multimedia de comunicare;
- precaritatea reglementărilor, cenzurii sau a altor forme de control guvernamental
- sursă de informare pentru jurnaliştii mediilor de comunicare tradiţionale de tip WEB 1.0.

Exploatarea acestor caracteristici a oferit organizaţiilor teroriste, în special celor jihadiste din Orientul Mijlociu, posibilitatea unui control asupra modului de distribuţie a mesajelor propagandistice destinate unei categorii extinse de receptori.

În acest context, s-a consolidat utilizarea de către extremiştii musulmani a New Media ce utilizează resursele WEB 2.0 ca o agora virtuală, liberă de constrângeri privind naţionalităţi şi graniţe, care integrează şi promovează curente de opinie extremiste pentru auditoriul unor publicaţii electronice ce asigură o pregătire religioasă, ideologică şi militară a voluntarilor jihadului.

Pe de altă parte, elementele definitorii ale New Media, precum Twitter, WhatsApp, Facebook, YouTube sunt intens utilizate de către activiştii jihadului, cu precădere de cei aparţinând ISIS.

Studii aprofundate de specialitate[1] au demonstrat că doar într-un interval temporal restrâns (septembrie-decembrie 2014) activiştii Statului Islamic au exploatat activ un număr considerabil de conturi Twitter estimat numeric în intervalul 46.000-70.000, localizate preponderent în Irak şi Siria, dar şi în ţări precum Arabia Saudită, Egipt, Tunisia, Libia, Zemen şi fâşia Gaza[2].

De remarcat că popularizarea ISIS pe platforma de comunicare amintită a fost cauzată de un grup restrâns de utilizatori cuprins între 500 şi 2.000. În Figura nr.1 este reprezentat grafic procesul de comunicare activat de nucleul „dur" al activismului ISIS pe reţeaua de Twitter. Evaluarea modului de creştere a bazei de susţinători ISIS, pe Twitter, a relevat şi aspecte inedite, precum posibilitatea documentării modului de separare ideologică a ISIS de Al-Qaida. Mulţi susţinători ai Al-Qaida au renunţat la conturile create anterior anului 2010 şi au recreat altele pentru a-şi demonstra loialitatea pentru ISIS.

[1] J.M. Berger and Jonat hon Morgan, "The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter", The Brookings Project on U.S. Relations with the Islamic World, analysis paper March 2015.

[2] Aaron Zelin, "The Islamic State's Model," *Washington Post*, 28 January 2015, http://www.washingtonpost.com/ blogs/monkey-cage/wp/2015/01/28/the-islamic-states-model.

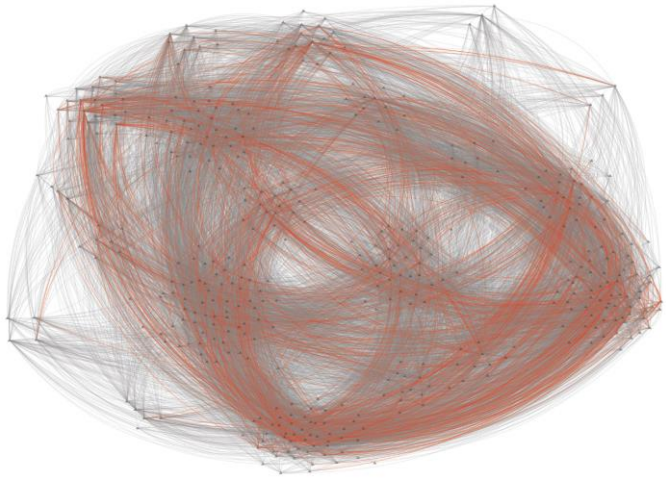


Figura nr. 1

Totodată, intensificarea comunicării toxice de geneză teroristă în spaţiul virtual permanentizează procesul de consolidare şi propagare a unui fenomen periculos, respectiv generarea de celule teroriste spontane ale căror membri se pot reuni ad-hoc în vederea executării operaţiunii teroriste ulterior comunicării în camere de chat codificate, fără un antrenament comun prealabil. Premiera nefericită a acestui tip nefast de activism, inaugurată în iulie 2005, prin cazul atentatelor din Londra, riscă să se multiplice exponenţial în viitor.

În subsidiar, din perspectivă managerială şi tehnologică, WEB 2.0 a permis o coordonare operaţională calitativ superioară activităţii entităţilor teroriste. De exemplu, pentru a securiza comunicarea, atât cu propriile celule, cât şi cu potenţialii candidaţi la recrutare, grupările teroriste au apelat la programe de criptare cu cheie exponenţială disponibile public, de tip Pretty Good Privacy (PGP), ce au permis codarea traficului de E-mail prin care erau diseminate informaţii despre arme, ţinte vizate şi tactici de luptă.

De asemenea, a fost consolidată procedura de utilizare a steganografiei care implică disimularea unor mesaje (instrucţiuni sub formă de hărţi, fotografii, direcţii şi detalii tehnice despre folosirea explozivilor) în interiorul unor fişiere grafice (de exemplu, fotografii cu conţinut explicit sexual transmise prin Email între extremiştii islamişti). Există indicii care conduc la concluzia că autorii atentatului sângeros de la Paris împotriva revistei Charlie Hebdo au utilizat steganografia. Anchetatorii francezi au identificat în anul 2010, în calculatoarele lui Amedy Coulibaly (autodeclarat susţinător ISIS) şi Cherif Kouachi (autodeclarat susţinător al Al-Qaida) fişiere cu pornografie infantilă, care mascau de fapt utilizarea de către cei doi terorişti a site-urilor de mesagerie pentru adulţi, în scopul evitării depistării de către autorităţi[3].

3. Componentele comunicării teroriste

Emiţătorii

Prezenţa grupărilor teroriste pe Internet are mai multe consecinţe, printre care ameninţarea stabilităţii şi credibilităţii surselor de informaţii (riscul sporit de apariţie a cazurilor de dezinformare şi fraudare), creşterea numărului membrilor şi simpatizanţilor teroriştilor nu numai în ţara de origine a grupării, dar şi la mare distanţă.

În mod obişnuit, site-urile teroriste conţin istoricul organizaţiei şi al acţiunilor sale, o analiză detaliată a formaţiei sale sociale şi politice, biografii ale liderilor, finanţatorilor,

[3] http://tempsreel.nouvelobs.com/charlie-hebdo/20150114.OBS9988/info-obs-les-cliches-pedophiles-une-couverture-pour-coulibaly-et-kouachi.html

eroilor, informaţii despre scopurile sale politice, ideologice, critici la adresa duşmanilor, noutăţi aduse la zi.

Mesajul

Până la începutul primului deceniu al mileniului actual, majoritatea site-urilor teroriste nu prezentau descrieri detaliate ale acţiunilor criminale şi ale consecinţelor lor catastrofale. Această strategie era în acord cu propaganda şi construcţia de imagine pe care teroriştii intenţionau să o prezinte potenţialilor susţinători prin intermediul Internetului.

În prezent, mesajele difuzate pe reţelele de socializare sau pe site-urile deţinute de organizaţiile teroriste precum Statul Islamic din Irak şi ash-Sham prezintă un nivel ridicat de rafinare şi, *respectă structura comunicaţională specifică unei acţiuni complexe, originară din domeniul de intelligence, cu trei etape secvenţializate distinct: propagandă, contrapropagandă şi influenţă, concomitent cu o exagerbare a violenţei în registrul comunicării, prin translatarea mesajului către o formă explicită şi ilustrativă de teroare.*

Prima structură retorică vizează propaganda şi promovează conceptul lipsei de alternativă în afară de lupta armată (atenţie, nu este uzitat termenul de violenţă) privită ca ultim resort prin care „cel slab", „sărac" şi „neajutorat" se poate opune cu succes celui „puternic" „bogat" şi „plin de resurse".

În timp ce acţiunile criminale orchestrate de teroriști împotriva populaţiei civile care nu împărtăşeşte aceeaşi „dreaptă credinţă" nu sunt menţionate, contramăsurile adoptate de guvernele şi regimurile care se opun terorismului sunt caracterizate prin termeni precum „genocid", „crimă în masă", „măcel sângeros".

Organizaţia teroristă este prezentată ca subiect de persecuţie, cu lideri vânaţi şi asasinaţi, membri şi susţinători masacraţi, totul în vederea anihilării libertăţii religiei şi a autodeterminării statale (Califatul Islamic).

Intenţionat mesajul pune accent pe intenţia opozanţilor terorismului de a îngrădi libertatea de expresie şi autodeterminarea „celui slab" apărat doar de luptătorii pentru dreptate, întrucât sunt concepte bine ancorate în mentalul colectiv occidental, euroatlantic, cu puternică rezonanţă simbolic-cognitivă pentru publicul european şi nord-american.

Cea de-a doua structură retorică vizează contrapropaganda şi se constituie într-un set de măsuri destinate motivării necesităţii actelor violente ale teroriştilor.

În general, cea mai uzitată metodă constă în folosirea şi promovarea în social media a unui limbaj non-violent. Mesajul comunicării în reţelele de socializare este distorsionat şi manipulat în sensul afirmării disponibilităţii mişcării teroriste pentru o posibilă „soluţionare paşnică", „prin negociere" în condiţiile în care regimurile ostile terorismului acceptă soluţia politică a ISIS.

Ultima structură retorică vizează influenţarea şi sensibilizarea unor potenţiali adepţi din segmentele tinere ale societăţii, care accesează site-urile teroriste, ca etapă preliminară punctării şi selecţionării acestora în vederea recrutării. Presupune o planificare atentă a modului de elaborare şi etapizare a mesajelor diseminate unidirecţional.

Deloc surprinzător, în pofida avansului tehnologic al canalului de diseminare, propaganda teroristă utilizează o metodă care, deşi arhaică, rămâne la fel de eficace, respectiv demonizarea şi lipsa legitimităţii acţiunilor inamicilor.

În acest context, mesajul conţine construcţii lingvistice agresive, brutale şi expresive întrucât trebuie să atace, de o manieră negativă, registrul emoţiilor primare, respectiv sentimentul de apartenenţă a individului la o religie ca precondiţie de stabilizare morală şi psihică umană. În acest sens, comunicarea difuzează un semnal de alarmă privind apărarea valorilor religioase de apartenenţă, aflate în pericol de dispariţie din cauza acţiunilor duşmanilor.

Recent, acest mesaj a fost amplificat intenţionat prin difuzarea în spaţiul virtual a unor videoclipuri de o violenţă extremă. Execuţiile ostaticilor ISIS atrag ca un magnet şi satisfac o dorinţă perversă de sânge, senzaţional şi dispreţ faţă de valorile umanităţii.

Pe de o parte, reluarea în slow-motion a momentului descărcării armei în capul victimei, precum obsesia de a prezenta detalii vizuale ale rănilor la nivelul capului şi a restului corpului intenţionează realizarea unei ancore la nivelul mentalului privitorului. Practic, se doreşte asocierea luptătorului ISIS cu imaginea de deţinător absolut al puterii, de judecător şi călău mai presus de viaţă sau moarte. Pe de altă parte, diseminarea execuţiilor prin decapitare derulate de ISIS are un potenţial mediatic necontrolabil, teroriştii devenind dependenţi de postarea unor detalii din ce în ce mai şocante pentru a menţine ratingul online şi a atrage noi adepţi (de exemplu, arderea de viu a pilotului iordanian închis în cuşcă).

Receptorii

Trebuie subliniat faptul că segmentul de populaţie tânără, predominant în sfera de influenţă musulmană, ce constituie ţinta principală a organizaţiilor teroriste din Orientul Mijlociu, este la fel de permeabil şi influenţabil la mesajul comunicaţional toxic de geneză teroristă, precum tineretul occidental, întrucât dispune de conexiune permanentă la instrumentele New Media prin intermediul smartphone-ului şi tabletei PC, care rulează pe platforma tehnologică oferită de WEB 2.0.

Studii de auditare online au demonstrat că susţinătorii organizaţiei Statul Islamic utilizează în proporţii de 69% smartphone cu sistem de operare Android, 30% utilizează iOS şi doar 1% Blackberry.

Adesea, modul de dispunere a receptorilor comunicării toxice de geneză teroristă urmează modelul cercurilor concentrice. În primul rând, gruparea teroristă va avea drept receptori ţintă susţinătorii locali, realizând pentru aceştia un site în limba locală, care va cuprinde informaţii detaliate ale activităţilor şi politicii interne de organizare, despre aliaţi şi duşmani. În al doilea rând, pe cercul exterior imediat următor se va situa opinia publică internaţională, care nu este implicată în mod direct în conflict, dar care ar putea fi interesată de acest subiect. În acest caz site-ul este elaborat în alte limbi decât cele vorbite în mod curent de terorişti. Sunt site-uri construite preponderent în limba engleză, în vederea unei diseminări internaţionale. Pentru acest tip de receptori, paginile web cuprind doar informaţii de bază despre organizaţie.

Ultimul cerc exterior de receptori este reprezentat de publicul considerat inamic (cetăţeni ai statelor împotriva cărora luptă grupările teroriste). Conţinutul site-urilor nu este explicit formulat pentru acest tip de public, dar există şi pagini web care depun evidente eforturi de a demoraliza inamicul prin ameninţarea cu atacuri şi inducerea sentimentului de vină pentru motivele şi acţiunile duşmanilor. Un alt scop urmărit este acela de a stimula dezbaterile publice din ţările inamice, de a schimba opinia publică şi de a slăbi suportul publicului faţă de guvernul ţării ţintă.

Un element de noutate extrem de periculos, introdus de către activismul ISIS şi care particularizează această organizaţie, constă în filtrarea pe criterii religioase a receptorilor din statele europene, americane sau asiatice, membre ale coaliţiei antiteroriste. Segmentul de populaţie vizat este reprezentat de adolescenţii proveniţi din a doua generaţie de emigranti islamici proveniţi din zonele de conflict şi stabiliţi în ţările care au oferit sanctuar[4]. Aceştia petrec majoritatea timpului online acumulând noi informaţii despre cultura şi obiceiurile de origine ale părinţilor sau vizând evoluţiile sociale, politice şi economice din ţările originare. În acest context, pot deveni vulnerabili faţă de propaganda agresivă a radicalismului fundamentalist religios, iar ulterior susceptibili la adeziunea faţă de acte de violenţă, motivând

[4]http://www.independent.co.uk/voices/comment/isis-in-the-uk-how-the-war-on-terror-radicalised-a-generation-9813362.html

acest demers prin dorinţa de a recupera „veche generaţie”, apatică şi coruptă de bunăstarea oferită de nivelul de trai din statele gazdă. Sunt vizate preponderent ţările occidentale, care au oferit azil.

Se poate aprecia că finalitatea demersurilor ISIS vizează coagularea unui sprijin covârşitor din partea Ummah, comunitatea islamică mondială formată din totalitatea musulmanilor.

4. Terorismul WEB 2.0 vs. Intelligence

Activităţile de documentare, planificare şi coordonare a resurselor logistice, financiare şi umane pe care le presupune o operaţiune teroristă sunt dificil de identificat şi controlat întrucât “semnătura” lor informaţională pe WEB 2.0 este difuză. Pe de altă parte, adeseori informaţiile colectate nu capătă o relevanţă a ameninţării decât poate prea târziu.

În acest context, replica comunităţilor de intelligence a fost focalizată asupra dezvoltării şi specializării capabilităţilor analitice concomitent cu înzestrarea acestora cu instrumente de tehnologie informaţională şi de comunicare (IT&C) capabile să identifice / să deceleze, cu oportunitate, “semnătura” activităţilor teroriste din mediul virtual ce se pot concretiza, credibil, în atentate. Produsul de intelligence se impune a fi actualizat şi prezentat de urgenţă factorului decizional pentru adoptarea măsurilor de limitare a efectelor atacului, mai ales în situaţia unui eşec al măsurilor preventive

În mod curent, serviciilor de intelligence le revine sarcina de a absorbi o cantitate imensă de date, de a le prelucra, a le trece apoi prin filtrul analitic şi, în final a le disemina, sub forma unui produs de intelligence valid, factorilor decizionali abilitaţi. Din acest motiv este vitală obţinerea unei superiorităţi tehnologice precum şi instruirea resursei umane proprii. În consecinţă, acestea vor conduce la o sporire a eficienţei de reacţie.

În practică, pe parcursul derulării etapelor procesului „clasic” de elaborare a unui produs de intelligence care întruneşte toate cerinţele pentru a fi diseminat către factorii decizionali abilitaţi, analiştii de informaţii consumă un fond de timp disproporţionat în cadrul activităţilor de cercetare, analiză şi producţie a datelor şi informaţiilor.

Astfel, majoritatea acestui timp este alocat cercetării (căutare, vizualizare, colectare, lecturare şi pre-procesare a datelor în vederea evaluării) şi în mai mică măsură procesului de analiză propriu-zisă (formularea unor opinii corecte, reale şi verificabile), adică exact etapa care defineşte valoarea produsului de intelligence.

Diverse experimente, derulate în plan internaţional[5], vizând dezvoltarea capabilităţilor analitice prin implementarea tehnologiilor informaţionale au demonstrat, indubitabil, că utilizarea IT&C a condus la o creştere impresionantă a calităţii produsului de intelligence. Mai mult, fondul de timp dedicat etapei de cercetare a fost redus în mod drastic, ceea ce a permis alocarea unui interval de timp adecvat pentru rafinarea şi certificarea procesului de analiză.

Instrumentele IT&C pentru suportul cooperării, în interiorul comunităţilor de intelligence, precum şi cele de analiză şi suport decizional pentru factorii abilitaţi, permit echipei om-maşină să analizeze şi să rezolve probleme informaţonale cu un grad ridicat de complexitate, în mod eficient şi oportun. Marele câştig al utilizării acestor instrumente rezidă în transformarea imensei cantităţi de date care, adeseori, tinde să suprasolicite capabilităţile analitice ale serviciile de informaţii şi securitate, în ceea ce putem numi precursori ai informaţiilor de intelligence.

De ce doar precursori şi nu informaţii de intelligence? Întrucât, în final, doar factorul

[5] Popp Robert, Armour Thomas, Senator Ted, Numrych Kristen, „Countering terrorism trough information tehnology, Comunications of the ACM”, vol. 47, no. 3, Minneapolis, 2004 accesat în 13 martie 2015 at http://information-retrieval.info/taipale/papers/p36-popp.pdf

uman poate transforma datele în informaţii, iar informaţiile în cunoaştere. Instrumentele IT&C pot doar să amplifice capacităţile intelectului uman. În domeniul prevenirii terorismului, abordarea problematicii prin utilizarea tehnologiilor informaţionale permite analistului evitarea capcanelor mentale generate de prejudecăţi sau interpretări eronate cauzate de un input limitat de date.

Concluzii

Evaluarea mesajului ISIS în spaţiul cibernetic devoalează faptul că organizaţia are o construcţie elaborată, care depăşeşte cu mult dimensiunile unei grupări teroriste, suprapusă cu atenţie pe modelul primordial al credinţei islamice pentru a răspunde unei nevoi de credinţă. In fapt, „Califatul Islamic" constituie o ofertă cu potenţial propagandistic uriaş: pe de o parte asigură un nou orizont de speranţă pentru populaţiile musulmane din regiune în condiţiile eşecului „primăverii arabe", iar pe de altă parte iniţiază un apel disperat la susţinere din partea comunităţii islamice mondiale.

Ar fi greşit să susţinem că dezvoltarea New Media este cauza propagării globale a fenomenului terorist. Se poate concluziona doar că revoluţia tehnologiei informaţionale a antrenat cu sine evoluţia tuturor resorturilor funcţionale intime şi manifestărilor (benefice sau nu) societăţii umane, în efortul acesteia de adaptare la cerinţele unui mediu globalizat.

Din perspectiva comunităţii de intelligence, problema principală pentru contracararea ameninţărilor teroriste derivate din spaţiul cibernetic rezidă nu în colectarea online a informaţiilor, ci în prelucrarea şi transformarea acestor informaţii în cunoaştere şi acţiune, prin identificarea unor răspunsuri practice, inclusiv din sfera IT&C, la întrebările:

- Care date şi informaţii sunt cu adevărat relevante?
- Care este modul optim de analiză şi transformare a datelor relevante într-un produs de intelligence valoros?

BIBLIOGRAFIE:

1. COMAN Daniela, „*Comunicarea în cadrul proceselor specifice fenomenului terorist"*, Bucureşti, SNSPA, 2007;
2. DELCEA Cristian, „*Psihologia terorismului: studiu psihologic asupra teroriştilor",* Cluj-Napoca, Editura Albastră, 2004;
3. http://tempsreel.nouvelobs.com/charlie-hebdo/20150114.OBS9988/info-obs-les-cliches-pedophiles-une-couverture-pour-coulibaly-et-kouachi.html;
4. http://www.huffingtonpost.co.uk/david-churchill/radical-islam_b_6115138.html;
5. http://www.ibtimes.co.uk/when-isis-jihadists-return-home-how-de-radicalise-islamic-extremists-1474905;
6. http://www.independent.co.uk/voices/comment/isis-in-the-uk-how-the-war-on-terror-radicalised-a-generation-9813362.html;
7. http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/01/28/the-islamic-states-model;
8. KAPLAN, Eben, „*Terrorists and the Internet",* Council on Foreign Relations, mai 2004, accesat în 15 martie 2015 la http://www.cfr.org/publication/10005;
9. POPP Robert, ARMOUR Thomas, SENATOR Ted, NUMRYCH Kristen, „*Countering terrorism trough information tehnology, Comunications of the ACM*",

vol. 47, no. 3, Minneapolis, 2004;
10. RESNYANSKY Lucy, „*The role of technoloy în intelligence practice: linking the developer and the user perspectives*", Prometheus, Sydney, 2010;
11. TRAN, Vasile, „*Teoria Comunicării",* Bucureşti, Editura comunicare.ro, 2002.
12. WEIMANN, Gabriel, *www.terror.net: „How Modern Terrorism Uses the Internet"*, United States Institute of Peace, martie 2004. http://www.usip.org/pubs/specialreports/sr116.html accesat in 15 martie 2015.

MONITORIZAREA ŞI CONTROLUL SISTEMELOR INFORMATICE ÎN SCOPUL PREVENIRII UTILIZĂRII IMPROPRII ŞI A ATACURILOR DIN INTERIORUL ORGANIZAŢIEI

Dan FOSTEA
Maior inginer, Cercetător Ştiinţific gr. III, doctorand, Agenţia de Cercetare pentru Tehnică şi Tehnologii Militare, Bucureşti, Romania, e-mail: dfostea@acttm.ro

Ştefan-Ciprian ARSENI
Locotenent inginer, Asistent de cercetare, doctorand, Agenţia de Cercetare pentru Tehnică şi Tehnologii Militare, Bucureşti, Romania, e-mail: sarseni@acttm.ro

Bebe-Răducu IONAŞCU*
Căpitan inginer, Cercetător Ştiinţific gr. III, Agenţia de Cercetare pentru Tehnică şi Tehnologii Militare, Bucureşti, Romania, e-mail: bionascu@acttm.ro

Rezumat: *De-a lungul timpului informaţia şi-a demonstrat rolul vital în organizaţiile civile, dar mai ales în cele militare. Urmărind evoluţia rapidă a tehnologiei informaţiei, forţele armate au integrat reţele informatice în diferitele nivele ierarhice, începând de la nivel batalion sau echivalent. În general, aceste reţele sunt protejate prin separare fizică la atacuri din exterior, însă rămâne problematică utilizarea improprie a acestora, intenţionată sau nu, din interior.În vederea reducerii riscului menţionat sau cel puţin a unei monitorizări stricte există o serie de soluţii informatice transparente pentru utilizatorii legitimi, dar care asigură integritatea reţelei. Monitorizarea unui sistem informatic poate fi realizată prin integrarea şi interogarea unor anumiţi parametri în cadrul acelui sistem, care să permită semnalarea apariţiei unor modificări ale elementului software. Pentru asigurarea controlului transferului documentelor, şi nu numai, folosind medii de stocare amovibile, poate fi implementată o soluţie software, care poate reduce considerabil riscul apariţiei unor breşe de securitate.*

Cuvinte cheie: *securitatea informaţiei, securitatea reţelelor, monitorizarea calculatoarelor, controlul transferurilor*

Introducere

Cea mai des răspândită şi cunoscută formă de securizare a transferurilor de informaţii, atât în mediul public şi privat, cât şi în cel militar, este cea dintre diferite reţele, militară sau de altă natură, sau dintre utilizatorii externi şi diferite tipuri de reţele. Păstrând nivelul descrierii la caracter militar, putem discuta despre schimburile de informaţii ce au loc între diferitele categorii ale propriilor forţe sau între forţele proprii şi cele aliate. În timp ce securizarea informaţiilor este o cerinţă cheie pentru asigurarea unei conexiuni sigure între persoane şi dispozitivele lor, o altă problematică de securitate a devenit o adevărată tendinţă în ultimii ani, şi anume atacurile/ameninţările interne.

Preocupate, în special, faţă de atacurile externe ale unor hackeri sau terorişti cibernetici, organizaţiile, militare sau civile, şi-au direcţionat atenţia în securizarea mai ales a acestei zone de risc, neacordând suficientă atenţie posibilelor ameninţări ce pot să apară din

* Cpt. ing. Bebe-Răducu IONAŞCU, Cercetător Ştiinţific gr. III, Agenţia de Cercetare pentru Tehnică şi Tehnologii Militare, Bucureşti, Romania. E-mail: bionascu@acttm.ro

interiorul organizaţiei, cel mai probabil cauzate de un angajat revoltat. Cu toate acestea, acest tip de ameninţare internă poate avea un impact mai amplu şi poate cauza pagube la o scară mai mare decât un tip normal de atac extern, fiind, în acelaşi timp, mai dificil de detectat.

Pentru a depăşi aceste situaţii administratorii de securitate pot implementa diferite politici de securitate care vor restricţiona şi vor încerca să controleze zonele de acces ale unui utilizator obişnuit. Cu toate acestea, o politică de securitate severă va tinde să restricţioneze excesiv performanţele unui sistem de calcul şi beneficiile aduse de lucrul cu acesta, existând posibilitatea de a irita şi utilizatorul. Însă, problemele apar în momentul în care discutăm despre utilizatorii privilegiaţi, persoane care nu sunt obligate să se conformeze acestor politici riguroase. În acest caz, posibilităţile existente pentru integrarea măsurilor de securitate sunt aplicaţiile software specializate, care pot monitoriza activităţile utilizatorilor şi pot controla modul în care aceştia executa transferurile de informaţii în şi din sistem.

1. Analiza problematicilor de securitate

După cum este descris în "An Introduction to Computer Security: The NIST Handbook", NIST (National Institute of Standards and Technology) menţionează opt elemente principale pe care o abordare geneală în domeniul securităţii ar trebui să bazată. Printre aceste opt elemente, următoarele pot fi considerate prioritare în momentul proiectării şi implementării unei arhitecturi de securitate în interiorul unei organizaţii militare:

- Continuarea misiunii organizaţiei trebuie susţinută prin măsurile şi politicile de securitate implementate;
- Factorul decizional trebuie să considere componenta de securitate drept un element integrat în structura organizaţiei;
- Politicile de securitate trebuie să ia în considerare constrângerile impuse de factorii sociali, aşadar este nevoie de reevaluarea periodică a acestora;
- În vederea asigurării unui grad ridicat de încredere în procedurile de securitate ale organizaţiei, acestea vor fi abordate într-o manieră integrată şi comprehensivă.

În calitate de personal militar, trebuie să luăm în considerare problematica apariţiei unei breşe în cadrul reţelei, a comunicaţiilor integrate sau a sistemelor informatice, din punct de vedere operaţional. Aceastea fiind spuse, problematicile prezentate pot fi generalizate pentru orice categorie de reţea considerată esenţială pentru capabilităţile funcţionale şi operaţionale ale unei anumite entităţi.

În prezent, un centru de comandă al unui batalion a devenit aglomerat, nu doar datorită numeroaselor echipamente necesare conducerii trupelor, ci şi datorită numărului crescut al operatorilor (Figura 1).

Figura 1. Centrul de comandă Lejeune al corpului de puşcaşi marini[1]

[1] Centrul de comandă LEJEUNE al corpului de puşcaşi marini, N.C. – Puşcaşi marini ai Batalionului 2 de Informaţii (fotografie a Lance Cpl. Joshua Brown), în http://www.iimef.marines.mil/Photos/tabid/131/igphoto/2000709438/Default.aspx, accesat la data de 28.03.2015

Principala problemă ce apare este controlul acestor persoane, în timp ce este asigurat un nivel superior de eficienţă al comenzii. Ca o cerinţă a colaborării perfecte dintre naţiuni, reţeaua naţională de informaţii a fiecărui stat trebuie interconectată cu cele ale aliaţilor săi, aşadar existând posibilitatea de multiplicare a riscurilor unei posibile ameninţări care ar putea induce diferite tipuri de pagube semnificative. Însă, datorită îmbunătăţirilor continue în privinţa securizării interacţiunilor externe cu o reţea, riscul propagării erorilor de la sistemele de calcul „infectate" a fost diminuat.

Similare atacurilor externe, ameninţările interne pot fi identificate sub forma fraudelor sau furturilor de date, a sabotajelor efectuate de angajaţi sau a unor aplicaţii software maliţioase introduse în reţea de către angajaţi. Ca urmare a familiarizării personalului cu sistemele pe care, în cel mai rău scenariu, au acces nelimitat, utilizatorii autentificaţi se găsesc în poziţia de a avea posibilitatea comiterii unor infracţiuni. În timp ce, chiar şi în cadrul unei reţele cu un nivel minim de securitate, utilizatorii au nevoie de anumite privilegii pentru a executa o acţiune, întreaga lor activitate nu este constrânsă total, prin urmare, indiferent dacă sunt utilizatori obişnuiţi sau membri ai echipelor tehnice, toţi pot reprezenta o ameninţare.

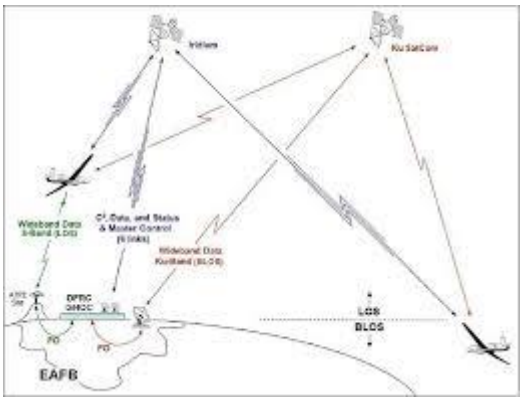


Figura 2. Arhitectura de comunicaţii globale HAWK[2]

În cazul în care discutăm despre sisteme informaţionale şi de comunicaţii complexe, prezentat spre exemplu în Figura 2, problematicile descrise anterior se însumează, rezultând o situaţie dificil de contracarat. Sistemul global de comunicaţii, HAWK, reprezintă un exemplu perfect, deoarece interacţiunile existente nu sunt doar între utilizatorii reţelelor interne, care controlează zborul, ci şi cu beneficiarii, anume părţile ce accesează informaţiile, şi cu senzorii, care acţionează drept conexiuni la distanţă cu reţeaua[2].

2. Identificarea soluţiilor

După cum a fost menţionat în capitolul 2, atacurile interne pot fi executate în maniere diferite şi pot provoca diferite tipuri de pagube, atunci când au avut succes. În vederea contracarării acestor ameninţări sau, de asemenea, de prevedere a lor, administratorii de securitate trebuie să implementeze diferite politici sau măsuri care ar putea, atât limita, cât şi direcţiona activităţile utilizatorilor în timpul unei sesiuni de lucru.

O posibilă metodă de atenuare şi depăşirea a provocărilor impuse de asigurarea unui mediu de lucru securizat şi protejat în faţa unor atacuri din interior, o reprezintă implementarea unei soluţii de monitorizare a sistemelor informatice. Aceasta ar permite administratorilor de securitate şi angajatorilor să aibă o privire de ansamblu mai detaliată

[2] Global Hawk UAS (Unmanned Aerial System) al NASA, în https://directory.eoportal.org/web/eoportal/airborne-sensors/global-hawk, accesat la data de 28.03.2015

asupra activităţilor desfăşurate de angajaţi în timpul programului de lucru, în vederea permiterii detecţiei rapide a unei ameninţări, înainte ca organizaţia să poată fi afectată. De asemenea, pe baza acestor informaţii detaliate, primite sub forma unor rapoarte zilnice, săptămânale sau lunare, asupra activităţii şi comportamentului utilizatorilor, pot fi concepute planuri de acţiune rapidă şi de răspuns la incidente.

În funcţie de nivelul de acces pe care îl are un utilizator, monitorizarea activă a activităţii acelei persoane va asigura blocarea oricăror tranzacţii neautorizate ce ar putea fi efectuate de la staţia de lucru personală. Prin înregistrarea şi stocarea activităţilor considerate a fi de risc ridicat, ca indicatori ai unor posibile ameninţări, poate fi implementată o strategie eficientă şi practică, care să asigure protecţia sistemelor şi reţelei în faţa atacurilor utilizatorilor cu privilegii.

Capitolul 4 descrie, din punct de vedere tehnic, o posibilă implementare a unei soluţii de monitorizare a activităţii utilizatorilor, pe care administratorii o pot utiliza pentru a identifica, activ sau pasiv, utilizatorii înclinaţi către activităţi maliţioase sau a sistemelor de calcul care au putut fi infectate.

Majoritatea organizaţiilor au implementate sisteme şi măsuri de securitate ce pot împiedica atacurile din exterior precum antivirus, firewall, sisteme de detecţia intruziunilor, dar prea puţine măsuri care iau în calcul ameninţările provenite din interiorul companiei, de la angajatul obişnuit care poate scoate informaţii confidenţiale din companie pentru a le valorifica sau le poate pierde.

Fără a compromite beneficiile portabilităţii, securitatea poate fi asigurată în primul rând făcând datele din dispozitivele compromise inaccesibile utilizatorilor şi proceselor neautorizate. O abordare comună este criptarea datelor stocate, precum şi scanarea dispozitivele de programe malware cu ajutorul unui program antivirus, existând în acelaşi timp şi alte metode.

Capitolul 5 descrie posibilele riscuri ale utilizării unui dispozitiv de stocare în cadrul organizaţiei şi prezintă soluţiile principale pentru diminuarea acestora.

3. Monitorizarea unui sistem informatic

Luând în considerare metodele utilizate pentru implementarea unei arhitecturi de monitorizare a sistemelor, putem afirma că acestea sunt împărţite în trei categorii:

- *Monitorizarea pasivă* – sistemele sunt monitorizate doar la anumite intervale de timp sau în anumite momente, atunci când se consideră că este posibilă apariţia unei breşe de securitate;
- *Monitorizarea activă* – sistemele sunt monitorizate de-a lungul întregii periode de funcţionare, iar orice activitate a utilizatorilor este fie înregistrată local, fie transmisă prin reţea către un punct de comandă central;
- *Monitorizarea mixtă* (pasivă la nivel reţea + activă la nivel local) – sistemele sunt monitorizate local într-o manieră activă, prin înregistrarea activităţii utilizatorilor sau aplicaţiilor software, emiţând o alertă oricând un anumit prag este depăşit. Însă, administratorul, localizat în punctul de comandă central, poate efectua interogări ale stării sistemului în orice moment (această opţiune este considerată a fi componenta pasivă).

3.1. Monitorizarea pasivă

O soluţie de monitorizare pasivă a sistemelor informatice este o aplicaţie software care, în principal, permite administratorilor de securitate crearea unor imagini ale sistemului, în anumite momente, şi compararea acestora, evidenţiind orice modificare sau alterare de date ce ar fi putut fi efectuată în intervalul de timp dintre două asemenea imagini. Referitor la fluxul operaţional implicat de utilizarea unui asemenenea tip de aplicaţii, următoarele etape pot fi

considerate punctul de plecare în definirea unor proceduri operaţionale specifice, în funcţie de fiecare problematică de securitate căreia îi este direcţionată:

- *Identificarea* – identificarea sistemului ce urmează a fi investigat;
- *Achiziţia datelor* – crearea unei imagini a sistemului „curat", pentru a avea valori de referinţă;
- *Analiza şi/sau Recuperarea datelor* – în cazul în care sistemul este considerat a fi infectat, o nouă imagine va fi creată. Apoi, aceasta va fi comparată cu imaginea anterioară, astfel încât orice alterare a datelor să fie identificată. După acest moment, în cazul în care anumite importante au fost pierdute, se poate încerca restaurarea acestora pe baza imaginii anterioare.
- *Raportarea* – pe baza informaţiilor adunate în cadrul etapei de analiză, pot fi create rapoarte specifice, care, ulterior, pot fi prezentate şi utilizate ca date de referinţă pentru analizele următoare.

Ţinând cont de funcţionalităţile pe care o soluţie de monitorizare pasivă le poate furniza, aceasta ar putea fi utilizată şi pentru analiza performanţelor sistemelor. Preluate la intervale de timp regulate, imaginile pot fi utilizate pentru observarea nivelului de încărcare al resurselor sau prognozarea unor posibile probleme software sau hardware.

3.2. Monitorizarea activă

Spre deosebire de monitorizarea pasivă, cea activă necesită un nivel mai scăzut de interacţiune între administratorul de securitate şi sistemul monitorizat. De asemenea, permite monitorizarea continuă a activităţii unui utilizator sau a unei aplicaţii software, prin implementarea unei infrastructuri bazate pe agenţi. Aceşia sunt compuşi din elemente software car pot produse rezultate bazându-se pe istoricul activităţii utilizatorului sau a tiparelor pre-definite, emiţând o alertă în momentul identificării unei posibile ameninţări. Aceste alerte sunt concentrate într-un centru de comandă, de unde administratorul poate lua măsurile impuse de situaţia respectivă.

Plecând de la infrastructura bazată pe agenţi, soluţia de monitorizare activă poate fi compusă din:

- Agenţi care să filtreze datele fără a modifica fluxul informaţional al sistemului. În acest caz, un atacator ar putea avea suficient timp pentru a induce anumite pagube, dacă alerta nu va fi emisă în cel mai scurt timp.
- Agenţi care să filtreze datele şi să poată modifica fluxul informaţioal al sistemului. În acest caz, agenţii vor administra datele din interiorul sistemului, iar în momentul iniţierii unui atac, aceştia nu vor emite doar o alertă, ci vor permite administratorilor să anuleze orice modificare efectuată de atacator. Restaurarea datelor poate fi posibilă deoarce agentul înregistreză orice acţiune produsă atât asupra locaţiei unui fişier, cât şi asupra conţinutului acestuia.

3.3 Monitorizarea mixtă

Monitorizarea mixtă combină funcţionalităţile celor două tipuri de monitorizare prezentate anterior, pasivă şi activă, prin implementarea unei infrastructuri bazate pe agenţi, controlaţi dintr-un punct de comandă central. Principala diferenţă dintre monitorizarea mixtă şi cea activă este faptul că în cea mixtă, administratorul de securitate poate interoga oricând un agent, extrăgând orice tip de informaţii din sistemul ţintă, nefiind obligat să aştepte agentul să semnaleze producerea unui atac.

Această metodă de interogarea asigură, de asemenea, monitorizarea performanţelor sistemului, permiţând administratorilor să efectueze modificări asupra politicilor de securitate astfel încât acestea să nu interfereze cu activităţile utilizatorilor, ce ar putea avea un impact negativ asupra acestora.

În ultima perioadă, pentru implementarea soluţiilor de monitorizare activă şi mixtă au fost dezvoltaţi noi algoritmi de filtrare a datelor, pentru agenţi, inclusiv integrarea noţiunii de „reţea neuronală”, care ar putea asigura o rată de detecţie ami bună, precum şi adaptarea rapidă, în cazul unor tipuri noi de atacuri.

1. Monitorizarea şi Controlul transferurilor

Conform unor studii recente, în companii se utilizează un număr din ce în ce mai mare de dispozitive portabile precum laptop-uri, notebook-uri, dispozitive USB flash, telefoane mobile avansate şi alte dispozitive mobile.

Dispozitivele USB flash de exemplu reprezintă cea mai bună soluţie pentru persoanele care au nevoie să mute documente între calculatoare şi aproape fiecare utilizator deţine cel puţin un dispozitiv USB flash. Acestea au dimensiuni mici, fiind uşor de pierdut, precum şi datele conţinute.

Dispozitivele USB flash vin cu două mari provocări în ceea ce priveşte securitatea sistemelor informatice: scurgerea de informaţii compromiterea sistemului prin infectarea cu viruşi sau alte programe software maliţioase.

Scurgerile de informaţii

Scurgerile de informaţii reprezintă un fenomen în creştere cauzat în primul rând de angajaţii care au acces la informaţii clasificate cu ajutorul unui număr din ce în ce mai mare de dispozitive capabile să multiplice sau să stocheze date digitale precum USB flash, telefoane mobile şi chiar camere foto.

Dispozitivele USB flash au o capacitate de stocare mare în comparaţie cu dimensiunile mici şi costurile scăzute, aceasta ducând la ameninţări serioase la adresa confidenţialităţii şi integrităţii informaţiei în cazul utilizării acestora pentru stocarea datelor fără măsuri de securitate adecvate. Pentru reducerea riscurilor unor breşe de securitate şi pentru securizarea dispozitivelor USB flash ar trebui luaţi în considerare următorii factori:

- *Stocare:* Dispozitivele USB flash pot fi depozitate în orice loc, precum portofele sau buzunarele hainelor, sau pot fi lăsate în calculatoare nesupravegheate, fiind greu de urmărit din punct de vedere fizic.
- *Utilizare:* o provocare semnificativă o reprezintă şi urmărirea datelor sensibile stocate pe dispozitivele flash personale care sunt mici şi în continuă mişcare. În timp ce multe companii au politici stricte de management al dispozitivelor de stocare portabile, unele chiar restricţionându-le în totalitate pentru minimizarea riscurilor, alte companii par să nu fie la curent cu riscurile de securitate aduse de utilizarea acestor dispozitive.

Infecţii malware

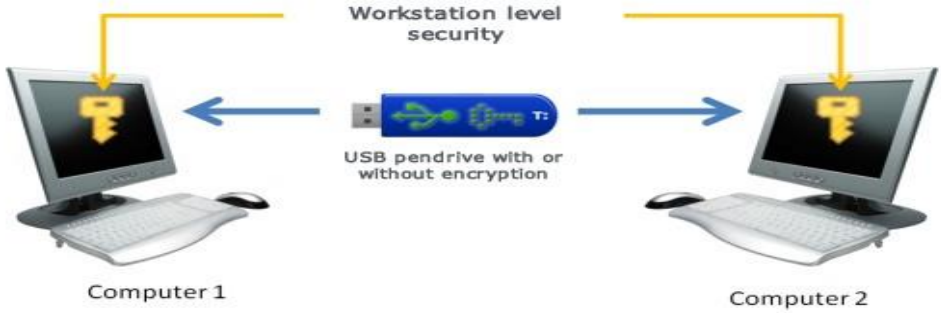
La începuturile viruşilor şi a programelor maliţioase de calculator principalul mijloc de transmitere a fost discul floppy. Acum, dispozitivele USB flash au acelaşi rol, fiind principala formă de infecţie a sistemelor informatice. Când un virus sau un malware ajunge pe un dispozitiv USB flash, poate infecta toate dispozitivele la care se conectează.

În anul 2011, un studiu Microsoft ce a analizat date de la peste 600 milioane de sisteme informatice din lume, a documentat răspândirea infectării cu viruşi şi programe malware prin intermediul dispozitivelor USB. Conform studiului, 26% din toate infecţiile sistemelor Windows au provenit prin exploatarea funcţionalităţii AutoRun din Microsoft Windows. Aceste concluzii sunt în concordanţă cu alte studii efectuate de către compania ESET, precum

raportările lunare ale celor mai comune programe malware detectate, care listează abuzul fişierului autorun.inf primul în top 10 ameninţări în 2011.

Fişierul Windows *autorun.inf* conţine de obicei informaţii despre programele programate să ruleze automat când dispozitivele portabile (USB flash sau dispozitive similare) sunt accesate de către utilizator. Setarea standard a *AutoRun* în toate versiunile Windows înainte de Windows 7 este să se execute automat orice program regăsit în fişierul *autorun.inf*. Acesta nefiind tot timpul primul mecanism de distribuire, autorii programelor malware proiectează tehnice de infectare adiţionale.

Soluţii



Având în vedere riscurile prezentate, securitatea transferului de date devine vitală. Aceasta se poate realiza atât la nivelul staţiilor de lucru, prin monitorizarea în timp real a porturilor fizice şi prin controlul (restricţionarea sau aprobarea) transferului documentelor folosind medii de stocare amovibile, cât şi la nivelul dispozitivelor, prin criptarea conţinutului, sau prin restricţionarea drepturilor de citire/scriere.

Criptarea Software

Criptarea automată şi transparentă a conţinutului unui dispozitiv USB poate fi efectuată cu soluţii software precum dm-crypt, FreeOTFE, Data Protecto and TrueCrypt. Ediţiile Windows 7 Enterprise şi Ultimate, Windows 8 şi 8.1, precum şi Windows Server 2008, 2012 asigură o soluţie de criptare folosind BitLocker. Pentru calculatoarele Apple, sistemul de operare Mac OS X a oferit software pentru criptarea discurilor de date încă din 2008, de la apariţia sistemului de operare Mac OS X Panther[3].

Pentru prevenirea accesului la fişiere în cazul pierderii sau furtului, pe dispozitivele de stocare portabile se pot instala programe software adiţionale.

Criptarea Hardware

Unii producători proiectează dispozitive USB criptate hardware cu microcip-uri ce oferă criptare automată şi transparentă. Unele dintre aceste dispozitive necesită, pentru acces la conţinut, introducerea unui cod cu ajutorul unei mici tastaturi pe dispozitiv[4].

[3] "How to create a password-protected (encrypted) disk image in Mac OS X 10.3 or later", în https://support.apple.com/en-us/HT201599, accesat la data de 26.03.2015

[4] "Toshiba Announces Encrypted USB Flash Drive", în http://www.toshiba.com/us/press-release/101244, accesat la data de 26.03.2015

Monitorizarea porturilor fizice

Instalarea unor soluţii software de securitate adiţionale în calculatoarele companiei, poate ajuta la urmărirea şi diminuarea riscurilor de infecţie şi scurgerile de informaţii.

Asemenea aplicaţii pot monitoriza în timp real toate evenimentele asociate porturilor fizice şi, utilizând liste albe sau negre, pot aproba sau restricţiona dispozitivele externe inserate în sistem, conform cu politicile de securitate ale companiei referitoare la informaţiile clasificate şi nivelul de clasificare la care are acces utilizatorul ce introduce un astfel de dispozitiv.

Concluzii

După cum a fost prezentat în cadrul articolului, există multe variante de implementare a unor strategii de protecţie a datelor unei persoane, însă elementul cheie este găsirea unei modalităţi de a realiza aceste implementări astfel încât utilizatorii să poată beneficia în totalitate de performanţele noilor tehnologii.

Monitorizarea şi controlul sistemelor informatice sunt activităţi importante, însă nu trebuie omis obiectivul introducerii utilizării sistemelor informatice în sistemele militare, acelaşi ca în sistemel publice, şi anume de a facilita execuţia unor activităţi.

BIBLIOGRAFIE:

1. D. Dasgupta, F. Gonzalez, K. Yallapu, J. Gomez, R. Yarramsettii, "CIDS: An agent-based intrusion detection system", Computers & Security, Elsevier, 2005
2. N. Kussul, S. Skakun, "Neural network approach for user activity monitoring in computer networks", Proceedings of the 2004 Joint Conference on Neural Networks, 2004
3. T.F. Lunt, "Detecting Intruders in Computer Systems", Proceedings of Auditing and Computer Technology Conference, 1993
4. V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time", Proceeding of the 7th USENIX Security Symposium, 1998
5. D. Spinellis, "User-level operating system transactions", Software: Practice & Experience, Wiley, 2009
6. Eset Global Threat Report, December 2011
7. „Secure USB flash drives", European Union Agency for Network and Information Security, 1 iunie 2008, ISBN 978-92-9204-011-6
8. Microsoft Security Intelligence Report Volume 11, Ianuarie-Iunie, 2011
9. "An Introduction to Computer Security: The NIST Handbook", Special publication 800-12, NIST, 1995

COMPUTINGUL AFECTIV – COMPONENTĂ A WEB 3.0

Cosmin Dragoş DUGAN

Doctorand Academia Naţională de Informaţii "MIHAI VITEAZUL", Bucureşti, Romania,
dugcosmin@yahoo.com

Rezumat: *Elementele de computing afectiv vor reprezenta o trăsătură definitorie a Web 3.0, în paralel cu intensificarea şi diversificarea modalităţilor de a interacţiona cu utilizatorul. Componenta cyber-afectivă va permite o centrare a conţinutului axată pe nevoile şi dorinţele consumatorului, facilitând modificarea continutului emotional cu scopul de a pune in evidenta aspecte ale fondului cognitiv. Pentru organizaţiile de intelligence computingul afectiv reprezintă o dimensiune suplimentară (şi complementară) destinată culegerii de informaţii şi identificarii cu o precizie sporita a intenţiilor. Posibilitatea de a modifica anvelopa emoţională atasata unui conţinut cognitiv oferă noi grade de libertate în cadrul operaţiunilor de influenţare a opiniei publice, componente ale conflictului de generaţia a V-a (războiul neocortical). Lucrarea de faţă îşi propune să prezinte şi să detalieze conceptul de computing afectiv, instrumentele de lucru (actuale şi viitoare) precum şi potenţialele aplicaţii în cadrul: OSINT, identificării biometrice online, rezilienţei şi ingineriei sociale, cu relevanţă în domeniul intelligence.*

Cuvinte cheie: *computing afectiv, biometrie, OSINT, razboi neocortical, propaganda, inginerie sociala*

Introducere

În societatea contemporană, accesul la informaţie a devenit tot mai facil, datorită dezvoltării şi utilizării în masă a tehnologiilor de comunicare şi transfer a datelor. Cu toate acestea, accesul la informaţie nu a însemnat automat şi obţinerea unui grad crescut de cunoaştere şi nu a determinat utilizarea informaţiilor doar în scopuri constructive sau cel puţin paşnice[1]. După emoţia iniţială, pe fondul primului deceniu al epocii post-bipolare, internetul a ajuns să devină o componentă importantă, apoi indispensabilă, a activităţii cetăţeanului conectat tot mai mult la demersul globalist. Aproape că nu există o activitate umană care să nu fie reflectată în cadrul internetului, comportamentul utilizatorilor reprezentând şi principalul factor cauzal responsabil de conţinutul, schimbările şi evoluţia acestuia. Considerat un mediu de expresie mai permisiv, uşor accesibil, care oferă accesul la o potenţială audienţă globală, internetul a devenit canalul ideal pentru comunicatori şi propagarea de mesaje – de la reclame publicitare, campanii umanitare, ştiri sau ideologii politice, mai mult sau mai puţin benigne. Cu toate că atât dimensiunea cât şi impactul social al comunicării via internet au fost iniţial recunoscute, analiza evenimentelor din ultimul sfert de secol demonstrează cât de mult a fost subestimată dimensiunea afectivă rezultată din conexarea unei audienţe la nivel global.

Apariţia şi dezvoltarea reţelelor sociale a permis studiul dimensiunii emoţionale a comunicării în grupuri selectate care utilizează internetul, fapt care a favorizat dezvoltarea unor tehnici noi de marketing comercial şi politic, utilizate astăzi la scară largă. Devenit cel mai mare hub comercial la nivel global, internetul s-a dovedit la fel de eficient în distribuirea mesajelor de propagandă şi ideologice maligne, determinad apariţia şi dezvoltarea unor fenomene precum auto-radicalizarea şi radicalizarea online, devenite astfel resurse ale

[1] Irena Chiru-Dumitru, *Gândire critică pentru intelligence în era informaţională*, Sesiunea de Comunicări ANI, Bucureşti, 2012.

terorismului de inspiraţie islamistă[2]. Multiplele modalităţi prin care utilizarea internetului poate afecta securitatea naţională sau prin care elemente ale securităţii naţionale au devenit tot mai dependente de utilizarea mediului online au generat necesitatea dezvoltării unor instrumente specializate destinate monitorizării, culegerii şi prelucrării de informaţii din mediul online precum şi instrumente destinate securităţii cibernetice.

Astfel, accesul tot mai extins şi în timp real la informaţia obţinută din surse deschise (OSINT – open source intelligence) a generat o adevărată „revoluţie OSINT", cu impact asupra activităţii de intelligence şi politicilor de securitate naţională. Dezvoltarea continuă a serviciilor oferite utilizatorilor via internet, a modalităţilor de interacţiune om-computer şi creşterea gradului de conectare la nivel global, precum şi dinamica actuală a mediului de securitate a determinat ca produsele OSINT să fie centrate în jurul conceptelor de alertă, avertizare timpurie şi avertizare strategică.

1. Computingul afectiv – etapa urmatoare a analizei sentimentelor exprimate in mediul online

Analiza conţinutului generat de utilizator (activităţi ale utilizatorului care sunt stocate de provideri – accesarea de saituri, achiziţii via internet, comentarii pe bloguri, în cadrul reţelelor sociale) a cunoscut o dezvoltare puternică în ultimul deceniu, permiţând (în cazurile ideale) identificarea utilizatorilor anonimi, analiza intenţiilor şi gradul de risc pentru siguranţa naţională. Deşi există o serie de dificultăţi, precum cantitatea mare de date nestructurate din surse multiple care necesită o procesare automată, dificultatea contextualizării, fuziunea automată a datelor multicanal, domeniul se află într-un proces de dezvoltare accelerată.

În particular, dorim să ne referim la tehnicile implicate în identificarea şi modelarea semnaturii afective individuale şi colective, pornind de la analiza conţinutului generat de utilizator. În prezent, cea mai utilizată tehnică este cea a analizei semantice a conţinutului online, care realizează o analiză automată a limbajului natural cu scopul de a identifica şi extrage informaţii cu caracter subiectiv din materialele analizate. Rezultatele constau în identificarea stării afective a autorului (exprimată sub forma emoţiilor, atitudinilor sau opiniilor) la redactarea textului precum şi a intensităţii emoţionale şi a tipului de emoţii pe care autorul doreşte să le împartă cu audienţa.

Limitările metodei sunt totuşi evidente – accesarea emoţiilor utilizând doar un singur canal (cel al limbajului scris), posibilitatea de fraudare din partea sursei, dificultăţile de traducere şi adaptare în cazul textelor multilingvistice sau multiculturale, dificultăţile de contextualizare, etc. În fapt, tocmai aceste limite au stimulat cercetarea unor modalităţi suplimentare destinate identificării statusului afectiv al unei surse de interes.

O arie de interes conexă, bazată tot pe prelucrarea datelor generate de utilizator, este cea a identificării biometrice online. Justificăm o astfel de abordare comună în cadrul acestei lucrări şi prin faptul că pe măsură ce metodele de analiză furnizează rezultate tot mai complexe, acestea permit elaborarea unor tipare de comportament care pot fi utilizate pentru identificarea sursei (personalitatea online – cyberprofilul afectiv). Demersul coroborat oferă un grad crescut de identificare a autorului sau autorilor, evaluarea intenţiilor şi a gradului de risc.

1. Într-o primă etapă s-a avut în vedere *diversificarea canalelor* destinate achiziţiei de date nesistematizate care pot fi utilizate în determinarea stării afective a sursei:

- *Comunicarea verbală* permite realizarea unei analize psiholingvistice a discursului şi identificarea unor particularităţi ale limbajului vorbit care permit identificarea autorului. Textul conversaţiilor verbale, rezultat din transcrierea automată cu ajutorul unor programe

[2] Cristian Barna, *Jihad în Europa – ameninţarea teroristă de "franciză Al-Quaida"*, Revista Intelligence martie 2011, pp. 14-18, accesibilă online la adresa http://www.sri.ro/fisiere/ publicatii/intelligencemartie2011.pdf.

specializate (exemplu softuri comercializate de către compania Sail Labs), este analizat din punct de vedere semantic utilizând instrumentele specifice analizei sentimentelor. Se încearcă astfel identificarea pasajelor din text care sunt puternic impregnate afectiv dar şi a momentelor tensionale, dramatice, care anticipează sau solicită o participare afectivă intensă din partea auditoriului[3] sau din contră, afirmaţiile vagi, aluzive (care pot fi clasificate greşit de un sistem clasic de analiză automată)[4]. În paralel este analizată şi prozodia (dimensiunea auditiv-vocală a comunicării verbale) – care oferă informaţii despre variabilitatea lingvistică a vocii înalte sau joase (intonaţia), ritmul (inclusiv pauzele) şi viteza vorbirii, ezitările (fluenţa)[5]. Softuri specializate permit apoi identificarea unor trăsături care prezintă interes pentru beneficiar – identificarea unor intenţii (ex. iminenţa unei acţiuni violente, propagarea de mesaje ideologice), aspecte ale personalităţii (potenţiale tulburări psihotice, PTSD, autism înalt funcţional, deficit cognitiv, etc)[6].

- *Limbajul non-verbal* se referă la identificarea şi procesarea imaginilor care conţin date despre expresii şi atitudini care exprimă o stare afectivă (decelabilă şi cunatificabilă), precum şi modul de exprimare a acestora şi evoluţia temporală (frecvenţă, durată, momentul declanşării).

Importanţa sa se datorează faptului că în medie, conţinuturile afectiv-atitudinale se transmit în proporţie de 55% nonverbal, 38% paraverbal şi doar 7% verbal, astfel, un mesaj verbal neînsoţit de component nonverbală şi paraverbală, va fi mai greu de decodificat. Studiul sistematic al faptelor gestuale reprezintă domeniul de interes al kineticii, care destructurează semnele comportamentale în cele mai mici unităţi de acţiune ale gestului sau mimicii (kineme), urmând să fie analizate şi integrate într-un context psihologic, social şi cultural.

Domeniul de cercetare este extrem de vast, fiind necesară o abordare diferenţiată.

- Expresiile mimico-faciale pot fi recunoscute cu ajutorul softurilor specializate, permiţând realizarea unei librarii individualizate de expresii şi ipostaze afective, pornind de la imagini sau capturi video (reţele de socializare)[7]. De interes deosebit este coroborarea analizei expresiilor faciale şi mişcărilor oculare cu cea a limbajului, având în vedere influenţele culturale care au tendinţa să codifice discursul, în contrast cu cvasi-universalitatea expresiilor mimico-faciale afective[8].

- Mişcările oculare şi pupilometria reprezintă un domeniu intens studiat, permiţând evaluarea atât a stării emoţionale dar şi evidenţierea unor particularităţi fiziologice şi patologice. Modificările dimensiunii, egalităţii sau reactivităţii pupilare în diverse condiţii (controlate sau care pot fi evaluate) permit evaluarea cu mare precizie a statusului emoţional,

---

[3] Brian O'Neel, , Mark Riedl, *Toward a Computational Framework of Suspense and Dramatic Arc*, pp. 246-256, in Sydney D'Mello, Arthur Graesser, Bjorn Schuller, *Affective Computing and Intelligent Interaction,* 4th International Conference, ACII 2011, oct. 2011, Ed. Springer-Verlag, SUA, 2011.

[4] Jeroen Dral, Dirk Heylen, Rieks op den Akker, *Detecting Uncertainty in Spoken Dialogues: An Exploratory Research for the Automatic Detection of Speaker Uncertainty by Using Prosodic Markers, in* Khurshid Ahmad (editor), *Affective Computing and Sentiment Analysis Emotion, Metaphor and Terminology,* Ed. Springer-Verlag, SUA, 2011.

[5] Thurid Vogt, Elisabeth Andre, Johannes Wagner, Automatic *Recognition of Emotions from Speech: A Review of the Literature and Recommendations for Practical Realisation,* pp. 74-92, în Russel Beale, Christian Peter, *Affect and Emotion in Human-Computer Interaction, From Theory to Application*, SUA, Ed. Springer-Verlag, 2008.

[6] Demetrios Sapounas, Vadim Kagan , Edward Rossini, *Sentiment Analysis for PTSD Signals,* Ed. Springer-Verlag, SUA, 2013, pag. 9, 30-32.

[7] Jiebo Luo, Quanzeng You, Hailin Jin, Jianchao Yang, *Robust Image Sentiment Analysis Using Progressively Trained and Domain Transferred Deep Networks*, 29th AAAI Conference on Artificial Intelligence in Austin, Texas, ian. 25-30/2015 , accesibil online la adresa http://www.cs.rochester.edu/u/qyou/papers/sentiment_analysis_final.pdf.

[8] Xiaozhou Wei, Johnny Loi, Lijun Yin, *Classifying Facial Expressions Based on Topo-Feature Representation,* pp. 69-83, în Jimmy Or, *Affective Computing Focus on Emotion Expression, Synthesis and Recognition*, Ed. I-TECH Education and Publishing, Vienna, 2008.

deoarece reacţiile oculare sunt involuntare şi prezintă un grad crescut de expresivitate. În practica medicală există pupilometre electronice care pot realiza o întreagă baterie de teste destinate evaluării reactivităţii spontane sau provocate ale pupilei, teste care pot fi adaptate metodei de achiziţie a imaginilor (surse video) şi scopului[9].

- Modificări ale posturii, atitudinii şi gesticii pot fi identificate din fişierele video şi ulterior interpretate cu ajutorul unor softuri dedicate. Utilizând chiar şi un număr redus de date se pot obţine informaţii despre tipul de personalitate al sursei[10], în timp ce utilizarea unor înregistrări seriate permite realizarea unor evaluări de înaltă calitate. De exemplu, prelucrarea computerizată a imaginilor video care îl redau pe Hitler în diverse acţiuni (în special în discursuri publice) a condus la concluzia că ar fi suferit în ultima perioadă a vieţii de boala Parkinson[11]. O analiză multidimensională realizată în anul 2008, care a inclus şi analiza automată a gesturilor, afirma că Vladimir Putin ar putea suferi de o tulburare neurodevelopmentală de tip autistic (sindromul Asperger)[12].

- Muzica, sunetele ritmice, alertele auditive pot avea un impact major asupra stării afective a auditoriului (componenta psihoacustică). De exemplu, înregistrările video realizate de grupările jihadiste prezintă frecvent un fond muzical care este coroborat cu mesajul, cu scopul de a-i potenţa impactul afectiv, reprezentând în acelaşi timp şi un puternic simbol identitar cultural (optimizare emoţională)[13].

- *Biosemnalele* reprezintă semnale din spectrul electromagnetic (electrice, magnetice, termice) emise de corpul uman ca urmare a activităţii electrochimice a celulelor. Biosemnalele suferă modificări decelabile în funcţie de starea subiectului (sănătate sau boală, status afectiv, modificări neuroendocrine) şi permit evaluarea specifică a sistemelor biologice investigate.

Experimental se încearcă procesarea datelor obţinute prin monitorizarea frecvenţei cardiace şi respiratorii, electrocardiogramei uni- şi multicanal, electroencefalogramei, fonocardiogramei, activităţii electrice a tegumentului (activitatea electrodermică), electromiograma la nivelul unor muşchi implicaţi în expresiile mimico-faciale (orbicular al gurii, rizorius, zigomatic), modificări discrete ale temperaturii faciale, etc. Avantajul constă în faptul că reprezintă indicatori involuntari ai stării afective, permiţând discriminarea dintre reacţiile controlate şi cele naturale.

Semnalele biologice obţinute prin ECG şi EEG sunt cele mai frecvent utilizate şi prezintă o specficitate înaltă. În ultimii ani s-au dezvoltat mijloace neinvazive de culegere a semnalului („uscate" sau chair „touchless"), care simplifică obţinerea de date. În mod particular, interfeţele creier-computer au cunoscut o dezvoltare semnificativă, existând un interes crescut de dezvoltare a acestui domeniu[14].

Iniţial achiziţia de semnale biologice a fost realizată experimental, în condiţii controlate, ulterior fiind aplicată în cadrul studiilor de neuromarketing sau marketing politic. Rezultatele consistente depind de bună achiziţie a semnalelor pe o perioadă relativ

---

[9] Andrew Duchowski, *Eye Tracking Methodology Theory and Practice*, Ed. Springer-Verlag, SUA, 2007 .

[10] Markus Koppensteiner *Motion cues that make an impression: Predicting perceived personality by minimal motion information* , Journal of Experimental Social Psychology Volume 49, Issue 6, November 2013, pp. 1137–1143 accesibil online la adresa http://www.sciencedirect.com/ science/article/pii/S0022103113001467.

[11] Neil Midgley, *New technology catches Hitler off guard, The Telegraph*, 22 nov 2006, accesibil online la adresa http://www.telegraph.co.uk/news/uknews/1534830/New-technology-catches-Hitler-off-guard.html

[12] Brenda Connors, *A Technical Report on the Nature of movement pattening*, the brain and decision-making, 2008, accesibil online la adresa http://www.naegele.com/documents/200report.pdf.

[13] Ana Tajadura-Jiménez, Daniel Västfjäll, *Auditory-Induced Emotion: A Neglected Channel for Communication in Human-Computer Interaction*, pp. 61 - 71 în Christian Peter, Russel Beale, *Affect and Emotion in Human-Computer Interaction*, Ed. Springer-Verlag, SUA, 2008.

[14] Christian Muhl, Egon L. van den Broek, Anne-Marie Brouwer, *Multi-modal Affect Induction for Affective Brain-Computer Interfaces*, pp. 235-245, în Sidney D'Mello, Arthur Graesser et all, *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011.

îndelungată, posibilitatea de a stabili un nivel bazal, cunoaşterea contextului care permite îndepărtarea artefactelor şi a reacţiilor nesemnificative. Procesul de achiziţie al biosemnalelor în timp real şi la distanţă, de la o ţintă anonimă, care adoptă un comportament de mascare a activităţii pe internet este încă dificil, însă nu imposibil. Astfel, biosemnalele pot fi achiziţionate cu ajutorul dispozitivelor utilizate în cadrul neuro-jocurilor (jocurilor afective care utilizează bio-feedbackul sau feedbackul afectiv – emotionally responsive computer games), jocurilor imersive sau a tehnologiilor purtabile utilizate în scopul monitorizării parametrilor fiziologici (extensii ale telefoanelor mobile, ceasuri sau brăţări inteligente, tatuaje electronice, microprocesoare implantabile – o piaţă aflată în continuă dezvoltare şi diversificare)[15]. O serie de semnale bioelectrice pot fi extrapolate sau achiziţionate indirect[16].

- *Datele relaţionale* se referă la mediul relaţional online, provenit din utilizarea reţelelor sociale sau cu care ţinta interacţionează în mod voluntar utilizând un canal de comunicare (cu valenţă afectivă). Prelucrarea specifică a acestor date oferă informaţii care ajută şi la conturarea profilului emoţional - de exemplu aspecte privind personalitatea, preferinţe personale - simpatii/ antipatii[17], orientarea sexuală[18], consumul de substanţe recreaţionale sau narcotice, etc. Sociologia computaţională a stărilor afective (Computational Affective Sociology[19]), ca subdomeniu specializat, îşi propune să dezvolte instrumente capabile să extragă informaţii relevante despre profilul afectiv al unui individ ca parte a unui grup şi modul în care un individ poate afecta statusul emoţional al unei reţele sociale.

- *Date biometrice* pot fi obţinute utilizând unul sau mai multe canale de comunicare via internet. În general se referă la elemente anatomice, fiziologice sau comportamentale foarte greu de duplicat sau falsificat care pot fi obţinute prin prelucrarea datelor achiziţionate[20].

- Amprentele digitale pot fi reproduse pornind de la fotografii de înaltă rezoluţie care permit generarea unei imagini complete a amprentei şi ulterior duplicarea acesteia[21]. Recent, un haker german – Jan Krissler („Starbug") a utilizat această tehnică pentru a obţine o amprentă digitală a ministrului german al Apărării – Ursula von der Layden[22].

- Desenul vascular (palmar, facial, retinian) poate fi obţinut cu ajutorul unor softuri specializate sau utilizând camere cu expunere specială[23].

- Aspectul irisului – necesită imagini de înaltă rezoluţie[24]

---

[15] William Sims Bainbridge, *Computational Affective Sociology*, pp. 23-35 în Russel Beale, Christian Peter, *Affect and Emotion in Human-Computer Interaction*, Ed. Springer-Verlag, SUA, 2008.

[16] Didem Gökçay, Gülsen Yildirim, *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives*, IGI Global, SUA, 2011, pp. 310-315.

[17] *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'*, The Huffington Post, 11.26.1013, accesibil online la adresa http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html.

[18] Carter Jernigan, Behram Mistree, *Gaydar: facebook friends expose sexual orientation*, First Monday, vol. 14, nr. 10, oct. 2009.

[19] Pentru date suplimentare se poate consulta saitul Asociatiei pentru dezvoltarea computingului afectiv la adresa http://emotion-research.net/.

[20] Omar Alzoubi, Md. Sazzad Hussain, Sidney D'Mello, Rafael A. Calvo**,** *Affective Modeling from Multichannel Physiology: Analysis of Day Differences*, pp. 4-14, în Sidney D'Mello, Arthur Graesser et all, *Affective Computing and Intelligent Interaction*, SUA, Ed. Springer-Verlag, 2011.

[21] Geppy Parziale, *Touchless Fingerprinting Technology*, pp. 31-38, în N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* SUA, Ed. Springer-Verlag, 2011.

[22] Alex Hern, *„Hacker fakes German minister's fingerprints using photos of her hands",* accesibil online la adresa http://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

[23] Masaki Watanabe, *Palm Vein Authentication*, pp. 8-14, în N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* SUA, Ed. Springer-Verlag, 2011.

[24] James R. Matey, David Ackerman, James Bergen, Michael Tinker, *Iris Recognition in less Constrained Enviroments*, pp. 110-117, în N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and*

- Recunoaşterea vocală reprezintă un domeniu de activitate intens cercetat, care permite realizarea de analize aprofundate asupra vocii umane.

- Dinamica buzelor (pronunţarea sunetelor, a cuvintelor, unele expresii mimico-faciale precum zâmbetul, râsul, dezgustul) – necesită multiple imagini seriate.

- Semnalele bioelectrice (EKG, EEG) – greu de falsificat, însă pot suferi modificări semnificative în funcţie de o serie de stări fiziologice sau patologice. Totuşi, în cazul unei monitorizări mai îndelungate, rezultatele sunt excelente.

- Comportamente rezultate din interacţiunea om-computer (recunoaştere comportamentală) – sunt rezultatul secundar al utilizării mediului online, însă constituie un tipar comportamental suficient de specific şi dificil de falsificat. O serie de comportamente în general involuntare rezultă din interacţia directă cu computerul – ritmul tastării (keystroke dynamics), presiunea cu care se apăsă un ecran cu cristale lichide, modul de mişcare al mouseului (mouse dynamics)[25]. Cele mai utilizate tipare comportamentale se referă la modul de utilizare al poştei electronice, stocarea datelor electronice, strategia utilizată în cadrul unor jocuri (de strategie, MMORPG, FPS, driving) etc. De exemplu, analiza contribuţiei unui participant la un joc poate fi utilă în generarea unui model statistic al aptitudinilor acestuia şi a posibilelor domenii în care profesează[26] sau în stabilirea rolului pe care şi-l asumă în cadrul unei ierarhii[27]. Tot în ultimii ani a fost propus ca marker comportamental memoria de scurtă durată, care ar putea fi extrapolată pornind de la analiza mişcărilor mouse-ului în situaţii care presupun rezolvarea unor activităţi complexe[28]. Perfecţionarea modelelor de recunoaştere comportamentală a permis elaborarea unor soluţii de securitate bazate pe aceste metode biometrice[29].

Cele mai bune rezultate sunt obţinute prin utilizarea simultană a mai multor metode, care să caracterizeze ţinta utilizând date achiziţionate şi prelucrate independent provenite de la mai multe canale[30]. Acestă fuziune a datelor permite realizarea unui număr foarte mare de combinaţii între diversele metode utilizate, oferind soluţii individualizate în funcţie de particularităţile obiectivului şi a canalelor de achiziţie accesibile[31].

Există mai multe metode prin care o sursă îşi poate minimiza „urma" biometrică online[32], inclusiv prin alterarea sau mascarea fizionomiei. De exemplu, versiuni mai avansate ale banalei cagule sunt măştile antisupraveghere[33] sau proiecţiile holografice faciale[34].

Systems, SUA, Ed. Springer-Verlag, 2011.

[25] Kenneth Revett, *Behavioral biometrics. A remote controll acces*, Editura Wiley, SUA, 2008, pp. 73-96.

[26] Gang Wang, Andrew Gallagher, Jiebo Luo, David Forsyth, *Recognizing Occupations Through Probabilistic Models: A Social View,* pp. 117-133, in Ming Shao, Yun Fu, *Human-Centered Social Media Analytics*, Ed. Springer-Verlag, SUA, 2014.

[27] Benedikt Fuchs, Didier Sornette, Stefan Thurner, *How Virtual Gaming Worlds Are Revealing the Nature of Human Hierarchies Emerging Technology*, în arXiv, 19.03.2014 accesibil online la adresa http://www.technologyreview.com /view/525696/how-virtual-gaming-worlds-are-revealing-the-nature-of-human-hierarchies/?utm_campaign=socialsync&utm _medium=social-post&utm _source=facebook.

[28] Roman V. Yampolskiy, *Behavioral, Cognitive and Virtual Biometrics*, în Albert Ali Salah, *Computer Analysis of Human Behavior*, Ed. Springer-Verlag, SUA, 2011, pp. 355-368.

[29] Chorng-Shiuh Koong, Tzu-I Yang, Chien-Chao Tseng, *A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices,* The Scientific World Journal, Volume 2014 (2014), Article ID 781234, accesibil online la adresa http://www.hindawi.com/journals/tswj/2014/781234/.

[30] University of Calgary, *"Researchers advance biometric security"*, ScienceDaily, 21 iunie 2012, accesibil online la adresa http://ucalgary.ca/news/utoday/june19-2012/biometric.

[31] Md. Sazzad Hussain, *Hybrid Fusion Approach for Detecting Affects from Multichannel Physiology* in Sydney D'Mello, Arthur Graesser, Bjorn Schuller, *Affective Computing and Intelligent Interaction,* 4th International Conference, ACII 2011, oct. 2011, Ed. Springer-Verlag, SUA, 2011.

[32] Ann Cavoukian, Alex Stoianov, *Biometric Encryption: The New Breed of Untraceable Biometrics*, pp. 655-661, în Nikolaos V. Boulgouris (editor), *Biometrics Theory, Methods, and Applications*, Ed. Wiley, SUA, 2010.

[33] Vezi înregistrarea video la adresa http://www.urmesurveillance.com/urme-prosthetic/.

[34] Vezi înregistrarea video la adresa https://vimeo.com/103425574.

2. *Modelarea afectivă (uni-/multicanal)* – cuprinde două domenii de activitate: *simularea afectivă*, responsabilă de emularea reacţiilor afective compatibile cu cele umane, utilizate în cadrul roboticii sociale (roboţi umanoizi sau agenţi autonomi care interacţionează cu publicul) şi *decodarea afectivă*, al cărei scop este identificarea automată a emoţiilor umane prin procesarea semnalelor uni-/multicanal emise de o sursă. Decodarea stărilor afective se poate realiza utilizând semnalele furnizate de un singur canal (analiza vocii, pupilometrie, analiza automată a expresiilor mimico-faciale, etc) sau prin fuzionarea datelor prelucrate provenite de la două sau mai multe canale[35]. Prin acestă asociere gradul de identificare a emoţiilor poate atinge 80%-90% (2 canale sincrone) sau peste 90% (3 canale), în comparaţie cu o rată de 30-60% când sunt utilizate informaţiile provenite de la un singur canal de comunicare emoţională[36]. Rezultatul procesului de modelare afectivă este redat sub forma unui avatar al subiectului (artificial affective profile), care totuşi reprezintă doar un model grosier, limitat în timp, al profilului afectiv al sursei, o potenţială faţetă a personalităţii acesteia[37].

3. *Contextualizarea datelor şi emularea personalităţii online şi reale* presupune realizarea unui profil psihologic amplu, utilizând toate informaţiile (cognitive, afective, biometrice, relaţionale) care pot fi obţinute despre ţintă via internet. Sunt luate în calcul trăsături ale personalităţii (modul în care se raportează la normele sociale şi culturale, raportarea la sursele de autoritate, imaginea de sine şi respectul de sine, componentele prestigiului personal, evaluarea inteligenţei cognitive şi emoţionale), tiparele comportamentale (în special cele online – obiceiuri, comportamente stereotipe sau compulsive, atitudinea faţă de anumiţi stimuli – ştiri selectate, violente, cu tentă religioasă, stimuli-declanşatori), viaţa instinctuală (orarul de activitate şi odihnă, apetit alimentar şi sexual), aptitudinile şi capacităţile pe care le posedă (pregătire, domenii de interes şi excelenţă, aptitudinile tehnice şi informatice, interesul faţă de tehnologie – este interesat de nou sau mai degrabă conservator, etc). O atenţie specială se acordă mediului relaţional – virtual şi real – şi analizei conţinutului cognitiv şi afectiv al comunicării cu diverse noduri ale reţelei sociale. Un domeniu emergent în acestă direcţie este procesarea semnalelor sociale (Social Signal Processing[38]), al cărui scop este decodarea şi sintetizarea automată a atitudinilor rezultate din comunicarea non-verbală dintre actorii conectaţi social. Astfel se poate stabili o ierarhie în cadul reţelei sociale - verticală care se referă la relaţiile impersonale de tip putere, prestigiu, leadership şi orizontală care descrie apropierea emoţională[39]. De o importanţă deosebită este şi identificarea gradului de contaminare emoţională (considerat a fi tendinţa de a mima şi a sincroniza automat expresii, posturi, atitudini, gesturi aparţinând altei persoane, realizându-se astfel un grad de convergenţă emoţională) pe care îl poate induce un mesaj într-o reţea socială. Capacitatea de a influenţa, polariza şi a converti afectiv elemente ale reţelei reprezintă un potenţial indicator al variaţiei importanţei şi prestigiului unui nod al reţelei, facilitând astfel propagarea mesajelor[40].

Rezultatul acestui proces este un profil complex, multidimensional al ţintei, care

---

[35] Massimo Piccardi, Maja Pantic, *From the Lab to the Real World: Affect Recognition Using Multiple Cues and Modalities,* pp.196-213, în Jimmy Or (coord.), *Affective Computing Focus on Emotion Expression, Synthesis and Recognition Hatice*, I-Tech Education Publishing, SUA, 2008.

[36] Mincheol Whang, Joasang Lim, *A Physiological Approach to Affective Computing*, pp. 309-321, în Jimmy Or (coord.), *Affective Computing Focus on Emotion Expression, Synthesis and Recognition Hatice*, I-Tech Education Publishing, SUA, 2008.

[37] Marcin Skowron, Stefan Rank, *The Good, the Bad and the Neutral: Affective Profile in Dialog System-User Communication*, în *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011, pp. 337-347.

[38] Pentru date suplimentare se poate consulta saitul proiectului european SSPNET la adresa http://sspnet.eu/.

[39] Oya Aran, Daniel Gatica-Perez, *Analysis of Group Conversations: Modeling Social Verticality,* pp. 293-310, în Albert Ali Salah, *Computer Analysis of Human Behavior,* SUA, Ed. Springer-Verlag, 2011.

[40] Goncalo Pereira, Joana Dimas**,** *A Generic Emotional Contagios Computational Model*, în Sidney D'Mello, Arthur Graesser et all, *Affective Computing and Intelligent Interaction*, Ed. Springer-Verlag, SUA, 2011, pp. 256-267,.

permite realizarea unor evaluări în privinţa intenţiilor şi riscului pentru securitatea naţională, precum şi a posibilelor reacţii comportamentale în cadrul unor scenarii[41].

4. Analiza intenţiilor se referă evaluarea riscului ţintei de a comite acte care pot afecta securitatea naţională – radicalizare sau auto-radicalizare online, atacuri cibernetice, promovarea unor doctrine sau idei extremiste, violente, rasiste; intenţiile de a comite un act antisocial sau terorist, etc. O astfel de evaluare cu caracter predictiv permite elaborarea unei strategii anticipative destinate prevenirii şi contracarării. O strategie complementară constă în identificarea persoanelor care prezintă un risc crescut de a suferi o agresiune via internet sau prezintă o vulnerabilitate crescută de recrutare sau radicalizare.

Un exemplu este tehnologia dezvoltată în premieră de firma Fujitsu destinată identificării persoanelor care prezintă o susceptibilitate crescută de a suferi un atac cibernetic. Metoda de lucru constă în realizarea unui profil psihologic al angajaţilor (chestionar electronic) şi un profil al activităţii online, fiind identificate elementele complementare care favorizează o conduită imprudentă sau neglijentă[42].

5. În unele situaţii, strategiile de prevenire pot utiliza agenţi virtuali (agenţi emoţionali destinaţi modificării comportamentale - affective agents for behavior change) capabili să realizeze automat unele elemente de analiză cognitivă şi afectivă a discursului. Aceşti agenţi prezintă un grad de inteligenţă artificială care le permite să genereze automat (pe baza unui algoritm prestabilit) contra-naraţiuni interactive (interactive storytelling) ca răspuns la naraţiunile violente sau care instigă la violenţă. Scopul este depistarea timpurie a nodurilor cu risc dintr-o reţea socială, monitorizarea automată a acestora, izolarea şi diminuarea capacităţii de proliferare a memelor indeziderabile[43].

Concluzii

Elementele de computing afectiv vor reprezenta o trăsătură definitorie a Web 3.0, în paralel cu intensificarea şi diversificarea modalităţilor de interacţie cu utilizatorul. Componenta cyber-afectivă va permite o centrare a conţinutului axată pe nevoile şi dorinţele consumatorului, facilitând transmiterea mesajului cognitiv prin optimizarea fondului afectiv în timp real. Totuşi, preţul plătit pentru aceste beneficii este sacrificarea spaţiului privat, aspect care probabil va fi însă dificil de conceptualizat şi cuantificat. "Lentila afectivă" prin care o audienţă globală va putea privi realitatea şi modul în care conţinutul obiectiv va fi interpretat şi prin intermediul experienţei afective are drept scop modificarea percepţiei, reprezentării şi motivaţiei, cu scopul declarat de a interfera cu procesul decizional individual şi colectiv.

Pentru organizaţiile de intelligence computingul afectiv reprezintă o dimensiune suplimentară (şi complementară) destinată culegerii de informaţii şi accesării unei audienţe globale. Posibilitatea de a modifica „anvelopa emoţională" ataşată unui conţinut cognitiv, în timp real şi individualizat, oferă noi grade de libertate în cadrul operaţiunilor de influenţare a opiniei publice, componente ale conflictului de generaţia a V-a (războiul neocortical). Pe lângă utilizarea în scop ofensiv, în contextul războaielor informaţionale, există şi o dimensiune protectivă, destinată amplificării gradului de rezilienţă emoţională a populaţiei, în

---

[41] Didem Gökçay, Gülsen Yildirim, *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives*, IGI Global 2011, SUA, pp. 425-435,.

[42] *Fujitsu Develops Industry's First Technology That Identifies Users Vulnerable to Cyber Attack Based on Behavioral and Psychological Characteristics*, accesibil online la adresa http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0119-01.html.

[43] Thurid Vogt, Elisabeth Andre, Johannes Wagner, *Automatic Recognition of Emotions from Speech: A Review of the Literature and Recommendations for Practical Realisation*, pp. 75-92, în William Sims Bainbridge, *Affect and Emotion in Human-Computer Interaction*, Ed. Springer-Verlag, SUA, 2008.

caz de conflict sau catastrofă antropică sau naturală[44]. "Epidemiile" de panică depăşesc cu mult impactul real al evenimentelor localizate, care sunt amplificate (frecvent iresponsabil, dar uneori şi dirijat) de cutia de rezonanţă a mediului online. O altă valenţă defensivă este utilizarea agenţilor virtuali cu inteligenţă artificială capabili să genereze automat sau în colaborare cu un supervizor uman contra-naraţiuni interactive modulate afectiv în funcţie de mesajele sursei monitorizate.

Posibilitatea de a stabili profilul şi starea afectivă a unei ţinte în timp real va determina, cel puţin teoretic, un grad mai mare de siguranţă (în transporturi, în viaţa socială curentă), datorită probabilităţii crescute de depistare a atentatelor teroriste, pasagerilor agresivi sau a personalului navigant necorespunzător. Rămâne de văzut însă care este limita dincolo de care aceste tehnici se vor dovedi detrimentale datorită gradului de intruzivitate care contribuie la dizolvarea măştii sociale – limita (încă!) dintre spaţiul public şi zona de confort a intimităţii gândurilor şi trăirilor afective individuale.

BIBLIOGRAFIE:

1. Albert Ali Salah, *Computer Analysis of Human Behavior*, SUA, Ed. Springer-Verlag, 2011.
2. Andrew Duchowski, *Eye Tracking Methodology Theory and Practice*, SUA, Ed. Springer-Verlag, 2007 .
3. Christian Peter, Russel Beale, *Affect and Emotion in Human-Computer Interaction*, SUA, Ed. Springer-Verlag, 2008.
4. Demetrios Sapounas, Vadim Kagan, Edward Rossini, *Sentiment Analysis for PTSD Signals,* SUA, Ed. Springer-Verlag, 2013.
5. Didem Gökçay, Gülsen Yildirim, *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives*, SUA, IGI Global 2011.
6. Jimmy Or (coord.), *Affective Computing Focus on Emotion Expression, Synthesis and Recognition Hatice*, I-Tech Education Publishing, 2008.
7. Jimmy Or, *Affective Computing Focus on Emotion Expression, Synthesis and Recognition*, Ed. I-TECH Education and Publishing, Vienna, 2008.
8. Kenneth Revett, *Behavioral biometrics. A remote controll acces*, pp. 73-96, Editura Wiley, SUA, 2008.
9. Khurshid Ahmad (editor), *Affective Computing and Sentiment Analysis Emotion, Metaphor and Terminology,* SUA, Ed. Springer-Verlag, 2011.
10. Ming Shao, Yun Fu, *Human-Centered Social Media Analytics*, SUA, Ed. Springer-Verlag, 2014.
11. N.K. Ratha, Venu Govindaraju, *Advances in Biometrics*, *Sensors, Algorithms and Systems,* SUA, Ed. Springer-Verlag, 2011.
12. Nikolaos V. Boulgouris (editor), *Biometrics Theory, Methods, and Applications*, SUA, Ed. Wiley, 2010.
13. Russel Beale, Christian Peter, *Affect and Emotion in Human-Computer Interaction, From Theory to Application*, SUA, Ed. Springer-Verlag, 2008.
14. Sydney D'Mello, Arthur Graesser, Bjorn Schuller, *Affective Computing and Intelligent Interaction,* 4th International Conference, ACII 2011, oct. 2011, SUA, Ed. Springer-Verlag, 2011.

[44] Sara B. King, *Military Social Influence in the Global Information Environment: A Civilian Primer*, Analyses of Social Issues and Public Policy, Vol.11, pp. 1–26, dec. 2011, accesibil online la adresa http://onlinelibrary.wiley.com/doi/10.1111/j.1530-2415.2010.01214.x/abstract;jsessionid=9D83E69CB59269B4FC11A8FEB318FCEB.f02t02.

LUPTA ÎMPOTRIVA TERORISMULUI – ÎNTRE ACŢIUNEA POLITICĂ ŞI ACTIVITATEA PROFESIONALĂ CHARLIE HEBDO, LIBERTATEA DE EXPRIMARE ŞI NOUL TERORISM

Luminiţa Ludmila (CÎRNICI) ANICA
Drd. Luminiţa Ludmila ANICA (CÎRNICI), Universitatea Naţională de Apărare "CAROL I" Bucureşti, România,
e-mail: ludmila.anica@gmail.com

Abstract: *În ultimele două decenii, terorismul a fost cel mai provocator subiect pentru securitatea euro-atlantică. „911" a demonstrat că teroristul nu are limite şi că nu există zone sigure pentru oamenii nevinovaţi. Noul terrorism a fost identificat în principal cu violenţa promovată de unii extremişti care pretind a fi credincioşi musulmani care fac parte din Al-Qaeda. În ultimul deceniu ne-am confruntat cu un nou tip de terorism – înrădăcinat în Europa prin susţinătorii locali ai Al-Qaeda. Terorismul local european a luat multe vieţi de civili inocenţi în Madrid şi Londra, şi recent în Franţa. Noua fază a terorismului este revendicată de ISIS care ne-a trimis un avertisment puternic asupra gradului de amplificare a acestui risc.*

Combaterea terorismului a devenit o sarcină a puterii politice, a structurilor de securitate şi, de asemenea, a cetăţenilor. Articolul intenţionează să dezvolte noi idei concentrate asupra acţiunii politice, în scopul prevenirii şi combaterii terorismului prin activităţi politice, economice şi sociale şi prin acţiunile profesionale ale serviciilor de securitate.

Cuvinte cheie: *Terorism, acţiuni teroriste, noul terorism, Paris, Charlie Hebdo, Al-Qaida.*

Introducere. Consideraţii teoretice despre terorism

Noţiunea de terorism are o importantă încărcătură politică, socio-psihologică şi emoţională, care accentuează dificultatea unei definiţii exacte. Definirea fenomenului terorist este, însă, o chestiune esenţială pentru reuşita înţelegerii acestuia şi pentru succesul măsurilor de prevenire şi contracarare.

Dicţionarul Explicativ al limbii române *defineşte terorismul* ca „*totalitatea actelor intenţionate de violenţă comise de un grup sau de o organizaţie pentru a provoca o teamă generalizată şi pentru atingerea unor scopuri politice*"[1]. Fiind considerat de origine franceză, etimologic, cuvântul „*terorism*" provine din cultura europeană şi limba latină, „*terrere*" înseamnând „*a tremura*", „*a speria*" (sau a fi speriat)[2], din care termenul a fost preluat şi şlefuit sub formele aflate în circulaţie astăzi, nu doar în limbile europene şi pe întreg mapamondul, sensul emoţional fiind acela de „*groază, spaimă acută, frică puternică*"[3].

[1]DEX, Dicţionarul Explicativ al limbii române, *Definiţia terorismului,* disponibil online la: http://www.dexonline.ro, accesat la data de 14 februarie 2015.

[2]·http://www.arduph.ro/domenii/diu-si-terorismul/consideratii-generale-privind-terorismul/ articol on-line, în care se citează afirmaţiile lui John F. Kennedy, 06 iunie 1962, disponibil online, accesat la data de 14 februarie 2015.

[3]Atanasiu, Mirela; Repez, Filofteia: *Securitatea şi apărarea ţării în contextul ameninţărilor teroriste,* Bucureşti: Editura Universităţii Naţionale de Apărare "Carol I", 2013, pagina 21, disponibil online la: http://cssas.unap.ro/ro/pdf_studii/securitatea_si_apararea_tarii_in_contextul_amenintarilor_teroriste.pdf, accesat la data de 14 februarie 2015

Terorismul este considerat principalul risc de securitate din ultimii ani iar atacurile teroriste îndreptate împotriva unor obiective reprezentând simboluri ale civilizaţiei sau puterii occidentale „*dovedesc faptul că terorismul internaţional, structurat în reţele transfrontaliere, reprezintă cea mai gravă ameninţare la adresa vieţii şi libertăţii oamenilor, a democraţiei şi celorlalte valori fundamentale pe care se întemeiază comunitatea democratică a statelor euroatlantice*”[4].

Mai nou, reţelele teroriste care operează la nivel internaţional au acces la tehnologia modernă *şi* „*se pot folosi de transferuri bancare şi mijloace de comunicare rapide, de infrastructura şi asistenţa oferite de organizaţii extremiste şi pot provoca pierderi masive de vieţi omeneşti şi distrugeri materiale de mare amploare*”[5]. Caracterul deschis al actualelor societăţi democratice moderne, ca şi „*modul complex şi contradictoriu în care se manifestă diferite aspecte ale globalizării, determină ca atât fiecare stat în parte cât şi comunitatea internaţională, în ansamblu, să rămână vulnerabile în faţa terorismului internaţional*”[6].

Terorismul internaţional pune o presiune tot mai mare asupra societăţilor democratice, obligându-le să ia masuri de prevenire şi contracarare tot mai complexe şi mai dure, cu riscul de a îngrădi exerciţiul liber al drepturilor fundamentale ale omului, de a se produce o pervertire a democraţiei de natură să slăbească încrederea popoarelor în capacitatea acesteia de a oferi bunăstare şi securitate în condiţii de libertate.

Violenţa teroristă trebuie înţeleasă nu ca un scop în sine, ci ca un mijloc pentru atingerea unui scop, o modalitate de a intimida, de a pedepsi, de a umili sau de a distruge[7]. Altfel spus, „*violenţa teroristă poate fi privită ca o formă de teatru politic unde actul de violenţă şi carnagiul pe care îl produce reprezintă un scenariu regizat atent pentru a comunica un anumit mesaj*”[8].

1. Evenimentul

A şaptea zi din ianuarie a calendarului gregorian reprezintă în mod normal o zi de sărbătoare pentru creştini, Biserica cinstindu-l pe Sfântul Ioan Botezătorul ca fiind cel mai mare dintre toţi sfinţii, după fecioara Maria[9], „*considerându-l mai mult decât un prooroc*”[10], adică „*prooroc al Celui Prea Înalt*”[11], el fiind acela care vesteşte venirea lui Christos, pe care îl botează când vine la el pentru a împlini planul lui Dumnezeu[12].

---

[4]*Strategia de Securitate Naţională a României*, Bucureşti, 2006, pagina 8, disponibilă online la: http://presidency.ro/static/ordine/CSAT/SSNR.pdf, accesat la data de 14 februarie 2015.

[5]*The National Security Strategy of the United States of America", President of the United States, White House, Washington DC, September 2002*, p.4, disponibil online la: http://www.state.gov/documents/organization/63562.pdf, accesat la data de 15 februarie 2015.

[6]*Strategia de Securitate Naţională a României*, Bucureşti, 2006, paginile 8-9, disponibilă online la: http://presidency.ro/static/ordine/CSAT/SSNR.pdf, accesat la data de 14 februarie 2015.

[7]L. Ludmila Anica (Cîrnici), *Europe between state terrorism and individual terrorism – The shooting down of passenger aircraft MH17*. Article *on International Scientific Conference Strategies XXI*, The Complex and dynamic nature of the security environment, "Carol I" National Defence University, Centre for Defence and Security Strategic Studies, 25-26 November, 2014, Bucharest, p. 138, volumul I.

[8]W, Reich, *"Understanding terrorist Behavior: The Limits and 1 Opportunities of Psychological Inquiry"* în ediţia *Origins of Terrorism: Psychologies, Ideologies, Theologies, State of Mind*, 1998, Woodrow Wilson Center Press, Washington, DC, pp. 261-280.

[9]Ene Braniște; Ecaterina Braniște, *Dicţionar enciclopedic de cunoştinţe religioase*, Editura Diecezana, Oradea, 2001, p. 218, la: https://archive.org/stream/EneSiEcaterinaBraniste-DictionarEnciclopedicDeCunostinteReligioase# page/n215/mode/2up, accesat la data de 15 februarie 2015.

[10]Ibidem.

[11]Ibidem .

[12]WIKIPEDIA, Enciclopedia Liberă, disponibil online la: http://ro.wikipedia.org/wiki/Ioan_Botez%C4%83torul, accesat la data de 15 februarie 2015.

Anul 2015 aduce un nou înţeles acestei zile după Atacul de la Charlie Hebdo, Paris, rămânând în mentalul colectiv ca zi de doliu pentru francezi şi nu numai. *Charlie Hebdo*, revistă săptămânală de satirică franceză, cunoscută fiind ca având un profund ton provocator, a declanşat în mod frecvent polemici, dintre acestea cele mai recente în legătură cu Islamul. Cele mai controversate dintre caricaturile publicate în acest săptămânal au fost cele privind profetul Mahomed[13].

Ziua de 7 ianuarie a anului 2015 a adus moartea în familiile celor 12 sacrificaţi pe *„Altarul Libertăţii de exprimare",* printre victime numărându-se cinci caricaturişti, trei editorialişti, un corector, un muncitor şi doi poliţişti, dintre aceştia din urmă unul fiind garda de corp a principalului caricaturist al revistei (Charb) încă din anul 2011, după publicarea caricaturilor cu Mahomed[14], iar cel de-al doilea, Ahmed Merabet, de religie musulmană, ofiţer de poliţie în vârstă de 42 de ani, care a fost împuşcat mortal afară, în timp ce răspundea atacului[15].

Atacatorii, îmbrăcaţi în negru şi purtând cagule pe faţă, au intrat în sediu înarmaţi cu puşti de asalt Kalaşnikov şi i-au executat, practic, pe cei în care au tras, directorul de redacţie (caricaturistul Charb) fiind ţinta principală a sângerosului atac[16]. În timpul atacului au mai fost răniţi un caricaturist, doi jurnalişti şi mai mulţi ofiţeri de poliţie.

Martorii spun că teroriştii ar fi strigat *Allah akbar,* o frază islamică arabă denumită *Takbir*, având semnificaţia că *Dumnezeu e mare* sau *Dumnezeu e (cel mai) mare*[17], după care au declamat în franceză că l-au răzbunat pe Profetul Mahomed (*On a vengé le prophète Mohamed*!)[18].

După atac, conform declaraţiilor oficialilor francezi, atacatorii au părăsit redacţia, fugind cu un Citroen C3 de culoare neagră şi, pentru a scăpa de urmărirea poliţiştilor, abandonând ulterior maşina undeva, în zona nord-estică a Parisului, pe lângă parcul Buttes-Chaumont şi dispărând la bordul unui Renault Clio, furat[19].

Principalii suspecţi, Cherif şi Said Kourachi, doi fraţi cetăţeni francezi de origine algeriană, au fost împuşcaţi mortal în timpul schimburilor de focuri dintre ei şi trupele speciale, după nu mai puţin de 54 de ore de la atentatul terorist. Un al treilea suspect, care era cumnatul celor doi, a fost eliberat după audieri îndelungate (aproape zece ore), dovedindu-se că nu are legătură cu atacul, el demonstrând că se afla la cursuri[20].

---

[13]Fran Blandy, *"12 dead in 'terrorist' attack at Paris paper"*, Articol online pe site-ul Yahoo News, publicat la 7 ianuarie 2015, disponibil online la:.http://news.yahoo.com/ten-dead-paris-newspaper-shooting-prosecutors-112635032.html, accesat la 15 februarie 2015,

[14]The Guardian, *Charlie Hebdo Attack Report*, *Tony Abbott condemns barbaric Charlie Hebdo attck in Paris*, publicat la 7 ianuarie 2015, disponibil online la: http://www.theguardian.com/world/2015/jan/08/tony-abbott-condemns-barbaric-charlie-hebdo-attack-paris, accesat la data de 15 februarie 2015.

[15]Newsweek-on-line, *Police officer Ahmed Merabet shot during Charlie Hebdo Massacre*, publicat la 7 ianuarie 2015, disponibil online la:-http://www.newsweek.com/officer-shot-during-charlie-hebdo-massacre-identified-297603, accesat la 10 ianuarie 2015.

[16]Rob Crilly, Raziye Akkoc, *Unity rally for Paris shootings: live, Telegraph.co.uk*. 8:45PM GMT, 11 ianuarie 2015, disponibil online la: http://www.telegraph.co.uk/news/worldnews/europe/france/11329976/Paris-Charlie-Hebdo-attack-live.html, accesat la data de 15 februarie 2015.

[17]WIKIPEDIA, the free encyclopedia, *Allahu Akbar (disambiguation)*, disponibil online la: http://en.wikipedia.org/wiki/Allahu_Akbar_%28disambiguation%29, accesat la data de 06 februarie 2015.

[18]*BBC*News Europe, on-line, publicat la 7 ianuarie 2015, disponibil la: http://www.bbc.com/news/world-europe-30710883, accesat la data de 10 februarie 2015.

[19]Patricia Tourancheau, *Un commando organisé, Liberation, Accueil, Société, Fusillade meurtrière à «Charlie Hebdo»* publicat la 7.01.2015, disponibil online la: http://www.liberation.fr/societe/2015/01/07/un-commando-organise-et-prepare_1175841, accesat la data de 10 februarie 2015.

[20]WIKIPEDIA, Enciclopedia Liberă, *Atentatul împotriva revistei Charlie Hebdo*, disponibil online la: http://ro.wikipedia.org/wiki/Atentatul_%C3%AEmpotriva_revistei_Charlie_Hebdo#Suspec.C8.9Bi, accesat la 06 februarie 2015.

2. Reacţiile naţionale şi internaţionale

Bineînţeles, după un astfel de atentat şi după un astfel de şoc, au apărut şi îndoieli în ceea ce priveşte versiunea oficială a firului evenimentelor, apărând întrebări cu privire la unele amănunte care par să nu se lege; de exemplu, a părut ciudat că doi atentatori care au pregătit acest atac cu precizie şi, aşa cum rezultă din înregistrările video de la faţa locului, aveau o foarte bună pregătire militară, având un comportament sigur şi precis, au putut să îşi uite un document de identitate pe bancheta maşinii. Astfel, dacă acesta aparţine sau nu adevăratului terorist, reprezintă una din îndoielile vehiculate în media[21].

Reacţiile internaţionale nu au întârziat să apară, condamnând acest atac asupra unor civili, jurnalişti, care, chiar dacă au împins cumva parodia până la extrem, au considerat că prin caricaturile lor protejează libertatea de religie, Gérard Biard, actualul redactor–şef al publicaţiei, declarând că aceste caricaturi nu fac altceva decât să asigure această libertate, pentru că ele „*declară că Dumnezeu nu trebuie să fie o figură politică sau publică, dar în schimb trebuie să fie una privată*”[22].

Totuşi, Papa Francisc Pontiful a declarat că „*în libertatea de exprimare există limită*”[23]. El a spus că libertatea de credinţă este un drept fundamental al omului, şi că „*nu se poate provoca, nu se poate insulta credinţa altor oameni, nu se poate face haz de credinţă*”[24].

Preşedintele Obama a condamnat atacul privind sediul ziarului satiric francez ca un act de violenţă împotriva nu doar a indivizilor, dar şi împotriva ideii de libertate de exprimare în lumea civilizată. El a afirmat că „*pentru noi a vedea astfel de atacuri laşe, diabolice (...) întăreşte încă o dată de ce este oare atât de important pentru noi să stăm în solidaritate cu ei la fel cum ei stau în solidaritate cu noi*”[25], adică se subliniază importanţa colaborării cu aliaţii în lupta împotriva terorismului.

În convorbirile avute cu vicepreşedintele american Joe Biden şi secretarul de stat John Kerry, în timpul unei reuniuni în Biroul Oval, Obama a adăugat şi că „*faptul că acesta a fost un atac asupra jurnaliştilor, un atac asupra presei noastre libere, de asemenea, subliniază faptul că aceşti terorişti se tem de libertatea de exprimare şi libertatea presei*”[26].

Secretarul de Stat american, John Kerry, a condamnat în termeni duri atentatul care a vizat redacţia Charlie Hebdo, oferind asigurări, într-o declaraţie făcută în limba franceză, că „*libertatea de exprimare nu poate fi ucisă*”[27].

---

[21]Articolul *Atac Terorist Paris. „L'Express" prezintă (falsele) teorii ale complotului,* publicat online la 08.01.15, disponibil online la: http://www.digi24.ro/Stiri/Digi24/Extern/Europa/ATAC+TERORIST+PARIS+teoriile+complotului, accesat la 02.02.2015

[22]Elisha Fieldstadt, *Charlie Hebdo Cartoons Protect Freedom of Religion, Editor Says*, NBC News on-line, publicat online la 18 ianuarie 2015, disponibil la: http://www.nbcnews.com/storyline/paris-magazine-attack, accesat la data de 10.02.2015.

[23]Alexandru Matei: *Papa Francisc: Oricine ridiculizează credinţa cuiva se poate aştepta la un pumn*, publicat în Presa Liberă.net » Home»Social» la 16 ianuarie, 2015., disponibil online la: http://www.presalibera.net/papa-francisc-oricine-ridiculizeaza-credinta-cuiva-se-poate-astepta-la-un-pumn_1817703.html, accesat la data de 14 februarie 2015.

[24]Elisha Fieldstadt, art, cit.

[25]Weinberg, Ali: "*Charlie Hebdo: President Obama Condemns 'Cowardly,' 'Evil' Paris Attacks*" publicat în ABC News, via Good Morning America, la 7 ianuarie 2015, disponibil la: http://abcnews.go.com/News/obama-condemns-cowardly-evil-paris-attacks/story?id=28058882, accesat la 12.02 2015.

[26]RFI România, Actualitate, informaţii, ştiri în direct, Presa internaţională, disponibil online la: http://www.rfi.ro/node/54804/ şi la http://www.rfi.ro/presa-interna%C5%A3ional%C4%83?page=69accesat la 14.02.2015.

[27]Articolul Reacţiile oficialilor internaţionali după atacul terorist de la Paris, publicat online la 7 ianuarie 2015 pe website-ul www.mediafax, disponibil online la: http://www.mediafax.ro/externe/reactiile-oficialilor-

François Hollande a denunţat „*un atentat terorist*" de o „*excepţională barbarie*"[28] şi a adăugat că „*în ultimele săptămâni, mai multe (alte) atacuri teroriste au fost dejucate*"[29].

Alţi lideri politici ai lumii contemporane au condamnat acest atentat terorist, printre aceştia numărându-se şi Angela Merkel, David Cameron, Regina Elisabetha a II a, dar şi Jean Claude Junker, calificându-l, pe drept cuvânt, un „*act intolerabil şi o barbarie*"[30]. De asemenea, reşedintele rus Vladimir Putin a exprimat condoleanţe preşedintelui Francois Holande, pentru pierderile de vieţi omeneşti cauzate de atacurile teroriste, condamnând actul barbar şi exprimându-şi, încă din 8 ianuarie, „*speranţa că vinovaţii vor fi pedepsiţi"*[31].

„*Un act terorist crud şi laş*" a fost catalogat de către preşedintele României, Klaus Iohannis, care şi-a exprimat „*compasiunea pentru familiile victimelor*"[32]. De asemenea, acesta şi-a schimbat fotografia de profil de pe un site de socializare cu celebra fotografie „*Je suis Charlie*!"[33], reprezentând „*sloganul de solidaritate cu victimele atentatului din Paris utilizat pe reţelele de socializare şi pe site-ul charliehebdo.fr după atac*"[34].

Dacă amintim aici definiţia dată de Hoffman cum că „*toate actele de terorism implică violenţa sau ameninţarea cu violenţa şi terorismul este special conceput să aibă efecte psihologice pe scară largă, dincolo de victima/victimele imediate sau obiectul atentatului terorist, că este menit să inducă frica şi, prin urmare, să intimideze un „public-ţintă" mai larg, care poate include un grup etnic sau religios rival, o întreagă ţară, un guvern naţional, partid politic sau opinia publică în general*"[35], am putea afirma că evenimentele petrecute la Paris au stârnit o reacţie inversă în rândul populaţiei şi că, în afară de uciderea celor 12 din redacţie, atacul nu şi-a realizat pe deplin obiectivele, declanşând un imens val de dezaprobare şi dorinţă de contracarare.

Hoffman aduce în discuţie faptul că terorismul se bazează pe putere şi că foloseşte publicitatea pentru a se induce schimbarea, exploatând în mod deliberat frica, prin violenţă sau ameninţare, precum şi efectele psihologice proiectate dincolo de grupurile-ţintă. Frica este diseminată de mass-media şi de răspunsurile noastre colective şi individuale la actele de terorism. Cea mai mare parte a puterii terorismului este derivată din răspunsul la actul terorist şi nu din actul în sine[36].

Populaţia a demonstrat teroriştilor că nu se lasă intimidată, participând, atât în Paris cât şi în alte comunităţi, la impresionante marşuri ale tăcerii (numai în Paris au participat peste zece mii de oameni), marşuri împotriva terorismului, participanţii dorind să arate că refuză să

---

internationali-dupa-atacul-terorist-de-la-paris-ban-ki-moon-e-un-atac-contra-democratiei-john-kerry-libertatea-de-exprimare-nu-poate-fi-ucisa-13752795, accesat la 10 februarie 2015.

[28]WIKIPEDIA, Enciclopedia Liberă, Atentatul împotriva revistei Charlie Hebdo, disponibil online la: http://ro.wikipedia.org/wiki/Atentatul_%C3%AEmpotriva_revistei_Charlie_Hebdo, accesat la data de 6 februarie 2015.

[29]FRANCE 24, International News 24/7, on-line, Manhunt after deadly Charlie Hebdo terrorist attack, 8 ianuarie 2015, disponibil la: http://www.france24.com/en/20150107-live-blog-gun-shots-french-paris-charlie-hebdo-satirical-magazine/ accesat la 14 februarie 2015.

[30]RFI România, Actualitate, informaţii, ştiri în direct, Presa internaţională, disponibil online la: http://www.rfi.ro/presa-interna%C5%A3ional%C4%83?page=69accesat la 14.02.2015.

[31]Official Internet Resources of the President of Russia, Telephone conversation with President of France Francois Holande, publicat la 8.01.2015, disponibil online la: http://eng.kremlin.ru/news/23479, accesat la data de 10 ianuarie 2015.

[32]WIKIPEDIA, Enciclopedia Liberă, Atentatul împotriva revistei Charlie Hebdo, disponibil online la: http://ro.wikipedia.org/wiki/Atentatul_%C3%AEmpotriva_revistei_Charlie_Hebdo, accesat la data de 6 februarie 2015.

[33]http://www.hotnews.ro/stiri-esential-19038290-klaus-iohannis-schimbat-poza-profil-sloganul-solidaritate-suis-charlie.htm

[34]WIKIPEDIA, Enciclopedia Liberă, art, cit.

[35]Bruce Hoffman, Inside Terrorism, 2nd Edition, Columbia University Press, New York, 2006, p.27.

[36]WIKIPEDIA, Enciclopedia Liberă, art, cit.

fie înfricoşaţi. Ei au purtat pancarte pe care scria „Je suis Charlie" (Eu sunt Charlie). Pe reţelele de socializare au fost postate mii de mesaje cu hashtagul #jesuischarlie[37].

Modul în care răspundem la terorism după un eveniment sau incident este la fel de important ca încercarea de prevenire a sa.

3. Analiză

Deşi nu există păreri contrare asupra diagnosticării evenimentului produs la 7 ianuarie 2015, am putea să ne punem pentru început întrebarea dacă este vorba aici de un atac terorist sau doar de o manifestare crudă şi criminală a unor indivizi care au pierdut pentru o clipă contactul cu realitatea sau cu conştiinţa umană.

Literatura de specialitate de astăzi defineşte mai degrabă terorismul ca fiind un act violent, premeditat, realizat de organizaţii conspirative cu caracter distructiv sau de persoane individuale împotriva unor demnitari, a unor instituţii politice, economice, ştiinţifice, militare, culturale, diplomatice, în scopul răzbunării, obligării „ţintei" să adopte o conduită convenabilă autorilor, sensibilizării opiniei publice în legatură cu o cauză anumită, subminării stabilităţii politice şi satisfacerii unor revendicări.

Pornind de la convingerea că principalele caracteristici ale terorii sunt violenţa şi ameninţarea cu violenţa, folosirea sistematică şi persistentă a violenţei, intimidare şi sensibilizare prin agresivitate şi ură, Christian Delanghe, afirma în 2001 în „*La guerre contre la terrorism"* că „*terorismul este o problemă a oamenilor care plonjează într-o logică a urii fără limite, pentru care toate valorile ce fundamentează societatea noastră şi mai ales respectul faţă de viaţa umană, nu mai au curs."*[38] Ţinând cont de această definiţie, putem afirma, fără tăgadă, că da, a fost un atac terorist.

La fel ca atentatele teroriste asupra Turnurilor Gemene din 11 septembrie 2011, care au reprezentat un moment istoric major care a determinat regândirea proceselor democratice şi a celor privind protecţia drepturilor omului, reevaluarea raportărilor la fenomenul globalizării şi a abordărilor cu privire la substanţa relaţiilor intercivilizaţionale, şi atacul asupra redacţiei franceze pune în evidenţă paradoxul coexistenţei dintre aspectele pozitive ale globalizării din perspectiva evoluţiilor tehnologiei moderne, cu aspectele negative materializate în folosirea, într-un mod distructiv, a acestor tehnologii.

Încă din 2001 a fost generată o nouă viziune cu privire la imaginea proiectată de „*noul terorism*" constând în definirea momentului 9/11 ca fiind o veritabilă retrezire a societăţii globale dintr-un vis frumos al globalizării şi aruncarea ei în coşmarul unei globalizări anarhice. Pentru mulţi analişti, atentatele teroriste par să confirme semnalul de alarmă tras de Samuel Huntington, potrivit căruia lumea s-ar afla în pragul declanşării „*unui război global între civilizaţii, fără câmpuri de bătălie şi fără frontiere*"[39].

Se ştie că acesta anticipa că războaiele viitorului vor fi nu între naţiuni, ci între civilizaţii, în special între Occident (considerat ca fiind preponderent: creştin catolic şi protestant; democratic; globalist; umanist; materialist; secular; multicultural) şi Orient (văzut

[37] Articolul *Atac Terorist Paris. Zeci de mii de persoane au ieşit în stradă,* publicat online la 08.01.15, diponibil online la: http://www.digi24.ro/Stiri/Digi24/Extern/Europa/ATAC+TERORIST+PARIS+Zeci+de+mii+de+ persoane +au+iesit+in+strada+d, accesat la 02 februarie 2015

[38]Christian Delanghe, *La guerre contre le terrorisme,* 18.09.2001, disponibil online la: www.fr.strategie.org, accesat la data de 18 ianuarie 2015, citat şi de Gheorghe Văduva în volumul *Terorismul. Dimensiune geopolitică şi geostrategică. Războiul terorist. Războiul împotriva terorismului,* Centrul de Studii Strategice de Securitate, Bucureşti, 2002, p.19, disponibil online la: http://cssas.unap.ro/ro/pdf_studii/terorismul.pdf, accesat la data de 18 ianuarie 2015.

[39]Glen E Perry, "Huntington and his critics: the Occident and Islam", in Samuel P. Huntington, *Arab Studies Quartely*, Winter 2002.

ca un amalgam ortodoxo-islamic: nondemocratic; conservatorist-religios, religios; ideologizat; intolerant; antiglobalist; antimodernist)[40].

Atentatele al-Qaida, sau presupuse a promova sau a fi susţinute de al-Qaida au fost prezentate, astfel, ca fiind o inevitabilă reacţie fundamentalistă faţăde modernitatea şi progresul tehnologic contemporan, şi, ca urmare, sursa principală a suferinţei şi frustrării civilizaţiilor tradiţionaliste (orientale, islamice, asiatice) ameninţate să fie înghiţite de civilizaţia materialist-vulgară consumeristă şi imorală americană şi vest-europeană.

Ideologii noului terorism prezintă (utilizând ca argument şi schiţa ciocnirii globale trasată de Huntington) lumea orientală ca fiind (din cauza agresiunii şi dominaţiei vestice timp de peste o mie de ani) într-un declin dramatic, într-o poziţie marginalizată, înapoiată din punct de vedere tehnologic şi neputincioasă faţă de provocările expansioniste ale ceea ce ei numesc a fi imperialismul euro-atlantic.[41] Aceste viziuni, alimentate de realitatea incontestabilă a evenimentului tragic, au focalizat atenţia asupra acestui gen de terorism (fundamentalist islamic), proiectându-l ca fiind principala (şi covârşitoarea) ameninţare la adresa securităţii comunităţii.

Aceasta a avut ca principal efect pozitiv coagularea rapidă şi eficientă a eforturilor marii majorităţi a actorilor naţionali şi internaţionali pe baricada respingerii acestui tip de violenţă catastrofală[42].

Este pusă o presiune tot mai mare asupra societăţilor democratice, obligându-le să ia masuri de prevenire şi contracarare tot mai complexe şi mai dure, cu riscul de a îngrădi exerciţiul liber al drepturilor fundamentale ale omului, de a se produce o pervertire a democraţiei de natură să slăbească încrederea popoarelor în capacitatea acesteia de a oferi bunăstare şi securitate în condiţii de libertate. Ca urmare, într-o astfel de situaţie complexă, fluidă şi supusă incertitudinii, sunt imperative: contracararea acestui flagel, precum şi cooperarea fără oprelişti a forţelor democratice, pentru contracararea lui - inclusiv prin acţiuni comune desfăşurate în zonele care generează principalele manifestări de terorism - constituie o cerinţă vitală[43]. În condiţiile mediului actual de securitate, terorismul, prin efectele şi consecinţele sale, pune în pericol însăşi existenţa valorilor umane universale. Explozia fără precedent a actelor teroriste a impus reacţia comunităţii internaţionale care, mai solidară şi mai unită ca niciodată[44], a şi declanşat lupta împotriva a ceea ce inseamnă terorism.

Noua ameninţare, precum şi reacţia comunităţii internaţionale faţă de aceasta, au implicaţii şi consecinţe majore asupra tuturor domeniilor vieţii sociale dar, mai ales, asupra modului în care responsabilii politici decid să fie angajate şi întrebuinţate capacităţile militare în viitoarele operaţiuni de combatere a terorismului.

Hoffman propune elemente concrete în definirea fenomenului, precum faptul că „*toate actele de terorism implică violenţa sau ameninţarea cu violenţa. (...) Terorismul este menit să genereze putere acolo unde nu există sau să o consolideze acolo unde este foarte puţină. Prin publicitatea generată de violenţa lor, teroriştii caută să dobândească influenţa, puterea şi*

[40]Langman, Lauren, Moris, Douglas., *Islamic Terrorism: From Retrenchment to Ressentiment and Beyond*, Loyola University Press, Chicago, 2002.
[41]Graham E. Fuller, *The Future of Political Islam*, Palgrave Macmillan Ed, New York 2004.
[42]Jeffrey Record, *Bounding the Global War on Terrorism,* Strategic Studies Institute, New York, Decembrie 2003;
[43]*Strategia de Securitate Naţională a României*, Bucureşti, 2006, paginile 8-9, disponibilă online la: http://presidency.ro/static/ordine/CSAT/SSNR.pdf, accesat la data de 14 februarie 2015.
[44]Anghel Andreescu; Nicolae Radu, *Organizaţiile teroriste, Conceptualizarea terorii versus securitatea europeană,* Editura M.I.R.A. Bucureşti, 2008, disponibil online la: http://www.editura.mai.gov.ro/documente/biblioteca/2008/ organizatii%20teroriste/organizatii%20teroriste.pdf, accesat la data de 20 februarie 2015.

controlul care altfel le lipsesc, pentru a impune o schimbare politică fie pe scară locală, fie internațională"[45].

În acelaşi spirit, Paul R. Pillar enumeră, în cartea „*Terrorism and U.S. Foreign Policy*" - o lucrare publicată în 2001 la Washington, patru elemente definitorii care se pot regăsi în majoritatea definiţiilor folosite de autorităţile implicate în combaterea terorismului. Potrivit opiniilor autorului, „*pot fi rezumate patru elemente ale terorismului care apar în definiţiile guvernamentale*"[46], fără însă ca acestea să poată fi absolutizate. Acestea sunt:

„*- Premeditarea – trebuie să existe intenţie şi o decizie anterioară comiterii unui act care să poată fi numit terorism – terorismul nu este provocat de furia spontană sau un impuls de moment.*

- Motivaţia politică – se exclude violenţa criminală motivată de câştiguri financiare sau răzbunare personală.

- Victimele sunt non-combatanţi – teroriştii atacă persoane care nu le pot răspunde cu aceleaşi mijloace violente.

- Autorii sunt fie grupuri subnaţionale, fie agenţi clandestini"[47].

Concluzii

Fraţii Cherif şi Said Kourachi şi-au premeditat acţiunea, în amănunt, îndreptându-se împotriva unor non-combatanţi (redacţia publicaţiei paiziene) şi făcându-şi cunoscut mesajul de pedepsire la adresa caricaturiştilor care au îndrăznit să insulte pe profetul Mahomed, declamând că „*Dumnezeu e mare*" sau „*Dumnezeu e (cel mai) mare*"[48] şi că l-au răzbunat pe Profet[49], atacul lor putând fi etichetat fără dubiu ca un atac terorist.

Desigur, astăzi, terorismul în multiplele sale forme, este considerat, de multe ori, ca fiind un atac asimetric al celor mai slabi împotriva celor mai puternici, în timp ce, ca act de violenţă spectaculară, terorismul este menit să transmită un mesaj, autorii simţind că nu au niciun alt mod de a se face auziţi şi fiind hotărâţi să îşi transmită mesajul, deşi de cele mai multe ori percepţia publică va fi cu totul alta decat cea dorita de aceştia[50].

Acest act premeditat în scopul declarat al răzbunării, a avut ca obiectiv obligarea „ţintei" să adopte o conduită convenabilă autorilor, sensibilizarea opiniei publice în legatură cu o cauză anumită, subminarea stabilităţii politice şi satisfacerea unor revendicări. George Friedman explică în articolul său: „*Paris Attack Underscores a Deeper Malaise*" publicat în Stratfor Geopolitical Diary la 8 ianuarie 2015, că indiferent de natura acestor atacuri, în sensul de a fi sau nu legate de jihadişti, astfel de incidente au ca efect agravarea tensiunilor existente în relaţiile dintre lumea occidentală şi cea musulmană, acest lucru fiind cu atât mai important în Europa, unde „*statele se confruntă cu o creştere a naţionalismului de dreapta, iar comunităţile musulmane se confruntă cu multă nemulţumire*"[51].

Mai mult decât atât, se face resimţit un conflict de lungă durată al valorilor celor două culturi şi civilizaţii (creştină versus musulmană) referitor la libertatea de exprimare, care este foarte preţuită de lumea occidentală, dar percepută „*de mulţi musulmani ca o licenţă pentru*

[45]Bruce Hoffman, *Inside Terrorism*, 2nd Edition, Columbia University Press, New York, 2006, p.27.
[46]Paul R. Pillar, *Terrorism and U.S. Foreign Policy*, Brookings Institution Press, Washington, 2001. pp. 13-14.
[47]Paul R. Pillar, *op. cit.*
[48]WIKIPEDIA, the free encyclopedia, *Allahu Akbar (disambiguation)*, disponibil online la: http://en.wikipedia.org/wiki/Allahu_Akbar_%28disambiguation%29, accesat la data de 06 februarie 2015.
[49]Ibidem.
[50]Constantin Mostoflei, "Riscuri şi ameninţări actuale: între criză economică şi terorism",. În *Securitate şi stabilitate regională.* Bucureşti, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2009.
[51]Articolul *Paris Attack Underscores a Deeper Malaise,* publicat online la 8.01.2015, în Geopolitical Diary, pe site-ul STRATFOR GLOBAL INTELLIGENCE, disponibil online la: https://www.stratfor.com/geopolitical-diary/paris-attack-underscores-deeper-malaise#axzz3O9XqOvot, accesat la 10 martie 2015.

sacrilegiu"[52]. Faptul că majoritatea musulmanilor nu se vor angaja în înfăptuirea unor violenţe ca răspuns la discursul considerat o blasfemie este evident, totuşi, unii au făcut-o şi probabil o vor mai face, la originea acestei atitudini aflându-se disconfortul extrem resimţit de aceştia în legătură cu „libera exprimare" cu privire la Profet, în viziunea tradiţionalistă acesta fiind imposibil de descris pictural şi, nici atât, în mod satiric.

Pentru Uniunea Europeană, prevenirea şi combaterea terorismului cere un control al mişcării indivizilor şi fluxurilor financiare, deşi construcţia europeană presupune, din contră, principiul fundamental al liberei circulaţii a persoanelor şi bunurilor[53].

Mai mult decât atât, proiectul european s-a construit pe ideea renunţării la război, având pacea drept orizont în toate acţiunile iniţiale întreprinse[54]. În contextul în care chestiunile de securitate ţintesc întâi problema legitimităţii, lupta împotriva terorismului a trebuit să urmeze diferitele etape, astfel cooperarea europeană în materie de luptă împotriva terorismului, multă vreme considerată informală la nivelul Uniunii, a fost întotdeauna puternic activată în cadrul Consiliului Europei. Dar competenţele sale s-au dezvoltat ca răspuns la terorismul autonom sau revoluţionar şi mai puţin pentru a face faţă amplorii terorismului islamist şi internaţional actual[55].

În privinţa terorismului, principalele pârghii de acţiune ale Uniunii sunt: armonizarea legislativă, coordonarea operaţională a serviciilor statelor membre şi dialogul cu ţările terţe[56]. Printre primele măsuri se numără: întărirea cooperării poliţieneşti şi financiare prin *instituirea unui mandat de arest european*, identificarea teroriştilor prin stabilirea unei *liste comune a organizaţiilor teroriste*, crearea unei *echipe de specialişti anti-terorişti* care ar trebui sa colaboreze strâns cu omologii săi americani, punerea în mişcare rapidă a *tuturor convenţiilor internaţionale existente în materie de luptă anti-teroristă*, luptă contra *finanţării terorismului şi întărirea securităţii aeriene*[57].

Lupta împotriva terorismului poate fi văzută, aşa cum afirma şi Alexandre Adam în lucrarea sa, ca un „*catalizator al eforturilor de a crea un spaţiu juridic european care s-a înscris încă de la început în logica penală*"[58].

Totuşi, cazul Charlie Hebdo demonstrează, încă o dată, că terorismul se poate manifesta oriunde şi oricând, neaşteptat şi surprinzător. Binele şi răul se află în noi şi este greu de prevăzut cu siguranţă care este dominanta în conştiinţa fiecăruia, pentru că „*terorismul este o problemă a oamenilor care plonjează intr-o logică a urii fără limite, pentru care toate valorile ce fundamentează societatea noastră occidentală şi mai ales respectul faţă de viaţa umană nu mai au curs*"[59].

---

[52]Constantin Mostoflei, art. cit.

[53]Wilkinson, Paul, *International terrorism: the changing threat and the EU's response*, publicat de Institutul European pentru Studii de Securitate, European Union Institute for Security Studies, Bruxelles, octombrie 2005, p.5, disponibil online la: http://www.iss.europa.eu/uploads/media/cp084.pdf, accesat la 5 martie 2015.

[54]Constantin Mostoflei, art. cit.

[55]Alexandre Adam, *La lutte contre le terrorisme: étude comparative Union Européenne*, Ed. Harmattan, 2005, p. 30.

[56]Ibidem, pp. 14-17.

[57]*Joint Declaration by the Heads of State and Government of the European Union, the President of the European Parliament, the President of the European Commission, and the High Representative for the Common Foreign and Security Policy* , publicat la 14 septembrie 2001, disponibil online la: http://www.europa-eu-un.org/articles/fr/ article_46_fr.htm, accesat la data de 10 martie 2015.

[58]Alexandre Adam, *La lutte contre le terrorisme: étude comparative Union Européenne*, Ed. Harmattan, 2005, p. 30.

[59]Christian Delanghe, *La guerre contre le terrorisme,* 18.09.2001, disponibil online la: www.fr.strategie.org, accesat la data de 18 ianuarie 2015.

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului POSDRU/159/1.5/S/138822, cu titulul „Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile "Ştiinţe Militare", "Securitate şi Informaţii" şi "Ordine Publică şi Siguranţă Naţională" - Program de Formare Continuă a Cercetătorilor de Elită –" SmartSPODAS", coordonat de Universitatea Naţională de Apărare „Carol I".

BIBLIOGRAFIE:

1. ADAM, Alexandre, *La lutte contre le terrorisme: étude comparative Union Européenne*, Ed. Harmattan, 2005, p. 30.
2. ALEXANDRU, Matei: *Papa Francisc: Oricine ridiculizează credinţa cuiva se poate aştepta la un pumn*, publicat în Presa Liberă.net » Home»Social» la 16 ianuarie, 2015., disponibil online la: http://www.presalibera.net/papa-francisc-oricine-ridiculizeaza-credinta-cuiva-se-poate-astepta-la-un-pumn_1817703.html.
3. ANDREESCU, Anghel; RADU, Nicolae, *Organizaţiile teroriste, Conceptualizarea terorii versus securitatea europeană,* Editura M.I.R.A. Bucureşti, 2008, disponibil online la: http://www.editura.mai.gov.ro/documente/biblioteca/2008/organizatii%20teroriste/organizatii%20teroriste.pdf.
4. ANICA (Cîrnici), L. Ludmila. *Europe between state terrorism and individual terrorism – The shooting down of passenger aircraft MH17*. Article *on International Scientific Conference Strategies XXI*, The Complex and dynamic nature of the security environment, "Carol I" National Defence University, Centre for Defence and Security Strategic Studies, 25-26 November, 2014, Bucharest, p. 138, volumul I.
5. ATANASIU, Mirela; REPEZ, Filofteia. *Securitatea şi apărarea ţării în contextul ameninţărilor teroriste,* Bucureşti: Editura Universităţii Naţionale de Apărare "Carol I", 2013, pagina 21, disp. la: http://cssas.unap.ro/ro/pdf_studii/securitatea_si_apararea_tarii_in_contextul_amenintarilor_teroriste.pdf.
6. BLANDY, Fran.*"12 dead in 'terrorist' attack at Paris paper"*, Articol online pe site-ul Yahoo News, publicat la 7 ianuarie 2015, disponibil online la:.http://news.yahoo.com/ten-dead-paris-newspaper-shooting-prosecutors-112635032.html.
7. BRANIŞTE, Ene; BRANIŞTE, Ecaterina. *Dicţionar enciclopedic de cunoştinţe religioase*, Editura Diecezana, Oradea, 2001, p. 218, accesat la data de 15 februarie 2015, disponibil online la: https://archive.org/stream/EneSiEcaterinaBraniste+DictionarEnciclopedicDeCunostinteReligioase#page/n215/mode/2up.
8. CRILLY, Rob; AKKOC, Raziye. *Unity rally for Paris shootings: live, Telegraph.co.uk*. 8:45PM GMT, 11.01.2015, la: http://www.telegraph.co.uk/news/worldnews/europe/france/11329976/Paris-Charlie-Hebdo-attack-live.html.
9. DELANGHE, Christian. *La guerre contre le terrorisme,* 18.09.2001, disponibil online la: www.fr.strategie.org.

10. FIELDSTADT, Elisha. *Charlie Hebdo Cartoons Protect Freedom of Religion, Editor Says*, NBC News on-line, 18.01.2015, disponibil la: http://www.nbcnews.com/storyline/paris-magazine-attack.
11. FULLER, Graham E. *The Future of Political Islam*, Palgrave Macmillan Ed, New York 2004.
12. HOFFMAN, Bruce. *Inside Terrorism*, 2nd Edition, New York, Columbia University Press, 2006, p.27.
13. LANGMAN, Lauren; MORIS, Douglas. *Islamic Terrorism: From Retrenchment to Ressentiment and Beyond*, Loyola University Press, Chicago, 2002.
14. MOSOFLEI, Constantin. "Riscuri şi ameninţări actuale: între criză economică şi terorism",. În *Securitate şi stabilitate regională.* Bucureşti Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2009.
15. PERRY, Glen E. "Huntington and his critics: the Occident and Islam", in Samuel P. Huntington, *Arab Studies Quartely*, Winter 2002.
16. PILLAR, Paul R., *Terrorism and U.S. Foreign Policy,* Brookings Institution Press, Washington, 2001. pp. 13-14.
17. RECORD, Jeffrey. *Bounding the Global War on Terrorism,* Strategic Studies Institute, New York, Decembrie 2003.
18. REICH, W. *"Understanding terrorist Behavior: The Limits and 1 Opportunities of Psychological Inquiry"* în ediţia *Origins of Terrorism: Psychologies, Ideologies, Theologies, State of Mind*, 1998, Woodrow Wilson Center Press, Washington, DC, pp. 261-280.
19. TOURANCHEAU, Patricia. *Un commando organisé,* Liberation, Accueil, Société, Fusillade meurtrière à «Charlie Hebdo» 7.01.2015, disponibil online la: http://www.liberation.fr/societe/2015/01/07/un-commando-organise-et-prepare_1175841.
20. VĂDUVA, Gheorghe, *Terorismul. Dimensiune geopolitică şi geostrategică. Războiul terorist. Războiul împotriva terorismului,* Centrul de Studii Strategice de Securitate, Bucureşti, 2002, disponibil online la: http://cssas.unap.ro/ro/pdf_studii/terorismul.pdf.
21. WEINBERG, Ali: "*Charlie Hebdo: President Obama Condemns 'Cowardly,' 'Evil' Paris Attacks*" publicat în ABC News, via Good Morning America, la 7 ianuarie 2015, disponibil la: http://abcnews.go.com/News/obama-condemns-cowardly-evil-paris-attacks/story?id=28058882.
22. WILKINSON, Paul, *International terrorism: the changing threat and the EU's response*, publicat de Institutul European pentru Studii de Securitate, European Union Institute for Security Studies, Bruxelles, octombrie 2005, p.5, disponibil la: http://www.iss.europa.eu/uploads/media/cp084.pdf.