
# BULETINUL
# UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”

**3/2019**
**IULIE-SEPTEMBRIE**

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
BUCUREȘTI, 2019

# BULETINUL

## UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”

3 / 2019

PUBLICAȚIE ȘTIINȚIFICĂ CU PRESTIGIU RECUNOSCUT DIN DOMENIUL „ȘTIINȚE MILITARE, INFORMAȚII ȘI ORDINE PUBLICĂ” AL CONSILIULUI NAȚIONAL DE ATESTARE A TITLURILOR, DIPLOMELOR ȘI CERTIFICATELOR UNIVERSITARE, INDEXATĂ ÎN BAZELE DE DATE INTERNAȚIONALE CEEOL ȘI GOOGLE SCHOLAR

PUBLICAȚIE FONDATĂ ÎN ANUL 1937

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
BUCUREȘTI, 2019

**Coperta:** Andreea GÎRTONEA



Articolele publicate în Buletinul Universității Naționale de Apărare „Carol I”, ISSN 1584-1928, se regăsesc în integralitate – titlu, autor, abstract, conținut, bibliografie – și în varianta în limba engleză a revistei, ISSN 2284-936X
L 2284-936X

# CONSILIUL EDITORIAL

## 1. CONSILIUL ONORIFIC

| | |
|---|---|
| Gl.bg.prof.univ.dr. Gheorghe CALOPĂREANU | Universitatea Națională de Apărare „Carol I” |
| Lect.univ.dr. Codrin MUNTEANU | Ministerul Apărării Naționale |
| Gl. bg. prof. univ. Constantin Iulian VIZITIU | Academia Tehnică Militară |
| Gl. bg. prof.univ.dr. Ghiță BÎRSAN | Academia Forțelor Terestre „Nicolae Bălcescu” |
| Gl. fl.aer. prof.univ.dr. Gabriel RĂDUCANU | Academia Forțelor Aeriene „Henri Coandă” |
| Cdor.prof.univ.dr. Octavian TARABUȚĂ | Academia Navală „Mircea cel Bătrân” |
| Col.prof.univ.dr. Valentin DRAGOMIRESCU | Universitatea Națională de Apărare „Carol I” |
| Col.prof.univ.dr. Ion PURICEL | Universitatea Națională de Apărare „Carol I” |
| Col.prof.univ.dr. Cezar VASILESCU | Universitatea Națională de Apărare „Carol I” |
| Cdor.prof.univ.dr. Ioan CRĂCIUN | Universitatea Națională de Apărare „Carol I” |
| Col. prof.univ.dr. Ioana ENACHE | Universitatea Națională de Apărare „Carol I” |
| Col.prof.univ.dr. Constantin POPESCU | Universitatea Națională de Apărare „Carol I” |
| Lect.univ.dr. Florian BICHIR | Universitatea Națională de Apărare „Carol I” |
| Col.prof.univ.dr. Doina MUREŞAN | Universitatea Națională de Apărare „Carol I” |
| Col.prof.univ.dr. Daniel GHIBA | Universitatea Națională de Apărare „Carol I” |
| Col.lect. univ.dr. Florin CÎRCIUMARU | Universitatea Națională de Apărare „Carol I” |
| Col. prof.univ.dr. Marinel-Dorel BUŞE | Universitatea Națională de Apărare „Carol I” |
| Lt.col.conf.univ.dr. Tudorel-Niculai LEHACI | Universitatea Națională de Apărare „Carol I” |
| Col.lect.univ.dr. Liviu BALABAN | Universitatea Națională de Apărare „Carol I” |
| Col.lect.univ.dr. Răzvan GRIGORAŞ | Universitatea Națională de Apărare „Carol I” |
| Inspector Carol Teodor PETERFY (Laureat al Premiului Nobel pentru Pace în 2013) | Organizația pentru Interzicerea Armelor Chimice – OPCW |

## 2. CONSILIUL ŞTIINȚIFIC

| | |
|---|---|
| Prof.univ.dr. Gheorghe CALOPĂREANU | Universitatea Națională de Apărare „Carol I” |
| Conf.univ.dr. Iulian CHIFU | Universitatea Națională de Apărare „Carol I” |
| Prof.univ.dr. Daniel DUMITRU | Universitatea Națională de Apărare „Carol I” |
| Prof.univ.dr. Gheorghe MINCULETE | Universitatea Națională de Apărare „Carol I” |
| Prof.univ.dr. Teodor FRUNZETI | Universitatea „Titu Maiorescu” |
| Prof.univ.dr. Gelu ALEXANDRESCU | Universitatea Națională de Apărare „Carol I” |
| Prof.univ.dr. Sorin TOPOR | Universitatea Națională de Apărare „Carol I” |
| Prof.univ.dr. Marian NĂSTASE | Academia de Studii Economice din București |
| CS II dr. Alexandra SARCINSCHI | Universitatea Națională de Apărare „Carol I” |
| CS II dr. Cristina BOGZEANU | Universitatea Națională de Apărare „Carol I” |
| Dr. Pavel OTRISAL | Universitatea de Apărare, Brno, Republica Cehă |

| | |
|---|---|
| Conf.univ.dr. Elena ŞUŞNEA | Universitatea Națională de Apărare „Carol I” |
| Dr. Elitsa PETROVA | Universitatea Națională Militară ”Vasil Levski”, Veliko Tarnovo, Bulgaria |
| Dr. Jaromir MAREŠ | Universitatea de Apărare, Brno, Republica Cehă |
| Lect.univ.dr. Cris MATEI | Centrul pentru relațiile Civili-Militar, SUA |
| Dr. Piotr GAWLICZEK | Universitatea ”Cuiavian” din Wloclawek, Polonia |
| Conf.univ. dr. Piotr GROCHMALSKI | Universitatea ”Nicolaus Copernicus” din Torun, Polonia |
| Dr. Marcel HARAKAL | Academia Forțelor Armate ”General Milan Rastislav Štefánik”, Liptovský Mikuláš, Republica Slovacă |
| Dr. Lucian DUMITRESCU | Academia Română |
| Prof.univ.dr. Anton MIHAIL | Universitatea Națională de Apărare „Carol I” |
| Prof.univ.dr. Constantin IORDACHE | Universitatea „Spiru Haret” |
| Prof.univ.dr. Gheorghe ORZAN | Academia de Studii Economice din București |
| Prof.univ.dr. Gheorghe HURDUZEU | Academia de Studii Economice din București |

**3. REFERENȚI**

Col.prof.univ.dr. Ioana ENACHE
Col.prof.univ.dr. Ion ANDREI
Col.prof.univ.dr. Dănuț TURCU
Col.prof.univ.dr. Dorin EPARU
Col.prof.univ.dr. Filofteia REPEZ
Cdor. prof.univ.dr. Florin NISTOR
Col.prof.univ.dr. Cristian-Octavian STANCIU
Col.conf.univ.dr. Daniel ROMAN
Col.instr.av.dr. Ștefan Antonio DAN-ȘUTEU
Lt.col.conf.univ.dr. Tudorel-Niculai LEHACI
Lt.col.conf.univ.dr. Dragoș BĂRBIERU
Mr.conf.univ.dr. Marinel-Adi MUSTAȚĂ
Lect.univ.dr. Florin BICHIR

# CUPRINS

# MIGRAŢIA ÎN RĂZBOIUL DE DEZINFORMARE AL KREMLINULUI

## *MIGRATION IN THE KREMLIN'S DISINFORMATION WAR*

## *LA MIGRATION DANS LA GUERRE DE DÉSINFORMATION DU KREMLIN*

**Drd. Magdalena CRIŞAN***

Criza migraţiei din 2015 a fost însoţită de un val de dezinformare şi de ştiri false legate de migranţi, menite să influenţeze percepţia publică asupra fenomenului, care serveşte interesului geopolitic al Rusiei: o Uniune Europeană şi societăţi europene scindate, cu lideri a căror legitimitate este pusă sub semnul întrebării.

*The migration crisis of 2015 was accompanied by a wave of disinformation and fake news related to migrants, meant to influence the public perception of the phenomenon, and which serves Russia's geopolitical interest: a divided European Union and split European societies with leaders whose legitimacy is called into question.*

*La crise migratoire de 2015 a été accompagnée d'une montée de la désinformation et d'une vague massive de fausses informations sur les migrants, censées influer l'image publique du phénomène et servir aussi à l'intérêt géopolitique de la Russie: une Union européenne et une division des sociétés européennes avec des dirigeants dont la légitimité était douteuse.*

**Cuvinte-cheie:** dezinformare; propagandă rusă; Uniunea Europeană; percepţie; migraţie; ştiri false.
***Keywords:*** *disinformation; Russian propaganda; European Union; perception; migration; fake news.*
***Mots-clés:*** *désinformation; propagande russe; Union européenne; perception; migration; fausses informations.*

În ultimii ani, se discută despre noi forme ale luptei pentru putere și hegemonie în relațiile internaționale. Acest fapt conduce nu numai la adoptarea de noi strategii, ci și la conceperea și utilizarea de noi arme. Războiul hibrid, de exemplu, presupune, printre alte tipuri de tehnologii, și utilizarea refugiaților ca armă[1].

Kelly M. Greenhill notează că „exploatarea şi manipularea” unui flux de migranţi, generat de alţii, poate deveni o armă nonmilitară de constrângere eficientă pe scena internaţională, mai ales dacă adversarul este un stat cu o democraţie liberală[2]. Scopul „constrângerii” adversarului este generarea unui „conflict intern” sau/şi „a nemulţumirii publice” în statul-ţintă fie prin diminuarea capacităţii, fie prin influenţarea voinţei unui stat de a primi şi de a integra un număr de migranţi[3].

***Universitatea Naţională de Apărare „Carol I”***
e-mail: *crisanmagda@yahoo.com*

Această a doua strategie, botezată „agitare politică”, reprezintă un mod eficient de a mări prăpastia dintre taberele pro şi contra dintr-o societate, mai ales în cazul temelor sensibile, precum migraţia, ceea ce se traduce printr-o vulnerabilizare a liderului ţării-ţintă, în consecinţă printr-o scădere a capacităţii lui de a negocia extern[4].

Pentru actorii slabi, transformarea migraţiei în armă înseamnă atingerea unui ţel politic care „cu greu ar fi putut fi atins prin mijloace militare”, iar pentru actorii puternici, „ar fi fost prea costisitoare”[5].

Nu este un secret că Rusia vrea să-şi recapete locul de jucător global important şi controlul asupra mai vechii ei sfere de influenţă din Europa, folosind toate mijloacele de luptă pentru a-şi atinge scopul. Pentru că Vestul îi este, din punctul de vedere al tehnicii militare, net superior, Rusia mizează pe o altă strategie de „luptă”, cu mijloace nonmilitare, precum campanii de dezinformare, de manipulare[6], de diseminare a unor ştiri false, al căror scop este

„influenţarea populaţiei (n.a. din ţări europene) în favoarea obiectivelor ruseşti”[7], strategie aplicată şi în cazul crizei migraţiei instalate în 2015.

„A venit ziua în care toţi trebuie să admitem că un cuvânt, o cameră video, o fotografie, internetul şi informaţia, în general, au devenit un alt tip de armă, o altă componentă a forţelor armate. Această armă poate fi folosită într-un mod bun sau într-unul rău”, declara, în 2015, ministrul rus al apărării, Serghei Şoigu[8]. Aşadar, câmpul de luptă este mintea oamenilor, populaţia statelor occidentale, adesea neglijată de strategiile militare vestice[9], iar scopul este „slăbirea coeziunii interne a societăţilor şi întărirea percepţiilor privind disfuncţionalităţile sistemului democratic şi economic al Vestului”, notează raportul Centrului pentru Studii Strategice şi Internaţionale din Washington, ”The Kremlin Playbook”[10]. Influenţarea percepţiei şi dinamitarea coeziunii au rezultat doar acolo unde există deja deficienţe instituţionale sau teme care deja polarizează opinia publică. O astfel de verigă slabă, speculată de Rusia, este criza migraţiei declanşate în anul 2015, când FRONTEX a înregistrat 1,8 milioane de treceri ilegale ale frontierelor Uniunii Europene[11], iar peste 1,2 milioane de migranţi au solicitat azil în statele UE, însemnând o cifră de două ori mai mare decât în anul precedent[12].

Cei mai mulţi dintre solicitanţii de azil erau, în 2015, sirieni, afgani şi irakieni[13]. Valul de migranţi a scos la iveală deficienţe ale instituţiilor europene şi ale instituţiilor statelor membre, care s-au dovedit a nu fi pregătite să gestioneze un număr atât de mare de migranţi, şi a stimulat discursurile politice populiste şi extremiste.

Criza migraţiei seamănă, din punct de vedere mediatic, cu operaţiunea militară „Furtună în Deşert”, din 1991, care, prin transmiterea sa live de către postul de televiziune CNN, a captat atenţia şi a influenţat opinia publică[14].

În 2015, imaginile cu migranţi veniţi pe mare sau pe ruta balcanică spre Vestul Europei au fost intens mediatizate, unele fiind difuzate în timp real la televiziuni şi în mediul online. Ele au generat îngrijorare[15] şi au polarizat opiniile în Uniunea Europeană[16]. Aşadar, tema migraţiei este un teren extrem de fertil pentru propaganda prorusă, căci are potenţialul să scindeze UE, „să cutremure încrederea cetăţenilor în instituţiile europene” şi să pună sub semnul întrebării legitimitatea unor lideri din statele membre[17]. Iar interesul geopolitic al Rusiei este o Uniune Europeană care vorbeşte pe mai multe voci şi unor state membre slăbite.

### *Fake news* şi propaganda rusă în problema migraţiei

Propaganda prorusă s-a dovedit a fi, „în mare parte, responsabilă pentru diseminarea unor ştiri false/*fake news* legate de migraţie”[18]. Fenomenul ştirilor false a preocupat intens literatura de specialitate[19], reţinându-se din multitudinea de definiţii trei aspecte esenţiale, „nivelul redus de factualitate”, „intenţia de a înşela” şi „încercarea de a părea ştiri reale”[20].

Tipul de discurs promovat de propaganda prorusă, însoţit de ştiri false, îl sprijină pe cel al partidelor antimigraţie şi are menirea să pună în antiteză, complet fals, imaginea unui „Vest debil” cu cea a „unei Rusii stabile şi liniştite”, care-şi păzeşte tradiţiile, valorile, identitatea[21]. Iar identitatea culturală este cartea pe care mizează Kremlinul în strategia sa de politică externă. Un document oficial privind politica externă a Rusiei, din anul 2010, notează că „este din ce în ce mai evident, competiţia la nivel global capătă o dimensiune culturală. Printre jocurile fundamentale din arena internaţională, lupta pentru influenţa culturală devine din ce în ce mai intensă”[22].

Conceptul de Politică Externă a Federaţiei Ruse, din 2008, arată că: „Rusia va căuta să fie percepută obiectiv în lume, să îşi dezvolte propriile mijloace de informaţie pentru influenţarea opiniei publice externe, să întărească rolul mass-mediei ruse în mediul informaţional internaţional, acordându-i sprijin din partea statului” şi „va lua măsurile necesare pentru a respinge informaţiile care reprezintă o ameninţare pentru suveranitatea şi securitatea ei”[23].

Cele mai sonore nume ale mass-mediei de propagandă, menţionate de documentul amintit anterior, sunt Sputnik şi Russia Today, ale căror ştiri sunt disponibile şi în limbile engleză, franceză, germană, astfel încât conţinutul lor să ajungă în mod direct la publicul din UE. Pericolul tacticii dezinformării din partea Kremlinului este considerat atât de periculos de Uniunea Europeană încât a fost înfiinţat, în 2015, Grupul de lucru East StratCom, în cadrul Serviciului European de Acţiune Externă, care se ocupă de demantelarea şi combaterea dezinformării din partea Kremlinului. O analiză EUvsDisinfo, parte a activităţii East

StratCom, arată că, din noiembrie 2015 până pe 6 august 2019, au fost identificate peste 6.000 de cazuri de dezinformare din partea Rusiei, iar în top 10 subiecte ale dezinformării este şi migraţia[24].

Un alt document EUvsDisinfo atrage atenţia asupra tacticilor de dezinformare ale Kremlinului, de exemplu, mesaje diferite şi canale de comunicare diferite (de exemplu, faţă în faţă, reţele de socializare, presă) pentru categorii-ţintă diferite, un număr necunoscut de canale de comunicare şi comunicatori[25]. Aceşti comunicatori pot fi din rândul personalului diplomatic, al serviciilor secrete, aşa-zise organizaţii nonguvernamentale şi bloguri finanţate de Kremlin, troli şi boţi pe reţelele de socializare[26] şi, nu în ultimul rând, mass-media de propagandă a Kremlinului, care diseminează ştiri false şi „generează confuzie”[27].

Modul în care acţionează dezinformarea este, în esenţă, acelaşi: alimentează artificial emoţiile negative, frica, furia, dezgustul într-o societate, obţinând, de exemplu, un val de antipatie faţă de Vest, faţă de o anumită minoritate etnică sau sexuală, ori un val antiimigraţie[28]. De exemplu, media de propagandă prorusă, care susţine discursul antiimigraţie transformă migraţia într-un pericol pentru securitatea societăţii europene, asociind-o cu terorismul şi cu infracţionalitatea crescută, inducând o stare de disconfort şi de frică în rândul populaţiei[29]. Iar o societate puternic polarizată, „mânată de sentimente puternice se va comporta (mai) iraţional şi va fi mai uşor de manipulat”[30].

Planul EUvsDisinfo de combatere a dezinformării la nivelul UE, lansat în iunie 2019, notează că există dovezi pentru existenţa unei „activităţi de dezinformare continuă și susținută din partea unor surse rusești, care urmărește să diminueze participarea la vot și să influențeze preferințele alegătorilor europeni[31]. Acelaşi document arată că „actori rău-intenţionaţi folosesc dezinformarea pentru a promova opinii extremiste și a polariza dezbaterile locale, inclusiv prin atacuri nefondate la adresa UE” şi că acest tip de discurs a fost preluat şi de actori naţionali din statele membre[32].

**Arma dezinformării în problema migraţiei**

Claire Wardle, expertă în reţele de socializare, a identificat mai multe tipuri de dezinformare cu intenţie, printre acestea numărându-se informaţiile inventate, informaţiile puse în context greşit şi cu conţinut înşelător[33]. De subliniat este faptul că dezinformarea păstrează de cele mai multe ori un sâmbure de adevăr, ea se construieşte în jurul unei probleme deja existente, ţinteşte un public vulnerabil în faţa informaţiilor false[34].

Un exemplu de dezinformare prin oferirea unui context şi a unor conexiuni greşite este o ştire, publicată de Sputnik, despre creşterea numărului de delicte sexuale în Suedia, în care autorul articolului sugerează, fără a aduce vreo dovadă, că de vină ar fi politica uşilor deschise pentru migranţi, practicată de Suedia[35]. „În timp ce conducerea politică suedeză refuză să admită o posibilă legătură între imigraţie, infracţionalitate şi sentimentul de insecuritate în creştere al populaţiei, modul în care Suedia gestionează infractorii străini a generat îngrijorare”, notează articolul, sugerând că migranţii sunt automat şi infractori[36]. După o lună, mesajul a fost preluat de către politicianul populist britanic Nigel Farage, care a scris pe Twitter că Suedia este „ţara care a preluat cel mai mare număr de migranţi, bărbaţi tineri, pe cap de locuitor din Europa”, iar rezultatul este că „Malmö este, acum, capitala violurilor din Europa”[37]. Informaţia, publicată de Sputnik şi preluată de Farage, nu menţionează că legea suedeză privind delictele sexuale cuprinde mai multe infracţiuni, din anul 2013, spre deosebire de alte ţări europene, în Suedia zece violuri, comise în zece zile asupra unei femei de un bărbat, sunt înregistrate ca fiind 10 cazuri distincte de viol; în plus, o acuzaţie de viol, care s-a dovedit, ulterior, a fi nefondată, rămâne în statistica suedeză a delictelor sexuale[38].

Numărul delictelor sexuale înregistrate în 2015, când Suedia a primit un număr mare de migranţi, este mai mic faţă de anul precedent[39].

Avem şi un exemplu de dezinformare prin afirmaţii false, însoţite de imagini reale. În 2017, după atacul de la Londra, fotografia unei femei cu hijab la locul atentatului, care a fost descrisă ca trecând nepăsătoare pe lângă victime, a fost speculată intens de propaganda rusă şi de cea antiimigraţie. Contul de Twitter, cu peste 16.000 de urmăritori, @SouthLoneStar, al cărui proprietar se recomanda „texan mândru şi american patriot”, cel care a postat fotografia cu pricina şi a făcut şi comentariul dovedit a fi neadevărat, s-a demonstrat a fi doar „unul din cele 2.700 de conturi false, create în Rusia, cu scopul de a influenţa politica britanică şi pe cea americană”[40].

Un alt caz de dezinformare, din februarie 2018, constând în informaţii false şi o fotografie manipulată digital, a ţintit, de data aceasta, publicul rus. Mai multe site-uri de ştiri în limba rusă şi o platformă de socializare rusească au relatat despre un flashmob, organizat de femei, în Germania, în Suedia, în Danemarca şi în alte ţări europene, intitulat *#sorry*, prin care acestea le cereau iertare migranţilor musulmani violatori, pentru că i-au provocat „prin comportament şi îmbrăcăminte depravată”[41]. Acest flashmob nu a existat, iar fotografia în care apare o tânără, din Europa, cu o pancartă pe care e scris „iartă-mă Mustafa” este editată grosolan. Fotografia reală a fost făcută în 2014, la o acţiune de sprijinire a soldaţilor ucraineni, iar pe pancartă era scris: „Ţi-e frig? Gândeşte-te la cei care dorm în tranşee”[42].

Un exemplu, deja cunoscut, de conţinut, fabricat şi promovat de Kremlin, este cazul Lisa, o adolescentă germană cu origini ruseşti, despre care s-a relatat, în 2016, că a fost violată de migranţi. Ştirea, care a produs emoţie în rândul germanilor şi a dat ocazia ministrului rus de externe, Serghei Lavrov, să reproşeze Germaniei că ascunde sub preş cazul, a apărut, iniţial, pe un site obscur, pentru expatriaţii ruşi care trăiesc în Germania, şi s-a dovedit a fi falsă[43].

Chiar şi preşedintele rus, Vladimir Putin, a căzut pradă unei ştiri false, publicate de postul de televiziune public Pervîi Canal. Liderul rus a declarat, în toamna lui 2016, că instanţa din Austria a achitat un migrant irakian care a violat un băiat, pe motivul că nu ştie limba germană şi deci nu a înţeles protestul verbal al victimei[44]. În realitate, la momentul declaraţiei lui Putin, migrantul irakian se afla în custodia autorităţilor austriece[45].

**Concluzii**

Migraţia poate deveni o armă în mâna actorilor care ţintesc destabilizarea adversarilor, diminuarea puterii lor de negociere pe scena internaţională. O demonstrează Rusia, care duce un război al dezinformării, al ştirilor false în Europa, scopul fiind influenţarea percepţiei populaţiei şi slăbirea unităţii Uniunii Europene şi adâncirea neîncrederii în instituţiile, în procesele democratice din Vest. Criza migraţiei a fost un teren fertil pentru campania de dezinformare susţinută de Kremlin, pentru că, în UE şi în statele membre, au existat deficienţe în gestionarea numărului mare de migranţi, opinia publică începea să fie polarizată, iar politicienii populişti se vedeau îndreptăţiţi să-şi ţină discursul antiimigraţie.

Propaganda rusă a susţinut discursul antiimigraţie, alimentând confuzia şi speculând disconfortul şi frica cetăţenilor din statele europene. Practica propagandei ruse constă în asocierea migrantului cu terorismul, cu infracţionalitatea, deci cu un pericol pentru securitatea statelor membre şi a cetăţenilor săi.

Prin războiul dezinformării în statele UE, Kremlinul încearcă să obţină un plus de imagine pentru Rusia, dornică să redevină un jucător global important, opunând imaginii unui Occident asaltat de migranţi, a cărui identitate este în pericol, imaginea unei Rusii care-şi apără valorile, tradiţiile şi identitatea culturală, practic un model de urmat. Dezinformarea rusă, inclusiv în cazul migraţiei, se face pe diferite canale, faţă în faţă, pe site-urile de socializare sau în presa de propagandă, care include Sputnik şi Russia Today, care oferă conţinut în mai multe limbi vorbite în statele UE. Mesajele agenţilor dezinformării sunt diferite pentru categorii de public-ţintă diferite instigă fie la sentimente antioccidentale, fie la ură faţă de o anumită minoritate sau faţă de migranţi.

Dezinformarea poate îmbrăca mai multe haine, numitorul comun este intenţia de a înşela şi conţinutul cu un nivel scăzut sau zero de factualitate. Putem avea informaţii scoase din context, altele puse într-un context greşit, ştiri în care autorul face cu intenţie conexiuni greşite sau pur şi simplu putem avea ştiri fabricate de la un capăt la altul.

Uniunea Europeană a recunoscut pericolul dezinformării ruseşti pentru securitatea UE şi a statelor membre şi a creat mecanisme de demantelare şi de combatere a ei. În decurs de aproape patru ani, au fost identificate 6.000 de cazuri de dezinformare, fabricată în Rusia, iar migraţia se numără printre temele predilecte.

**NOTE:**

1 Kelly M. Greenhill, ”Strategic Engineered Migration as a Weapon of War”, *Civil Wars*, vol. 10, nr. 1, 2008, pp. 6-21, DOI: 10.1080/13698240701835425, accesat la 12 iulie 2019.

2 Kelly M. Greenhill, ”Migration as a Weapon in Theory and in Practice”, *Military Review*, noiembrie/decembrie 2016, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2016/, p. 25, accesat la 14 iunie 2019.

3 *Ibidem.*

4 *Ibidem*, pp. 26, 28.

5 *Ibidem*, p. 27.

6 Timothy P. McGeehan, „Countering Russian Disinformation”, *Parameters* 48(1), Army War College, 2018, https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf, p. 5, accesat la 2 mai 2019.

7 Ofiţerii ruşi P. A. Doulnev şi V. I. Orlianski notau, în 2015, că adversarul trebuie înfrânt sau cel puţin vulnerabilizat economic, politic, înainte ca războiul propriu-zis să înceapă, inclusiv prin manipularea opiniei publice. P. A. Doulnev, V.I. Orlansk, ”Basic Changes in the Character of Armed Struggle in the First Third of the 21st Century”, *Journal of the Academy of Military Science*, nr. 1 (2015): 46, citat în Lt. Col. Timothy L. Thomas, ”Russian Forecasts of Future War”, *Military Review*, Army University Press, mai-iunie 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accesat la 2 iulie 2019.

8 ”Shoigu: Information becomes another armed forces component”, *Interfax*, 28 martie 2015, http://www.interfax.com/newsinf.asp?id=581851, accesat la 20 aprilie 2019.

9 H. Conley, J. Mina, R. Stefanov, M. Vladimirov, ”The Kremlin Playbook. Understanding Russian Influence in. Central and Eastern Europe”, *CSIS Europe Program CSD Economic Program*, octombrie 2016, p. X.

10 „Societatea civilă reprezintă un punct orb, în concepţia americană a războiului”, motiv pentru care ea a fost transformată în armă de adversari, precum Rusia sau China. Buddhika B. Jayamaha, Jahara Matisek, ”Social Media Warriors:Leveraging a New Battlespace”, *Parameters*, vol. 48, nr. 4, Army War College, 2018-2019, p. 11.

11 Numărul trecerilor ilegale nu înseamnă număr de migranţi ilegali. ”Risk Analysis for 2017”, FRONTEX, februarie 2017, Varşovia, https://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2017.pdf, p. 18, accesat la 3 iulie 2019.

12 ”Record number of over 1.2million first timeasylum seekers registered in 2015”, *Comunicat de presă Eurostat*, 4 martie 2016, https://ec.europa.eu/eurostat/documents/2995521/7203832/3-04032016-AP-EN.pdf/790eba01-381c-4163-bcd2-a54959b99ed6, accesat la 13 iulie 2019.

13 *Ibidem.*

14 Philp Seib, ”Effects of Real-Time News Coverage on Foreign Policy”, *Journal of Conflict Studies*, volum XX, nr. 1, 2000, https://journals.lib.unb.ca/index.php/jcs/article/view/4309/4920, accesat la 2 iunie 2019.

15 Procentul europenilor care consideră că migraţia este o provocare pentru UE a crescut, la finalul lui 2015, cu 33% faţă de iunie 2013. În timp ce cetăţenii unor state, precum Germania şi Suedia, ţintă a valului de migranţi, consideră că, în contextul valului de migranţi, este nevoie de migranţi pe piaţa muncii în proporţie de 72%, respectiv 77%, state, precum Ungaria, Cehia, Slovacia, Polonia, erau de acord în proporţie de sub 40%. „Parlemeter 2015 – Part I The main challenges for the EU, migration, and the economic and social situation”, Parlamentul European, Bruxelles, 14 octombrie 2015, http://www.europarl.europa.eu/pdf/eurobarometre/2015/2015parlemeter/eb84_1_synthese_analytique_partie_1_migration_en.pdf, accesat la 2 decembrie 2018, pp. 10, 34.

16 Sprijinul pentru o politică comună privind migraţia a scăzut în 23 de state membre din primăvara până în toamna lui 2015, iar în nouă state, chiar cu 10%. Eurobarometrul Standard 84, ”Europeans’ views on the priorities of the European Union”, Comisia Europeană, 2015, https://bit.ly/2UjGxfs, accesat la 12 ianuarie 2019 p. 45.E.

17 Attila Juhász, Patrik Szicherle, ”The political effects of migration-related fake news, disinformation and conspiracy theories in Europe”, Fundaţia Friedrich Ebert şi Political Capital Policy Research and Consulting Institute, 2017, https://www.politicalcapital.hu/pc-admin/source/documents/FES_PC_FakeNewsMigrationStudy_EN_20170607.pdf, p. 4, accesat la 3 mai 2019.

18 *Ibidem.*

19 Edson C. Tandoc Jr., Yheng Wei Lim, Richard Ling, ”Defining Fake News”, *Digital Journalism*, 6(2), pp. 137-153, 2018, DOI: 10.1080/21670811.2017.1360143, pp. 147-148, accesat la 15 martie 2019.

20 Multitudinea de definiţii pentru ştiri false: Grafic 1 ”Overview of characteristics in fake news definitions”, în Jana Laura Egelhofer, Sophie Lecheler, ”Fake news as a two-dimensional phenomenon: a framework and research agenda”, *Annals of the International Communication Association*, 43:2, 97-116, DOI: 10.1080/23808985.2019.1602782 , accesat la 2 noiembrie 2018.

21 *Ibidem.*

22 Document al Federaţiei Ruse din 2010, ”Basic Guidlines Concerning the Policy of the Russian Federation in the Sphere of International-Humanitarian Cooperation”, citat în Marcel H. Van Herpen, ”Putin’s Propaganda Machine: Soft Power and Russian Foreign Policy”, Rowman & Littlefield, Lanham Maryland, SUA, 2015, p. 28.

23 ”The Foreign Policy Concept of the Russian Federation”, Preşedinţia Federaţiei Ruse, 12 ianuarie 2008, http://en.kremlin.ru/supplement/4116, accesat la 3 iunie 2019.

24 ”Figure of The Week: 6000+”, EUvsDisinfo, 6 august 2019, https://euvsdisinfo.eu/figure-of-the-week-6000/, accesat la 7 august 2019.

25 ”The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign”, EUvsDisinfo, 27 iunie 2018, https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/, accesat la 23 august 2018.

26 *Ibidem.*

27 Într-o lucrare din anul 2012, S. G. Chekinov şi S. A. Bogdanov, ofiţeri ai Academiei Statului Major Rus, notau că, în pregătirea unui viitor război, „obţinerea superiorităţii informaţionale şi utilizarea mass-mediei vor genera haos şi confuzie în guvernul şi în sistemele de comandă şi control militare ale adversarului”. S. G. Chekinov şi S.A. Bogdanov, ”Initial Periods of War and their Impact on a Country’s Preparations for Future War”, *Military Thought*, nr. 11 (2012): 16, citat în lt.col. Timothy L. Thomas, ”Russian Forecasts of Future War”, *Military Review*, Army University Press, mai-iunie 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accesat la 2 iulie 2019.

28 Strategii militari ruşi consideră că influenţarea voinţei, emoţiilor, comportamentului, psihologiei şi moralei adversarului joacă un rol fundamental în luptă. Valeriy A. Kiselev, ”For What Kinds of Conflict Should the Armed

Forces of Russia Prepare?”, Military Thought, nr. 3 (2017): 37, citat în Lt. Col. Timothy L. Thomas, ”Russian Forecasts of Future War”, *Military Review*, Army University Press, mai-iunie 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accesat la 2 iulie 2019.

29 Attila Juhász, Patrik Szicherle, *op.cit*., p. 7.

30 *Ibidem.*

31 ”Action plan against desinformation. Report on progress”, *EUvs Disinfo*, Comisia Europeană, iunie 2019, https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf, p. 2, accesat la 1 iulie 2019,.

32 *Ibidem.*

33 Claire Wardle, ”Fake News. It’s complicated”, 16 februarie 2017, First Draft, https://firstdraftnews.org/fake-news-complicated/, accesat la 17 mai 2019.

34 ”The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign”, *op.cit*.

35 ”More Swedish Women Haunted by Fears of Rape”, *Sputnik*, 11 ianuarie 2017, https://sputniknews.com/europe/201701111049464215-swedish-women-rape-fears/, accesat la 23 martie 2019.

36 *Ibidem.*

37 ”Reality Check: Is Malmö the «rape capital» of Europe?”, 24 februarie 2017, *BBC*, https://www.bbc.com/news/uk-politics-39056786, accesat la 14 februarie 2019.

38 Attila Juhász, Patrik Szicherle, *op.cit*., p. 12; „Reality Check: Is Malmo the ‘rape capital’ of Europe?”, *op.cit*.

39 ”Reality Check: Is Malmo the «rape capital» of Europe?”, *op.cit.*

40 ”Anti-Muslim online surges driven by fake accounts”, *The Guardian*, 26 noiembrie 2017, https://www.theguardian.com/media/2017/nov/26/anti-muslim-online-bots-fake-acounts, accesat la 10 aprilie 2019.

41 ”Fake Russian Story Stokes Anti-Immigrant Fears”, *StopFake*, 8 februarie 2018, https://www.stopfake.org/en/fake-russian-story-stokes-anti-immigrant-fears/, accesat la 15 decembrie 2018.

42 *Ibidem.*

43 Jakub Janda, ”The Lisa Case: STRATCOM Lessons for European states“, *Security Policy Working Paper*, No. 11/2016, Academia Federală pentru Politica de Securitate, https://www.baks.bund.de/de/node/1577, accesat la 23 mai 2019.

44 ”Putin-Kritik an Österreich: Schuldgefühl Migranten gegenüber”, *Die Presse*, 2 noiembrie 2016, https://diepresse.com/home/ausland/aussenpolitik/5111245/PutinKritik-an-Oesterreich_Schuldgefuehl-Migranten-gegenueber, accesat la 23 ianuarie 2019.

45 *Ibidem.*

## BIBLIOGRAFIE


Conley H., Mina J., Stefanov R., Vladimirov M., *”The Kremlin Playbook. Understanding Russian Influence in Central and Eastern Europe”,* CSIS Europe Program CSD Economic Program, octombrie 2016.

Egelhofer Jana Laura, Lecheler Sophie, ”Fake news as a two-dimensional phenomenon: a framework and research agenda”, *Annals of the International Communication Association*, 43:2, 97-116, online DOI: 10.1080/23808985.2019.1602782

Greenhill Kelly M., ”Migration as a Weapon in Theory and in Practice”, *Military Review*, noiembrie/decembrie 2016, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2016/

Greenhill Kelly M., ”Strategic Engineered Migration as a Weapon of War”, Civil Wars, vol. 10, nr. 1, 2008, DOI: 10.1080/13698240701835425

Janda Jakub, ”The Lisa Case: STRATCOM Lessons for European states“, *Security Policy Working Paper*, No. 11/2016, Academia Federală pentru Politica de Securitate, https://www.baks.bund.de/de/node/1577

Jayamaha Buddhika B., Matisek Jahara, ”Social Media Warriors:Leveraging a New Battlespace”, *Parametres*, vol. 48, nr. 4, Army War College, 2018-2019.

Juhász Attila, Szicherle Patrik, ”The political effects of migration-related fake news, disinformation and conspiracy theories in Europe”, Fundaţia Friedrich Ebert şi Political Capital Policy Research and Consulting Institute, 2017, https://www.politicalcapital.hu/pc-admin/source/documents/FES_PC_FakeNewsMigrationStudy_EN_20170607.pdf

McGeehan Timothy P., ”Countering Russian Disinformation”, *Parameters,* 48(1), Army War College, 2018, https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf

Seib Philp, ”Effects of Real-Time News Coverage on Foreign Policy”, *Journal of Conflict Studies*, volum XX, nr. 1, 2000, https://journals.lib.unb.ca/index.php/jcs/article/view/4309/4920

Thomas Timothy L., ”Russian Forecasts of Future War”, *Military Review*, Army University Press, mai-iunie 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/

Tandoc Jr. Edson C., Lim Yheng Wei, Ling Richard, ”Defining Fake News”, *Digital Journalism*, *6*(2), online DOI:10.1080/ 21670811.2017.1360143

Van Herpen Marcel H., ”Putin’s Propaganda Machine: Soft Power and Russian Foreign Policy”, Rowman & Littlefield, Lanham Maryland, SUA, 2015.

Wardle Claire, ”Fake News. It’s complicated”, 16 februarie 2017, First Draft, https://firstdraftnews.org/fake-news-complicated/

”Shoigu: Information becomes another armed forces component”, *Interfax*, 28 martie 2015, http://www.interfax.com/newsinf.asp?id=581851

”More Swedish Women Haunted by Fears of Rape”, *Sputnik*, 11 ianuarie 2017, https://sputniknews.com/europe/201701111049464215-swedish-women-rape-fears/

”Reality Check: Is Malmö the «rape capital» of Europe?”, 24 februarie 2017, *BBC*, https://www.bbc.com/news/uk-politics-39056786

”Anti-Muslim online surges driven by fake accounts”, *The Guardian*, 26 noiembrie 2017, https://www.theguardian.com/media/2017/nov/26/anti-muslim-online-bots-fake-acounts

”Fake Russian Story Stokes Anti-Immigrant Fears”, *StopFake*, 8 februarie 2018, https://www.stopfake.org/en/fake-russian-story-stokes-anti-immigrant-fears/

”Putin-Kritik an Österreich: Schuldgefühl Migranten gegenüber”, *Die Presse*, 2 noiembrie 2016, https://diepresse.com/home/ausland/aussenpolitik/5111245/PutinKritik-an-Oesterreich_Schuldgefuehl-Migranten-gegenueber

http://frontex.europa.eu

http://ec.europa.eu

http://europarl.europa.eu

http://euvsdisinfo.eu

http:// stopfake.org

# FIZIONOMIA OPERAŢIEI ÎNTRUNITE MULTINAȚIONALE

## *PHYSIOGNOMY OF JOINT MULTINATIONAL OPERATIONS*

## *LA PHYSIONOMIE DE L'OPÉRATION INTÉGRÉE MULTINATIONALE*

**Lt.col.conf.univ.dr. Alexandru HERCIU***

Doctrina pentru operaţiile întrunite multinaţionale stabileşte ansamblul noţiunilor şi principiilor de întrebuinţare a forţelor armate ale României în operaţiile întrunite multinaţionale. Această doctrină prezintă operaţiile multinaţionale la care România poate participa în cadrul unei alianţe, coaliţii sau altor angajamente convenite şi evidenţiază structurile organizatorice întrunite, necesare coordonării operaţiilor de securitate (apărare) colectivă terestre, aeriene, maritime şi speciale, într-un mediu multinaţional.

În acest context, articolul își propune să analizeze caracteristicile și fizionomia operațiilor întrunite multinaționale, unde forțele care aparțin Armatei României pot participa în context de alianță sau de coaliții de voință, din perspectiva specificității mediului operațional actual.

*In general, the doctrine for joint multinational operations establishes the set of notions and principles of the use of the Romanian armed forces in the joint multinational operations. It presents the multinational operations to which Romania can participate in an alliance, coalitions or other agreed commitments and highlights the joint organizational formations needed to coordinate land, air, maritime and special joint security operations (defense) in a multinational environment.*

*In this context, the present paper aims to analyze the characteristics and physiognomy of the joint multinational operations in which forces belonging to the Romanian Army can participate in the context of alliance or coalitions of will, given the specificity of the current operational environment.*

*La doctrine des opérations intégrées multinationales envisage l'ensemble des concepts et des principes sur l'utilisation des forces armées roumaines dans des opérations multinationales conjointes. La doctrine présente les opérations multinationales auxquelles la Roumanie peuvent prendre part dans le cadre d'une alliance, d'une coalition ou d'autres engagements convenus, et met en évidence les structures organisationnelles conjointes nécessaires pour la coordination des opérations intégrées de sécurité (de défense) terrestres, aériennes, maritimes et de sécurité spéciale, dans un environnement multinational.*

*Ainsi, le présent article vise à analyser les caractéristiques et la physionomie des opérations intégrées multinationales auxquelles les forces de l'armée roumaine peuvent participer dans le cadre d'une alliance ou des coalitions, vu la spécificité de l'environnement opérationnel actuel.*

**Cuvinte-cheie:** operații întrunite; operații multinaționale.
***Keywords:*** *joint operations; multinational operations.*
***Mots-clés:*** *opérations intégrées; opérations multinationales.*

Realitatea evidențiată de conflictele recente demonstrează faptul că, în actualul mediu de securitate, operaţiile militare au caracter întrunit şi multinaţional, iar acţiunile convenţionale se întrepătrund cu cele neconvenţionale şi asimetrice. Indiferent că vorbim despre adversari de tipul actorilor statali, actorilor nonstatali, sau despre o combinaţie între aceştia, într-un eventual conflict de tip hibrid aceştia vor utiliza o paletă largă de acţiuni asimetrice pentru a exploata vulnerabilităţile oponentului. În această categorie sunt incluse acţiunile teroriste, insurgente, separatiste şi ale criminalităţii organizate, ca parte a unei mixturi dinamice şi diversificate, sintetizată de către

***Universitatea Națională de Apărare „Carol I”***
e-mail: *herciu_alexandru12@yahoo.ro*

analiştii fenomenului militar în conceptul „conflict hibrid”.

Angajarea capabilităţilor specifice fiecărui tip de operaţii se va produce sub influenţa unui set de factori, condiţii, conjuncturi şi presiuni particulare care definesc mediul de securitate actual. Acesta cuprinde beligeranţii şi actorii neutri, mediul fizic şi mediul informaţional (virtual).

## Aspecte teoretice privind operaţia întrunită multinaţională

*Operaţia militară*

*Operaţia militară* poate fi definită ca reprezentând totalitatea acţiunilor de luptă duse de către structurile militare în vederea îndeplinirii unor scopuri, la diferite niveluri ale artei militare: tactic, operativ sau strategic. Preluând definiţia din *AAP-6, Glosarul de termeni şi definiţii NATO*, prevederile doctrinare româneşti definesc operaţia ca fiind o „acţiune militară sau procesul de executare a unei misiuni strategice, tactice, specifice unei categorii de forţe, administrative, de antrenament sau de serviciu; procesul de ducere a unei lupte, incluzând mişcarea, susţinerea, atacul, apărarea şi manevrele necesare pentru a îndeplini obiectivele unei bătălii, operaţii sau campanii[1].

Unele publicaţii mai vechi precizează faptul că operaţia reprezintă totalitatea acţiunilor de luptă duse de către mari unităţi operative și tactice după un plan unic în vederea îndeplinirii unui scop operativ sau strategic şi se compune, de regulă, dintr-un şir de lupte, coordonate în timp şi spaţiu, în baza unei concepţii unitare[2].

*Operaţia întrunită*

Adjectivul „întrunit” este utilizat pentru a descrie cadrul coordonat în care se desfăşoară activităţile militare, unde sunt implicate cel puţin două arme, componente sau categorii de forţe cu destinaţie diferită.

*Operaţia întrunită* este definită ca fiind „totalitatea acţiunilor terestre, aeriene şi maritime duse de o grupare constituită din forţe sau elemente și mijloace aparţinând mai multor categorii de forţe ale armatei, în mediul corespunzător specific fiecăreia dintre ele, într-o zonă geografică determinată, într-o concepţie unitară şi sub comandă unică, exercitată de un comandament operaţional întrunit în scopul îndeplinirii unor obiective strategice”[3].

O definire mai cuprinzătoare a operaţiei întrunite stipulează faptul că, în cadrul acesteia, efortul se concentrează pentru sincronizarea forţelor şi capabilităţilor asigurate de componenta „terestră, navală, aeriană, spaţiu, spaţiul cibernetic, operaţiile speciale şi alte forţe funcţionale”[4], una/unele dintre acestea putând să predomine într-o anumită etapă a operaţiei.

Această definiţie este mai cuprinzătoare, deoarece nu se limitează doar la caracterul fizic al acţiunii, ci ia în calcul și alte componente participante la operaţie, cum ar fi cea informaţională.

În consecinţă, consider că procesul de analiză a operaţiei întrunite nu se poate realiza decât în contextul înţelegerii noii fizionomii a conflictelor militare moderne, care presupune desfăşurarea lor într-un mediu operaţional extins – în care mediul social este o componentă de bază – şi include o componentă informaţională extrem de activă.

În aceste condiţii, acţiunile desfăşurate presupun implicarea integrată şi întrunită a tuturor categoriilor de forţe care se intersectează, se suprapun, se completează reciproc şi se intercondiţionează dimensional, informaţional şi acţional, precum și cu celelalte entităţi sociale participante la operaţie.

Operaţia întrunită se execută într-o perioadă determinată de timp, în limitele fizice ale unei zone geografice, denumită zona de operaţii întrunită (ZOI), în care comandantul forţei întrunite planifică şi execută o misiune la nivel operativ[5].

Publicaţiile militare de referinţă[6] includ forţele pentru operaţii speciale (FOS) ca fiind una dintre componentele operaţiei întrunite.

Prin urmare, componentele operaţiei întrunite sunt: componenta terestră, componenta aeriană, componenta navală și componenta pentru operaţii speciale.

Operaţia întrunită are caracter preponderent ofensiv și este îndreptată spre centrele de greutate la nivel strategic şi operativ ale adversarului. Sincronizarea şi coordonarea forţelor şi activităţilor în cadrul operaţiei întrunite se asigură permanent în cadrul procesului operaţiilor, pe timpul planificării, pregătirii, execuţiei și evaluării acesteia.

În contextul dat, succesul operaţiilor militare are la bază efortul conjugat al tuturor componentelor forţei (componenta terestră, componenta aeriană, componenta navală și componenta pentru operaţii speciale sau pe efortul întrunit a cel puţin două dintre acestea) sub un singur comandant, structură

pregătită pentru angajarea într-o operaţie de tip hibrid.

*Operaţia integrată*

Operaţia integrată este acţiunea militară în care sunt angajate în mod coordonat structuri civile și militare cu roluri şi poziţii dintre cele mai diferite, care pot contribui, prin implicarea în domeniul specific de activitate, la soluţionarea conflictului și la atingerea scopurilor operaţiei militare. Prin urmare, acţiunea integrată presupune, în opinia mea, o conjugare a efortului individual al entităţilor pentru realizarea unui scop comun, rezultat din asamblarea finalităţilor proprii.

Acest fapt impune, în primul rând, o identificare a tuturor actorilor care acționează în mediul operaţional de securitate, a motivaţiilor/intereselor, a influenţelor și a resurselor fiecăruia dintre aceştia şi coagularea forţelor care prezintă interes pentru acţiunea proprie. Aceşti actori pot fi: forţe militare convenţionale; forţe militare neconvenţionale; oponenţi asimetrici, neutri sau indecişi; organisme internaţionale; organizaţii internaţionale (OI); organizaţii neguvernamentale (ONG); instituţii şi autorităţi locale și naţionale; mass-media; agenţi economici; societăţi de securitate private; populaţia civilă.

În al doilea rând, procesul de integrare presupune o abordare diferită a fiecărui actor în parte şi găsirea unei modalităţi adecvate de interfaţare între forţa întrunită multinaţională care operează în teatrul de operaţii și acesta. Acest fapt poate constitui o importantă provocare pentru comandantul forţei întrunite multinaţionale, situaţie care poate fi depășită prin cunoaşterea foarte bună a tuturor actorilor, a relaţiilor dintre aceştia și prin fructificarea abilităţilor de comunicare și negociere. În plus, integrarea solicită din partea acestuia activităţi de mediere și armonizare a relaţiilor dintre anumiţi actori, care pot manifesta adversităţi în planul relaţiilor interpersonale, dar care sunt deopotrivă benefici scopului militar.

Nu în ultimul rând, consider că procesul de integrare este unul continuu, dinamic care trebuie avut în vedere în toate etapele conflictului, înainte de declanşarea confruntării armate, pe timpul operaţiilor militare şi după stingerea acestora, în strânsă corelaţie cu evoluţia mediului operaţional de securitate. Un alt element demn de remarcat este acela că operaţiile militare au căpătat un aspect întrunit de-a lungul întregului spectru al conflictului şi la toate nivelurile la care se desfăşoară.

Procesul de integrare trebuie înţeles şi abordat în toate planurile sale de manifestare: structural, cognitiv, acţional şi logistic. Astfel, organizaţiile, înţelegerea comună corectă a realităţii, activităţile desfăşurate și resursele puse la dispoziţie și utilizate în comun vor putea fi canalizate, pe baza design-ului operaţional conturat, în sensul îndeplinirii scopurilor operaţiei.

*Operaţia multinaţională*

Astăzi, majoritatea operaţiilor militare se desfăşoară în cadru multinaţional, datorită necesităţii vizibilităţii consensului politic şi dobândirii legitimităţii acţiunii militare. Cooperarea în cadrul operaţiei multinaţionale se realizează atât cu membri şi parteneri tradiţionali în cadrul alianţelor, cât şi cu alţii mai puţin familiari, forţe în cadrul coaliţiilor de state[7].

Operaţia multinaţională este operaţia militară în care sunt implicate forţe din cel puţin două naţiuni, care acţionează împreună pentru îndeplinirea unei misiuni. Adjectivul „multinaţional” este utilizat pentru a desemna atât participarea elementelor naţionale la constituirea forţei, cât şi angajarea acestora în activităţi şi operaţii. În cadrul NATO, pentru operaţia multinaţională se acceptă atât sintagma „forţa combinată” (”combined force”), cât și forţa „multinaţională combinată” (”multinational combined force”), pentru a descrie o operaţie desfăşurată de către o forţă compusă din două sau mai multe naţiuni care acţionează împreună şi din care fac parte elemente din cel puţin două categorii de forţe ale armatei[8].

**Caracteristicile operaţiei întrunite desfăşurate în context multinaţional**

„Structurile militare ale viitorului vor fi concepute și antrenate pentru a desfăşura acţiuni militare complexe, în context întrunit, de foarte multe ori cu o structură multinaţională, modulară, care poate fi adaptată în timp scurt la misiune şi la condiţiile concrete de manifestare”[9].

Conceptul de *operaţie întrunită* nu este cu totul nou pentru teoria și practica militară românească. Cunoscut, în ultimele decenii, sub denumirea de „bătălia aeroterestră”, acest concept a fost studiat doar din punctul de vedere al apărătorului, respectiv al părţii care trebuia să contracareze

o acţiune militară întrunită. Aplicaţiile de nivel operativ și strategic desfăşurate în armata română, în ultimii douăzeci de ani, au constituit un model în această privinţă, reglementările în vigoare obligând eşaloanele de concepţie sau de execuţie la crearea unui cadru tactic, operativ sau strategic complex, în care acţiunile planificate, indiferent de armă sau de categoria de forţe participante, trebuiau integrate.

Din punct de vedere istoric, acţiunile desfăşurate în comun de două sau mai multe categorii de forţe au avut loc încă de la prima diviziune a armatelor (infanteria şi cavaleria), la care s-au adăugat, mai târziu, artileria şi navele de luptă. Dar ele au reprezentat acţiuni militare complementare sau de sprijin reciproc, și nu acţiuni militare de tip *joint*.

Două evenimente au precedat punerea oficială în discuţie a conceptului de acţiuni militare tip *joint*.

Primul a fost *războiul din Falkland/Malvine*, din 1982, în care forţele militare regale britanice moderne au avut de confruntat armata argentiniană mai greoaie, dar având imensul avantaj al terenului de partea sa. Lipsa de protecţie aeriană a convoaielor britanice de către RAF a produs numeroase pierderi umane și de echipament și s-a constituit, cu rapiditate, într-un factor aproape destabilizator.

Al doilea exemplu l-a reprezentat *misiunea de salvare americană din Grenada*, din 1983, în care incompatibilitatea mijloacelor de comunicaţii, procedurilor de luptă şi chiar a hărţilor a slăbit intensitatea operaţiilor aeriene desfăşurate. Ca rezultat al lecţiilor desprinse în urma acestor conflicte, în 1986 Congresul american a aprobat aşa-numitul *Act Goldwater-Nichols*, care a reprezentat piatra de temelie a viitoarei integrări a categoriilor de forţe americane şi crearea *USJCOM*, la 7 octombrie 1999.

Urmând modelul american, în acelaşi an Guvernul britanic a aprobat constituirea unui comandament permanent de tip *joint la nivel strategic (PJHQ)* și transformarea colegiilor militare ale categoriilor de forţe într-un singur *colegiu militar de stat major tip joint (JSCSC)*[10].

Din analiza semantică a sintagmei „caracter integrat”, prin asocierea înţelesului celor două noţiuni rezultă că aceasta reprezintă o trăsătură distinctivă, care constituie specificul unei acţiuni militare „armonizate într-un tot”[11]. Altfel spus, caracterul integrat al acţiunilor militare exprimă gradul de armonizare și de sincronizare a tuturor elementelor care compun un sistem acţional de tipul luptă, bătălie, operaţie, campanie, înţelegând prin aceasta toate forţele şi mijloacele, indiferent de genul de armă şi de categoria de forţe din care fac parte, participante la acţiunile menţionate.

Caracterul integrat al acţiunilor militare constituie o trăsătură a operaţiilor, a cărei apariţie a fost determinată de multiplicarea cuplurilor acţionale care o compun, fiind o consecinţă firească a creşterii numărului de genuri de armă şi a organizării armatelor moderne pe categorii de forţe ale armatei. Totodată, această caracteristică reprezintă o consecinţă normală a evoluţiei fenomenului război, care, ca urmare a dezvoltării ştiinţei şi tehnicii, a crescut permanent în complexitate, rezultând o continuă amplificare a conexiunilor dintre elementele componente.

Operaţiile întrunite sunt inevitabil componente importante (campanii, bătălii sau operaţii) ale războiului, ştiut fiind faptul că războiul are o arie foarte extinsă, depăşind cu mult sfera confruntărilor violente. Astfel, apariţia conceptului de *operaţie întrunită* este o consecinţă a procesului evolutiv-istoric al artei militare. Accepţiunea actuală a sintagmei *operaţie întrunită* înglobează aspectele multiple şi complexe ale acesteia, definind, în principiu, suma acţiunilor militare, şi nu numai, desfăşurate la nivel operativ, strategic şi tactic, din compunerea mai multor categorii de forţe ale armatelor moderne, sub o conducere unică, după o concepţie unitară şi având un obiectiv/misiune unic.

Procedând la o translaţie a problematicii din domeniul teoriei în cel al practicii, este de remarcat faptul că acest caracter integrat a implicat o sporire considerabilă a importanţei cooperării dintre forţele participante la acţiunile militare integrate, pentru îndeplinirea scopului operaţiei. Ca urmare, în conţinutul regulamentelor de luptă proprii fiecărui gen de armă şi categorie de forţe ale armatei au început să apară prevederi privind modalităţile, formele şi procedeele concrete de cooperare în vederea îndeplinirii în comun a unor misiuni de luptă.

Necesitatea interconectării modului specific de îndeplinire a misiunilor proprii cu cel caracteristic celorlalte arme a apărut nu numai în interiorul unei categorii de forţe, care, de regulă, duce acţiuni în acelaşi mediu şi împotriva aceluiaşi adversar, ci şi între genuri de armă aparţinând diferitelor categorii de forţe ale armatei.

De aceeaşi manieră poate fi analizat şi caracterul intercategorii de forţe ale armatei al acţiunilor

militare moderne, trăsătură care exprimă relaţiile funcţionale dintre cel puţin două categorii de forţe în cadrul operaţiilor care pot fi de nivel strategic, dar şi operativ.

În cadrul eşaloanelor strategice, caracterul interarme al acţiunilor este aproape implicit, datorită participării, de regulă, a mai multor categorii de forţe ale armatei şi, prin urmare, a genurilor de armă care le compun.

În acelaşi context, caracterul integrat, intercategorii de forţe ale armatei se manifestă, în principal, în cadrul operaţiilor strategice, dar nu trebuie exclusă posibilitatea materializării sale şi la nivel operativ, ca de pildă în cazul constituirii unor grupări operaţionale, formate din mari unităţi şi unităţi tactice sau/şi operative aparţinând mai multor categorii de forţe ale armatei.

Adâncind analiza, caracterul integrat interarme şi intercategorii de forţe ale armatei poate fi pus în evidenţă şi va trebui realizat în toate etapele pregătirii şi ducerii acţiunilor militare. Astfel, pe timpul pregătirii acţiunilor militare, realizarea caracterului integrat interarme şi intercategorii de forţe are o însemnătate deosebită şi trebuie să se regăsească în fiecare dintre activităţile care se desfăşoară la nivelul comandamentelor. Ca atare, elaborarea concepţiei de întrebuinţare în operaţie, dimensionarea forţelor, realizarea dispozitivelor etc. trebuie să pornească de la o analiză temeinică a misiunilor, a adversarului, a spaţiului şi a timpului avut la dispoziţie.

Pe această bază, în etapa analizată trebuie să se realizeze o corelare şi o interconectare a misiunilor, în raport cu posibilităţile forţelor şi mijloacelor avute la dispoziţie şi pe baza caracterului complementar al acţiunilor diferitelor genuri de armă şi de categorii de forţe participante.

Finalitatea acestor preocupări o va constitui focalizarea eforturilor, în vederea îndeplinirii scopurilor operaţiei întrunite, prin punerea în valoare a tuturor elementelor care conferă caracter unitar luptei armate, în general. Toate aceste elemente de concepţie vor fi materializate într-un plan al operaţiei unic şi unitar, pe baza căruia se emit ordine şi dispoziţii pentru toate structurile subordonate.

Important de menţionat este şi faptul că, într-o concepţie integratoare asemănătoare, vor fi rezolvate şi problemele de logistică, detaliate într-un plan unic, chiar dacă responsabilităţile asigurării materiale vor aparţine în continuare altor structuri neangajate nemijlocit în acţiunile militare. O sincronizare şi o interconectare reale, complementaritatea şi sinergia acţiunilor militare se vor manifesta, îndeosebi, pe timpul ducerii operaţiilor întrunite.

Armonizarea eforturilor tuturor marilor unităţi şi unităţilor participante, în scopul îndeplinirii obiectivelor operaţiilor întrunite, se va realiza prin conducerea unică a acţiunilor şi prin coordonarea permanentă a acestora. Baza realizării acestui deziderat, care conferă caracterul integrat interarme şi intercategorii de forţe ale armatei, o va constitui organizarea şi menţinerea unei permanente cooperări.

*Operaţia întrunită* reprezintă un ansamblu de acțiuni militare, duse concomitent pe uscat, în aer, uneori, și pe mare (fluviu), pe mare adâncime și pe front larg, de către grupări de forțe întrunite cu rol operativ, pregătite și desfășurate în baza unei concepții unitare și a unui plan unic, în una sau mai multe zone de operații care includ obiective de importanță politică, economică și militară, a căror menținere sau eliberare permite realizarea unor scopuri parțiale ale războiului. Operațiile întrunite desfășurate de forțele militare sunt planificate și executate pe trei niveluri: strategic, operativ și tactic.

În concepţia unor armate străine, ulterior preluată și de doctrinele românești în vigoare, scopul desfăşurării cu succes a operaţiei întrunite urmăreşte cu consecvenţă „... angajarea și lovirea simultană a inamicului pe întreaga adâncime a spaţiului de luptă, astfel încât dispozitivul de luptă advers să fie blocat şi, în consecinţă, reacţiile acestuia să fie încetinite, desincronizate și, în final, paralizate, creându-se astfel condiţiile necesare pentru continuarea cu succes a acţiunilor ofensive viitoare”[12].

Acțiunile întrunite actuale necesită o doctrină corespunzătoare și forțe capabile, care să acționeze împreună, întrunit și integrat, care să se completeze și să se sprijine reciproc în toate fazele angajării și desfășurării luptei. Pentru a putea să conducă o forță întrunită capabilă să acționeze în timp scurt, comandantul comandamentului forței trebuie să aibă la dispoziție un suport tehnic corespunzător, adaptat tipului de operație și cerințelor spațiului de luptă modern. Fără un sistem integrat de comandă, control, comunicații și informatică, capabil să

integreze fluxul informaţional şi să asiste statul major în elaborarea deciziei, nu se vor putea crea condiţiile optime organizării şi funcţionării unui comandament întrunit.

Un răspuns satisfăcător pentru rezolvarea unor situaţii de criză poate fi oferit de intervenţia comunităţii internaţionale prin mijloace politice, diplomatice şi economice. Folosirea instrumentelor militare în cadrul operaţiilor întrunite multinaţionale este o ultimă soluţie. Acţiunea integrată a forţelor în operaţiile întrunite multinaţionale este rezultatul constituirii unor alianţe sau coaliţii între naţiuni, care asigură cadrul necesar îndeplinirii scopurilor şi obiectivelor comune, având în vedere realităţile diplomatice, constrângerile, limitările şi obiectivele ţărilor membre, ale celor participante sau contributive.

Alianţa este o înţelegere, încheiată pe baza unor acorduri oficiale între două sau mai multe state, cu obiective politice şi militare pe termen mediu şi lung, care urmăreşte realizarea unor interese şi scopuri comune, precum şi promovarea valorilor naţionale ale membrilor săi.

Coaliţia reprezintă un aranjament politic şi militar ad-hoc între două sau mai multe state în vederea desfăşurării unor acţiuni comune. În coaliţie, acţiunea multinaţională are loc în afara legăturilor stabilite în cadrul alianţei şi se referă la situaţii unice sau la o cooperare de durată într-un domeniu specific, unde există un interes comun.

Războiul de coaliţie presupune abordarea şi rezolvarea următoarelor probleme principale: crearea unei forţe militare multinaţionale întrunite, sub egida naţiunii conducătoare; constituirea organelor de conducere multinaţionale; coordonarea eforturilor politice, economice, militare, tehnico-ştiinţifice, realizarea compatibilităţii logistice şi dezvoltarea infrastructurii.

*Operaţiile întrunite multinaţionale* sunt acele acţiuni militare la care participă două sau mai multe state cu forţe militare de mărimi diferite aparţinând mai multor categorii de forţe ale armatei, aflate sub control politic şi comandă unică şi pentru care a fost stabilit un obiectiv unic.

*Multinaţionalitatea* reflectă necesitatea politică de a căuta consensul internaţional şi legitimitatea acţiunilor militare[13]. NATO trebuie să fie întotdeauna pregătită să conlucreze cu membrii şi partenerii tradiţionali, dar şi cu alte forţe, mai puţin familiare, în coaliţii. Încrederea reciprocă este esenţială când se lucrează în mediul multinaţional.

Scopul fundamental al unei operaţii multinaţionale este *de a direcţiona efortul militar pentru atingerea obiectivului comun.* Operaţiile multinaţionale sunt unice. Fiecare comandant naţional este responsabil în faţa comandantului forţei multinaţionale, în faţa lanţului său naţional de comandă şi, nu în ultimul rând, este responsabil pentru îndeplinirea misiunii încredinţate [14].

În cadrul NATO, operaţiile întrunite multinaţionale *(Multinational Combined Joint Operations)* sunt acele operaţii la care participă forţe armate din două sau mai multe ţări şi la care iau parte cel puţin două categorii de forţe armate. Conceptul de *Operaţie Aliată Întrunită* (Allied Joint Operation) se referă la operaţiile la care participă forţele aparţinând numai ţărilor membre ale NATO[15].

La astfel de operaţii pot participa următoarele tipuri de forţe armate:

- forţele comandate (Command Forces) – acele forţe care se află încă în timp de pace sub comandă operaţională (Operational Command) sau sub control operaţional (Operational Control) NATO;
- forţele subordonate operativ (Assigned Forces) – prevăzute pentru acţiuni sub controlul NATO;
- forţele care sunt prevăzute pentru acţiuni viitoare sub comandă NATO (Earmarked Forces) – vor întări forţele angajate iniţial. Pentru desfăşurarea acestor operaţii, NATO utilizează diferite modele pentru organizarea unităţilor multinaţionale.

În Doctrina NATO, operaţiile militare multinaţionale desfăşurate pe timp de război sunt considerate *operaţiile întrunite multinaţionale pentru apărarea colectivă*, conform *articolului 5* din *Tratatul Atlanticului de Nord*, iar cele desfăşurate *pe timp de pace* sunt considerate *operaţiile în sprijinul păcii sub egida ONU/OSCE şi conduse nemijlocit de către acestea* împreună cu *operaţiile non-articolul 5, de răspuns la crize, conduse de NATO sub mandat ONU/OSCE.*

Acţiunea conjugată a forţelor în operaţiile întrunite multinaţionale este rezultatul constituirii unor alianţe sau coaliţii între naţiuni, care asigură cadrul necesar îndeplinirii scopurilor şi obiectivelor comune, ţinând cont de realităţile diplomatice, de constrângerile, de limitările şi de obiectivele ţărilor membre, ale celor participante sau contributive[16].

În situaţia în care acţiunile militare se vor desfăşura împreună cu forţele aliate, în cadrul unor operaţii întrunite multinaţionale, eficienţa cooperării marilor unităţi (unităţilor) Armatei României cu acestea este dependentă de o serie de factori, dintre care cei mai importanţi îi considerăm a fi: scopurile urmărite de către fiecare membru al alianţei (coaliţiei); doctrina de luptă; nivelul de instruire; interoperabilitatea tehnicii, a mijloacelor de lovire și a altor echipamente; deosebirile culturale; limbajul; încrederea reciprocă; lucrul în echipă.

În cadrul cooperării cu forţele aliate, scopurile naţionale pot fi armonizate pe baza unei strategii comune, întrucât, dacă sunt exprimate într-un mod foarte tranşant de către fiecare membru, fără a se face concesii, atunci, în loc ca acestea să le unească și să contribuie la coeziunea coaliţiei, vor scoate în evidenţă deosebirile de interese. Caracterul comun al scopurilor urmărite asigură funcţionalitatea coaliţiei, deoarece, punând accentul pe elementele comune, se pot reduce disfuncţionalităţile, menţinând-o operaţională.

Pe lângă scopurile comune urmărite în operaţiile întrunite multinaţionale, una dintre problemele fundamentale care dau conţinut cooperării cu forţele aliate o constituie compatibilitatea doctrinelor de luptă a trupelor române cu cele ale partenerilor. Compatibilitatea despre care aminteam va trebui realizată în cadrul tuturor sistemelor de operare funcţionale ale acţiunilor militare (funcţiilor de luptă), și anume: cercetarea, manevra, sprijinul reciproc cu foc, protecţia forţelor, logistica și conducerea forţelor.

Realizarea unei compatibilităţi între doctrinele de luptă ale forţelor române și cele ale trupelor aliate are o importanţă vitală pentru fizionomia şi deznodământul operaţiilor, influenţând alegerea formelor şi procedurilor de luptă adoptate de parteneri, scopurile propuse în cadrul acţiunilor comune și echilibrul acţional al forţelor. Dacă nu s-ar ţine cont de aceste aspecte, acţiunile ansamblului forţelor ar putea fi prejudiciate de apariţia unor dezechilibre şi fracturi, operaţiile suferind, în mod evident, de incompatibilitate în plan conceptual și acţional. Totodată, trebuie avut în vedere că nu toate deosebirile dintre doctrinele de luptă au determinare subiectivă, datorată diferenţierilor existente în înzestrarea cu armament și tehnică de luptă.

Eliminarea consecinţelor nefavorabile, cauzate de diferenţierile existente între doctrinele de luptă, s-ar putea realiza prin: sprijinul acordat partenerului mai slab înzestrat, pentru ca marile sale unităţi să fie aduse, din punctul de vedere al capacităţii combative, la un nivel cât mai apropiat de cel al partenerului cel mai puternic; încredinţarea diferenţiată a responsabilităţilor şi a misiunilor între aliaţi, în funcţie de capacităţile operaţionale reale ale fiecăruia dintre ei.

Alături de compatibilitatea doctrinelor de luptă, unul dintre factorii care contribuie la reuşita operaţiilor combinate îl considerăm a fi nivelul relativ apropiat al instruirii forţelor angajate şi al celor aliate. Acesta va fi influenţat de gradul de profesionalizare a forţelor partenerilor, de compatibilitatea doctrinelor de instrucţie, de gradul de integrare a sistemelor de instruire și de nivelul tehnic al dotării specifice.

Atingerea scopurilor urmărite în acţiunile militare, duse în cooperare cu forţe aliate, și realizarea compatibilităţii doctrinelor de luptă sunt, în general, dependente de interoperabilitatea tehnicii, a mijloacelor de lovire și a diferitelor echipamente folosite. Comandantul grupării multinaţionale de forţe constituite va avea de rezolvat problemele datorate diferenţelor inevitabile dintre sistemele de armament, tehnică și echipamente, utilizate de forţele participante la acţiunile comune duse împotriva agresorului. Acestea sunt mult mai mari în acţiunile declanșate în cooperare cu alte forţe, într-o coaliţie realizată ad-hoc; dar chiar și în cadrul grupărilor de forţe, realizate de o alianţă deja constituită, cu caracter permanent, rămâne totuşi un număr mare de incompatibilităţi, care vor trebui depăşite.

**Concluzii**

În cadrul conflictelor de tip hibrid, sensul în ceea ce privește ponderea tipologiei acţiunilor, din perspectiva pericolelor, riscurilor și ameninţărilor care le determină, prezintă o deplasare de la cele regulate, tradiţionale spre cele neconvenţionale şi, mai cu seamă, către cele asimetrice, care tind să se generalizeze şi să se manifeste pe întreaga durată a conflictului şi în întreg spectrul său.

Acestea se vor exprima și în viitor prin acţiuni coordonate, în special în condiţii – în sens real şi figurat deopotrivă – de noapte și de vizibilitate redusă, fără o amprentă clară, distinctă, fapt care

va determina un ritm de luptă intens şi constant din partea forţei oponente. Pentru a realiza acest imperativ, aceasta se va constitui într-un conglomerat atent proporţionat de tipuri de structuri şi de forţe care să fie capabile să angajeze adversarul hibrid pe fiecare componentă a sa în mod distinct, dar în acelaşi timp coordonat, pentru a menţine continuitatea şi ritmul crescut al operaţiilor.

Din acest punct de vedere, forţele armate trebuie să fie pregătite să execute o gamă variată de misiuni în context întrunit şi multinaţional, în diferite regiuni şi într-un mediu operaţional complex, şi, în consecinţă, incert, unde se vor confrunta cu o diversitate de ameninţări hibride și de combinaţii simultane ale unor tipuri de activităţi care se vor schimba și se vor adapta în permanenţă.

Această realitate necesită anticiparea, identificarea şi înţelegerea obiectivelor unei mari varietăţi de actori cu rol în soluţionarea conflictului încă din faza de planificare a operaţiei întrunite, pentru a integra, a coordona şi a sincroniza efortul acestora.

Înţelegerea complexităţii mediului operaţional hibrid constituie o provocare majoră pentru comandantul și structura de comandă a grupării de forţe întrunite multinaţionale.

În contextul conflictului hibrid, operaţiile se execută prin acţiunea comună, integrată a componentelor categoriilor de forţe, a genurilor de arme şi specialităţi, într-un mediu operaţional complex în care operează o multitudine de entităţi – instituţii, autorităţi, organizaţii internaţionale, organizaţii neguvernamentale, naţiuni – care pot influenţa pozitiv sau negativ desfăşurarea operaţiilor militare.

**NOTE:**

1 *** *Doctrina Armatei României*, Bucureşti, 2012, Anexa nr. 1, p. 136.

2 *** *Lexicon militar*, Editura Militară, Bucureşti, 1980, p. 474.

3 *** *Doctrina Armatei României*, Bucureşti, 2012, *Anexa nr. 1*, p. 136.

4 *** *AJP-3(B), Allied Joint Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 2011, p. ix.

5 *** *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p. 2-J-1.

6 *** *AJP-3(B), Allied Joint Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 2011, pp. 1-10.

7 *Ibidem.*

8 *** *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p. 2-C-9, 2-M-10.

9 Gl.dr. Mircea Mureşan, gl.bg. (r) dr. Costică Ţenu, col. (r) dr. Lucian Stăncilă, *Operaţiile întrunite în războiul viitorului*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2005, p. 11.

10 http://www.Joint_Services_Command_and_Staff_College, accesat la 27 iulie, 2019.

11 *** *Dicţionarul explicativ al limbii române*, Editura Academiei Române, Bucureşti, 1984, p. 119.

12 *** AJP-3.2, *Allied Joint Doctrine for Land Operatios*, Edition A, Version 1, 2016, pp. 1-12, art. 0134.

13 *** AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, Edition C, Version 1, 2019, pp. 2-6.

14 *** JP 3-16, *Multinational Operations*, 2013, p. II-3.

15 *** AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, Edition C, Version 1, 2019, pp. 1-7.

16 *Ibidem*, p. 12.

## BIBLIOGRAFIE

*** *Dicţionarul explicativ al limbii române*, Editura Academiei Române, Bucureşti, 1984.

*** *Doctrina Armatei României*, Bucureşti, 2012.

*** *Lexicon militar*, Editura Militară, Bucureşti, 1980.

*** *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012.

***AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, Edition C, Version 1, 2019.

*** *AJP-3(B), Allied Joint Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 2011.

*** AJP-3.2, *Allied Joint Doctrine for Land Operatios*, Edition A, Version 1, 2016.

*** JP 3-16, *Multinational Operations*, 2013.

Gl.dr. Mureşan Mircea, gl.bg. (r) dr. Ţenu Costică, col. (r) dr. Stăncilă Lucian, *Operaţiile întrunite în războiul viitorului*, Editura Universităţii Naţionale de Apărre „Carol I”, Bucureşti, 2005.

http://www.Joint_Services_Command_and_Staff_College

# SECURITATEA SOCIETALĂ ÎN CONTEXTUL ACTUAL

## *SOCIETAL SECURITY IN THE CURRENT CONTEXT*

## *LA SÉCURITÉ SOCIÉTALE DANS LE CONTEXTE ACTUEL*

**Drd. Octavian Victor Mihail DIMA***

Pornind de la ideea că securitatea modernă nu mai este strict o problemă legată de amenințările de natură militară la adresa statului, Școala de la Copenhaga a dezvoltat un concept extins de securitate, bazat pe sectoare de securitate și pe teoria securitizării. În acest context, Școala a dezvoltat un sector special de securitate, numit securitate societală, care abordează capacitatea de conservare a unei societăți prin păstrarea identității, valorilor spirituale și caracterului său peren. Din această perspectivă, securitatea societății contemporane este subiectul unei varietăți de riscuri și amenințări, printre care cele datorate procesului de regionalizare și de integrare europeană ocupă un loc central. Acest articol are ca obiectiv central introducerea conceptului de securitate societală și analiza înțelesului său în contextul geopolitic european actual.

*Starting from the idea that modern security is no longer strictly a matter of state and military threats, the Copenhagen School has developed an extended security concept based on security sectors and securitization theory. In this context, it has developed a special security sector, called societal security, to address the conservation capacity of a society by preserving its identity, spiritual values and perennial character. From this perspective, contemporary societal security is the subject of a variety of risks and threats, among which those due to the process of regionalization and European integration occupy a central place. This article is focused on introducing the societal security concept and analyzing its mining in the current european geopolitical context.*

*L'École de Copenhague a développé, à partir de l'idée que la sécurité moderne n'était plus un domaine lié aux menaces strictement de nature militaire contre l'État, un vaste concept de sécurité basé sur des secteurs de sécurité et sur la théorie de la sécuritisation. Dans ce contexte, l'école a développé ainsi un secteur de sécurité spécial, nommé sécurité sociétale, qui traite la capacité de conservation de la société en préservant son identité, ses valeurs spirituelles et son caractère de pérennité. Là-dessus, la sécurité de la société contemporaine fait l'objet d'une série de risques et de menaces, dont ceux dus au processus de régionalisation et de l'intégration européenne occupent une place centrale. Cet article vise à introduire le concept de sécurité sociétale et à en analyser le sens dans le contexte géopolitique européen actuel.*

**Cuvinte-cheie:** securitate societală; identitate; sectoare de securitate.
***Keywords:*** *societal security; identity; security sectors.*
***Mots-clés:*** *sécurité sociétale; identité; secteur de sécurité.*

Securitatea societală este un concept dezvoltat de *Școala de studii de securitate de la Copenhaga*, care se concentrează pe capacitatea unei societăți de a se conserva prin păstrarea caracterului său esențial. Conceptul a apărut în anii '90, odată cu sfârșitul Războiului Rece, și a fost dezvoltat în contextul integrării statelor în Uniunea Europeană. Această paradigmă minimizează rolul puterii statului în garantarea securității prin confruntarea amenințărilor, pentru a aduce în prim-plan probleme privind identitatea comunităților și dinamica socială.

Ținând cont de aceste aspecte, prezentul articol abordează conceptul de *securitate socială* și analizează semnificația acestuia în contextul geopolitic actual.

### Ce este securitatea societală?

Sfârșitul Războiului Rece, care a culminat cu prăbușirea Uniunii Sovietice și cu apariția de noi state, urmate de eforturi susținute pentru o continuă

* ***Administrația Școlilor Sector 6***
e-mail: *dimavictor2000@yahoo.com*

integrare în Uniunea Europeană, i-a determinat pe specialiști și pe factorii decidenți politici să regândească paradigma securității, independent de stat și de armată[1].

Noua ordine mondială a impus o reconceptualizare a Europei și a securității europene, care nu se mai putea baza pe vechea înțelegere a securității, ca aranjament între state. De aceea preocupările pentru securitate au fost marcate îndeaproape de întrebările privind identitatea socială, valorile naționale, libera circulație a persoanelor sau criminalitatea transfrontalieră.

Conceptul de securitate societală, dezvoltat de către specialiștii Școlii de la Copenhaga, se situează în contextul acestor preocupări[2]. Securitatea societății se referă la „capacitatea unei societăți de a persista în caracterul său esențial în condiții schimbătoare și amenințări posibile sau reale”[3].

În viziunea lui Ole Waever, conceptul de securitate societală reprezintă „capacitatea unei societăţi de a subzista în caracteristicile sale esenţiale, în circumstanţe fluctuante şi în faţa ameninţărilor posibile sau prezente”[4]. Dacă până în prezent statul era obiectul dimensiunilor militare, politice, economice şi de mediu ale securităţii, în cazul securității societale, obiectul de studiu este societatea, a cărei caracteristică esențială este aceea de identitate națională.

**Caracteristicile securității societale**

În lucrarea *Security: a new framework for analysis*, Barry Buzan și colaboratorii săi formalizează înțelegerea mai largă a securității, prin introducerea a cinci sectoare, fiecare guvernat de *caracteristici și dinamici distinctive* și conceptualizat în jurul unor obiecte și actori de referință (adică militare, de mediu, economice, societale și politice). Securitatea societății reprezintă supraviețuirea unei comunități ca unitate de coeziune; obiectul său de referință este *identitatea colectivă*, la scară largă, care poate funcționa independent de stat[5].

Nesiguranța societală apare atunci când o societate se teme că nu va putea trăi ca ea însăși și provine din: migrație (afluxul de oameni *va depăși sau va dilua* identitatea unui grup, de exemplu, nevoia de a defini britanicitatea), competiție verticală (integrarea unui grup în cadrul unei organizații mai largi, de exemplu, euroscepticism în ceea ce privește viitorul UE), revendicări național-separatiste și concurență orizontală (comunitatea este obligată să integreze identități influente în propriile lor grupuri, de exemplu, excepționalismul cultural francez, care se apără de influențele americane).

Securitatea societății nu este legată de un teritoriu, așa cum este securitatea statului, de exemplu, pe teritoriul locuit de kurzi, problemele de securitate ale statului și ale societății sunt divergente în mare măsură și intră în conflict[6].

Din perspectivă sociologică, conceptul de *securitate societală* întruchipează o anumită viziune a securității, care consideră securitatea ca fiind un *fenomen independent.* Astfel, securitatea societății nu este nici o amenințare, nici o oportunitate, ci este atât un centru, cât și o bază, pe fundamentul căreia s-ar putea construi fiabilitatea și certitudinea vieții colective. Asta înseamnă că securitatea este considerată ca fiind bazată pe viața colectivă – viața oamenilor obișnuiți –, în loc să privească diferențele și să insiste asupra dezacordului dintre grupuri și state, care este un factor cheie în determinarea amenințărilor și în identificarea prietenilor sau dușmanilor.

Securitatea, ca *fenomen social*, nu are nevoie de soluții militare și nici de soluții *soft*. Astfel, securitatea societății nu poate fi asimilată cu puterea, dimpotrivă ea trebuie văzută ca un mecanism de transformare a legăturilor sociale. În cele din urmă, amenințările și oportunitățile societale nu pot fi considerate decât factori care pot disuada sau impulsiona. Cu alte cuvinte, scopul final al securității societale este confortul și înțelegerea frumuseții vieții colective, nu un interes pentru guvern, nu eliminarea inamicilor, nu confruntarea amenințărilor percepute pentru națiune[7].

**Contextul actual al securității**

Securitatea unei societăți este în pericol atunci când se percepe o ameninţare la adresa ei, cu privire la identitatea și la supraviețuirea ei ca și comunitate. Suprapunerea dintre stat şi societate a determinat analiștii să ia în considerare identitatea societală, ca valoare care trebuie apărată şi, astfel, să promoveze conceptul de securitate a identităţii, ca bază a securității societale.

În accepţiunea Școlii de la Copenhaga, există două tipuri de societăţi care participă la configurarea identității specifice omului, respectiv comunităţile etnico-naţionale şi comunitățile religioase.

În acest context, apare problema identificării actorilor care ar trebui să deţină competenţa asigurării securităţii. Dacă, în mod tradiţional, furnizorul de securitate este statul prin organismele sale politico-instituţionale, în cazul securităţii societale, statul se confruntă cu anumite dificultăţi. Uneori, acţiunile statului pot genera insecuritate în sectorul societal, iar încercările de influenţare a identităţii nu sunt întotdeauna eficace, ele putând avea consecinţe negative, provocând puternice manifestări împotriva tendinţelor opresive ale statului.

Pentru a identifica ameninţările la adresa identităţii unui stat, trebuie să stabilim valorile în jurul cărora se coagulează comunitatea, în speţă naţiunea, inclusiv factorii obiectivi, precum limba naţională, teritoriul și alte elemente de identificare, specifice statului în cauză.

Barry Buzan identifică trei mari tipuri de ameninţări la adresa securităţii societale, și anume:

- migraţia – când un popor primește un procent de străini prea mare, identitatea sa poate fi afectată de modificarea compoziţiei sale sociale;
- competiţia orizontală – caracteristicile culturale şi lingvistice ale unei societăți pot fi afectate de influența unor culturi vecine, cu efecte clare asupra identității respectivului popor;
- competiţia verticală – uneori, proiectele integraționiste sau secesioniste fac ca oamenii să înceteze a se mai identifica cu poporul Z (de exemplu, Catalonia, Kosovo etc.).

Pe lângă cele trei tipuri de ameninţări, la ora actuală se mai identifică încă trei ameninţări la adresa securităţii societale, și anume:

- depopularea are caracter ambivalent şi din această cauză este menţionată separat. Depopularea are caracter ambivalent, pentru că nu reprezintă o ameninţare propriu-zisă la adresa identităţii unei societăţi, ci, în primul rând, la adresa indivizilor, care sunt purtătorii identităţii unei naţiuni. Ea devine o ameninţare la adresa securităţii societale când ameninţă să distrugă societatea;
- discriminarea;
- terorismul.

În contextul integrării în Uniunea Europeană, identitatea statelor devine din ce în ce mai importantă, deoarece graniţele aproape că dispar. „Într-o Europă unită se vor bucura de securitate acele societăţi naţionale care reuşesc să-şi prezerve bazele moral-identitare”[8].

Conform analizei furnizate de Școala de la Copenhaga, se poate spune că integrarea în structuri suprastatale, de tipul Uniunii Europene, poate fi interpretată drept renunţare la identitatea şi la suveranitatea naţională, determinând fenomene circumscrise competiţiei verticale.

Nu numai renunţarea la identitate, deținută în favoarea unei identităţi supranaţionale, corespunde unor astfel de dinamici, ci şi exacerbarea unor identităţi subnaţionale ale minorităţilor.

În acest sens, fac referire la multitudinea discursurilor care au ca subiect autonomia sau chiar secesiunea unor regiuni, din unele state ale Uniunii Europene, după Brexitul din Marea Britanie, din anul 2016.

**Concluzii**

Plecând de la noua paradigmă a securităţii contemporane, articolul de faţă nu reprezintă altceva decât o justificare a necesităţii aplecării cu mare atenţie asupra dimensiunii societale a acesteia.

Conform aprecierilor multor analiști de specialitate, în acest sector se produc cele mai mari schimbări şi, de aceea, este necesar să înţelegem mult mai bine care sunt mecanismele de organizare a societăţii în faţa ameninţărilor de securitate care sunt variate şi deosebit de greu de anticipat.

Consider că se poate vorbi despre o dilemă a securităţii societale, în sensul că efectele ameninţărilor la adresa societăţii sunt greu de stopat cu adevărat, acestea repercutându-se pe termen lung.

Într-un conflict identitar, părţile tind să trateze ameninţările ca vizând însăşi existenţa şi supravieţuirea lor, iar astfel de răni se închid foarte greu. Demersul de cunoaştere a acestui sector nu este unul facil, mai ales având în vedere multidisciplinaritatea inerentă, dar şi necesitatea de dezvoltare a unor instrumente de analiză cât mai potrivite. Deși conceptul de securitate societală ar trebui să aibă o abordare academică unitară, este totuși dificil să ne imaginăm o teorie unică, care să corespundă, în aceeaşi abordare, tuturor societăţilor din Uniunea Europeană.

Efortul de a avea o construcţie unitară a securităţii societale, care să cuprindă aceste

specificităţi, este de maximă importanţă pentru a imagina o Uniune Europeană stabilă şi adaptată nevoilor actuale ale cetăţenilor săi. Totuși, dinamica specifică dimensiunii societale, inclusiv riscurile și amenințările de securitate, reprezintă preocupările constante ale factorilor politico-sociali, chiar dacă abordările lor nu sunt identice sau nu se referă la același palier societal.

Migraţia, îmbătrânirea populaţiei, competiția orizontală, competiția verticală, depopularea, discriminarea și terorismul au un impact societal pe termen lung, care trebuie integrat în politicile socioeconomice ale Uniunii Europene, iar acestea, la rândul lor, trebuie implementate de toate statele membre.

În concluzie, toate aceste probleme pot fi soluționate doar prin colaborarea dintre statele membre şi reclamă discuţii serioase pentru a stabili clar care este granița dintre național și european în lupta pentru apărarea valorilor tradiționale specifice fiecărui stat și, implicit, identitatea națională.

**NOTE:**

1 P. Bilgin, ”Individual and Societal Dimensions of Security”, *International Studies Review*, 2003, https://www.academia.edu/393273/_2003_Individual_and_Societal_Dimensions_of_Security, accesat la 15.08.2019.

2 *Ibidem,* p. 211.

3 Ole Wæver, *Identity, Migration and the New Security Agenda in Europe*, 1993, p. 23.

4 Barry Buzan, *Societal Security, State Security and Internationalization*, în Ole Weaver, Barry Buzan, Morten Kelstrup, Pierre Lemaitre, *Identity, Migration and the New Security Agenda in Europe*, Pinter, London, 1993, p. 213.

5 Barry Buzan, Wæver & de Wilde, *Security a new Framework for Analysis*, Lynne Rienner Publishers, 1998, p. 22.

6 *Ibidem*, p. 119.

7 Navidnia Manijeh, *Societal Security*, Research Institute of Strategic Studies (Rahbordi), Tehran, 2009, pp. 69-83.

8 Ionel Nicu Sava, *Studii de securitate*, Centrul român de studii regionale, Bucureşti, 2005, p. 252.

## BIBLIOGRAFIE


Buzan Barry, Hansen Lene, *The Evolution of International Security Studies*, Cambridge University Press, Cambridge, 2009.

Buzan Barry, *Popoarele, statele şi frica*, Editura Cartier, Chişinău, 2005.

Buzan Barry, Waever Ole, De Wilde Jaap, *Security: a new framework for analisys*, Lynne Rienner Publishers Inc, London, 1998.

Buzan Barry, *Societal Security, State Security and Internationalization*, în Weaver Ole, Buzan Barry, Kelstrup Morten, Lemaitre Pierre, *Identity, Migration and the New Security Agenda in Europe*, Pinter, London, 1993.

Chifu Iulian, Nantoi Oazu, Sushko Oleksandr, *Securitate societală în regiunea trilateralei România-Ucraina-Republica Moldova*, Editura Curtea Veche, Bucureşti, 2008.

Sava Ionel Nicu, *Studii de securitate*, Centrul român de studii regionale, Bucureşti, 2005.

Stoica Ionel, *Tentaţia migraţiei: necesitate şi oportunitate într-o lume globalizată*, Editura Militară, Bucureşti, 2011.

Ştefănescu Simona, Velicu Anca, *Naţional şi/sau european? Reprezentări sociale ale identităţii în societatea românească actuală*, Editura Expert, Bucureşti, 2006.

*Strategia Naţională de Apărare a Ţării pentru perioada 2015-2019*, http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf

# UNELE ELEMENTE DISFUNCȚIONALE PRIVIND CONDUCEREA UNITĂȚILOR SANITARE CU PATURI DIN REȚEAUA SANITARĂ PROPRIE A MINISTERULUI APĂRĂRII NAȚIONALE

## *SOME DYSFUNCTIONAL ELEMENTS WITH REGARD TO THE MANAGEMENT OF HEALTH FACILITIES WITH BEDS WITHIN THE OWN SANITARY NETWORK OF THE MINISTRY OF NATIONAL DEFENSE*

## *QUELQUES ÉLÉMENTS DE DISFONCTIONNEMENT DU PROCESSUS DE GESTION DES UNITÉS SANITAIRES DISPOSANT DE LITS DANS LE RÉSEAU MÉDICAL APPARTENANT AU MINISTÈRE DE LA DÉFENSE NATIONALE*

**Lt.col.med.drd. Ionuț RĂDULESCU***

Unitățile sanitare publice cu paturi sunt, în opinia mea, entitățile organizaționale medicale cele mai complexe din cadrul sistemului românesc de asigurări sociale de sănătate. Managementul acestora ridică adeseori probleme deosebite și provocări redutabile, ținând cont de faptul că, în aceste veritabile „temple” ale medicinei, sunt furnizate, deopotrivă, practic toate tipurile de asistență medicală existente: preventivă/profilactică, de urgență, primară/de familie, ambulatorie de specialitate, spitalicească și chiar de recuperare și de reabilitare.

*Public health facilities with beds are, in our opinion, the most complex medical organisational entities within the Romanian social health insurance system. Their management often raises particular issues and redoubtable challenges, considering that in these veritable “temples” of medicine is provided basically all existing types of medical assistance: preventive/ prophylactic, emergency, primary/ family, outpatient clinic, hospital and even recovery and rehabilitation.*

*Les unités sanitaires publiques disposant de lits sont, selon moi, les entités organisationnelles médicales les plus complexes du système d’assurance maladie roumain. Leur gestion soulève souvent de grands problèmes et lance aussi de vrais défis, prenant en compte le fait que dans ces véritables ”temples” de la médecine sont fournis pratiquement tous les types de soins de santé disponibles: préventif/prophylactique, d’urgence, primaire/familial, ambulatoire, hospitalier et même physique et de réadaptation.*

**Cuvinte-cheie:** unități sanitare militare; criterii; performanță; valoare indicatori; evaluare; consiliu de administrație; comandant interimar.

***Keywords:*** *military health facilities; criteria; performance; value; indicators; assessment; board of directors; interim commander.*

***Mots-clés:*** *unités sanitaires militaires; critères; performance; indicateurs de valeur; évaluation; conseil d’administration; commandant par intérim.*

***Comandamentul Logistic Întrunit***
e-mail: *drionut2002@yahoo.com*

Abordând schematic subsistemul de conducere și/sau coordonare a unităților sanitare cu paturi din rețeaua sanitară proprie Ministerului Apărării Naționale, putem afirma că acesta este constituit, potrivit cadrului normativ incident național/ republican[1] și celui specific[2], din următoarele cinci entități structural-organizaționale distincte: consiliu de administrație, comandant numit prin concurs/ examen, organizat de consiliul de administrație, comitet director, consiliu medical și consiliu etic.

Practic, potrivit prevederilor art. 176, alin.(4) din *Legea nr. 95/2006 privind reforma în domeniul sănătății*, republicată, comandantul desemnat, în urma câștigării concursului/promovării examenului de încadrare a funcției de manager general, încheie un contract de management cu Ministerul Apărării Naționale, reprezentat de ministrul apărării naționale, pe o perioadă de maximum trei ani, contractul de management putând înceta înainte de termen, în urma evaluării anuale sau ori de câte ori este nevoie. Această evaluare este efectuată pe baza criteriilor generale de performanță, stabilite prin ordin al ministrului sănătății, precum și pe baza criteriilor specifice de performanță și a ponderilor, stabilite și aprobate prin act administrativ al conducătorilor ministerelor sau instituțiilor cu rețea sanitară proprie.

Totodată, alin.(7) al articolului de lege de mai sus statuează faptul că valorile optime ale indicatorilor de performanță ai activității spitalului se stabilesc și se aprobă prin ordin al ministrului sănătății. Acest aspect poate constitui o disfuncționalitate importantă, ținând cont de faptul că, în cazul criteriilor de performanță specifice, acestea și, respectiv, valorile optime ale indicatorilor de performanță se stabilesc neunitar și necorelat de instituții diferite, situate în domenii aparte.

Pentru implementarea și aplicarea prevederilor art.176 alin.(4) din legea sus-menționată, ministrul sănătății a emis un ordin[3] care prevede faptul că activitatea de evaluare în discuție se face anual, până la data de 30 aprilie a fiecărui an, pentru anul anterior, luându-se în calcul un număr de 17 criterii de performanță. Consider că și acest fapt este de natură disfuncțională, întrucât aceste criterii de performanță nu au prevăzute valori/ niveluri aferente, evaluarea făcându-se, astfel, de o manieră arbitrară, nejudicioasă, subiectivă și chiar inexactă și eronată, exclusiv prin raportare la valorile autoasumate și stabilite de însăși persoana evaluată pentru indicatorii în speță, în conținutul contractului de management încheiat.

Dorind să motivez cele afirmate anterior, formulez cazul ipotetic al unui comandant de spital militar, care, deținând un nivel ridicat de „ambiție instituțională”, și-a autofixat, în contractul de management, valori/niveluri ridicate ale criteriilor de performanță, cu procente de realizare crescute, de 70 %, 80 % sau chiar mai mult. Paradoxal, dar cât se poate de veridic și de plauzibil, în situația nerealizării acestor *targeturi* înalte, comisia de evaluare anuală a activității acestui comandant, numită de către ministrul apărării naționale, poate, și chiar este obligată de „litera legii”, să propună încetarea contractului de management al acestuia și eliberarea sa din funcție.

De asemenea, tot în acest sens, a fost emis inclusiv un ordin al ministrului sănătății[4], care statuează modelul-cadru pentru contractul de management al unităților sanitare cu paturi din sistemul de sănătate public, aplicabil, inclusiv, în cazul spitalelor militare. Acesta conține, în mod distinct, o listă cu 28 de indicatori de performanță, grupați în patru categorii diferite, astfel: indicatori de performanţă a activităţii managerului spitalului public, indicatori de utilizare a serviciilor, indicatori economico-financiari și, respectiv, indicatori de calitate. Ca o disfuncție a acestui act normativ, subliniez faptul că nici această normă nu fixează neechivoc niveluri/valori clare pentru acești indicatori de performanță, îngreunând o evaluare corectă și justă.

Astfel, în baza celor de mai sus, inclusiv la nivelul spitalelor militare, anual, o comisie de evaluare, numită de către ministrul apărării naționale, evaluează activitatea comandanților acestora, pe baza a două tipuri de criterii de performanță, unele generale, aplicabile oricărui spital public, și altele specifice instituției militare, cele două categorii de criterii mai sus amintite și ponderea lor fiind stabilite prin ordin al ministrului apărării naționale[5].

Analizând cu minuțiozitate normativele opozabile ale activității în discuție, putem afirma că, deși există stabilite o serie de criterii/indicatori de performanță, utilizabili în evaluarea conducătorilor spitalelor publice din sistemul românesc de asigurări sociale de sănătate, Ministerul Sănătății nu a emis, până în prezent, o normă care să stabilească clar, concis, coerent și unitar, nivelurile

și/sau valorile optimale ale acestora, sub formă cifrică, procentuală, interval etc., aspect grav și îngrijorător din punctul nostru de vedere.

Trebuie totuși menționat faptul că, în anul 2007, Ministerul Sănătății a făcut o încercare de normalizare a acestei situații, fiind emis un ordin al ministrului, care a rezolvat problematica temporar, doar pentru anul respectiv[6]. Ordinul în speță conținea valorile medii naționale ale indicatorilor de performanță ai managementului spitalelor, realizați în anul 2006, și preciza, în mod expres, faptul că respectivele valori stau la baza stabilirii nivelului indicatorilor de performanță pentru fiecare spital public, în anul 2007, nicidecum pe o durată multianuală.

Toate aspectele disfuncționale enunțate anterior pot genera cazuri în care, la data încheierii lor, contractele de management ale comandanților spitalelor militare să nu conțină valori/niveluri ale unor criterii/indicatori de performanță generali, comuni celor utilizați de alte spitale publice din România.

În ceea ce privește evaluarea activității derulate de către comandanții unităților sanitare cu paturi din rețeaua sanitară proprie Ministerului Apărării Naționale, au fost introduse și elemente aparte, de specificitate, în consonanță cu sarcinile, activitățile, responsabilitățile și obligațiile aparte, respectiv *Criteriile specifice de performanță pentru evaluarea anuală sau ori de câte ori este nevoie a activității comandanților unităților sanitare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale, în baza cărora contractul de management poate fi prelungit sau poate înceta înainte de termen,* aprobate prin *Ordinul ministrului apărării naționale nr. M.68/2013*.

Analizând acest ultim normativ, apreciem, ca un prim aspect disfuncțional, faptul că nu a suferit niciun fel de modificări și/sau completări, de la momentul apariției sale, în anul 2013, până în prezent, în condițiile în care domeniul reglementat a cunoscut un dinamism crescut în această perioadă. Totodată, norma precizează că evaluarea acestor criterii se face prin „analizarea dimensiunilor corespunzătoare fiecărui criteriu” și prin acordarea, în consecință, de către evaluator a unui punctaj de la 0 la 5 puncte, fără a fi fost instituite, așa cum era normal și firesc, niveluri sau valori de referință la evaluare. De exemplu, indicatorul „îndeplinirea atribuțiilor funcționale” este prevăzut în ordin cu trei dimensiuni care trebuie evaluate, respectiv „prioritizarea acțiunilor și corelarea acestora cu resursele disponibile”, „modul de rezolvare a problemelor identificate și îndeplinirea atribuțiilor specifice” și „impactul deciziilor asupra modului de îndeplinire a atribuțiilor funcționale specifice”, dar nu se indică niciun fel de reper standard sau nicio referință.

În calitate de cadre militare în activitate, comandanții unităților sanitare militare cu paturi sunt supuși, în fiecare an, inclusiv unui proces de evaluare profesională, specific organismului militar, în vederea întocmirii aprecierii de serviciu anuale, activitate stabilită prin ordin de către ministru[7]. Scopul aprecierii de serviciu este tocmai evaluarea competenței profesionale, a calității morale și a perspectivelor de dezvoltare a cadrelor militare.

Trebuie precizat că, printre obiectivele acestei activități de apreciere anuală de serviciu, se regăsesc: îmbunătățirea eficienței structurilor militare prin aprecierea performanțelor profesionale individuale, utilizarea eficientă a cadrelor militare și încadrarea lor potrivit cerințelor posturilor, pregătirii profesionale și performanțelor obținute, precum și, nu în ultimul rând, conștientizarea cadrelor militare evaluate asupra importanței modului de îndeplinire a atribuțiilor funcționale și asupra modalităților de îmbunătățire a performanței și competențelor profesionale.

Parcurgând logic și sistematic cele expuse anterior, putem afirma că, în cazul comandanților unităților sanitare militare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale, aceștia sunt supuși, în mod nefiresc, la două procese independente de evaluare anuală, având însă o serie de elemente de suprapunere contraproductivă și chiar cronofagă. Astfel, primul proces de evaluare anuală se încheie în luna ianuarie, pentru anul precedent, cu aprecierea de serviciu anuală, iar al doilea are loc ulterior, până în luna aprilie, pentru anul precedent, finalizându-se cu acordarea unui calificativ general, reprezentat de calificativul obținut la evaluarea criteriilor generale de performanță din contractual de management, asociat cu calificativul obținut la evaluarea îndeplinirii criteriilor de performanță specifice.

O prevedere greu, dacă nu chiar imposibil, de respectat și de aplicat este cea dispusă prin art. 4, alin.(4) din *Ordinul ministrului apărării naționale nr. M.68/2013*, respectiv luarea în

calcul, la întocmirea aprecierii de serviciu anuale a comandanților nominalizați, în calitate de cadre militare în activitate, a calificativului general, stabilit în urma evaluării ca și comandanți de unități sanitare. „Fractura cronologică” este, în opinia mea, extrem de evidentă, antepunând o activitate din luna aprilie uneia din luna ianuarie, în cadrul aceluiași an calendaristic.

Un alt element disfuncțional este cel care ține de aplicarea, în cazul unităților sanitare cu paturi din rețeaua Ministerului Apărării Naționale, a prevederilor *Legii nr. 95/2006 privind reforma în domeniul sănătății*, republicate, cu modificările și completările ulterioare, referitoare la suspendarea contractului de muncă al managerului unității sanitare cu paturi și a membrilor comitetului director, incomplet armonizate, în opinia mea, cu prevederile statutului cadrelor militare, reglementat de *Legea nr. 80/1995 privind statutul cadrelor militare, cu modificările și completările ulterioare*. Astfel, în situația încetării, înainte de termen, a mandatului comandantului unității sanitare militare cu paturi, ministrul apărării naționale „împuternicește” prin ordin, potrivit art. 4, alin. (4) din *Ordinul ministrului apărării naționale nr. M.129/2009 privind conducerea unităților sanitare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale*, cu modificările și completările ulterioare, la propunerea șefului Direcției medicale sau, după caz, a șefului/comandantului structurii care are în coordonare unitatea sanitară cu paturi, un comandant interimar pe o perioadă de cel mult șase luni, perioadă în care se organizează concursul de ocupare a postului. În acest caz, comandantul interimar nu încheie contract de management pentru perioada cât asigură temporar comanda unității sanitare cu paturi, similar procedându-se și în cazul celorlalți membri ai comitetului director.

În aceste situații, nu se atinge scopul pentru care a fost instituit contractul de management, întrucât, în cazul asigurării interimatului de către persoane împuternicite, nu există obligația încheierii acestor contracte și, implicit, nici obligația îndeplinirii indicatorilor generali și specifici de performanță. Mai mult, în aceste perioade de interimat nu se poate realiza nici evaluarea activității managerului, întrucât, potrivit art. 1, alin.(2) din *Ordinul ministrului sănătății publice nr. 112/2007 privind criteriile de performanţă în baza cărora contractul de management poate fi prelungit sau poate înceta înainte de termen*, cu modificările și completările ulterioare, evaluarea activității managerului spitalului public, pentru anul calendaristic precedent, se face până la data de 30 aprilie a anului următor, fiind evaluați doar managerii care au contractul de management în perioada de valabilitate și care au condus spitalul public respectiv pe o perioadă de cel puțin șase luni în anul evaluat.

**Concluzii**

Optimizarea procesului de conducere a unităților sanitare cu paturi din rețeaua sanitară proprie a Ministerului Apărării Naționale necesită un efort intens, concentrat și concertat, dus ritmic, constant și riguros, în special în vederea armonizării conceptuale/doctrinare cu cadrul normativ incident republican/național. În același timp, nu trebuie trecută cu vederea nici sistematizarea, unificarea și coordonarea normativelor specifice/departamentale în domeniu.

**NOTE:**

1 *** *Legea nr. 95/2006 privind reforma în domeniul sănătății*, republicată, cu modificările și completările ulterioare, cap. III.

2 *** *Ordinul ministrului apărării naționale nr. M.129/2009 privind conducerea unităților sanitare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale*, cu modificările și completările ulterioare, art. 1, alin.(2), art. 7, alin.(1), art. 18, alin.(1), art. 21, art. 25 alin.(1).

3 *** *Ordinul ministrului sănătății publice nr. 112/2007 privind criteriile de performanţă în baza cărora contractul de management poate fi prelungit sau poate înceta înainte de termen*, cu modificările și completările ulterioare, art. 1, alin.(2).

4 *** *Ordinul ministrului sănătății nr. 1.384/2010 privind aprobarea modelului-cadru al contractului de management şi a listei indicatorilor de performanţă a activităţii managerului spitalului public*, cu modificările și completările ulterioare, art. 1, alin.(1).

5 *** *Criteriile specifice de performanță pentru evaluarea anuală sau ori de câte ori este nevoie a activității comandanților unităților sanitare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale*, în baza cărora contractul de management poate fi prelungit sau poate înceta înainte de termen, aprobate prin *Ordinul ministrului apărării naționale nr. M. 68/2013*, Anexa nr. 4.

6 *** *Ordinul ministrului sănătății publice nr. 1.567/2007 privind aprobarea valorilor medii naționale ale indicatorilor de performanţă ai managementului spitalului,* Anexa nr. 1.

7 *** *Metodologia întocmirii aprecierilor de serviciu pentru cadrele militare din structurile Ministerului Apărării Naționale, pe timp de pace* aprobată prin *Ordinul ministrului apărării naționale nr. M.122/2014*, cu modificările și completările ulterioare, art. 3, alin.(1).

## BIBLIOGRAFIE

*** *Legea nr. 95/2006 privind reforma în domeniul sănătății*, republicată, cu modificările și completările ulterioare.

*** *Legea nr. 80/1995 privind statutul cadrelor militare, cu modificările și completările ulterioare*.

*** *Ordinul ministrului apărării naționale nr. M.129/2009 privind conducerea unităților sanitare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale*, cu modificările și completările ulterioare.

*** *Ordinul ministrului sănătății publice nr. 112/2007 privind criteriile de performanţă în baza cărora contractul de management poate fi prelungit sau poate înceta înainte de termen*, cu modificările și completările ulterioare.

*** *Ordinul ministrului sănătății nr. 1.384/2010 privind aprobarea modelului-cadru al contractului de management şi a listei indicatorilor de performanţă a activităţii managerului spitalului public*, cu modificările și completările ulterioare.

*** *Criteriile specifice de performanță pentru evaluarea anuală sau ori de câte ori este nevoie a activității comandanților unităților sanitare cu paturi din rețeaua sanitară a Ministerului Apărării Naționale, în baza cărora contractul de management poate fi prelungit sau poate înceta înainte de termen*, aprobate prin *Ordinul ministrului apărării naționale nr. M. 68/2013*.

*** *Ordinul ministrului sănătății publice nr. 1.567/2007 privind aprobarea valorilor medii naţionale ale indicatorilor de performanţă ai managementului spitalului*.

*** *Metodologia întocmirii aprecierilor de serviciu pentru cadrele militare din structurile Ministerului Apărării Naționale, pe timp de pace*, aprobată prin *Ordinul ministrului apărării naționale nr. M.122/2014*, cu modificările și completările ulterioare.

# UTILIZAREA COMPLEXITĂȚII ÎN STUDIUL SECURITĂȚII SOCIETALE

## *THE USE OF COMPLEXITY IN SOCIETAL SECURITY STUDIES*

## *UTILISATION DE LA COMPLEXITÉ DANS L'ÉTUDE DE LA SÉCURITÉ SOCIÉTALE*

**Prof.univ.dr. Ioan CRĂCIUN***
**Drd. Octavian Victor Mihail DIMA****

*Securitatea societală*, așa cum a fost dezvoltată de Școala de Securitate de la Copenhaga, reprezintă un domeniu extrem de important al conceptului abordării securității contemporane, care, pe lângă problemele militare, ține cont și de o serie de alte amenințări ce provin din domenii conexe, precum cele politice, economice, societale sau de mediu. În studiul *securității societale* contemporane, a fost împrumutată o serie de concepte specifice teoriei sistemelor complexe, cum ar fi: complexitatea, autoorganizarea, pragul haosului etc., care au îmbogățit în mod substanțial hermeneutica discursului de securitate pe baza interpretărilor nemecaniciste ale sistemelor sociale.

Acest articol își propune să arate că, în studiul securității societale, folosirea unor instrumente specifice studiului sistemelor moderne complexe a produs rezultate destul de interesante, care ar putea da un nou sens cercetărilor din acest domeniu.

*Societal security, as developed by the Copenhagen School of Security, is an extremely important area of the broader contemporary security concept which, in addition to military issues, also takes into account a number of other threats coming from the fields such as political, economic, societal or environmental ones. In the study of contemporary societal security, a number of concepts specific to the theory of complex systems, such as complexity, self-organization, the threshold of chaos, etc., have been borrowed, which have substantially enriched the hermeneutics of security discourse on the basis of non-mechanistic interpretations of social systems.*

*This article aims to show that in the study of societal security the use of tools specific to the study of modern complex systems has produced quite interesting results, which could give a new meaning to the research in this field.*

*La sécurité sociétale, dans la forme conçue par l'École de Sécurité de Copenhague, est un sujet extrêmement important du concept plus large de la sécurité contemporaine, qui, outre les problèmes militaires, prend également en compte un certain nombre de menaces provenant des domaines connexes, commes la politique, l'économie, le domaine sociétale ou de l'environnement. Pour analyser la sécurité sociétale contemporaine, on fait appel à plusieurs concepts spécifiques à la théorie des systèmes complexes, tels que la complexité, l'auto-organisation, le seuil de chaos etc. qui ont considérablement enrichi l'herméneutique du discours de sécurité en fonction des interprétations non mécanistes des systèmes sociaux.*

*Cet article a pour but de montrer que, dans l'étude de la sécurité sociétale, l'utilisation des instruments spécifiques à l'analyse des systèmes modernes complexes a donné des résultats assez intéressants, qui pourraient donner un nouveau sens à la recherche dans ce domaine.*

**Cuvinte-cheie:** securitate societală; știința complexității; gândire sistemică; securitate în context sistemic.
***Keywords:*** *societal security; complexity science; systemic thinking; security in a systemic context.*
***Mots-clés:*** *sécurité sociétale; science de la complexité; pensée systémique; sécurité dans un contexte systémique.*

** Universitatea Națională de Apărare „Carol I”*
e-mail: *craciun64@gmail.com*
*** Administrația Școlilor Sector 6*
e-mail: *dimavictor2000@yahoo.com*

Gândirea sistemică a avut un impact semnificativ în multe domenii de studiu și cercetare, printre care domeniul relațiilor internaționale și, în particular, cel al studiilor de securitate au ocupat un loc important. Astfel, conceptele complexității au fost folosite în studiul conflictului militar și în cel al războiului de către o serie de analiști, precum Quincy Wright sau Pitrim Sorokin, iar alți analiști, precum Lewis F. Richardson sau Frederick Lanchester, au aplicat aceste concepte, în special elementele de teoria jocurilor, în studiul securității naționale/militare.

În studiul relațiilor internaționale, elemente de teoria complexității au fost folosite de către Morton A. Kaplan și Karl W. Deutsch[1], iar, mai târziu, Barry Buzan împreună cu alți specialiști ai Școlii de la Copenhaga au aplicat astfel de elemente în studiile contemporane de securitate. Astfel, ei au elaborat *conceptul extins de securitate* propus de această școală, bazat pe cinci domenii distincte de analiză (politic, economic, militar, societal și de mediu) și au introdus *teoria securitizării*[2], ca bază a unei noi paradigme de securitate post-Război Rece.

În timp, elementele de teoria complexității au devenit extrem de importante în studiul și cercetarea noilor amenințări militare și, mai ales a celor nemilitare la adresa securității contemporane. În acest context, scopul principal al acestui articol este să arate că, în studiul conflictelor contemporane, al terorismului, al criminalității transnaționale, al migrației sau al degradării necontrolate a mediului, folosirea unor instrumente specifice studiului sistemelor moderne complexe a produs rezultate destul de interesante, ceea ce ar putea da un nou sens cercetărilor din acest domeniu.

Totuși, există și situații în care folosirea metodologiilor care derivă din cercetarea sistemelor complexe pentru studiile de securitate a fost pusă la îndoială de înțelegerea insuficientă a conceptelor științelor sociale sau a teoriilor specifice sistemelor complexe. Având în vedere aceste dificultăți, prin prezentul articol ne propunem să identificăm unele dintre răspunsurile posibile referitoare la modul în care ar trebui să înțelegem și să depășim barierele conceptuale pentru aplicarea conceptelor teoriei sistemelor complexe în studiile de securitate contemporane.

**Utilizarea complexității în științele sociale**

În sociologie, complexitatea socială reprezintă un cadru conceptual folosit pentru analiza societății, iar utilizarea curentă a termenului *complexitate* se referă, în mod specific, la teoriile sociale care tratează societatea ca pe un sistem adaptativ complex. Acest aspect motivează faptul că atât complexitatea socială, cât și proprietățile sale emergente reprezintă teme centrale recurente pentru studiul evoluției istorice a gândirii sociale, dar și pentru studiul schimbărilor sociale[3]. În plus, teoria complexității sociale oferă o platformă teoretică de nivel mediu pentru formarea unor ipoteze de lucru[4] în studiul fenomenelor sociale de nivel micro și macro, conceptul de complexitate socială fiind unul neutru din punct de vedere metodologic.

Primele utilizări ale conceptului de *complexitate* în științele sociale și comportamentale, având ca bază teoretică teoria sistemelor complexe, s-au regăsit în studiile referitoare la organizațiile moderne și în studiile de management[5]. Totuși, în studiile de management, mai cu seamă, complexitatea a fost adesea folosită într-o manieră metaforică mai degrabă decât într-o manieră teoretic calitativă sau cantitativă[6]. Cu toate acestea, către mijlocul anilor ’90, complexitatea a fost încorporată în domeniul științelor sociale, concomitent cu adoptarea unor instrumente de studiu și cercetare similare celor folosite, în general, în știința complexității. În 1998, a fost creată prima publicație on-line de specialitate, denumită *Journal of Artificial Societies and Social Simulation*, urmată de numeroase alte publicații de profil, care au contribuit la promovarea teoriei complexității în domeniul social. Pe de altă parte, aceste preocupări au fost conexate cu alte tradiții teoretice specifice domeniului social, precum epistemologia constructivistă și pozițiile filosofice ale fenomenologiei, postmodernismului și realismului critic.

Așa cum am arătat deja, complexitatea socială este o noțiune teoretică neutră, ceea ce înseamnă că poate fi folosită atât în abordările locale, cât și în cele globale ale cercetărilor sociologice. În acest context, metodologiile de cercetare sunt determinate în funcție de nivelul analizei stabilit de către fiecare cercetător în parte sau în funcție de nivelul de descriere sau de explicație cerut de către ipotezele de cercetare[7].

La nivel micro, ca metode de analiză pot fi adecvate analiza de conținut, observațiile etnografice sau alte metode de cercetare calitativă. Mai nou, au fost dezvoltate metodologii de cercetare cantitativă extrem de sofisticate, care pot

fi utilizate în cercetările sociologice atât la nivelul de analiză micro, cât și la nivelul de analiză macro. Astfel de metode includ, dar nu se limitează, la diagrame cu bifurcație, analiză de rețea, modelare neliniară și computațională, inclusiv programarea de tip celular, sociocibernetică și alte metode de simulare socială.

Din punct de vedere teoretic, complexitatea socială poate fi aplicată oricărei cercetări care privește interacțiunea socială sau rezultatele unor astfel de interacțiuni, mai ales atunci când aceste interacțiuni pot fi măsurate și exprimate ca date continue sau discrete. O critică obișnuită, citată adesea, cu privire la utilitatea științei complexității în sociologie este dificultatea obținerii unor date adecvate[8]. Cu toate acestea, aplicarea conceptului de complexitate socială și analiza unei astfel de complexități au început și continuă să fie un domeniu neîntrerupt de cercetare în sociologie.

**Se poate utiliza complexitatea în studiile de securitate?**

Noile realități de după încheierea Războiului Rece au condus la o extindere a conceptului neorealist al securității, din cauza unei game mai largi de amenințări potențiale cu care lumea s-a confruntat. Aprofundarea agendei studiilor de securitate a impus folosirea unor referenți ai securității diferiți de cei ai statului, atât la nivelurile inferioare, până la individ, transpus în conceptul de *human security*, cât și la nivelurile superioare, până la cel global, transpus în conceptul de *securitate internațională* sau *globală*, securitatea regională și societală fiind referenți intermediari ai acestei interpretări. Această extindere și aprofundare paralelă a conceptului de securitate au fost propuse de abordarea constructivistă, asociată cu cercetările Școlii de la Copenhaga[9]. Aceste caracteristici constituie nucleul conceptului de securitate și pot fi folosite ca punct de plecare pentru identificarea atributelor sistemice ale securității contemporane[10].

Pentru a păstra și a dezvolta proprietățile analitice ale conceptului de securitate în sens sistemic, propunem o abordare de compromis, pe care o denumim eclectică. Aceasta combină, cel puțin la nivel declarativ, valoarea obiectivă a conceptului de securitate neorealist extins cu ideea constructivistă aprofundată a securității, privită ca discurs convingător[11].

În această abordare eclectică, urmând interpretarea lui Buzan și a colaboratorilor săi de la Copenhaga, securitatea se referă la următoarele sectoare: militar, economic, politic, de mediu și societal, iar conceptele de bază folosite sunt cele de amenințare existențială și de securitizare. Orice problemă publică, prezentată ca o amenințare existențială, poate fi securitizată, adică necesită măsuri de urgență și justifică acțiuni în afara limitelor procedurale normale.

Securitatea este o practică autoreferențială, deoarece o anumită problemă devine *de Securitate*, nu neapărat pentru că există o amenințare existențială reală, ci din cauza faptului că problema este descrisă ca o amenințare[12].

Opus conceptului de securitizare este *desecuritizarea* care poate fi definită ca un proces în care un factor, denumit amenințare, este perceput/descris ca unul care nu mai este de actualitate și, prin urmare, nu mai impune măsuri extraordinare, după ce, printr-un discurs persuasiv, anterior, fusese prezentat cu nevoia de a impune astfel de măsuri[13]. Abordarea propusă ajută la identificarea unei stratageme de compromis, aflată între abordarea neorealistă de predictibilitate a amenințărilor obiective și abordarea constructivistă de negare a oricăror posibilități de predicție a securității. Rezolvarea acestei dileme poate fi găsită prin abandonarea viziunilor mecaniciste și liniare ale proceselor sociale și prin adoptarea unor viziuni bazate pe teoria sistemelor complexe. În locul rafinării extrapolărilor, modelelor de calculator, scenariilor și prognozelor, se pune accentul pe mecanismele de învățare care duc la realizarea predicțiilor, așa cum se întâmplă în management[14] sau la metodele de rafinare aplicate în prognoze, ori în cazul studiilor despre viitor[15].

Aceste aprecieri ne permit să concluzionăm că respectivul corpus științific, denumit complexitate, se poate aplica cu succes în studiile de securitate, ceea ce ne propunem să explorăm în continuare.

**Aplicarea complexității în teoria și practica securității**

Specialiștii în securitate, alături de factorii de decizie politică din acest domeniu, au mari așteptări față de cercetările din domeniul complexității. În aceeași marjă de așteptări, se plasează și specialiștii, și decidenții din domeniul militar. Din acest motiv, deseori s-a încercat adaptarea unor metode specifice complexității la toate nivelurile și situațiile cu caracter militar, și nu numai, adică în

situațiile postconflict sau în așa-numitele situații de urgență.

Extinderea și aprofundarea conceptului de securitate contribuie la creșterea complexității reale sau percepute a lumii în care trăim astăzi. Prin urmare, studiile de securitate tradiționale stato-centriste, orientate pe abordarea liniară de tip cauză-efect, chiar dacă se bazau pe modele științifice (inclusiv cele împrumutate din gândirea sistemică timpurie, precum: stabilitate, polaritate sau stabilitate hegemonică), trebuiau înlocuite cu abordări noi, axate pe gândirea sistemică, în care studiile de securitate folosesc conceptele sistemelor complexe ca analogii, metafore sau modele matematice.

Astfel, în prezent tot mai mulți analiști sunt de părere că, doar într-un număr limitat de cazuri, se mai pot aplica conceptele *mecaniciste* ale funcționării sistemelor sociale. Prin urmare, o serie de concepte specifice teoriei sistemelor complexe, cum ar fi: complexitatea, autoorganizarea, pragul haosului și altele asemănătoare, au fost preluate în analizele de securitate. Desigur, în majoritatea acestor abordări nu este clar specificat, de exemplu, ce este cu adevărat haotic, dar, fără îndoială, astfel de metafore reprezintă instrumente valoroase, din punct de vedere euristic. Prin urmare, așa cum am afirmat deja, noțiunile preluate din studiul sistemelor complexe au îmbogățit în mod substanțial hermeneutica discursului de securitate, pe baza interpretărilor nemecaniciste ale sistemelor sociale.

Astfel, realitatea indică faptul că, între cercetarea sistemelor complexe și politica de securitate contemporană, s-au stabilit legături din ce în ce mai strânse. Pe de altă parte, comunitatea științifică oferă analize/lucrări care se înscriu în aceleași coordonate. Susținem această afirmație cu câteva exemple: J.D. Holland, *Hidden Order. How Adaptation Builds Complexity*, Basic Books (New York), 1995, S.A. Kauffman, *The Origins of Order: Self-Organization and Selection in Evolution*, Oxford University Press (New York/ Oxford), 1993, I. Prigogine, *End of Certainty*, The Free Press (New York), 1997 și altele.

Necesitatea înțelegerii acestor concepte a determinat evoluția și dezvoltarea cercetărilor în domeniu. Astfel, dezbaterile specifice au cunoscut o extindere constantă și s-au concentrat pe explicarea măsurii în care acești termeni noi permit descrierea corectă/exactă a fenomenelor sociale specifice.

În acest context, au apărut multe păreri, cărora ne raliem și noi, care susțin validitatea acestor concepte, dar au apărut și multe critici aduse acestora. De partea cui se află adevărul rămâne în continuare să fie dovedit, ceea ce este însă sigur este faptul că astfel de termeni îmbogățesc semnificativ limbajul discursului social, referitor la politicile și la strategiile de securitate contemporane.

Așadar, cercetările în domeniul sistemelor complexe au oferit o nouă abordare a analizelor de securitate contemporane. Astfel, au apărut noi posibilități de explicare/predicție a fenomenelor de securitate la nivel macro, pornind de la comportamentul elementelor la nivel microsistem.

Un bun exemplu al acestei strategii este proiectul *Sugarscape*[16], parte a unui proiect mai larg, *Proiectul 2050*, dezvoltat de Santa Fe Institute, în colaborare cu World Resources Institute și Brookings Institution. Proiectul presupune identificarea condițiilor pentru un sistem global durabil în secolul următor și pentru elaborarea unor politici care să ajute la realizarea unui astfel de sistem[17].

**Concluzii**

Toate cele arătate până acum demonstrează faptul că studiile de complexitate au devenit o parte indispensabilă a epistemologiei teoriei securității contemporane și chiar un instrument util pentru politica de securitate. Utilizarea în studiile de securitate a modelelor matematice, a analogiilor și a metaforelor legate de complexitate a lărgit fundamentele epistemologice ale cercetării în acest domeniu. Asta nu înseamnă totuși că studiile de complexitate au răspuns direct tuturor așteptărilor studiilor de securitate în ceea ce privește predicția, explicarea efectelor cauzale, abordarea normativă, reziliența și îmbunătățirea (întotdeauna limitată) a capacităților de influențare a fenomenelor sociale.

Aplicațiile complexității în discursul de securitate prezintă două neajunsuri esențiale. În primul rând, așteptările prea mari de la teoria și politica de securitate și, pe de altă parte, folosirea incorectă a conceptelor și abuzurile. Specialiștii în securitate, analiștii și politicienii tratează adesea abordările legate de complexitate ca pe un element nou, modern și cu un oarecare sens de magie al limbajului contemporan de securitate.

În același fel, cercetătorii familiarizați cu metodologia complexității reduc fenomenele

sociale la modele foarte simple, irelevante pentru realitatea în care trăim. În opinia noastră, referirile la neliniaritate, autoorganizare și haos permit aprofundarea înțelegerii tuturor fenomenelor sociale. Totuși, în cercetarea orientată spre securitate, ele au o semnificație specială, pentru că oferă un răspuns referitor la nevoia de predicție și studii normative, orientate spre acțiune.

De aceea trebuie să acordăm o atenție sporită atât eficienței, cât și legitimității aplicațiilor complexității în teoria și practica securității contemporane. Datorită ideilor asociate cu complexitatea diversificată, epistemologia studiilor de securitate s-a îmbogățit cu instrumente utile în analiză și cercetare. Noile fenomene sociale specifice societății informaționale au primit nume, care facilitează înțelegerea lor, precum și procesele de comunicare socială pe care le vizează. Folosirea unor termeni, precum stabilitate, turbulență, neliniaritatea, autoorganizarea, haos etc., utilizate în studiile de securitate, întăresc argumentul folosirii teoriilor complexității pentru explicarea și modelarea fenomenelor securității contemporane.

Deși studiile de complexitate au oferit argumentul final al imposibilității elaborării unor previziuni profunde în cercetarea din domeniul securității, totuși ele au dat metode concrete pentru îmbunătățirea capacităților predictive fie prin utilizarea modelelor matematice, fie cu ajutorul aplicațiilor de tip analogii și metafore sau de stimulare euristică.

**NOTE:**

1 C. Mesjasz, ”Applications of Systems Modelling in Peace Research”, Journal of Peace Research, 25/1988, p. 3, http://journals.sagepub.com/doi/10.1177/002234338802500319, accesat la 14.05.2018.

2 B. Buzan, O. Wver, J. de Wilde, *Security. A New Framework for Analysis*, Lynne Rienner Publishers, Boulder-London, 1998.

3 Eve Raymond, Sara Horsfall, Mary E. Lee (eds.), *Chaos, Complexity and Sociology: Myths, Models, and Theories*, Thousand Oaks, CA: Sage Publications, 1997.

4 Lee Freese, ”Formal Theorizing”, *Annual Review of Sociology*, 6/1980, pp. 187-212.

5 Douglas L. Kiel, *Managing Chaos and Complexity in Government: A New Paradigm for Managing Change, Innovation and Organizational Renewal.* Jossey-Bass: San Francisco, 1994, http://infra-eu.cinecardz.com/l8u3t4q5dhyf/04-santina-waelchi-iv/read-9780787900236-managing-chaos-and-complexity-in-government-a-ne.pdf, accesat la 12.05.2018.

6 Eve Raymond & co., *op.cit*.

7 Niklas Luhmann, *The Differentiation of Society*, Columbia University Press, New York, 1982.

8 Peter Stewart, ”Complexity Theories, Social Theory, and the Question of Social Complexity”, *Philosophy of the Social Sciences*, 31(3), 2001, pp. 323-360, http://journals.sagepub.com/doi/abs/10.1177/004839310103100303, accesat la 12.05.2018.

9 B. Buzzan et comp., *op.cit.*

10 C. Mesjasz, ”Complex Systems Studies and the Concepts of Security”, *Kybernetes*, 35/2006, pp. 3-4, https://www.emeraldinsight.com/doi/full/10.1108/03684920610653755, accesat la 15.05.2018.

11 B. Buzzan et comp., *op.cit.*

12 *Ibidem.*

13 O. Wver, *Securitization and Desecuritization*, în R.D. Lipschutz (ed.), *On Security*, Columbia University Press, New York, 1995, https://www.scribd.com/doc/95165611/Securitization-and-Desecuritization, accesat la 14.05.2016.

14 Heijden van der K., *Scenarios. The Art of Strategic Conversation*, John Wiley & Sons, New York, 1996.

15 J.C. Glenn, T.J. Gordon, *2006 State of the Future*, The Millennium Project, American Council for the United Nations University, Washington DC, 2006.

16 Acest proiect încearcă/intenționează să aplice tehnici de modelare bazate pe calculator pentru a studia fenomenele sociale complexe (împerecherea, procrearea, migrația sezonieră, interacțiunea cu mediul, comerțul, propagarea bolilor, dinamica populației și multe altele). Scopul general este de a dezvolta o soluție computerizată care să permită studiul diverselor tipuri de activități umane dintr-o perspectivă evolutivă. Utilitatea proiectului în scop educativ și de cercetare, inclusiv în domeniul securității, necesită capacitatea de a configura diferiți parametri care controlează simularea.

17 J.M. Epstein, R.L. Axtell, *Growing Artificial Societies. Social Science from the Bottom Up*, MIT Press (Cambridge, MA), 1996, p. 177, https://mitpress.mit.edu/books/growing-artificial-societies.

## BIBLIOGRAFIE

Buzan B., Wver O., de Wilde J., *Security. A New Framework for Analysis*, Lynne Rienner Publishers, (Boulder-London), 1998.

Epstein J.M., Axtell, R.L., *Growing Artificial Societies. Social Science from the Bottom Up*, MIT Press (Cambridge, MA), 1996, https://mitpress.mit.edu/books/growing-artificial-societies

Freese Lee, ”Formal Theorizing”, *Annual Review of Sociology*, 6/1980.

Glenn J.C., Gordon T.J., *2006 State of the Future*, The Millennium Project, American Council for the United Nations University, Washington DC, 2006.

Heijden van der K., *Scenarios. The Art of Strategic Conversation*, John Wiley & Sons, New York, 1996.

Kiel L. Douglas, *Managing Chaos and Complexity in Government: A New Paradigm for Managing Change, Innovation and Organizational Renewal.* Jossey-Bass, San Francisco, 1994, http://infra-eu.cinecardz.com/l8u3t4q5dhyf/04-santina-waelchi-iv/read-9780787900236-managing-chaos-and-complexity-in-government-a-ne.pdf

Luhmann Niklas, *The Differentiation of Society*, Columbia University Press, New York 1982.

Mesjasz C., ”Applications of Systems Modelling in Peace Research”, *Journal of Peace Research*, 25/1988, http://journals.sagepub.com/doi/10.1177/002234338802500319

Mesjasz C., ”Complex Systems Studies and the Concepts of Security”, Kybernetes, 35/2006, https://www.emeraldinsight.com/doi/full/10.1108/03684920610653755

Raymond Eve, Horsfall Sara, Lee E. Mary (eds.), *Chaos, Complexity and Sociology: Myths, Models, and Theories*, Thousand Oaks, CA: Sage Publications, 1997.

Stewart Peter, ”Complexity Theories, Social Theory, and the Question of Social Complexity”, *Philosophy of the Social Sciences*, 31(3), 2001, http://journals.sagepub.com/doi/abs/10.1177/004839310103100303

Wver O., *Securitization and Desecuritization*, în Lipschutz, R.D. (ed.), On Security, Columbia University Press, New York, 1995, https://www.scribd.com/doc/95165611/Securitization-and-Desecuritization

# PLATFORMA SOFTWARE INTEGRATĂ PENTRU ANALIZA MALWARE A TERMINALELOR MOBILE

## *INTEGRATED SOFTWARE PLATFORM FOR MALWARE ANALYSIS OF MOBILE TERMINALS*

## *PLATE-FORME LOGICIELLE INTÉGRÉE POUR L'ANALYSE MALWARE DES TERMINAUX MOBILES*

**Lt.col.dr.ing. Dragoș BĂRBIERU***
**Col.dr. Ștefan-Antonio Dan ȘUTEU****
**Conf.univ.dr. Elena ȘUȘNEA*****

Dincolo de marketingul companiilor IT, în contextul escaladării atacurilor cibernetice, care afectează organizațiile din întreaga lume, soluțiile de securitate cibernetică devin elementul principal în protejarea infrastructurilor și dispozitivelor IT. Diversitatea dispozitivelor mobile inteligente și apariția tehnologiilor cloud, Internet of Things necesită noi soluții tehnologice, implementate atât la nivel hardware, cât și la nivel software în scopul combaterii amenințărilor.

Acest articol prezintă rezultatele parțiale din proiectul de cercetare care are ca obiectiv realizarea platformei software integrate pentru analiza programelor malware ale terminalelor mobile. Platforma integrează diverse tehnologii software pentru protejarea dispozitivelor mobile.

*Beyond the marketing of IT companies, în the context of escalating cyber-attacks that affect organizations around the world, cyber security solutions become the primary element în protecting IT infrastructures and devices. The proliferation of Intelligent Mobile Devices and Cloud Technologies, the Internet of Things requires new technological solutions, implemented both at hardware and software, to combat threats.*

*This paper summarizes the Integrated Software Platform for Malware Analysis of Mobile Terminals which aims to integrate various software technologies to protect mobile devices.*

*Dans le contexte d'une augmentation d'attaques informatiques qui touchent les organisations du monde entier, les solutions de cybersécurité, au-delà du marketing des entreprises de TI, deviennent l'élément principal de la protection des infrastructures et des dispositifs TI. La diversité des appareils mobiles intelligents et l'émergence des technologies de cloud computing, Internet of Things exigent, pour lutter contre les menaces, de nouvelles solutions technologiques, mises en œuvre tant au niveau du hardware, que du software.*

*L'article présente les résultats partiels lors du projet de recherche dont le but est la création d'une plate-forme logicielle intégrée pour l'analyse des programmes malware des terminaux mobiles. La plate-forme intègre une variété de technologies logicielles pour protéger les appareils mobiles.*

**Cuvinte-cheie:** analiză malware; securitate cibernetică; terminale mobile.
***Keywords:*** *malware analysis; cyber security; mobile terminal.*
***Mots-clés:*** *analyse malware; cybersécurité; terminaux mobiles.*

***Universitatea Națională de Apărare „Carol I”***
e-mail: *dragos.barbieru@adlunap.ro*
****Universitatea Națională de Apărare „Carol I”***
e-mail: *dan-suteu.antonio@unap.ro*
*****Universitatea Națională de Apărare „Carol I”***
e-mail: *esusnea@yahoo.com*

Analiza aplicațiilor malware destinată terminalelor mobile este un proces dificil, din cauza diversității platformelor mobile și a mecanismelor de securitate existente, frecvenței de apariție a noilor versiuni ale sistemelor de operare și utilizării tehnicilor de protecție a codului malware. În contextul situației naționale și internaționale, modelată de tendințele din domeniul securității, s-a simțit nevoia realizării unei platforme software care să integreze, într-un mod unitar, diferite soluții de analiză malware atât open-source, cât și comerciale, dedicate telefoniei mobile. Majoritatea actorilor din spațiul cibernetic se adaptează mediului existent, dar supremația informațională și tehnologică se obține prin inovare, așa cum susține Vice Admiral Arthur K. Cebrowski: ”I realized that military competition wasn’t about how fast one could align with reality, but how fast one could leap over it and create a new reality”[1].

Securitatea și securitatea cibernetică sunt într-o strânsă legătură, din securitate izvorând majoritatea metodelor și tehnicilor de atac și de apărare în mediul cibernetic.

Cele șapte etape ale modelului Cyber Kill Chain[2], prezentate de corporația Lockheed-Martin, sunt identice cu etapele unui atac elaborat asupra unei persoane sau unui grup de persoane. Analiza statică a aplicațiilor malware poate fi comparată cu o investigație privind stabilirea unui profil psihologic al unei persoane. Deși este mult mai rentabilă economic față de analiza dinamică, în cazul acestei analize, un program poate ascunde cod malware prin criptare sau prin diferite alte metode, la fel cum o persoană poate completa cu date false un chestionar privind personalitatea sa.

Analiza dinamică presupune execuția unui program și urmărirea tuturor parametrilor pentru a identifica activitățile suspecte, într-un mediu controlat.

Conceptul *honeypot* (borcan cu miere) și tehnicile utilizate pentru verificarea siguranței mediului în care acesta se manifestă au corespondențe în viața reală, cum ar fi, de exemplu, persoana care se află sub lupa unui detector într-un mediu sigur sau proiectat ca fiind aparent sigur de către cel care dorește să urmărească anumite evenimente. Atacurile de tipul ”distributed denial of services” sunt similare intoxicării unui adversar cu informații false, acesta consumând timp și resurse până la epuizare. Dezvoltarea rapidă a tehnologiei informației și comunicațiilor și „accesul ușor la Internet nu numai că au adus beneficii incontestabile, dar, de asemenea, aduc unele vulnerabilități mediului de securitate”[3]. Războiul hibrid, dus prin diferiți terți, se oglindește, astăzi, în lumea Internetului prin utilizarea diferitelor tehnologii proxy și a grupărilor specializate de hacking.

Atât în cazul tehnologiilor actuale, cât și în cazul celor viitoare, se vor putea identifica tipare, care, deși sunt într-un număr limitat, modurile de manifestare sunt inepuizabile. Aceste tipare nu sunt caracteristice prezentului, ci își au rădăcinile în istoria speciei noastre și reprezintă forme de atac și apărare, multe dintre ele împrumutate din biologie. Camuflajul și mimetismul sunt arme din arsenalul animalelor și pot asigura victoria împotriva unui posibil adversar[4]. Considerăm că, în spațiul cibernetic, unde manifestările de intruziune și de protecție sunt mult mai diversificate, acționează un set limitat de tipare pe care le regăsim și în biologie, acestea fiind rezultatul unui lung proces de evoluție.

Aplicațiile malware utilizează diferite tehnici de camuflaj. Acestea pot fi instalate în lanțul de distribuție, astfel un utilizator nu va putea observa nicio modificare a activității dispozitivului, care apare adesea după instalarea unui program. Compromiterea procesorului de semnal duce inevitabil la interceptarea apelurilor telefonice și a mesajelor, însă, prin folosirea corelărilor existente între DSP și CPU, atacatorii pot obține capabilități extinse asupra aplicațiilor care rulează pe terminalul mobil. Prin oferirea de aplicații gratuite sau de aplicații din magazinele neoficiale, persoanele rău intenționate pot insera cod malware. Procedura de tipul „control flow obfuscation” împiedică analiza dinamică a aplicațiilor malware. Utilizarea algoritmilor de criptare va conduce la imposibilitatea de a dezasambla și de a decompila codul unei aplicații.

Detectarea comportamentului malițios al terminalelor mobile presupune trei tipuri de analiză: analiza statică, analiza dinamică și analiza hibridă. Analiza statică presupune dezasamblarea și decompilarea unei aplicații pentru a identifica un cod malware. Analiza dinamică urmărește diferiți parametri și evenimente într-un mediu controlat de tip *sandbox*, pentru a identifica acele comportamente suspecte. Analiza hibridă combină cele două tipuri

de analiză prezentate succint anterior. Detectarea codului malware, de regulă, implică existența unei liste de semnături, dar în cazul în care acest proces eșuează, se pot utiliza algoritmi de inteligență artificială sau se poate realiza o analiză manuală. Din perspectiva învățării automate, abordarea comportamentului malițios are în vedere o serie de etape, precum: „alegerea setului inițial de date (set de antrenament), de regulă, un număr egal de aplicații sigure și de aplicații malware din care se extrag anumite caracteristici”[5].

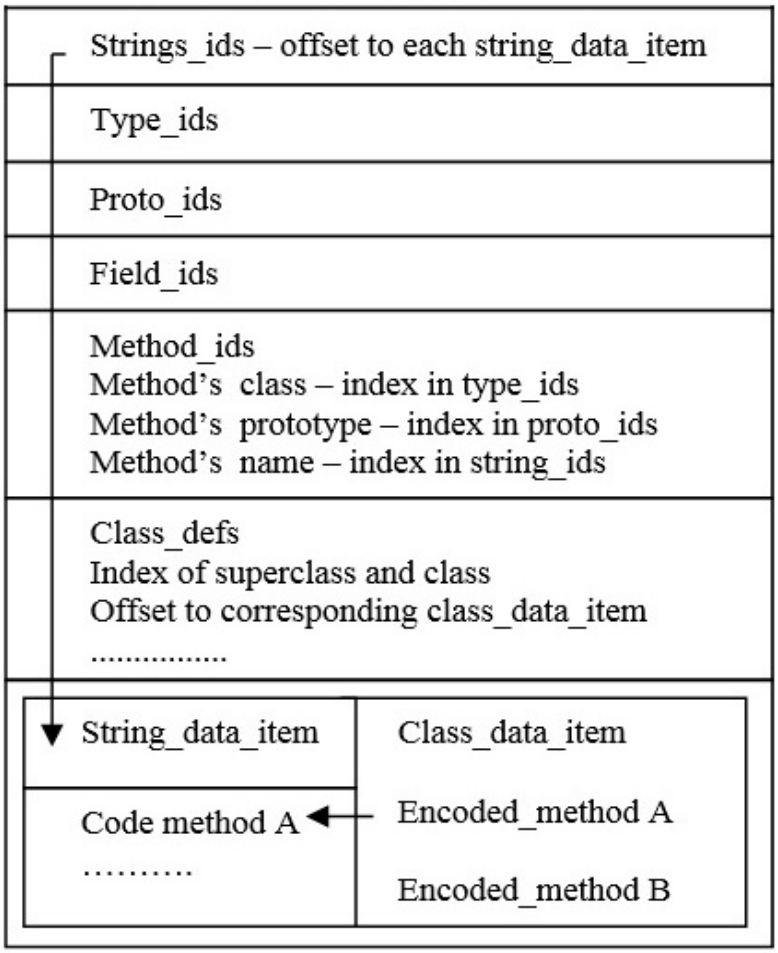



**Figura 1** *Structura unui fișier cu extensia .dex*

**Sursa:** Xiaolu Zhong, Frank Bratinger, Ibrahim Baggali, ”Rapid Android Parser for Investigating DEX files”, *Digital Investigation Journal*, vol. 17, June 2016.

Aplicând metode de selecție a caracteristicilor și algoritmi de clasificare, se obțin caracteristicile cele mai relevante pentru construirea modelului. În faza de testare, se utilizează diferite metrici pentru a evalua acuratețea modelului. Alegerea caracteristicilor nu este un proces aleatoriu. Gama algoritmilor de clasificare este diversă, abordările bazându-se pe statistică, pe rețele neuronale artificiale și pe metode axate pe nucleu. Cei mai folosiți algoritmi de clasificare sunt Naive Bayes, k- Nearest Neighbors și Suport Vector Machine.

Vulnerabilitățile pot fi de două tipuri, preinstalate sau generate de complexitatea mediului Internet. Este aproape imposibil să poți verifica și testa fiecare bucată de cod.

Platformele de dezvoltare software, cum ar fi GitHub, ar putea oferi în viitor instrumente pentru verificarea diferitelor erori apărute în cod, evitându-se astfel exploatarea lor de către atacatori.

Metodele pentru ascunderea codului malware sunt diverse și depind de facilitățile sistemului de operare al terminalului mobil[6]. De exemplu, structura unui fișier (Fig. 1) cu extensia .dex are zone alocate pentru Header, String_ids, Type_ids, Proto_ids, Fields, Methods, Classes and Data.

O clasă se regăsește în matricea *class_defs* sub forma unui index care pointează către un alt index din matricea *strings_ids*, acesta din urmă fiind conectat cu *string_data_item*, care poate returna numele clasei. Fiecare clasă definită în zona de cod este descrisă de o structură *class_data_item* care conține variabilele și metodele ei. Metodele sunt declarate sub forma unei structuri cu numele *encoded_method*. Această structură se compune din: *acces flag* – specifică cum este metoda (publică, privată, protejată etc.), *offset code* – indică adresa unde se găsește codul metodei față de începutul fișierului .dex și *method_idx_diff* – constituie un index de incrementare pentru fiecare metodă din structura *method_ids*. Primul pas pentru ascunderea unei metode constă în manipularea structurii *encoded_method* pentru a referenția o altă metodă, recalcularea sumei de control SHA1, modificarea headerului fișierului .dex și împachetarea aplicației. Manipularea structurii *encode_method* presupune o valoare pentru *method_idx_diff*, care poate fi 0 și modificarea adresei care accesează codul metodei.

Tehnica camuflajului utilizată în spațiul cibernetic poate fi recunoscută prin metode precum: criptare, oligomorfism, polymorfism și metamorpfsm[7]. Aplicațiile malware de tipul semi-polimorfic sau oligomorfic utilizează diferiți algoritmi de criptare la fiecare infecție. Diferența majoră dintre oligomorphism și polimorfism este că acesta din urmă poate utiliza un număr nelimitat de algoritmi de criptare. Metamorfismul schimbă complet codul aplicației malware și nu utilizează algoritmi de criptare. Tehnicile de mimetism se pot identifica în metodele de obfuscation a codului. Cele mai comune metode de obfuscation sunt utilizarea unui junk code (cod gunoi), substituția de variabile și regiștri, permutarea și înlocuirea instrucțiunilor, transpoziția codului și bucle infinite. Atunci când aplicațiile malware rezidă în componentele hardware, procesul de analiză este mult mai dificil.

**Platforma software integrată pentru analiza malware a terminalelor mobile**

Dezvoltarea platformei software pentru analiza malware a terminalelor mobile constă în parcurgerea unei succesiuni de etape. Astfel, prima etapă presupune identificarea modalităților uzuale și mai puțin uzuale de infectare a terminalelor mobile cu ajutorul diferitelor rapoarte de securitate și definirea unei taxonomii după anumite caracteristici, cum ar fi: vectori de atac, sursă, obiective, vulnerabilitate exploatată, tip amenințare etc.

Următoarea etapă constă în testarea aplicațiilor open-source sau comerciale pentru alegerea soluțiilor care să satisfacă cerințele de securitate. În acest sens, sunt studiate diferite proiecte de cercetare și lucrări științifice, care se referă la detectarea comportamentului suspicios și este propus un concept tehnic de firmware customizat pentru îmbunătățirea sistemului de operare. Printre soluțiile testate menționăm: Cellebrite UFED Pro Series, Cellebrite UFED Field, Cellebrite UFED Analytics, Oxygen Forensics, BlackBag Technologies, Forensic Toolkit, EnCase Forensic Software, Belkasoft Evidence Center, Autopsy, Computer Aided INvestigative Environment, Mobile security testing live environment, MOBILedit etc. Detecția aplicațiilor malware a impus instalarea și/sau verificarea unor framework-uri, cum ar fi: MODELZ[8], Andromaly[9], MADAM[10], ComDroid[11], ProfileDroid[12]. Aceste framework-uri analizate utilizează diferite caracteristici ale terminalelor mobile. De exemplu, MODELZ analizează puterea consumată de baterie atunci când rulează diferite aplicații și pe baza acestei caracteristici identifică o semnătură. În opinia noastră, principalul dezavantaj al acestei analize este necesitatea implementării unui dispozitiv extern care să achiziționeze istoricul consumului de energie într-un mod precis. În acest sens, pe perioada testării se utilizează un osciloscop extern, Agilent Infinium 54851-A, iar având în vedere rezultatele obținute, propunem construirea unui circuit extern ieftin bazat pe un microcontroler Atmel AVR.

Un alt framework utilizat este Andromaly, care necesită instalarea unei aplicații pe dispozitivul mobil pentru monitorizarea unor parametri, cum ar fi consumul CPU, numărul de pachete trimise prin Wi-Fi, numărul de procese care rulează, nivelul bateriei. Pe baza datelor colectate, sunt deduse informațiile referitoare la funcționarea normală a dispozitivului. Numărul maxim de parametri care pot fi monitorizați este de optzeci și opt.

Utilizarea algoritmilor de inteligență artificială pentru clasificare pe un număr mare de caracteristici extrase din terminalul mobil, unele dintre ele redundante sau irelevante, generează mai multe probleme, cum ar fi: infectarea algoritmului de învățare, suprasolicitarea, reducerea generalității, creșterea complexității modelului și a timpului de execuție. În opinia noastră, aplicația care implementează algoritmii de clasificare nu trebuie sa ruleze pe dispozitivele mobile, deoarece acestea sunt adesea restricționate de capacitățile de stocare și de prelucrare a datelor, precum și de puterea bateriei.

Procesul detectării comportamentului malițios devine anevoios, când unele activități malițioase sunt de scurtă durată și nu oferă date suficiente pentru detecție sau pentru antrenarea modelului. Prin urmare, nu există posibilitatea de a accesa un număr mare de baze de date cu aplicații rău intenționate pentru a crește acuratețea algoritmilor. Comportamentul malițios al unei aplicații poate fi generat de mai mulți vectori de atac, astfel clasificarea devine dificil de realizat, iar numărul mic de aplicații malware folosite ca date de intrare generează un dezechilibru. Frameworkul MADAM, deși folosește treisprezece caracteristici și a fost testat pe dispozitive mobile reale, are dezavantajul că impune drepturi de administrare asupra sistemului de operare. Acest framework

monitorizează apelurile de sistem, procesele care rulează, memoria și nivelul de utilizare a procesorului, numerele de telefon apelate, funcționarea Bluetooth și Wi-fi, mesajele SMS primite sau recepționate, perioadele de inactivitate și activitate, apăsarea tastelor.

Frameworkul Droid Detective[13] propune, pentru detectarea aplicațiilor malware, o analiză pe baza grupării permisiunilor. După extragerea permisiunilor, se va calcula frecvența de apariție a acestora când sunt grupate (gruparea permisiunilor pornește cu o permisiune și continuă până la un grup

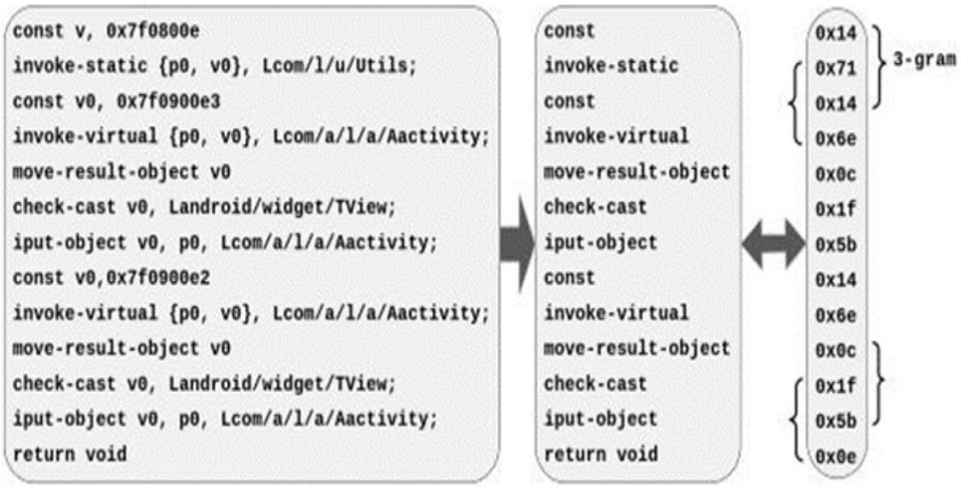



**Figura 2** *Extragerea instrucțiunilor dintr-un fișier .smali și generarea vectorului 3-gram*

**Sursa:** BooJoong Kang, Suleiman Y. Yerima, Sakir Sezer, Kieran McLaughlin, *International Journal on Cyber Situational Awareness,* vol. 1, No. 1, 2016.

de șase permisiuni) atât pentru aplicațiile sigure, cât și pentru aplicațiile malware. Grupul de permisiuni care indică un comportament malițios este identificat pentru aplicațiile care folosesc caracteristicile: ACCESS_NETWORK, INTERNET, READ_PHONE_STATE, READ_SMS și WRITE_SMS. O serie de autori[14] propun utilizarea mai multor algoritmi de clasificare pentru a îmbunătăți acuratețea detecției de malware. Se utilizează mai multe seturi de caracteristici în faza de învățare, cum ar fi: funcții API, permisiuni și comenzi ale sistemului de operare. Algoritmii utilizați sunt: Decision Tree, Simple Logistic, Naive Bayes, Partial Decision Tree și Ripple Down Rule. Numărul total de caracteristici selectate este de 179, din care 125 de permisiuni și 54 de funcții API și comenzi OS. Ca set de date de intrare, se folosește baza de date McAfee cu 2.925 de aplicații malware și 3.938 de aplicații sigure. Pentru evaluarea performanțelor algoritmilor de clasificare, se utilizează metoda 10-fold cross validation (presupune împărțirea setului de date inițial în zece părți, antrenarea pe nouă dintre ele și testarea pe unul, repetarea procedurii și verificarea acurateței). Clasificatorii RIDOR și PART au cea mai bună rată de detecție. Această abordare este completă, deoarece utilizează seturi de caracteristici diferite simultan cu algoritmi de clasificare variați. Nu se specifică modul de selecție a caracteristicilor relevante.

O abordare interesantă[15] este analiza permisiunilor cerute de aplicație în timpul execuției și cele existente în fișierul manifest. O permisiune care nu este cerută în faza inițială, poate fi cerută utilizatorului mai târziu. Ideea este că poate exista o diferență între permisiunile cerute și cele folosite de aplicație. Concluzia este că aplicațiile malware cer mai multe permisiuni decât aplicațiile sigure.

Există posibilitatea construirii unui clasificator pe baza setului de instrucțiuni de nivel jos, utilizând modelul N-gram[16]. Ca procedură de lucru, se dezasamblează aplicația pentru a genera fișiere de tip .smali. Fiecare fișier conține o clasă cu metodele aferente în formatul Dalvik bytecode. Dezasamblarea unei aplicații se face cu utilitarul apktool (Fig. 2). Din fișierele rezultate, se extrag instrucțiunile din fiecare metodă într-un șir și se calculează frecvențele lor de apariție. Fiecare instrucțiune în format Dalvik bytecode are dimensiunea de 1 byte. Numărul de instrucțiuni este de 256 la puterea 130, din care sunt folosite 218 instrucțiuni. Există 218 la puterea n posibilități de a aranja aceste instrucțiuni.

Numărul unic de n-opcodes se calculează după formula:

N = X – (N - 1),

unde X este numărul de instrucțiuni din aplicație și N reprezintă numărul de instrucțiuni dintr-o pereche. Astfel, o metodă cu 10 instrucțiuni are 10 perechi de câte o instrucțiune, nouă perechi de două instrucțiuni, opt perechi de trei instrucțiuni etc.

Clasificarea aplicațiilor malware se poate face și după un set redus de instrucțiuni[17], respectiv șase instrucțiuni. Acestea pot fi: move, jump, packed-switch, sparse-switch, invoke și if. Premisa inițială pleacă de la două întrebări: „Caracteristicile alese sunt în măsură să facă distincția între aplicațiile malware și cele sigure?”, respectiv, „Combinarea caracteristicilor alese aduce plusvaloare comparativ cu cazul în care acestea sunt tratate individual în analiza malware?”. Contribuția științifică se poate rezuma la unicitatea caracteristicilor alese cu rezultate bune, folosind resurse puține pentru analiza malware. Diferența semnificativă în identificarea aplicațiilor malware este dată de instrucțiunile *move* și *jump*. Instrucțiunile *if* și *invoke* nu aduc diferențe semnificative. Ideea de bază este că aplicațiile malware nu implementează o logică de aplicație la fel de complexă ca aplicațiile sigure.

Deoarece sistemul iOS este unul închis, provocările la adresa securității sunt mai puține. Astfel, permite revocarea/acceptul permisiunilor în mod dinamic, execută cod binar ARM, care este dificil de dezasamblat, împachetează conținutul printr-un proces anevoios față de fișierele .dex. Unul dintre vectorii de atac este reprezentat de utilizarea apelurilor API private în aplicații.

Arhitectura platformei este proiectată modular astfel încât să poată integra instrumente software criminalistice fără probleme de compatibilitate (Fig. 3). Fiecare modul este specializat pe îndeplinirea anumitor sarcini, după cum urmează:

• *Modulul interfață utilizator* – acest modul desfășoară activități de management pentru cazurile de investigație, producând atât rapoarte de securitate dinamice, cât și statice și alocând scoruri de risc pentru terminalele mobile, pe baza unei analize și evaluări specifice.

• *Modulul de autentificare/autorizare* – gestionează privilegiile de autentificare pentru utilizatorii definiți, precum și accesul la platforma web centrală.

• *Modulul parametrizare* – gestionează nomenclatoarele și oferă mijloacele de configurare a parametrilor platformei web centrale.

• *Modulul de colectare a datelor* – colectează datele și diseminează rezultatele analizelor, de asemenea calculează nivelul de infectare a aplicațiilor specifice terminalelor mobile.

• *Modulul de analiză forensic* – gestionează instrumentele și procedurile criminalistice de lucru, asigură identificarea caracteristicilor tehnice ale terminalelor mobile pentru a include aplicațiile instalate, colectează informații din terminalele mobile și susține procesul de analiză criminalistică pentru servicii web.

• *Modulul de monitorizare* – funcționează ca un agent Push, în sensul că analizează și evaluează toate aplicațiile instalate pe terminalele mobile, generând liste cu aplicații suspecte, alerte, stări și indicatorii cheie de performanță. Acest modul este conceput pentru a extinde spectrul de identificare a amenințărilor prin monitorizarea comportamentului aplicațiilor instalate pe terminalul mobil și prin transmiterea rezultatelor obținute către aplicația centrală responsabilă de colectarea și analiza datelor.

• *Modulul de inginerie inversă* – oferă capabilități de inversare prin efectuarea de încărcări și descărcări ale programelor specifice, care urmează să fie analizate.

• *Modulul de integrare a comportamentului online* – este conectat direct la modulul de analiză a comportamentului online către care transmite algoritmii de inteligență artificială și învățare automată (AI/ML) actualizați și de la care primește rezultatele analizei comportamentale online pentru o prelucrare ulterioară.

• *Modulul de analiză a comportamentului online* – dispune de o interfață web administrativă, care oferă diverse funcții, precum: Proxy, SSL, VPN, Wireless, USB și Ethernet. Modulul înregistrează datele de trafic produse atunci când terminalul mobil este conectat la platforma web prin Wi-Fi. Prin analiza rețelei, modulul oferă servicii de prevenire a intruziunilor, execută algoritmi AI/ML, detectează anomaliile cauzate de malware și transmite aceste anomalii de trafic către modulul de integrare online a comportamentului, pentru o prelucrare ulterioară. Modulul creează un profil al terminalului mobil, în corelație cu configurațiile implicite și cu traficul înregistrat, achiziționând

liste cu site-uri web clasificate drept periculoase, accesând și integrând informații furnizate de surse online despre amenințări.

• *Modulul cu instrumente criminalistice* – afișează o interfață prietenoasă cu utilizatorul, care permite extragerea și analiza paralelă, de la mai multe terminale mobile, și îndeplinește diferite sarcini, cum ar fi: extragerea datelor, analiza ulterioară a datelor, configurarea raportului pentru extragerea datelor, analiza avansată a aplicațiilor mobile, precum și funcționalitățile de recuperare a parolelor și fișierelor.

• *Agentul pentru modulul de colectare a datelor* – adună datele despre aplicațiile mobile, monitorizând mai multe caracteristici de securitate.

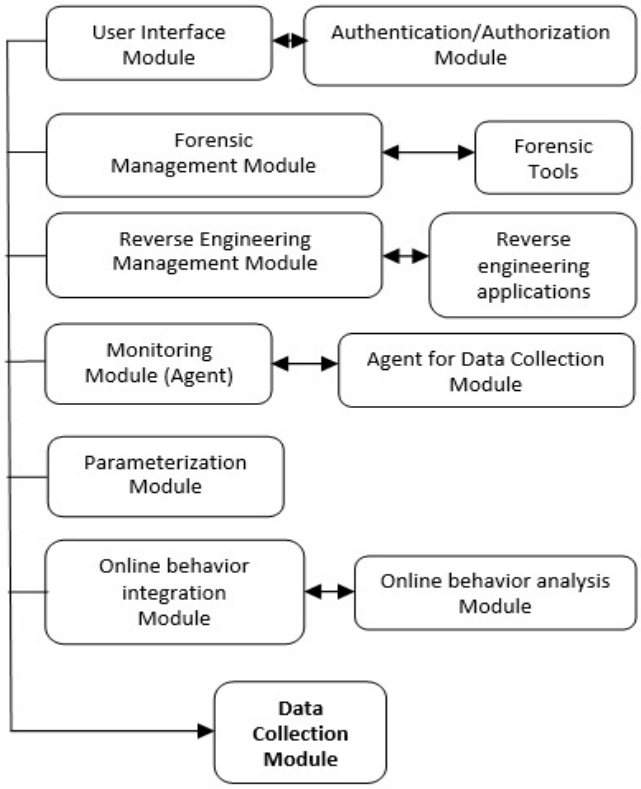



**Figura 3** *Arhitectura pentru platforma software integrată*

Astfel, colectează indicatori cheie de performanță, comparând hashes-urile primite de la magazinele de aplicații cu hashes-ul aplicațiilor mobile instalate, gestionează alertele, sprijină detectarea de malware cu ajutorul listelor de semnături, profilează terminalul mobil, corelează configurația implicită cu aplicațiile instalate.

• *Modulul de aplicații de inginerie inversă* – este proiectat să realizeze analiza statică și dinamică a terminalelor mobile printr-un sistem de tip Sandbox. Acesta trimite rapoarte JSON/HTML către platforma centrală web, evaluează rezultatele analizei și identifică automat comportamentul unei aplicații malware.

Pentru a asigura funcționalitatea necesară, este folosit un server de virtualizare Proxmox KVM, pe care sunt create mașinile virtuale care susțin diferite servicii și aplicații. Mașinile virtuale folosesc containere Docker, care integrează Kubernetes pentru a coordona planificarea și execuția containerelor. Pentru administrarea containerelor, se folosește LXD, care este un sistem de generație nouă și oferă servicii de tipul API REST.

Utilizarea containerelor permite crearea de microservicii, aplicațiile fiind astfel decuplate pentru a putea fi instalate și administrate în mod dinamic.

Mașina virtuală VM3 este responsabilă de baza de date PostgreSQL pentru rularea serviciului torsim-database. Tot în această mașină virtuală sunt instalate instrumentele Apache Kafka și Elasticsearch. Utilitarele ADB folosite pentru asigurarea funcționalităților forensic sunt: Android Debug Bridge și MOBILedit. Serviciul torsim-adb înglobează clientul de ADB, care comunică cu serverul ADB instalat pe laptop, iar acesta comunică cu deamonul ADB de pe terminalul mobil. Momentan, integrarea cu MOBILedit este realizată la nivel procedural, rularea MOBILedit se face manual și se obține raportul dorit, care se încarcă apoi în platforma centrală.

Pentru interceptarea traficului generat de dispozitivele mobile, se folosește utilitarul Bro. Acesta trimite pachetele interceptate într-o coadă de mesaje Kafka, care sunt apoi preluate de serviciul torsim-messageprocessor și trimise în Elasticsearch. Pentru analiza traficului și determinarea comportamentului malițios, se folosește un sistem de detecție a traficului malițios, denumit Maltrail. Aplicația Mailtrail utilizează listele publice cu site-uri de încredere și cu site-uri malițioase, informațiile din rapoartele diferitelor produse antivirus, listele particularizate, unde semnăturile pot fi nume de domenii, IP-urile, valoarea din header a HTTP User-Agent și mecanismele euristice, care pot ajuta la descoperirea de malware încă necunoscut.

Tabelul 1

**FLUXURI ÎNTRE APLICAȚII ȘI SERVICII**

| Nr. | Table Column Head | | |
|---|---|---|---|
| | *Serviciu/aplicație* | *Mașină virtuală* | *Rol* |
| 1 | nginx | VM 1 | Frontend-ul web preia cereri de la clienți |
| 2 | torsim-proxy | VM 1 | Interfața grafică a aplicației și serviciile securizate primesc cereri de la frontend-ul web (nginx) |
| 3 | torsim-bro-logtail | VM 2 | Preia traficul înregistrat de mașină și îl salvează într-o coadă din Kafka |
| 4 | torsim-message-processor | VM 1 | Preia cereri de la torsim-proxy |
| 5 | MobSF, CuckooDroid | VM 1 | Preia cereri de la torsim-proxy |
| 6 | torsim-adb | VM 1 | API-ul torsim-adb preia cereri de la torsim-proxy |
| 7 | Torsim-database | VM 3 | API-ul torsim-database preia cereri de la torsim-adb și torsim-proxy |
| 8 | PostgreSQL | VM 3 | Preia cereri de la containerul torsim-database |
| 9 | Elasticsearch | VM 3 | Preia cereri de la torsim-message-processor |
| 10 | Kafka | VM 3 | Preia cereri de la torsim-message-processor |

Mașina virtuală VM 1 are instalat CuckooDroid, o extensie a Cuckoo Sandbox. CuckooDroid este un software open source, utilizat în analiza fișierelor suspicioase, cu capabilități în analiza statică și dinamică a aplicațiilor Android. De asemenea, framework-ul MobSF permite analiza statică și dinamică a aplicațiilor mobile. S-a folosit un container Docker pentru aplicația MobSF, care face analiza statică, iar integrarea cu platforma centrală s-a făcut prin API-ul MobSF. Astfel, aplicațiile pot fi trimise spre a fi analizate, obținându-se raportul atât în format PDF, cât și în format JSON. Acesta din urmă este folosit pentru a stoca datele scanării în baza de date și pentru a le afișa în interfața web.

O etapă importantă în analiza malware o constituie testarea platformei prin verificarea tuturor parametrilor introduși și obținerea de rapoarte corecte. Modulul agent este încă în faza de dezvoltare și va fi suportat de Android și IOS. Agentul trebuie să ruleze pe telefoane nerootate și urmărește permisiunile solicitate de aplicații, instalate înainte și în timpul rulării aplicațiilor. Se pot urmări respectivele caracteristici: accesarea rețelei și a datelor sensibile (precum lista de contacte și locația), recepționarea și transmiterea de SMS-uri, datele din clipboard, accesul la diferite componente hardware, numărul de click-uri în perioada de activitate intensă a utilizatorului, corelată cu perioada de inactivitate. În plus, agentul poate fi integrat cu API-ul public, pus la dispoziție de către VirusTotal, pentru a verifica autenticitatea pachetului apk, prin compararea hash-ului aplicației cu baza de date a site-ului. Se verifică fișierele de configurare a aplicațiilor, pentru a identifica versiunea aplicației, resursele hardware care vor fi solicitate, permisiunile care urmează să fie alocate, componentele, lista de permisiuni periculoase. Existența unor șiruri suspecte de caractere în aplicație poate fi un indicator al prezenței unei infectări cu malware. Cu ajutorul entropiei se identifică dacă există zone de cod criptate.

## Concluzii

Noile progrese în materie de inteligență artificială și de învățare automată au permis apariția unei noi etape în evoluția securității cibernetice. Literatura studiată pentru dezvoltarea arhitecturii platformei include doar algoritmi de învățare supervizată. Au fost testate diverse soluții software de securitate a terminalelor mobile și a fost construită infrastructura hardware și software. Proiectul de cercetare nu este finalizat, urmează

faza de testare a aplicațiilor malware selectate de experții proiectului.

Această lucrare a fost posibilă cu sprijinul financiar al UEFISCDI/Ministerului Educației Naționale din România, proiectul PN-III-P2-2.1-SOL-2016-05-0070, cu titlul „Platformă software integrată pentru analiza programelor malware pe terminalele mobile”.

**NOTE:**

1 James R. Blake, *Transforming military*, Praeger Security International, May 2007, accesat la 12 feb. 2019.

2 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, accesat la 12 feb. 2019.

3 Elena Șușnea, Adrian Iftene, ”The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT)”, *Conference on Mathematical Foundations of Informatics MFOI’2018, Institute of Mathematics and Computer*, Chișinău, Moldova, pp. 230-240, 2018.

4 Reza Hedayat, Lorenzo Cavallaro, ”The Devil’s Right Hand: An Investigation on Malware-oriented Obfuscation Techniques”, *Computer Weekly*, August 2016.

5 Dragoș Bărbieru, Alexandru Stoica, ”Malware Analysis on Mobile Phone”, *The International Scientific Conference eLearning and Software for Education*, vol. 4, ”Carol I” National Defence University, Bucharest, 2018, pp. 11-15.

6 https://fortiguard.com/events/755/2013-10-25-playing-hide-and-seek-with-dalvik-executables, accesat la 12 feb. 2019.

7 Babak Bashari Rad, Maslin Masrom, Suhaimi Ibrahim, ”Camouflage in Malware: from Encryption to Metamorphism”, *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, No. 8, August 2012.

8 Hannsang Kim, Member IEEE, Kang G. Shin, Padmanabhan Pillai, ”MODELZ: Monitoring, Detection and Analysis of Energy-Greedy Anomalies in Mobile Handsets”, *IEEE Transactions on mobile computing*, vol. 10, July 2011.

9 Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, Yael Weiss, *Andromaly: a behavioral malware detection framework for android devices.*

10 Gianluca Dini, Fabio Martinelli, Andrea Saracino, Daniele Sgandurra, ”MADAM: a Multi-Level Anomaly Detector for Android Malware, Computer Network Security”, *6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012*, St. Petersburg, Russia, October 17-19, 2012.

11 C E.hin, A.P. Felt,. K Greenwood, D. Wagner, ”Analyzing inter-application communication in Android”, *Proc. 9th Int. Conf. On Mobile Systems, Applications, and Services (MobiSys ‘11). ACM*, Washington, DC, USA, June 2011, pp. 239-252.

12 X. Wei, L. Gomez, I. Neamtiu, M. Faloutsos, ”ProfileDroid: multi-layer profiling of android applications”, *Proc. 18th Int. Conf. On Mobile Computing and Networking (Mobicom ‘12). ACM*, Istanbul, Turkey, August 2012, pp. 137-148.

13 Shuang Liang, Xiaojiang Du, *Permission-combination-based scheme for Android mobile malware detection*, IEEE International Conference on Communications (ICC), Sydney, June 2014.

14 Suleiman Y. Yerima, Sakir Sezer, Igor Muttik, ”Android Malware Detection Using Parallel Machine Learning Classifiers”, *Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*, December, 2014.

15 Xing Liu, Jiqiang Liu, ”A Two-Layered Permission-Based Android Malware Detection Scheme, *2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, April, UK, Oxford, 2014.

16 BooJoong Kang, Suleiman Y. Yerima, Sakir Sezer, Kieran McLaughlin, *International Journal on Cyber Situational Awareness*, vol. 1, No. 1, 2016, pp. 231-255.

17 Gerardo Canfora, Francesco Mercaldo, Corrado Aaron Visaggio, ”Mobile malware detection using op-code frequency histograms”, 12th International Joint Conference on e-Business and Telecommunications (ICETE), Paris, July 2016.

## BIBLIOGRAFIE

Babak Bashari Rad, Maslin Masrom, Suhaimi Ibrahim, ”Camouflage in Malware: from Encryption to Metamorphism”, *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, No. 8, August 2012.

Bărbieru Dragoş, Stoica Alexandru, ”Malware Analysis on Mobile Phone”, *The International Scientific Conference eLearning and Software for Education*, vol. 4, ”Carol I” National Defence University, Bucharest, 2018.

Blake R. James, *Transforming military*, Praeger Security International, May 2007.

Canfora Gerardo, Mercaldo Francesco, Visaggio Corrado Aaron, ”Mobile malware detection using op-code frequency histograms”, *12th International Joint Conference on e-Business and Telecommunications (ICETE)*, July 2016.

Chin E., Felt A.P., Greenwood K., Wagner D., ”Analyzing inter-application communication în Android”, *Proc. 9th Int. Conf. On Mobile Systems, Applications, and Services (MobiSys ‘11). ACM*, Washington, DC, USA, June 2011.

Dini Gianluca, Martinelli Fabio, Saracino Andrea, Sgandurra Daniele, ”MADAM: a Multi-Level Anomaly Detector for Android Malware”, *Computer Network Security: 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012*, St. Petersburg, Russia, October 17-19, 2012.

Hannsang Kim, Member IEEE, Kang G. Shin, Padmanabhan Pillai, ”MODELZ: Monitoring, Detection and Analysis of Energy-Greedy

Anomalies în Mobile Handsets”, *IEEE Transactions on mobile computing*, vol. 10, July 2011.

Hedayat Reza, Cavallaro Lorenzo, ”The Devil’s Right Hand: An Investigation on Malware-oriented Obfuscation Techniques”, *Computer Weekly*, August 2016.

Kang BooJoong, Yerima Y. Suleiman, Sezer Sakir, McLaughlin Kieran, *International Journal on Cyber Situational Awareness*, Vol. 1, No. 1, 2016.

Shabtai Asaf, Kanonov Uri, Elovici Yuval, Glezer Chanan, Weiss Yael, *Andromaly: a behavioral malware detection framework for android devices*.

Shuang Liang, Xiaojiang Du, ”Permission-combination-based scheme for Android mobile malware detection”, *IEEE International Conference on Communications (ICC)*, June 2014.

Șușnea Elena, Iftene Adrian, ”The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT)”, *Conference on Mathematical Foundations of Informatics MFOI’2018*, Institute of Mathematics and Computer, Chisinau, Moldova, 2018.

Wei X., Gomez L., Neamtiu I., Faloutsos M., ”ProfileDroid: multi-layer profiling of android applications”, *Proc. 18th Int. Conf. On Mobile Computing and Networking (Mobicom ‘12). ACM*, Istanbul, Turkey, August 2012.

Xing Liu, Jiqiang Liu, ”A Two-Layered Permission-Based Android Malware Detection Scheme”, 2nd *IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, April, 2014.

Yerima Y. Suleiman, Sezer Sakir, Muttik Igor, ”Android Malware Detection Using Parallel Machine Learning Classifiers”, *Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*, UK, Oxford, December, 2014.

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://fortiguard.com/events/755/2013-10-25-playing-hide-and-seek-with-dalvik-executables

# ANALIZA STRATEGIILOR MARITIME ALE NATO ȘI UE

## *ANALYSIS OF NATO AND EU MARITIME STRATEGIES*

## *ANALYSE DES STRATÉGIES MARITIMES DE L'OTAN ET DE L'UE*

**Cpt.cdor.drd. Valentin - Cătălin VLAD***

În contextul actualizării sau inițializării strategiilor maritime ale NATO sau ale Uniunii Europene, asigurarea, menținerea și promovarea securității, stabilității și prosperității spațiului maritim euroatlantic trebuie să ocupe prim-planul procesului de eficientizare și armonizare a securității maritime transatlantice prin prisma faptului că Alianța și Uniunea și-au asumat valori și interese similare și vizează același spațiu maritim vital – spațiul maritim euroatlantic.

În acest sens, analiza strategiilor maritime ale NATO și Uniunii Europene reprezintă elementul cheie al înțelegerii viziunii, nivelului de ambiție și intereselor promovate de cele două organizații în scopul determinării elementelor de convergență pe care să poată fi clădit un curs de acțiune complementar, în sprijinul asigurării securității maritime euroatlantice.

*In the context of the upgrading or initiation of NATO or European Union's maritime strategies, ensuring, maintaining and promoting the security, stability and prosperity of the Euroatlantic maritime space must be at the forefront of the process of streamlining and harmonizing transatlantic maritime security due to the fact that the Alliance and the Union have assumed similar values and interests and have targeted the same vital maritime space - the Euro-Atlantic maritime space.*

*In this respect, the analysis of NATO and the European Union's maritime strategies is the key element of understanding the vision, ambition and interest of the two organizations in order to determine the convergence elements on which a complementary action course to support maritime security euro-Atlantic.*

*Dans le contexte de l'actualisation ou de l'initialisation des stratégies maritimes de l'OTAN ou de l'Union européenne, la nécessité d'assurer, de maintenir et de promouvoir la sécurité, la stabilité et la prospérité de l'espace maritime euro-atlantique doit s'imposer dans le processus d'harmonisation et de rendre plus efficace la sécurité maritime transatlantique, compte tenu du fait que l'Alliance et l'Union partagent des valeurs et des intérêts similaires et visent le même espace maritime vital – l'espace maritime euro-atlantique.*

*À cet égard, l'analyse des stratégies maritimes de l'OTAN et de l'Union européenne constitue l'élément essentiel pour comprendre la vision, l'ambition et les intérêts de ces organisations afin de déterminer les éléments de convergence sur lesquels un plan d'action complémentaire pourrait être adopté à l'appui de la sécurité maritime euro-atlantique.*

**Cuvinte-cheie:** securitate maritimă euroatlantică; strategii de securitate maritimă; cooperare regională.
***Keywords:*** *Euroatlantic maritime security; maritime security strategies; regional cooperation.*
***Mots-clés:*** *sécurité maritime euro-atlantique; stratégies de sécurité maritime; coopération régionale.*

Evoluția mediului de securitate global din ultimii ani a fost determinată de o accentuare a provocărilor și amenințărilor venite în special din spațiul maritim, drept pentru care comunitatea euroatlantică și-a reevaluat și și-a declarat prioritățile și interesele de securitate maritimă prin intermediul propriilor strategii maritime de securitate.

***Statul Major al Forțelor Navale**
e-mail: *valentin.vlad@navy.ro*

În acest sens, doamna Federica Mogherini (Înalt Reprezentant pentru politica externă de securitate al UE) afirma faptul că EUMSS este modalitatea prin care Uniunea Europeană „își reafirmă rolul de furnizor global de securitate maritimă, promovând cooperarea, multilateralismul maritim și dreptul maritim în directă corelație cu prioritățile indicate de Strategia Globală a UE”[1].

Prin *Strategia Maritimă Aliată (AMS)* și *Strategia Maritimă a Uniunii Europene (EUMSS)*, NATO și UE au vizat, pe de o parte, să contracareze amenințări la adresa securității maritime

euroatlantice și internaționale, precum migrația ilegală, pirateria, criminalitatea transfrontalieră, terorismul, traficul de armament și de materiale interzise, iar pe de altă parte, să fructifice credibilitatea și legitimitatea, dobândite ca urmare a recunoașterii acordate de Organizația Națiunilor Unite (ONU) pentru contribuția determinantă la reușita principalelor operații sau acțiuni desfășurate în ultimii ani, pentru asigurarea securității maritime internaționale în Marea Mediterană, în Marea Egee sau în Golful Aden – operațiile ”Ocean Shield” (OOS), ”Atalanta”, ”Unified Protector” (OUP), ”Sophia”, ”Active Endeavour” (OAE) / ”Sea Guardian” (OSG) sau Acțiunea pentru Combaterea Migrației Ilegale din Marea Egee (AEG).

**Fundamentele strategiilor maritime euroatlantice**

Sub deviza că „marea contează”[2], UE și-a elaborat și și-a adoptat, în premieră, în anul 2014, Strategia Maritimă de Securitate a Uniunii Europene (EUMSS)[3], centrată, în principal, pe asigurarea securității maritime proprii, dar mai ales pe promovarea și valorificarea statutului de actor relevant pentru securitatea regională și internațională, în baza legitimității oferite de cadrul legal internațional.

EUMSS are drept curs de acțiune inițierea și dezvoltarea cooperării în domeniul securității maritime cu principalii actori internaționali, într-o abordare cuprinzătoare interinstituțională și multidomeniu, la nivelul principalelor bazine din spațiul maritim european – Marea Baltică, Marea Neagră, Marea Mediterană, Marea Nordului, Oceanul Atlantic, apele arctice și internaționale.

Focalizarea regională a EUMSS subscrie teoriei lui Taylor[4], de evitare a globalizării unei comunități de securitate, drept pentru care se poate spune că strategia are un fundament conceptual care să-i permită să poate fi pusă în aplicare eficient pe cele patru direcții definite de abordarea interinstituțională, integritatea funcțională, respectul pentru reguli și principii și multilateralismul maritim.

Prin cele patru direcții de acțiune, Uniunea Europeană își propune să-și angajeze și să-și relaționeze credibil și legitim toate structurile militare și civile într-un efort comun, propriu și internațional, pentru asigurarea securității maritime proprii și internaționale.

Astfel, multilateralismul cooperării maritime de securitate cu actori internaționali relevanți (NATO, ONU, Organizația Maritimă Internațională – IMO) se completează reciproc cu integritatea funcțională care asigură afirmarea și impunerea drepturilor și jurisdicției oferite Uniunii de cadrul legislativ internațional.

Ca urmare a prevederilor Conceptului Strategic Aliat[5], NATO își adoptă, la 18 martie 2011, propria Strategie Maritimă Aliată (AMS)[6], cu scopul de a securiza spațiul maritim euroatlantic prin cooperare interinstituțională și multidomeniu cu actorii relevanți regionali și internaționali, în condiții de deplină legitimitate.

Ca și în cazul Uniunii, NATO, în calitatea sa de promovatoare a valorilor, drepturilor și libertăților garantate de prevederile legale internaționale, își propune să subscrie eforturilor regionale și internaționale pentru garantarea securității maritime.

Astfel, prin intermediul Strategiei Maritime Aliate, NATO își propune să realizeze securitatea maritimă euroatlantică și internațională, acționând pentru descurajarea și apărarea colectivă, pentru managementul crizelor și pentru securitatea maritimă, prin cooperare, în deplină concordanță cu prevederile legilor, acordurilor și tratatelor internaționale (Carta ONU, Convenția Internațională privind Dreptul Mării).

În esență, elementele definitorii care creează fundamentul celor două strategii maritime sunt reprezentate așadar de respectul față de valorile, drepturile și libertățile internaționale, așa cum sunt ele promovate de Carta Națiunilor Unite, dar mai ales de faptul că NATO și Uniunea Europeană sunt deschise cooperării și se indică reciproc ca fiind principalii parteneri pe linia asigurării, menținerii și garantării securității, stabilității și prosperității maritime euroatlantice și internaționale. De asemenea, orientarea NATO și UE spre cooperare regională este văzută ca fiind elementul cheie al procesului de eficientizare a securității maritime euroatlantice și internaționale și, așa cum subliniam anterior, ea subscrie teoriei lui Taylor, conform căreia universalitatea unei comunități de securitate este imposibilă[7].

**Elementele comune ale AMS și EUMSS**

Pentru a putea vorbi despre o eficientizare a procesului de asigurare a securității maritime

euroatlantice, este necesară aducerea la un numitor comun, din punct de vedere conceptual și acțional, a strategiilor maritime ale NATO și UE.

Conform prevederilor propriilor strategii maritime, NATO și UE vizează descurajarea amenințărilor, asigurarea apărării colective, managementul crizelor și securitatea maritimă, respectiv managementul riscului, prevenirea conflictelor și răspunsul la crize, ceea ce evidențiază viziuni strategice comune din punctul de vedere al asigurării securității maritime euroatlantice și internaționale, aspect absolut firesc, ținând cont de faptul că Alianța și Uniunea promovează și apără valorile și interesele a 22 de state care se regăsesc în rândul ambelor organizații.

Astfel, elementele care definesc numitorul comun al celor două strategii sunt reprezentate de încrederea și respectul reciproc, de considerația față de legislația maritimă internațională, de valorile și drepturile individuale și colective universale, de interesul pentru cooperarea maritimă regională cuprinzătoare, de nivelul de ambiție global, de spațiul maritim de interes comun (euroatlantic) și, în special, de faptul că vizează, în proporție de peste 75 %, capabilități maritime ce aparțin acelorași state (22 din 29 de state membre ale NATO sunt și membre ale UE – 76 %).

Afirmarea disponibilității de a-și promova și de a-și apăra interesele la nivel global în condiții legitime conferă NATO și UE anvergura de actori maritimi internaționali, agreați și creditați de ONU ca adevărate repere pentru securitatea, stabilitatea și prosperitatea maritimă internațională.

În acest sens, interesul NATO și UE pentru dezvoltarea comunităților regionale de securitate la nivelul principalelor bazine maritime euroatlantice se încadrează perfect în prevederile Cartei ONU[8] și devine centrul de greutate al procesului de eficientizare a securității maritime euroatlantice și internaționale prin cooperare regională, deoarece va considera și va fructifica oportunitățile și vulnerabilitățile fiecărui bazin maritim în parte.

Această abordare pune în valoare considerația statelor și actorilor regionali și internaționali relevanți pentru legile și tratatele internaționale, favorizează acceptarea, sprijinul, responsabilizarea și implicarea acestora în cadrul efortului comun de asigurare a securității maritime internaționale.

Astfel, dacă este să ne referim la cea de-a doua mare putere maritimă a lumii, Federația Rusă, notăm că aceasta își declară, prin noua sa Doctrină Maritimă[9], intenția de a-și promova și de a-și apăra interesele maritime globale într-o abordare cuprinzătoare, bazată pe dezvoltarea unor capabilități maritime moderne care să-i permită prezența la nivel regional și internațional, în condiții de deplină legitimitate internațională.

Aceeași orientare asupra cooperării maritime regionale legitime este împărtășită și de principala putere maritimă a lumii, Statele Unite ale Americii, prin propria strategie maritimă, croită în jurul viziunii fostului comandant al Forțelor Navale Americane, amiralul Jonathan William Greenert: „Realitatea prezentă este că trebuie să ne gândim la o rețea globală de forțe navale. Tot ceea ce trebuie să facem este să avem voința de a coopera, nefiind nevoie de un angajament sau de o subscriere la o alianță, ci numai de a contribui pe sistemul – te conectezi și joci. Este o misiune pentru fiecare, fie că este vorba despre asistență umanitară și sprijin, în caz de dezastre naturale, fie despre contraterorism, combaterea criminalității transfrontaliere sau combaterea pirateriei”[10].

Totuși, numitorul comun conceptual al celor două strategii maritime euroatlantice (AMS, EUMSS), focalizat pe cooperare maritimă regională cuprinzătoare, nu a fost întotdeauna completat de o unitate de efort pentru transpunerea în practică a prevederilor lor, din diverse cauze, care pot fi atribuite lipsei viziunii strategice comune și complementarității acționale dintre NATO și UE, care nu de puține ori a consemnat rivalități, indecizii, precipitare sau reorientare, ce au tensionat legătura istorică transatlantică, marcată de numeroase episoade declarative tăioase[11] [12] între principalii liderii europeni, Angela Merkel, Emmanuel Macron și președintele Statelor Unite ale Americii, Donald Trump.

Astfel, aserțiuni ca „vremurile în care europenii se puteau baza pe alții (Marea Britanie și SUA – NATO) s-au terminat”[13] și ei „trebuie să-și ia soarta în propriile mâini”[14] rezonează negativ cu faptul că „armata UE nu reprezintă o armată împotriva NATO, ci un bun complement al acesteia”[15], unde Marea Britanie și SUA reprezintă două superputeri maritime, ale căror capabilități nucleare sunt completate de cea a Franței, rămasă singulară, în ipoteza creditării viziunii doamnei Merkel, pentru asigurarea descurajării nucleare strategice împotriva oricăror amenințări de natură

simetrică sau asimetrică, ce ar putea pune în pericol securitatea și stabilitatea euroatlantică.

Toată această polemică a generat lipsa unei viziuni strategice complementare a binomului NATO – UE și a determinat statele din flancul estic, confruntate cu provocări și amenințări crescânde de natură economică sau de securitate, să inițieze și să dezvolte comunități de cooperare, precum *Inițiativa celor Trei Mări (3SI)*[16] sau *București 9 (B9)*[17]. Această direcție de acțiune a reprezentat dovada înțelegerii nevoii eficientizării strategiilor euroatlantice prin focalizarea regională, dar și prin nedumerirea statelor europene mici în ceea ce privește percepția unei viziuni euroatlantice comune care să respecte aranjamentele politico-militare sau politico-economice existente.

Cu toate acestea, trebuie remarcat faptul că, cel puțin până la acest moment, polemica declarativă nu a fracturat legătura transatlantică, iar NATO a continuat să beneficieze de suportul de neegalat al SUA[18] și să formuleze o poziție fermă în ceea ce privește garanțiile de securitate colectivă a membrilor săi prin sporirea prezenței și sprijinului pe flancul estic, ca urmare a evoluției situației geopolitice, după evenimentele din bazinul Mării Negre, din 2014.

De asemenea, trebuie remarcat și efortul pe care Uniunea Europeană l-a depus și continuă să-l depună pentru asigurarea securității maritime euroatlantice și internaționale împotriva migrației ilegale sau pirateriei în Marea Egee, în Marea Mediterană sau în Golful Aden.

**Concluzii**

Diminuarea efortului operativ al capabilităților maritime care aparțin statelor membre ale NATO și ale UE și articularea unui răspuns strategic euroatlantic comun reprezintă esența procesului de eficientizare a strategiilor maritime ale NATO și UE, iar în acest sens, definirea complementarității conceptuale și acționale euroatlantice și adoptarea unui posibil model de securitate prin cooperare maritimă, care să fructifice teoriile comunităților de securitate, inițiate și dezvoltate de Wagenen, Deutsch, Adler, Barnett, Taylor, Cohen sau Mihalka, trebuie să ocupe agendele liderilor NATO și UE.

Numai în acest mod relația dintre NATO[19] și Uniunea Europeană va căpăta dimensiunea unui tot unitar, și cele două organisme vor putea valorifica forța legăturii transatlantice istorice și avantajele oferite de instrumentele politico-militare, pe de o parte, și politico-economice, pe de altă parte.

Drept urmare, adoptarea unui model de securitate maritimă prin cooperare regională, bazat pe complementaritatea NATO – UE, ar asigura valorificarea numitorului comun conceptual și, implicit, execuția oportună, credibilă și legitimă a celor două strategii maritime euroatlantice, în beneficiul securității maritime euroatlantice și internaționale.

În concluzie, cele două strategii, Strategia Maritimă Aliată și Strategia Maritimă a Uniunii Europene, promovează viziuni conceptuale convergente asupra asigurării securității maritime, iar eficientizarea procesului securității maritime euroatlantice și internaționale trebuie să se situeze pe coordonatele complementarității doctrinale și acționale ale binomului NATO – UE.

**NOTE:**

1 *** *Maritime security: EU revises its action plan*, EU, 26 iunie 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/, accesat la 20 aprilie 2019.

2 *** *European Union Maritime Security Strategy (EUMSS)*, 2014, p. 2, https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT, accesat la 22 aprilie 2019.

3 *Ibidem*.

4 Michael Taylor, *Community, Anarchy and Liberty*, Cambridge University Press, New York, 1982, pp. 167-168.

5 *** *NATO Strategic Concept, NATO*, 2010, https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf, accesat la 24 aprilie 2019.

6 *** *Alliance Maritime Strategy*, NATO, 2011, https://www.nato.int/cps/ua/natohq/official_texts_75615.htm, accesat la 24 aprilie 2019.

7 Michael Taylor, *op.cit.*, pp. 167-168.

8 *** *Carta ONU*, 1945, cap. VIII, https://www.un.org/en/sections/un-charter/chapter-viii/index.html, accesat la 26 aprilie 2019.

9 *** *Maritime Doctrine of the Russian Federation*, Russian Maritime Studies Institute (US Naval War College translation), 2015, pp. 7-8., https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/Maritime%20Doctrine%20TransENGrus_FINAL.pdf?sr=b&si=DNNFileManagerPolicy&sig=fqZgUUVRVRrKmSFNMOj%2FNaRNawUoRdhdvpFJj7%2FpAkM%3D, accesat la 29 aprilie 2019.

10 *** *A Cooperative Strategy for 21st Century Seapower*, US Navy, martie 2015, p. 5., http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf, accesat la 3 mai 2019.

11 *** „Angela Merkel: EU cannot completely rely on US and Britain any more”, *The Guardian*, 2017, https://www.theguardian.com/world/2017/may/28/merkel-says-

eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks, accesat la 4 mai 2019.

12 ”Trump demands NATO countries meet defense spending goals «immediately»”, *CNBC*, 2018, https://www.cnbc.com/2018/07/11/trump-demands-nato-countries-meet-defense-spending-goals-immediately.html, accesat la 5 mai 2019.

13 ”Angela Merkel: EU cannot completely rely on US and Britain any more”, *The Guardian*, 2017, https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks, accesat la 4 mai 2019.

14 *Ibidem*.

15 ”Merkel joins Macron in calling for EU army to complement NATO”, *Politico*, Bruxelles, 2018, https://www.politico.eu/article/angela-merkel-emmanuel-macron-eu-army-to-complement-nato/, accesat la 5 mai 2019.

16 Inițiativa celor trei mări, http://three-seas.eu/, accesat la 11 mai 2019.

17 *** *Declarație comună a miniștrilor de externe din statele Formatului București 9 (B9)*, MAE, 2017, https://www.mae.ro/node/43571, accesat la 11 mai 2019.

18 *** *SNMG-1 and SNMCMG-1 Conduct Change of Command*, NATO, 2019, https://mc.nato.int/media-centre/news/2019/snmg1-conducts-change-of-command.aspx, accesat la 18 aprilie 2019.

19 *** *Relations with the European Union*, https://www.nato.int/cps/en/natohq/topics_49217.htm, accesat la 18 mai 2019.

## BIBLIOGRAFIE


*** *A Cooperative Strategy for 21st Century Seapower: Forward, Engaged, Ready (CS21R),* http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf

*** AAP 6, *NATO Glossary Of Terms And Definitions* (English And French), Edition 2013.

*** *A ”comprehensive approach”’ to crises*, NATO, 2016, https://www.nato.int/cps/en/natolive/topics_51633.htm

*** *A comprehensive approach*, NATO, 2009, https://www.nato.int/summit2009/topics_en/19-comprehensive_approach.html

*** *A Cooperative Strategy for 21st Century Seapower*, US Navy, martie 2015, http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf

*** *A framework for enhanced international maritime security cooperation and awareness*, CJOS COE, 2011, http://cjoscoe.org/docs/MSA_Strategic_Framework_V1.0.pdf

*** *A Global Strategy for the European Union's Foreign and Security Policy*, EU, 2016, http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

*** *AlliedJointDoctrine(AJP-01)*,NATO,2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf

*** *Allied Maritime Strategy – A theory for success?*, Kiel International Seapower Symposium Conference Report, 2018, https://www.kielseapowerseries.com/files/ispk/content/KISS18/KISS2018_final_Web.pdf

*** *Alliance Maritime Strategy*, NATO, 2011, https://www.nato.int/cps/ua/natohq/official_texts_75615.htm

*** *Carta Națiunilor Unite*, ONU, 1945, https://www.un.org/en/sections/un-charter/chapter-viii/index.html

*** Angela Merkel, „EU cannot completely rely on US and Britain any more”, *The Guardian*, 2017, https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks

*** *Consolidated Version of the Treaty on European Union*, UE, 2007.

*** *Cooperarea în domeniul apărării: Consiliul instituie cooperarea structurată permanentă (PESCO), cu participarea a 25 de state membre*, Consiliul Uniunii Europene, 2017.

*** *Cooperarea la nivelul UE în domeniul apărării: Consiliul instituie o capabilitate militară de planificare și conducere (MPCC)*, Consiliul Uniunii Europene, 8 iunie 2017, https://www.consilium.europa.eu/ro/press/press-releases/2017/06/08/military-mpcc-planning-conduct-capability/

*** Council conclusions on the revision of the European Union Maritime Security Strategy - Action Plan, EU, 26 iunie 2018, accesat de pe http://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf

*** European Union Maritime Security Strategy, EU, 2014, https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT

*** European Union Maritime Security Strategy – Action Plan (EUMSS AP), EU, 2014, https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf

*** Joint declaration on eu-nato cooperation by the president of the european council, the president of the european commission, and the secretary general of the north atlantic treaty organization,

EU, 2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm

*** Lisbon Summit Declaration, NATO, 2010, https://www.nato.int/cps/en/natolive/official_texts_68828.htm

*** Maritime Doctrine of the Russian Federation, Russian Maritime Studies Institute (US Naval War College translation), 2015, https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/Maritime%20Doctrine%20TransENGrus_FINAL.pdf?sr=b&si=DNNFileManagerPolicy&sig=fqZgUUVRVRrKmSFNMOj%2FNaRNawUoRdhdvpFJj7%2FpAkM%3D

*** Maritime security: EU revises its action plan, EU, 26 iunie 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/

*** NATO Strategic Concept, NATO, 2010, https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

*** Tratatul Nord-Atlantic, NATO, Washington DC, 1949, http://www.mae.ro/sites/default/files/file/pdf/TRATATUL%2520NORD-ATLANTIC.pdf

*** United Nations Convention on the Law of the Sea (UNCLOS), UN, 1982.

Adler E., Barnett M., *Security Communities*, Cambridge University Press, 1998.

*Angela Merkel: EU cannot completely rely on US and Britain any more* (2017), https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks

Buzan B., *People, States and Fear*, Harvester Wheatsheaf, 1991.

Cohen R., Mihalka M., ”Cooperative Security: New Horizons for International Order”, *The Marshall Center Papers*, No. 3, 2001.

D’Aponte T., ”A geopolitical overview on the Mediterranean Sea the approach of the euro-med policy towards the countries of the southern front (from Morocco to Egypt)”, *Rivista Italiana di Economia Demografia e Statistica*, Volume LXVIII n.2, Aprile-Giugno 2014.

De Coning C., *The United Nations and the comprehensive approach*, Danish Institute for International Studies, Report 2008.

Deutsch K.W. et al., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton University Press, Princeton, 1957.

*Donald Trump: Without the US, the French would be speaking German* (2018, noiembrie 13), https://www.politico.eu/article/donald-trump-without-the-us-the-french-would-be-speaking-german/

Drent M., ”The EU’s Comprehensive Approach to Security: A Culture of Co-ordination?”, *Studia Diplomatica*, LXIV-2, 2011.

Feldt L., Dr. Roell P., Thiele R.D., ”Maritime Security – Perspectives for a Comprehensive Approach”, *ISPSW Strategy Series: Focus on Defense and International Security*, No. 222, 2013, https://www.files.ethz.ch/ isn/162756/222_Feldt_Roell_Thiele.pdf

Fransas A., Nieminen E., Salokorpi M., *Maritime Security and Security Measures – Mimic Study in the Baltic Sea Area*, Kymenlaakso University, Kotka, Finland, 2013.

*German Chancellor Supports Creation of European Security Council* (2018, octombrie 7), https://www.strategic-culture.org/news/2018/10/07/german-chancellor-supports-creation-of-european-security-council.html

Glaser C., ”The Security Dilemma Revisited”, *World Politics*, Vol. 50, No. 1, 1997.

Horrell S., Nordenman M., Slocombe W.B., *Updating NATO’s Maritime Strategy*, Brent Scowcroft Center on International Security, 2016.

Hoyt T.D., Winner A.C., ”A Cooperative Strategy for 21st CenturySeapower: Thinking About the New US Maritime Strategy”, *Maritime Affairs*, National Maritime Foundation, Vol. 3, No. 2, 2007.

Kaim M., Kempin R., *A European Security Council Added Value for EU Foreign and Security Policy?*, German Institute for International and Security Affairs – SWP, 2019.

Kegö W., Molcean A., *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, Institute for Security and Development Policy, Stockholm-Nacka, 2012.

Krasner S., *International Regimes*, Cornell University Press, Ithaca, 1983.

Lachowski Z., *Confidence and Security Building Measures in the New Europe*, Oxford University Press, 2004.

*Noua doctrină militar-maritimă: Rusia şi-a definit inamicii în oceanul planetar*, (2017), https://sputnik.md/russia/20170722/13705010/doctrina-maritima-rusia-inamici.htm

*** *Merkel joins Macron in calling for EU army to complement NATO* (2018, noiembrie 13), accesat de pe https://www.politico.eu/article/angela-merkel-emmanuel-macron-eu-army-to-complement-nato/

Pirozzi N., *The EU's Comprehensive Apprroach to Crisis Management*, DCAF Brussels, EU Crisis Management Papers Series, iunie 2013.

Proelss A., Müller T., *The Legal Regime of the Arctic Ocean*, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, 2008.

Puchala D.J., *International Politics Today*, New York, 1971.

Puheloinen A., *Russia's geopolitical interests in the Baltic Area,* Finnish Defense Studies, 1999.

Rahman C., *Concepts of Maritime Security – A strategic perspective on alternative visions for good order and security at sea, with policy implications for New Zealand*, Centre for Strategic Studies: New Zealand Victoria University of Wellington, 2009.

Roberts P., "Will the Alliance discover navies again?", *NATO Review Magazine*, 30 April 2018.

Roucek J.S., "The Geopolitics of the Baltic States", *The American Journal of Economics and Sociology*, Vol. 8, No. 2, Jan., 1949.

Stohs J., Dr. Bruns S., *Maritime Security in the Eastern Mediterranean*, Kiel International Seapower Symposium 2017, Kiel, 2017.

Taylor M., *Community, Anarchy, and Liberty*, Cambridge University Press, New York, 1982.

*Trump demands NATO countries meet defense spending goals 'immediately'* (2018, iulie 12), preluat de pe https://www.cnbc.com/2018/07/11/trump-demands-nato-countries-meet-defense-spending-goals-immediately.html

# ABORDAREA CUPRINZĂTOARE A SECURITĂȚII MARITIME EUROATLANTICE

## *EUROATLANTIC MARITIME SECURITY COMPREHENSIVE APPROACH*

## *APPROCHE GLOBALE DE LA SÉCURITÉ MARITIME EURO-ATLANTIQUE*

**Cdor.prof.univ.dr. Ioan CRĂCIUN***
**Cpt.cdor.drd. Valentin - Cătălin VLAD****

Actualizarea sau elaborarea strategiilor maritime euroatlantice a rezonat în mare măsură cu afirmarea intențiilor Alianței Nord-Atlantice și Uniunii Europene de a-și promova și de a-și apăra valorile și interesele atât la nivelul spațiului vital reprezentat de spațiul maritim euroatlantic, cât mai ales dincolo de acesta, oriunde situația și nevoile securității maritime internaționale o impun.

În acest sens, eficientizarea procesului de asigurare și de menținere a securității maritime euroatlantice trebuie să constituie un element definitoriu pentru reușita acestui proces, drept pentru care vizarea unei abordări cuprinzătoare a securității maritime, calibrată pe teoria comunităților de securitate, poate reprezenta o eventuală soluție viabilă.

*The update or development of the Euroatlantic Maritime Strategies has largely resonated with the assertion of the intentions of the North Atlantic Alliance and the European Union to promote and defend their values and interests both at the level of the vital space, represented by the Euroatlantic Maritime Space, and beyond wherever the situation and the needs of international maritime security impose it.*

*To this end, streamlining the Euroatlantic maritime security process and maintaining it must be a defining element for the success of this process, for which the aim of a comprehensive approach to maritime security calibrated on security community theory may be a viable solution.*

*L'actualisation ou l'élaboration des stratégies maritimes euro-atlantiques a largement trouvé écho dans les declarations d'intention de l'Alliance de l'Atlantique Nord et de l'Union européenne de promouvoir et de défendre leurs valeurs et leurs intérêts tant dans l'espace vitale, représenté par l'espace maritime euro-atlantique, que notamment au-delà, partout où la situation et les besoins de la sécurité maritime internationale l'imposent.*

*À cet égard, le renforcement de l'efficacité du processus visant à assurer et à maintenir la sécurité maritime euro-atlantique doit représenté un élément déterminant pour la réussite du processus en cause, de sorte que la recherche d'une approche globale de la sécurité maritime, fondée sur la théorie des communautés de sécurité, puisse constituer une solution viable.*

**Cuvinte-cheie:** securitate maritimă cuprinzătoare; strategii maritime euroatlantice; cooperare regională.
***Keywords:*** *maritime security comprehensive approach; euroatlantic maritime security strategies; regional cooperation.*
***Mots-clés:*** *sécurité maritime globale; stratégies maritimes euro-atlantiques; coopération régionale.*

Sfârșitul secolului al XX-lea și începutul secolului al XXI-lea au găsit comunitatea euroatlantică conectată la provocările și amenințările la adresa securității maritime regionale și internaționale, iar diversitatea și dinamica acestora au determinat NATO și UE să-și reevalueze și să-și calibreze propriile opțiuni doctrinare și acționale la cotele impuse de menținerea credibilității și legitimității internaționale într-o abordare cuprinzătoare – interinstituțională și multidomeniu.

Regăsim așadar NATO și UE, mandatate de ONU, să conducă sau să acționeze în cadrul unui efort conjugat, integrat pentru asigurarea

***Universitatea Națională de Apărare „Carol I”***
e-mail: *craciun64@gmail.com*
****Statul Major al Forțelor Navale***
e-mail: *valentin.vlad@navy.ro*

și menținerea securității maritime internaționale în Marea Mediterană sau în Golful Aden, pe de o parte, pentru combaterea amenințărilor la securitatea maritimă – pirateria, migrația ilegală, terorismul –, iar pe de altă parte, pentru sprijinul națiunilor riverane zonelor de operații în depășirea provocărilor existente și în realizarea propriilor capabilități maritime de conducere și de execuție.

În acest sens, Margriet Drent[1] semnala faptul că reușita deplină a operațiilor și a acțiunilor militare, desfășurate pentru restabilirea sau menținerea climatului de pace și stabilitate, așa cum este el promovat de Carta Națiunilor Unite, este dependentă de abordarea cuprinzătoare a binomului, determinat de instituțiile militare și civile, în sprijinul inițierii și dezvoltării capabilităților proprii în vederea permiterii statelor în nevoie să se stabilizeze și să se autosusțină social, economic, militar sau politic.

Observăm faptul că dinamica mediului de securitate internațional a constrâns comunitatea internațională către determinarea și adoptarea unui curs de acțiune cuprinzător, care să asigure implicarea, responsabilizarea și cooperarea, pe direcții multiple convergente, a tuturor actorilor relevanți guvernamentali sau nonguvernamentali.

**Abordarea strategică cuprinzătoare a securității maritime euroatlantice**

NATO și Uniunea Europeană au preluat conceptul abordării cuprinzătoare sau integrate a procesului securității individuale și colective de la promotorii și dezvoltatorii acestuia, Organizația pentru Securitate și Cooperare în Europa (OSCE)[2] și Organizația Națiunilor Unite (ONU), cu scopul de a iniția și de a dezvolta cooperarea de securitate la nivel regional și internațional, conform particularităților regionale, prevederilor legislative internaționale, precum și intereselor, nevoilor și garanțiilor comune de securitate.

Importanța cooperării în domeniul securității pentru reușita abordării cuprinzătoare a procesului de securitate colectivă, este foarte bine reliefată de OSCE în propriul concept de securitate, unde aceasta este văzută ca fiind „în beneficiul tuturor statelor, așa cum și insecuritatea internă sau a unui stat afectează bunăstarea tuturor”[3].

Drept urmare, asigurarea și menținerea securității interne, la nivel individual și colectiv, a fiecărui stat sunt vizualizate ca fiind definitorii pentru securitatea, stabilitatea și prosperitatea comună regională sau internațională, în condițiile respectării prevederilor tratatelor și legilor fundamentale internaționale (*Carta ONU*), fapt care va asigura, în final, credibilitatea și legitimitatea întregului proces de securitate.

Adoptarea abordării cuprinzătoare a procesului de asigurare a securității maritime euroatlantice, la nivelul NATO și UE, este determinată, pe de o parte, de faptul că toate statele membre ale celor două organizații și-au asumat abordarea cuprinzătoare împreună cu statutul lor de membre ale ONU și ale OSCE, iar pe de altă parte, de faptul că au acceptat, au dezvoltat și au implementat această abordare în propriile concepte și strategii prin combinarea instrumentelor politice, civile și militare[4].

Astfel, dinamica mediului de securitate euroatlantic și diversitatea provocărilor și amenințărilor la adresa securității euroatlantice și internaționale au determinat NATO să-și reevalueze și să-și adapteze opțiunile de răspuns preponderent politico-militare[5], aducând în discuție, în cadrul Summiturilor de la București (2008) și de la Lisabona (2010), conceptul abordării cuprinzătoare, ca urmare a faptului că „mijloacele militare, deși esențiale, nu sunt suficiente pentru a contracara provocările complexe la adresa securității comune”[6], dacă nu sunt completate de măsuri interinstituționale și de multidomeniu, care să asigure dezvoltarea, stabilitatea și autosusținerea mediului de securitate la nivel regional și internațional.

Reușita abordării cuprinzătoare a procesului de securitate euroatlantic este strâns legată de deschiderea Alianței către cooperare și consultare regională cu actorii relevanți, cu instituțiile și cu organizațiile internaționale de securitate și cooperare, în scopul promovării valorilor democratice și întăririi încrederii reciproce, așa cum este, de altfel, stipulat și în Carta Națiunilor Unite[7].

La un an de la Summitul de la Lisabona, direcția noului Concept Strategic[8] se oglindea deja în noua Strategie Maritimă Aliată[9], care plasa acțiunea componentei maritime aliate sub incidența abordării cuprinzătoare a securității euroatlantice pentru managementul crizelor și pentru securitatea maritimă prin cooperare (dialog, parteneriate, consultare).

În acest sens, componentei maritime a NATO îi este recunoscută și valorificată tradițională caracteristică de a interacționa într-o abordare

cuprinzătoare și în condiții de deplină legitimitate, în spațiul maritim euroatlantic și internațional cu alți actori maritimi, interesați de promovarea și menținerea securității maritime regionale și globale.

În cadrul abordării cuprinzătoare a NATO, Strategia Maritimă Aliată urmărește să mențină parteneriatele tradiționale cu actorii maritimi relevanți (ONU, UE) și să contribuie alături de aceștia la prevenirea conflictelor, la dezvoltarea capabilităților maritime, în concordanță cu amenințările prezente, la menținerea libertății de navigație și la impunerea regimului juridic maritim internațional.

În cadrul acestei abordări cuprinzătoare, Alianța își propune ca procesul de planificare a eventualelor operații maritime proprii să considere posibilele urmări sau influențe pe care acestea le-ar putea avea asupra agențiilor și organizațiilor regionale sau internaționale, asupra partenerilor sau nonpartenerilor, dar mai ales să fructifice avantajele oferite de cooptarea și implicarea acestora.

De asemenea, adoptarea abordării cuprinzătoare s-a materializat doctrinar odată cu implementarea, în 2017, la nivelul Alianței a noii Doctrine Aliate Întrunite (AJP-01)[10], asigurându-se prin aceasta „sincronizarea acțiunilor NATO cu cele ale organizațiilor internaționale”[11] prin asumarea, ca obiective, a sporirii cooperării cu partenerii și a creșterii contribuției alături de aceștia pentru stabilizarea și reconstrucția regională și internațională.

În esență, prin adoptarea abordării cuprinzătoare, NATO se delimitează clar de poziționarea unilaterală și își declară ferm disponibilitatea și deschiderea către cooperarea interinstituțională și multidomeniu pe linia securității maritime euroatlantice și internaționale.

Tributară acelorași libertăți și valori democratice ca și NATO, era firesc ca și Uniunea Europeană să arate același interes pentru orientarea cuprinzătoare a propriului proces de securitate.

Drept urmare, prin intermediul politicilor de securitate și apărare, Politica Europeană de Securitate și Apărare (European Security and Defense Policy – ESDP) și Politica de Securitate și Apărare Comună (Common Security and Defense Policy – CSDP), UE își manifestă dorința de a aborda disputele și crizele de securitate într-o manieră integrală, desfășurată între faza apariției acestora și procesul de reconstrucție politică, socială, militară și economică, caracteristic atingerii stării finale dorite[12].

Implicarea activă a Uniunii Europene, alături de Organizația Națiunilor Unite, de Organizația Tratatului Nord-Atlantic sau de alți actori relevanți pentru securitatea maritimă regională și internațională (China, India, Japonia, Rusia, SUA), în combaterea pirateriei din Golful Aden, precum și în acțiunile de sprijinire a Somaliei pentru eradicarea cauzelor fenomenului pirateresc și pentru dezvoltarea capabilităților decizionale și acționale proprii de gestionare a acțiunilor ilegale reprezintă bune exemple ale abordării cuprinzătoare a securității maritime internaționale, cu directe beneficii asupra securității maritime europene și, implicit, euroatlantice[13].

Astfel, abordarea cuprinzătoare a securității europene vizează creșterea nivelului de cooperare dintre UE și partenerii săi și responsabilizarea[14] tuturor membrilor în acest sens, pentru formularea unor concepte și strategii complementare, care să susțină unitatea de efort la nivelul tuturor instituțiilor militare și civile, guvernamentale sau nonguvernamentale[15], cu efecte directe în prevenirea conflictelor și eliminarea amenințărilor (terorism, migrația ilegală, criminalitatea transfrontalieră, traficul de armament) la adresa securității maritime regionale și internaționale.

Strategia Maritimă de Securitate a Uniunii Europene (EUMSS), apărută în anul 2014 sub sintagma „marea contează”[16], reprezintă dovada înțelegerii depline a importanței spațiului maritim euroatlantic pentru securitatea europeană, iar ancorarea ei de conceptele comunităților de securitate regionale, promovate de Wagenen[17], Deutsch[18], Adler[19], Taylor[20], Cohen[21] sau Mihalka[22], dovedește realism, măsură și oportunitate.

Principalele direcții de acțiune ale strategiei maritime europene urmează cursul de acțiune definit de abordarea integrală a securității maritime și constau în inițierea și dezvoltarea cooperării maritime regionale, adaptată particularităților principalelor bazine maritime euroatlantice (Marea Baltică, Marea Nordului, Marea Mediterană, Marea Neagră, Oceanul Atlantic, Oceanul Arctic).

Interesul pentru abordarea cuprinzătoare a securității maritime europene este evidențiat de faptul că, prin EUMSS, Uniunea își propune să „acopere aspectele interne și externe ale securității

maritime”[23], strategia maritimă fiind o „platformă cuprinzătoare prin care se contribuie la un mediu maritim global stabil și sigur”[24].

EUMSS definește cadrul politic și strategic, prin care, pentru depășirea provocărilor și combaterea amenințărilor, simetrice sau asimetrice la adresa securității maritime europene, vor fi implicați toți actorii (militari, civili, guvernamentali, nonguvernamentali) la nivel național, european și internațional, în cadrul unei cooperări interinstituționale și multidomeniu[25].

Întreg procesul cuprinzător al securității maritime europene va urmări respectarea prevederilor legale internaționale, fiind canalizat pe planificarea securității maritime comune, managementul riscului, prevenirea conflictelor și răspunsul la crize.

## Concluzii

Abordarea cuprinzătoare a securității maritime euroatlantice se înscrie perfect prevederilor Cartei ONU și abordărilor cuprinzătoare ale ONU și OSCE, fapt ce conferă Alianței și Uniunii, în egală măsură, credibilitate și legitimitate internațională atât de necesare cooptării și responsabilizării tuturor statelor, instituțiilor sau agențiilor internaționale, în cadrul procesului de inițiere și dezvoltare a comunităților regionale de securitate maritimă.

Dimensionarea comunităților de securitate maritimă la nivelul principalelor bazine maritime euroatlantice subscrie teoriei de eficientizare a procesului de securitate, promovate de Taylor[26], și reprezintă elementul cheie al abordării cuprinzătoare, prin faptul că ia în considerare particularitățile, oportunitățile și limitările culturale, sociale, geopolitice sau de orice altă natură, transferând responsabilitatea securității maritime regionale pe umerii actorilor regionali și în același timp conectând-o la securitatea maritimă internațională.

Considerând contribuția directă la securitatea maritimă euroatlantică și internațională a NATO și UE, precum și scopul și obiectivele propriilor lor strategii maritime de securitate, se poate spune fără niciun dubiu faptul că Alianța și Uniunea sunt pe deplin conectate la evoluția mediului de securitate maritimă euroatlantic și internațional, iar abordarea cuprinzătoare, interinstituțională și multidomeniu este identificată ca fiind esențială pentru succesul procesului de asigurare a securității, stabilității și prosperității[27] europene și internaționale.

## NOTE:

1 Margriet Drent, ”The EU’s Comprehensive Approach to Security: A Culture of Co-ordination?”, *Studia Diplomatica*, 2011, LXIV-2, p. 3, https://www.clingendael.org/sites/default/files/pdfs/20111000_sd_drent_approach.pdf, accesat la 26 mai 2019.

2 Actul final al securității și cooperării europene, OSCE, https://www.osce.org/helsinki-final-act?download=true, accesat la 27 mai 2019.

3 Conceptul securității cuprinzătoare și prin cooperare al OSCE, OSCE, https://www.osce.org/secretariat/37592?download=true, accesat la 28 mai 2019.

4 A ”comprehensive approach” to crises, NATO, 2016, https://www.nato.int/cps/su/natohq/topics_51633.htm, accesat la 30 mai 2019.

5 Pagina oficială a NATO, https://www.nato.int/nato-welcome/index.html, accesat la 30 mai 2019.

6 *** Lisbon Summit Declaration, NATO, 2010, https://www.nato.int/cps/en/natolive/official_texts_68828.htm?selectedLocale=en, accesat la 30 mai 2019.

7 *** *UN Charter*, ONU, cap. VIII, https://www.un.org/en/charter-united-nations/, accesat la 31 mai 2019.

8 *** *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, NATO, 2010, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, accesat la 31 mai 2019.

9 *** Alliance Maritime Strategy, NATO, 2011, https://www.nato.int/cps/ua/natohq/official_texts_75615.htm, accesat la 1 iunie 2019.

10 *** *Allied Joint Doctrine (AJP-01)*, NATO, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf, accesat la 2 iunie 2019.

11 *Ibidem*, p. 1.6.

12 *** *European Security Strategy – A secure Europe in a better world, EU*, 2009, http://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/, accesat la 3 iunie 2019.

13 *** *Fight against piracy*, EU, 03 May 2016, https://eeas.europa.eu/topics/maritime-security/428/fight-against-piracy_en, accesat la 3 iunie 2019.

14 *** *EU enhances its comprehensive approach to external conflicts and crises*, EU, 2013, http://europa.eu/rapid/press-release_IP-13-1236_en.htm, accesat la 3 iunie 2019.

15 Lutz Feldt, dr. Peter Roell, Ralph D. Thiele, ”Maritime Security – Perspectives for a Comprehensive Approach”, *ISPSW Strategy Series: Focus on Defence and International Security*, No. 222, 2013, https://www.files.ethz.ch/ isn/162756/222_Feldt_Roell_Thiele.pdf, accesat la 4 iunie 2019.

16 *** *European Union Maritime Security Strategy (EUMSS)*, UE, 2014, p. 2, https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT, accesat la 4 iunie 2019.

17 Donald J. Puchala, *International Politics Today*, New York, 1971, p. 165.

18 Karl W. Deutsch et al., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton: Princeton University Press, 1957.

19 Emanuel Adler, Michael Barnett, *Security Communities*, Cambridge University Press, New York, 1998.

20 Michael Taylor, *Community, Anarchy, and Liberty,* New York, Cambridge University Press, 1982.

21 R. Cohen, M. Mihalka, ”Cooperative Security: New Horizons for International Order”, *The Marshall Center Papers*, No. 3, 2001.

22 *Ibidem*.

23 *** European Union Maritime Security Strategy (EUMSS), *op.cit.*, p. 2.

24 *Ibidem*, p. 2.

25 *Ibidem*, p. 3.

26 Michael Taylor, *op.cit.*, pp. 167-168.

27 *** *A Global Strategy for the European Union's Foreign and Security Policy*, EU, 2016, p. 9, https://europa.eu/globalstrategy/sites/globalstrategy/files/pages/files/eugs_review_web_5.pdf, accesat la 05.06.2019.

## BIBLIOGRAFIE


*** AAP 6, *NATO Glossary Of Terms And Definitions* (English And French) Edition 2013.

*** *A comprehensive approach to crises*, NATO, 2016, https://www.nato.int/cps/en/natolive/topics_51633.htm

*** *A comprehensive approach*, NATO, 2009, https://www.nato.int/summit2009/topics_en/19-comprehensive_approach.html

*** *A framework for enhanced international maritime security cooperation and awareness*, CJOS COE, 2011, http://cjoscoe.org/docs/MSA_Strategic_Framework_V1.0.pdf

*** *A Global Strategy for the European Union's Foreign and Security Policy*, EU, 2016, accesat de pe http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

*** *Actul final al securităţii şi cooperării europene*, OSCE, https://www.osce.org/helsinki-final-act?download=true

*** *Allied Joint Doctrine (AJP-01)*, NATO, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf

*** *Allied Maritime Strategy – A theory for success?*, Kiel International Seapower Symposium Conference Report, 2018, https://www.kielseapowerseries.com/files/ispk/content/KISS18/KISS2018_final_Web.pdf

*** *Alliance Maritime Strategy*, NATO, 2011, https://www.nato.int/cps/ua/natohq/official_texts_75615.htm

*** *Conceptul securităţii cuprinzătoare şi prin cooperare al OSCE*, OSCE, https://www.osce.org/secretariat/37592?download=true

*** *Consolidated Version of the Treaty on European Union*, UE, 2007.

*** *Cooperarea în domeniul apărării: Consiliul instituie cooperarea structurată permanentă (PESCO)*, cu participarea a 25 de state membre, Consiliul Uniunii Europene, 2017.

*** *Cooperarea la nivelul UE în domeniul apărării: Consiliul instituie o capabilitate militară de planificare şi conducere (MPCC)*, Consiliul Uniunii Europene, 8 iunie 2017, https://www.consilium.europa.eu/ro/press/press-releases/2017/06/08/military-mpcc-planning-conduct-capability/

*** *Council conclusions on the revision of the European Union Maritime Security Strategy - Action Plan*, EU, 26 iunie 2018, http://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf

*** *EUCAP Nestor renamed as EUCAP Somalia*, EU, https://www.eucap-som.eu/eucap-nestor-renamed-as-eucap-somalia-new-website/

*** EUCAP Sahel Niger, EU, https://eeas.europa.eu/csdp-missions-operations/eucap-sahel-niger_en

*** *EU enhances its comprehensive approach to external conflicts and crises*, EU, 2013, http://europa.eu/rapid/press-release_IP-13-1236_en.htms

*** *European Union Maritime Security Strategy*, EU, 2014, https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT

*** *European Union Maritime Security Strategy – Action Plan (EUMSS AP)*, EU, 2014, https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf

*** *European Security Strategy – A secure Europe in a better world*, EU, 2009, http://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/

*** *Fight against piracy*, EU, 03 May 2016, https://eeas.europa.eu/topics/maritime-security/428/fight-against-piracy_en

*** *Joint declaration on eu-nato cooperation by the president of the european council, the*

*president of the european commission, and the secretary general of the north atlantic treaty organization*, EU, 2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm

*** *Lisbon Summit Declaration*, NATO, 2010, https://www.nato.int/cps/en/natolive/official_texts_68828.htm

*** *Maritime security: EU revises its action plan*, EU, 26 iunie 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/

*** *NATO Strategic Concept*, NATO, 2010, https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

*** Pagina oficială a NATO, https://www.nato.int/nato-welcome/index.html

*** Sahel Region, https://www.britannica.com/place/Sahel

*** *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, NATO, 2010, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

*** *Tratatul Nord-Atlantic*, NATO, Washington DC, 1949, http://www.mae.ro/sites/default/files/file/pdf/TRATATUL%2520NORD-ATLANTIC.pdf

*** *UN Charter*, ONU, https://www.un.org/en/charter-united-nations/

*** *United Nations Convention on the Law of the Sea (UNCLOS)*, UN, 1982.

Adler E., Barnett M., *Security Communities*, Cambridge University Press, 1998.

Cohen R., Mihalka M., ”Cooperative Security: New Horizons for International Order”, *The Marshall Center Papers*, No. 3, 2001.

D’Aponte T., ”A geopolitical overview on the Mediterranean Sea the approach of the euro-med policy towards the countries of the southern front (from Morocco to Egypt)”, *Rivista Italiana di Economia Demografia e Statistica*, Volume LXVIII n.2, Aprile-Giugno 2014.

De Coning C., *The United Nations and the comprehensive approach*, Danish Institute for International Studies, Report 2008:1, https://www.diis.dk/files/media/publications/import_efter1114/report-2008-14_the_united_nations_and_the_comprehensive_approach.pdf

Deutsch K. W. et al., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton University Press, Princeton, 1957.

Drent M., *The EU’s Comprehensive Approach to Security: A Culture of Co-ordination?*, Studia Diplomatica, 2011, LXIV-2, https://www.clingendael.org/sites/default/files/pdfs/20111000_sd_drent_approach.pdf

Feldt L., Dr. Roell P., Thiele R.D., ”Maritime Security – Perspectives for a Comprehensive Approach”, *ISPSW Strategy Series: Focus on Defense and International Security*, No. 222, 2013, https://www.files.ethz.ch/ isn/162756/222_Feldt_Roell_Thiele.pdf

Fransas A., Nieminen E., Salokorpi M., *Maritime Security and Security Measures – Mimic Study in the Baltic Sea Area*, Kymenlaakso University, Kotka, Finland, 2013.

Glaser C., ”The Security Dilemma Revisited”, *World Politics*, Vol. 50, No. 1, 1997.

Horrell S., Nordenman M., Slocombe W.B., *Updating NATO’s Maritime Strategy*, Brent Scowcroft Center on International Security, 2016.

Hoyt T.,D., Winner A.C., ”A Cooperative Strategy for 21st CenturySeapower: Thinking About the New US Maritime Strategy”, *Maritime Affairs*, National Maritime Foundation, Vol. 3, No. 2, 2007.

Kaim M., Kempin R., *A European Security Council Added Value for EU Foreign and Security Policy?*, German Institute for International and Security Affairs - SWP, 2019.

Pirozzi N., ”The EU’s Comprehensive Approach to Crisis Management”, *EU Crisis Management Papers Series*, DCAF Brussels, 2013.

Proelss A., Müller T., *The Legal Regime of the Arctic Ocean*, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, 2008.

Puchala D.J., *International Politics Today*, New York, 1971.

Roberts P., ”Will the Alliance discover navies again?”, *NATO Review Magazine*, 30 April 2018.

Stohs J., Dr. Bruns S., ”Maritime Security in the Eastern Mediterranean”, *Kiel International Seapower Symposium 2017*, Kiel, 2017.

Taylor M., *Community, Anarchy, and Liberty,* Cambridge University Press, New York, 1982.

# RISCURI ȘI AMENINȚĂRI ÎN MEDIUL OPERAȚIONAL ACTUAL

## *RISKS AND THREATS IN THE CURRENT OPERATIONAL ENVIRONMENT*

## *RISQUES ET MENACES DANS L'ENVIRONNEMENT OPÉRATIONNEL ACTUEL*

**Lt.col.conf.univ.dr. Alexandru HERCIU***

Evoluţia dinamică a fenomenului războiului de la fizionomia clasic-convenţională, prin dimensiunea sa fizică, la una preponderent neconvenţională, manifestată extrem în medii speciale (spaţiul cibernetic, mediul înconjurător, mediul electromagnetic, informaţional, chimic, biologic, radiologic şi nuclear, psihicul uman), în zilele noastre şi în viitorul predictibil, este consecinţa adaptării continue la complexitatea provocărilor care se manifestă la adresa umanităţii, provocări exprimate şi consacrate în literatura de specialitate prin termenii: pericole, riscuri, ameninţări, vulnerabilităţi.

*The dynamic evolution of the phenomenon of warfare from its classical-conventional physiognomy to a predominantly unconventional one, manifested in extreme environments (cyberspace, electromagnetic environment, informational environment, CBRN environment, human psyche) today and in the predictable future, is the consequence of the continuous adaptation to the complexity of today's challenges to humanity. These challenges are expressed and established in the literature by the terms: hazards, risks, threats, vulnerabilities.*

*L'évolution dynamique du phénomène de guerre, à travers sa dimension physique, d'une physionomie classique, conventionnelle vers une physionomie essentiellement non conventionnelle, fortement révélée, de nos jours et dans un avenir prévisible, dans des environnements particuliers (cyberespace, l'environnement, environnement électromagnétique, informationnel, chimique, biologique, radiologique et nucléaire, le mental) constitue la conséquence d'une incessante adaptation à la complexité des défis d'aujourd'hui auxquels l'humanité est confrontée, défis exprimés dans la littérature spécialisée par des termes consacrés comme: dangers, risques, menaces, vulnérabilités.*

**Cuvinte-cheie:** ameninţare hibridă; asimetrie; componenta neregulată; componenta neconvenţională.
***Keywords:*** *hybrid threat; asymmetry; irregular component; unconventional component.*
***Mots-clés:*** *menace hybride; asymétrie; la composante irrégulière; la composante non conventionnelle.*

Conflictele contemporane prezintă fizionomia (re)cunoscută a războaielor de uzură, în care forţele convenţionale superioare sunt atrase în zone care le dezavantajează, în ambuscade, şi sunt hărţuite până la uzura completă de către un adversar inferior, dar care deţine avantajul cunoaşterii perfecte a terenului şi care este sprijinit, în general, de către populaţia locală. Astăzi, aceste operaţii se desfăşoară în jungla urbană şi sunt caracterizate de continuitate şi, în acelaşi timp, de o intensitate diferită a angajării forţelor oponente de către inamicul care desfăşoară acţiuni hibride.

În cadrul conflictelor de tip hibrid, tendinţa, în ceea ce priveşte ponderea tipologiei acţiunilor, din perspectiva pericolelor, riscurilor şi ameninţărilor care le determină, prezintă o deplasare de la cele regulate, tradiţionale spre cele neconvenţionale şi, mai cu seamă, către cele asimetrice, care tind să se generalizeze şi să se manifeste pe întreaga durată a conflictului şi în întreg spectrul său.

Ameninţările hibride reprezintă cel mai mare risc operaţional în viitorul apropiat şi, prin urmare, sunt punctul asupra căruia trebuie să se focalizeze o eventuală angajare a unei structuri de forţe întrunite multinaţionale.

***Universitatea Naţională de Apărare „Carol I”***
e-mail: *herciu_alexandru12@yahoo.ro*

**Consideraţii privind conceptul de „conflict de tip hibrid”**

Ameninţările hibride apar acolo unde ameninţările convenţionale, neregulate şi asimetrice se suprapun în timp şi în spaţiu. Conflictul poate implica participanţi la nivel individual, grupuri sau state care operează la nivel local, transnaţional sau global. Astfel de conflicte pot include acte de violenţă în cadrul comunităţilor, acte de terorism, atacuri cibernetice, insurgenţă, criminalitate sau generatorul de dezordine[1].

Din analiza celor prezentate anterior, putem sintetiza în ceea ce priveşte conceptul „ameninţare hibridă/Hybrid Threat (HT)”[2] faptul că, în abordarea teoreticienilor militari americani (analizând condiţiile particulare ale experienţelor militare din Afganistan şi din Irak), acesta exprimă combinaţia dintre forţele militare convenţionale, înzestrate cu arme sofisticate, sisteme de comandă şi control (C2) complexe şi tactici combinate ale armelor, şi acţiuni ale forţelor neregulate de tipul celor insurgente sau organizaţii criminale.

Această combinaţie de convenţional şi neregulat, capacitatea respectivelor forţe de a migra şi de a se transforma în ambele sensuri, care are drept rezultat violenţa nerestricţionată, îndreptată împotriva punctelor slabe, fac din ameninţarea hibridă una extrem de eficientă. Pentru a determina caracterul „hibrid”, aceste entităţi (unităţi militare, facţiuni rebele, grupuri criminale, gherile, teroriști, insurgenţi, partizani) vor coopera, în contextul îndeplinirii intereselor proprii.

De aceea se consideră că viitoarele conflicte nu pot fi privite separat, pe tipuri de ameninţări sau provocări separate. Cel mai probabil, armatele trebuie să fie în măsură să facă faţă simultan tuturor tipurilor de ameninţări, să poată opera cu succes împotriva tuturor tipurilor de adversari, în cadrul unor conflicte complexe, în toate mediile posibile. Această sinteză constituie esenţa războiului hibrid[3].

În ceea ce priveşte teoria şi practica războiului hibrid, abordarea rusească diferă de cea americană. În conflictul din Ucraina (2014), Rusia a aplicat un evantai de acţiuni care au avut drept rezultat realizarea scopurilor sale politice, în afara unui război clasic declarat. În luna februarie 2013, Valeri Gherasimov, şeful Statului Major al armatei ruse, scria, într-un articol, publicat în jurnalul apărării ruse VPK, că războiul şi pacea devin din ce în ce mai amestecate. Metodele de conflict s-au schimbat şi acum implică uzul larg de măsuri politice, economice, informaţionale, umanitare şi altele nonmilitare. Toate acestea, spunea el, pot fi suplimentate prin instigarea populaţiei locale şi prin folosirea forţelor armate deghizate[4].

În lumina evenimentelor petrecute un an mai târziu, declaraţia oficialului militar rus demonstrează premeditarea şi aplicarea conştientă a acţiunilor hibride, care au avut drept rezultat anexarea urgentă a Crimeii şi proclamarea independenţei Noii Rusii. Generalul Gherasimov continua, în discursul său: „Regulile de angajare s-au schimbat semnificativ. Utilizarea metodelor nonmilitare pentru îndeplinirea obiectivelor politice sau strategice s-a dovedit, în anumite cazuri, de departe, mult mai eficace decât utilizarea forţei. [...] Utilizarea largă a mijloacelor asimetrice poate ajuta la neutralizarea superiorităţii militare a inamicului. Aceasta include utilizarea forţelor speciale şi opoziţia internă pentru crearea unui front permanent în interiorul unui stat inamic, precum şi impactul instrumentelor de propagandă, forme şi metode care sunt în mod constant îmbunătăţite”[5].

Din studiul acestor încercări, de explicare şi de definire a „războiului sau conflictului hibrid”, apreciem faptul că acesta este o strategie de luptă care include atât o multitudine de *actori diferiţi*: actorii statali, nonstatali, state sponsor, dar şi *pericole, riscuri şi ameninţări* multiple, care se manifestă în *mediul fizic*, de natură *convenţională* (forţe militare convenţionale, aflate în serviciul legitim al statului), *neconvenţională* (forţe nucleare, forţe pentru operaţii speciale, arme de distrugere în masă chimice, biologice, radiologice şi nucleare – ADMCBRN – şi materiale toxice industriale – MTI – dispozitive explozive improvizate – IED) şi *asimetrice* (gherile, grupuri insurgente şi separatiste activate, organizaţii teroriste şi criminale), cât şi în *mediul cibernetic virtual (informaţional)*, toate acestea angajate în luptă în mod combinat şi coordonat împotriva unui adversar superior în forţe şi mijloace militare.

**Tipologia riscurilor şi ameninţărilor în conflictele de tip hibrid**

În general, se foloseşte sintagma „riscuri şi ameninţări” fără a face neapărat o diferenţiere a sensurilor celor două noţiuni. Utilizate împreună, la o primă vedere am înţelege faptul că riscul se referă la obiectul care ar putea genera un pericol

specific la un moment dat şi în anumite condiţii, adică sursa pericolului – primul care se manifestă –, iar ameninţarea presupune îndeplinirea acestor condiţii şi iminenţa producerii evenimentului ostil de către un agresor (adică autorul), explicaţie care nu este departe de adevăr.

În opinia mea, riscul este parte componentă a ameninţării, primul indiciu identificat al pericolului potenţial, în raport cu scopul în care ar putea fi folosit. Starea de „ameninţare” este generată pe măsura conturării obiectivelor, pentru atingerea cărora riscul identificat ar putea fi exploatat, şi a concretizării ţintei, în condiţiile unei amplificări graduale a stării de pericol sau chiar a trecerii directe de la un nivel de ameninţare foarte mic la unul foarte mare. Cu alte cuvinte, unul sau mai multe riscuri de un anumit tip poate/pot genera o ameninţare de acelaşi tip.

În general, mediul operaţional este definit ca fiind „un sistem de sisteme în care fiecare actor implicat urmăreşte să-şi realizeze propriile interese”. În acest context, în conflictele de tip hibrid, strategia adoptată de un potenţial adversar pentru realizarea finalităţii dorite este complicată, completă şi se manifestă în toate variabilele mediului operaţional. Acesta poate fi descris ca un conglomerat de condiţii, circumstanţe şi influenţe care determină angajarea capabilităţilor şi decizia comandantului[6].

Referitor la problematica „ameninţărilor hibride”, *Doctrina Armatei României* utilizează construcţia cu sensul acelor ameninţări care sunt generate de un adversar capabil să desfăşoare acţiuni atât clasice, cât şi asimetrice, caracterizate prin utilizare simultană şi coordonată de către un adversar determinat, pentru a exploata vulnerabilităţile proprii, situate în afara cadrului legal, fapt care le face greu de anticipat[7].

Odată identificate aceste vulnerabilităţi, adversarul va încerca să îşi realizeze obiectivele prin orice mijloace, utilizând toate resursele pe care le are la dispoziţie în locul, la momentul oportun. Intenţia sa va fi aceea de a crea efecte asupra elementelor vulnerabile, care, odată afectate, produc schimbările dorite şi, în final, îndeplinirea obiectivelor propuse.

În funcţie de natura lor, riscurile şi ameninţările hibride pot fi descompuse în:

- riscuri şi ameninţări convenţionale;
- riscuri şi ameninţări neconvenţionale;
- riscuri şi ameninţări asimetrice.

În funcţie de mediul de manifestare, riscurile şi ameninţările hibride pot fi o combinaţie de:

- riscuri şi ameninţări în mediul fizic;
- riscuri şi ameninţări în mediul virtual (informaţional).

Suprapunerea riscurilor şi ameninţărilor, care se manifestă în aceste planuri şi dimensiuni, generează prin întrepătrundere şi prin complementaritate un mozaic de o complexitate aparte, exprimată în literatura de specialitate ca fiind combinaţia „ameninţări hibride/Hybrid Threats”.

**Riscuri şi ameninţări asimetrice (neregulate)**

Ultima decadă a secolului trecut şi prima decadă a secolului al XXI-lea au fost etape marcate de cele două războaie din Irak (1991 şi 2003), Afganistan (2001), Georgia (2008) şi Ucraina (2014), confruntări care au implicat angajarea forţelor regulate şi care au demonstrat faptul că, astăzi, războaiele purtate prin angajarea directă a forţelor armate convenţionale tind să devină de domeniul trecutului din cauza caracterului disproporţionat şi iraţional, rezultat din potenţialul militar diferit şi a rezultatului final evident, în sensul că intervenţia militară nu este întotdeauna soluţia optimă sau absolut necesară pentru realizarea scopului războiului.

Analiza fenomenului din perspectiva hibridităţii ne conduce către două concluzii, şi anume:

- atunci când forţele convenţionale au fost întrebuinţate având drept obiectiv pedepsirea liderilor sau a guvernelor pentru acţiuni nejustificate, politici sau orientări divergente, avem de-a face cu o asimetrie fizică totală, un avantaj net superior în forţe şi în mijloace din partea agresorului;
- ponderea componentei convenţionale în economia războiului prin angajarea în operaţii tinde să scadă, ea devenind forţă de descurajare şi de intimidare pentru realizarea scopurilor prin alte mijloace care să substituie acţiunea militară.

Din această perspectivă consider că atât în prezent, cât şi în viitor tendinţa de manifestare a confruntărilor convenţionale este aceea de a fi înlocuite de conflictele duse cu mijloace şi metode neconvenţionale, asimetrice prin natura lor.

Concomitent cu războaiele evocate mai sus, s-au manifestat în această etapă de tranziţie

către o nouă eră a confruntărilor armate, o serie de conflicte duse de grupuri armate de valoare şi origini diferite, prin mijloace şi căi de obţinere a avantajului asupra unui agresor superior din punct de vedere convenţional, şi deci a unei asimetrii alta decât cea obţinută prin capabilităţi tehnologice, potenţial sau superioritate decizională şi acţională.

Persistenţa inegalităţilor, efectele adverse ale procesului continuu de globalizare, distribuţia resurselor şi dezvoltarea inegală din punct de vedere economic, activarea, revigorarea şi alimentarea mişcărilor tradiţionaliste şi etnice ca formă de manifestare a rezistenţei împotriva asimilării sub diverse forme sunt tot atâtea cauze care pot alimenta conflictele.

Caracterul asimetric al acestora rezultă din lipsa de vizibilitate a adversarului, natura obiectivelor şi a idealurilor sale care contravin valorilor, credinţelor, priorităţilor, constrângerilor legale şi morale general acceptate şi din metodele neconvenţionale pe care le utilizează pentru anularea superiorităţii oponentului[8] sau pentru influenţarea şi controlul maselor.

Acest tip de ameninţări se referă la acele acţiuni care presupun utilizarea sau ameninţarea cu utilizarea forţei de către forţe neregulate, grupuri sau indivizi, de regulă, motivaţi ideologic sau infracţional, pentru a determina schimbarea sau menţinerea unei anumite stări de lucruri, care constituie o provocare pentru guvernare sau autoritatea statului[9]. Specificitatea acestora constă în ambiguitatea privind spaţiul de manifestare (în faţa sau în spatele liniilor), nivelurile operaţiilor şi statutul actorilor implicaţi[10].

Riscurile şi ameninţările asimetrice cele mai reprezentative sunt insurgenţa, gherila, separatismul, terorismul şi crima organizată. În ceea ce urmează vom analiza principalele caracteristici ale celor mai reprezentative dintre acestea.

*Insurgenţa/insurecţia.* Termenul insurgenţă provine din cuvântul latinesc „insurgent”, împrumutat din limba franceză, sub forma „insurgence”, utilizat cu înţelesul de insurecţie, răscoală, revoltă[11]. Aceasta reprezintă o formă de luptă armată organizată de forţe răzvrătite pentru a schimba situaţia politică existentă[12] utilizând subversiunea şi violenţa[13].

Spre deosebire de alte forme de luptă asimetrice, specificitatea acestui tip de revoltă constă în susţinerea şi participarea maselor largi populare sau a unei părţi semnificative a lor, împotriva unui regim politic reacţionar, sau pentru izgonirea de pe teritoriul naţional a unei armate ocupante. Răsturnarea/disoluţia guvernului legal constituit este realizată prin acţiuni subversive şi prin conflict armat.

De regulă, consimţământul şi sprijinul larg popular sunt obţinute şi mobilizate în jurul ideii de nedreptate socială, considerată legitimă şi adesea ideologică, dar poate, de asemenea, avea la bază ambiţii criminale. Pentru realizarea finalităţii dorite, insurgenţii caută să profite din plin de mediul operaţional, încercând să determine schimbările politice prin convingerea şi prin coerciţia populaţiei, concentrând efortul pe evidenţierea şi exagerarea nedreptăţilor percepute, reale sau fabricate.

Insurgenţa poate fi considerată o activitate neregulată, desfăşurată de către o mişcare sau un grup organizat. Aceasta poate fi inclusă într-o paletă mai amplă de acţiuni neregulate, care, în ansamblul lor constituie o ameninţare la adresa statelor sau a societăţii umane în special în regiuni, ale lumii mai puţin stabile. Insurgenţa poate fi considerată activitatea neregulată fundamentală, date fiind caracterul şi natura cauzelor ei. Ea poate recurge, la rândul ei, la alte tipuri de acţiuni neregulate, în scopul atingerii finalităţii dorite.

*Grupurile insurgente* sunt grupurile armate aparţinând unor mişcări rebele, cu revendicări de natură socială, etnică sau religioasă, care luptă pentru determinarea unei schimbări politice într-o anumită zonă geografică sau administrativă, beneficiind de sprijinul populaţiei[14].

Menţionez faptul că revolta, insurgenţa, insurecţia sunt stadii diferite ale unei mişcări ideologice. Revolta este prima etapă de exprimare a sentimentului de nemulţumire la adresa situaţiei politice ori a autorităţilor guvernamentale, manifestată, de regulă, spontan şi care se poate transforma într-o mişcare de insurgenţă violentă.

Pe măsura câştigării sprijinului popular al maselor largi, concomitent cu slăbirea puterii politice legitime, mişcarea de insurgenţă îşi îndeplineşte scopurile politice şi capătă caracteristicile insurecţiei. Prin urmare, dacă revolta este o acţiune spontană, manifestată punctual la un anumit moment şi într-un anumit loc, insurgenţa, ca formă de luptă, capătă caracter local sau regional şi tinde să crească în intensitate şi ca arie de cuprindere a teritoriului şi a populaţiei, până capătă amploare

la nivel naţional şi sunt îndeplinite condiţiile producerii schimbărilor politice.

*Gherila*

Termenul ”guerrilla” provine din limba spaniolă, a fost preluat în limba franceză cu forma ”guérilla” şi defineşte acele forţe neregulate care operează în teritoriile ocupate sau controlate de inamic, acţionează după regulile atacului prin surprindere, ale hărţuirii, distrugerii şi chiar prin mijloace teroriste şi urmăreşte îndeplinirea unor scopuri limitate la nivel local (răsturnarea unui guvern, obţinerea unor drepturi, independenţă statală, separatism teritorial sau autonomie, cucerirea puterii politice etc.).

Denumirea provine de la războiul de partizani din Spania şi din ţările Americii Latine, unde ”guerrilla” desemna o trupă de partizani, adepţi ai unei idei/doctrine, luptători pentru o cauză comună, într-un detaşament organizat neîncadrat formal[15]. Războiul de gherilă este definit ca fiind acele operaţii militare sau paramilitare executate în teritoriul ostil, deţinut de inamic, de către forţele neregulate, predominant indigene[16].

*Formaţiile de partizani/grupurile de rezistenţă* sunt acele grupuri formate din luptători care provin din personalul civil sau fost militar din teritoriile ocupate, care pun cauza mişcării de eliberare înaintea interesului personal şi care acţionează violent asupra unui invadator, independent sau în cooperare cu forţele convenţionale regulate prin tactici specifice gherilei[17].

Gherila vizează lovirea unui adversar superior, în punctele descoperite, sensibile/vulnerabile, identificate, fără nicio logică şi etică, ritmicitate sau alte reguli; gherila acţionează permanent, ziua şi noaptea, pretutindeni şi prin orice mijloace împotriva unei armate regulate de ocupaţie, cu o mare capacitate de luptă, dar nu prin tactica proprie unei armate, ci prin acţiuni specifice războiului de hărţuire (atentate, sabotaje, ambuscade, incursiuni, raiduri).

Luptătorii gherilelor acţionează, de regulă, în grupuri mici, conspirativ, cu armament uşor, uneori şi prin mijloace specifice terorismului – în special, în mediul urban, provocând în mod sistematic uzură psihică şi pierderi umane. Obiectivul final al gherilei nu este obţinerea victoriei în termenii înfrângerii decisive în luptă a forţelor de ocupaţie, ci atragerea şi menţinerea acestora într-un război de durată, uzura şi slăbirea acestora. Angajarea atacurilor la scară mică, specifice gherilei, cu îndeplinirea unor obiective limitate, trebuie analizată prin prisma unei judicioase planificări şi coordonări a acestora pentru a avea o perspectivă corectă a amplorii şi a eficienţei în timp a acestui tip de mişcare de rezistenţă.

O altă caracteristică definitorie a gherilei este superioritatea cunoaşterii mediului de confruntare, acoperirea şi sprijinul populaţiei din zona de angajare, ceea ce îi permite să lovească şi să se retragă. Aspectul este unul semnificativ din punct de vedere operaţional şi delimitează acest tip de ameninţare asimetrică de toate celelalte. De aceea gherila este considerată a fi un fenomen foarte greu de controlat şi contracarat.

*Terorismul structurat*

Terorismul desemnează totalitatea acţiunilor comise de un grup sau de o organizaţie prin folosirea deliberată şi sistematică a unor mijloace violente sau ameninţări, de natură să provoace teamă şi neîncredere, panică şi nesiguranţă, ignorând orice norme umanitare[18].

Scopul este acela de a crea un climat de insecuritate prin practica terorii, îndreptată împotriva obiectivelor selectate pe criteriul simbolului reprezentativ al unui adversar net superior, de regulă stat-naţiune (demnitari, comandanţi militari, populaţie majoritară sau minoritară, simboluri naţionale, simboluri religioase, simboluri şi valori ale democraţiei), care să faciliteze îndeplinirea obiectivelor politice, religioase sau ideologice de către actori nonstatali prin acţiune în sine sau coordonată cu alte acţiuni.

În funcţie de motivaţia care îl generează, terorismul poate fi de natură etnică, naţionalistă şi ideologică, iar în funcţie de natura riscului exploatat, identificăm terorism: chimic, biologic, radiologic, nuclear (CBRN), de mediu, cibernetic, cel manifestat prin asasinat, deturnare de avioane, răpire de persoane etc., sub diferite motivaţii.

*Celulele teroriste* sunt elementele de execuţie ale terorismului, în special cele care asigură îndeplinirea obiectivelor grupărilor teroriste rebele, extremiste, fundamentaliste prin acţiuni care au impact psihologic asupra maselor şi care determină constrângeri de ordin politic sau militar, în favoarea lor, din partea liderilor statelor sau alianţelor.

Elementele definitorii ale terorismului sunt: violenţa extremă, executată prin surprindere,

îndreptată împotriva unor ţinte civile punctuale, extrem de vulnerabile, pe teritoriul naţional sau în afara acestuia, impactul psihologic devastator asupra comunităţilor umane, efectele nediscriminante şi asigurarea condiţiilor de mediatizare a atacurilor. Dacă, în cazul celorlalte forme de manifestare asimetrică a conflictului de tip hibrid, avem de-a face cu faţete recunoscute ale războiului, putem afirma că terorismul, prin mijloacele sale de manifestare împotriva ţintelor civile într-un mod neselectiv, nu are nimic de-a face cu războiul[19].

*Crima organizată transfrontalieră*

Prin sintagma „crimă organizată” este definită existenţa unor grupări infracţionale prezente la un moment dat în societate, structurate în „branşe”, pe principiul apartenenţei la una dintre activităţile ilegale pe care le desfăşoară, în scopul obţinerii de venituri ilicite semnificative.

Organizaţiile criminale sunt constituite, în general, din structuri de tip piramidal (bande, carteluri de droguri, familiile mafiei, triade, asociaţii de hoţi, traficanţi, laboratoare şi imprimerii clandestine şi, mai nou, „academii ale infractorilor”), pe baza normelor interne de disciplină şi a codului de conduită, construit în jurul apărării cu orice preţ a secretului şi conspirativităţii acţiunilor, în care rolurile membrilor sunt clar stabilite în cadrul ierarhiei (specializare strictă).

Liderul grupării criminale manifestă un stil de conducere dictatorial, bazat pe principiul loialităţii totale şi necondiţionate, pe suprimarea libertăţii de gândire, pe pedepsirea exemplară a abaterilor de la normele grupului şi pe accesul strict la informaţii privind organizarea grupului, activitatea, pregătirea şi recrutarea noilor membri.

Forma principală de manifestare a crimei organizate este corupţia, ca efect al folosirii mijloacelor financiare, în scopul obţinerii unor avantaje economice sau politice, prin utilizarea unor forme de constrângere, şantaj, mituire, cumpărare, influenţă sau intimidare.

Formele caracteristice de manifestare a grupurilor criminale înarmate în cadrul conflictului de tip hibrid iau, deseori, forma unor *false mişcări de insurgenţă sau gherilă*. Aceste activităţi criminale sunt desfăşurate în statele eşuate sau subdezvoltate, în regiunile bogate în resurse naturale şi acolo unde controlul autorităţilor este inexistent sau ineficient. Acţiunile violente sunt cel mai adesea îndreptate împotriva populaţiei civile, în scopul terorizării şi menţinerii controlului asupra zonei şi comunităţilor, obţinerii beneficiilor materiale şi financiare, rezultate din colectarea produselor şi taxelor. Spre deosebire de mişcarea de rezistenţă, care are ca mobil principal o cauză nobilă, ce primează în faţa interesului personal al luptătorilor, lupta gherilelor false are la bază interesul personal şi de grup al membrilor săi, iar acţiunile specifice războiului de gherilă împotriva forţelor de securitate vizează supravieţuirea organizaţiei şi menţinerea avantajelor economice şi a superiorităţii psihologice.

*Insurgenţa criminală* diferă de insurgenţa clasică şi poate fi definită ca activitatea unor grupuri cu interese economice, care îşi creează propriile structuri de producţie, de transport, pieţe pentru produse ilegale, cum ar fi traficul de arme, de stupefiante, de carne vie, răpiri de persoane, şantaj şi orice altă activitate criminală prin care ar putea obţine profit. Grupurile criminale transnaţionale, organizate în carteluri, îşi creează reţele arborescente proprii şi complementare cu alte grupuri criminale, cu care cooperează pentru controlul pieţelor de produse ilicite. Aspectele care definesc activitatea grupurilor insurgente false sunt legate de caracterul economic ilegal, clandestin, de activităţi criminale extrem de violente de pedepsire şi intimidare a populaţiei civile şi autorităţilor guvernamentale pentru a-şi demonstra determinarea, de acţiuni de influenţare, corupţie şi subminare a puterii politice, de controlul regiunilor şi al forţelor de ordine.

**Riscuri şi ameninţări în mediul virtual (informaţional)**

*Operaţiile informaţionale (INFOOPS)* reprezintă o componentă a spectrului operaţiilor militare şi cuprinde acţiunile militare dirijate, planificate şi executate în scopul influenţării procesului de luare a deciziilor a unui potenţial adversar, facilitarea realizării obiectivelor politice şi militare prin influenţarea voinţei liderilor, exploatând în acelaşi timp propriile informaţii şi protejând propriile sisteme informaţionale[20]. Desfăşurarea acestor acţiuni vizează alterarea puterii de înţelegere a situaţiei reale existente, precum şi a evoluţiei probabile în cadrul componentei ofensive, concomitent cu protejarea capacităţii factorilor de decizie proprii şi a mijloacelor de care dispun forţele proprii în cadrul componentei defensive a operaţiei.

Acest tip de operaţii vizează, în special, afectarea calităţii informaţiilor şi procesului informaţional al inamicului şi, în acelaşi timp, exploatarea în condiţii de siguranţă sistemului propriu şi protecţia acestuia. Ele presupun angajarea integrată a unei largi palete de capabilităţi, instrumente şi tehnici pentru obţinerea efectelor specifice, în sprijinul operaţiilor. Acest tip de acţiuni vor fi integrate la toate nivelurile operaţiilor şi vor fi aplicate de-a lungul întregului spectru de misiuni. Efectele în mediul informaţional pot fi create printr-o diversitate de acţiuni militare coordonate, care vor contribui la îndeplinirea obiectivului general al operaţiei[21].

INFOOPS sunt desfăşurate în scopul menţinerii superiorităţii decizionale şi acţionale împotriva influenţelor externe existente sau potenţiale ale adversarului şi se realizează prin acţiuni de:

- influenţare a percepţiilor şi a atitudinilor adversarului sau ale potenţialului adversar (activităţi de influenţare);
- protecţia informaţiilor, concentrate pe menţinerea libertăţii de manevră în spaţiul informaţional prin apărarea datelor şi informaţiilor care susţin procesul decizional (activităţi de protecţie a informaţiilor);
- atac al sistemului de furnizare a datelor şi informaţiilor care sprijină adversarul sau potenţialul adversar şi acele sisteme C2, de informaţii, supraveghere şi sisteme de achiziţie a ţintelor (activităţi îndreptate împotriva comenzii).

Obiectivele operaţiilor informaţionale sunt realizate prin coordonarea şi sincronizarea planificată a capabilităţilor militare, instrumentelor şi tehnicilor care influenţează sau protejează informaţiile ori sistemele informaţionale. Acestea sunt: operaţiile psihologice; prezenţa, atitudinea şi postura; operaţiile de securitate a informaţiilor (OPSEC); securitatea informaţiilor (INFOSEC); înşelarea; războiul electronic; distrugerea fizică; angajarea liderilor cheie; operaţiile în reţeaua informatică (CNO).

*Operaţiile psihologice (PSYOPS)* sunt acţiuni nonviolente de natură psihologică, planificate şi desfăşurate pentru a influenţa atitudini şi comportamente în sensul facilitării realizării obiectivelor politice şi militare. Operaţiile psihologice pot fi considerate un adevărat „război al minţii contra minţii”, care practică manipularea informaţiei, dezinformarea, intoxicarea informaţională şi conduc la destabilizarea psihică, la influenţarea şi descurajarea adversarului.

Prin operaţii psihologice (PSYOPS), se urmăreşte discreditarea sau îmbunătăţirea imaginii anumitor guverne sau lideri, uneori crearea unor situaţii confuze, uşor de exploatat, descurajarea unor iniţiative şi încurajarea altora etc. Operaţiile psihologice se bazează pe o vastă bază de date referitoare, în principal, la aspecte geografice, politice, economice, culturale, religioase, psihosociale, istorie, tradiţie, obiceiuri, infrastructura teatrului de operaţii.

Operaţiile psihologice presupun, de asemenea, difuzarea de documente adverse trucate, cu scopul de a-i discredita pe adversari şi de a produce disensiuni şi diviziuni în rândul acestora. Dezinformarea (manipularea informaţiei), element esenţial al războiului psihologic, începe încă din timp de pace, înaintea conflictului propriu-zis, şi are obiective foarte complexe, urmărind, în general, destabilizarea psihologică şi polarizarea populaţiei, şi se intensifică odată cu pregătirea şi declanşarea primelor faze ale conflictului.

PSYOPS reţine controlul direct asupra conţinuturilor, diseminării şi audienţei. Eficacitatea operaţiilor psihologice reclamă pregătirea din timp a resurselor, cum ar fi sprijinul lingvistic, capabilităţile grafice şi de tipărire, capabilităţile de transmisii radio şi TV şi alte mecanisme de diseminare.

*Propaganda* este o practică comună politică de pace între naţiuni, ca formă de agresiune indirectă în loc de agresiune militară. În Doctrina pentru operaţii psihologice a forţelor armate ale SUA, din 2003, se poate găsi una dintre puţinele definiţii oficiale ale propagandei, înscrisă într-un document doctrinar militar. Ea este definită ca fiind „orice formă de comunicare în sprijinul unor obiective naţionale, în scopul influenţării opiniilor, emoţiilor, atitudinilor sau comportamentelor oricărui grup de oameni, în beneficiul direct sau indirect al sponsorului acestei comunicări”[22].

Tot aici, propaganda este clasificată în Propagandă Neagră, în care se lasă să se înţeleagă faptul că informaţia ar emana de la altă sursă decât cea reală; Propagandă Gri, în care nu este identificată sursa, şi Propagandă Albă, în care, ori sponsorul, ori sursa, este cunoscut/ă publicului.

Curtea Internaţională de Justiţie nu poate să se pronunţe pentru protecţia împotriva agresiunilor psihologice, deoarece ele nu pot fi incriminate în mod legal. Singura apărare este folosirea aceloraşi mijloace de război psihologic. Deoarece propagandiştii vizează un adversar străin, al cărui moral îl caută pentru a-l distruge prin mijloace psihologice, astfel încât acesta să înceapă să se îndoiască de validitatea convingerilor şi acţiunilor sale, rămâne în sarcina fiecărui guvern de a-şi apăra statul împotriva agresiunii propagandei[23].

Din cele prezentate anterior, rezultă faptul că inamicul care desfăşoară acţiuni hibride utilizează tactica terorii, urmărind să identifice şi să exploateze acele părţi descoperite şi vulnerabilităţi ale adversarului, net superior din punct de vedere militar, care, lovite prin angajarea unei cantităţi minime de efort şi energie, să genereze efecte maxime, traumatizante asupra mentalului colectiv, sentimentul de nesiguranţă şi neîncredere în capacitatea guvernului de a asigura protecţia naţiunii şi presiune asupra factorului politic, pentru obţinerea „victoriei” fără angajarea forţelor militare.

*Surprinderea*

În contextul conflictului de tip hibrid, realizarea surprinderii devine o condiţie extrem de importantă şi este realizată prin executarea unor acţiuni de luptă cu caracter special, punctiforme, pe obiective bine definite, cu efecte decisive asupra moralului forţelor şi conducerii. Forţele specializate, constituite în structuri de elită (echipe sau detaşamente de forţe pentru operaţii speciale sau comando), pregătite să execute acţiuni cu mare putere de distrugere, vor avea un rol esenţial în obţinerea succesului.

*Tactica terorii* este una dintre cele mai eficiente metode de luptă, utilizată de către inamicul care desfăşoară acţiuni hibride împotriva oponenţilor, ca parte a conceptului de „război total”. Grupările teroriste afiliate sau independente pot ataca adversarul oriunde şi oricând. Forţele pentru operaţii speciale pot utiliza, de asemenea, tactica terorii, pentru care sunt bine echipate, înarmate, pregătite şi motivate.

Elementele sensibile, vizate cu precădere de adversarul de tip hibrid, sunt populaţia civilă şi mediul înconjurător şi, prin urmare, cheia contracarării acestui tip de ameninţare constă în adoptarea acelor măsuri de educaţie, supraveghere, monitorizare, protecţie şi acţiune pentru reducerea nivelului de vulnerabilitate a acestora.

**Caracteristicile operaţiilor asimetrice**

Forţele şi acţiunile specifice războiului neregulat creează condiţiile favorabile apariţiei şi dezvoltării *asimetriilor*, care, de cele mai multe ori, se manifestă în planul confruntării convenţionale şi au drept efect înfrângerea forţelor oponentului. Unele forţe armate statale, în special cele aparţinând regimurilor totalitare sau unor state cu guvernări defectuoase, pot desfăşura, concomitent cu acţiunile convenţionale, şi acţiuni asimetrice, complementare şi în sprijinul îndeplinirii unor obiective militare convenţionale. Efectul operaţiilor specifice luptei armate poate fi exacerbat, perpetuat sau exploatat prin acţiuni asimetrice, în scopul menţinerii instabilităţii prin intermediul insurgenţei, terorismului, criminalităţii şi a dezordinii sociale.

Operaţiile asimetrice cuprind o plajă largă de acţiuni ale forţelor militare şi paramilitare, care, de regulă, sunt de durată şi sunt conduse cu sprijinul sau de către populaţia indigenă. Forţele neregulate pot demonstra capabilităţi combinate de elemente înarmate separatiste, insurgente, de gherilă şi criminale.

Forţele neregulate favorizează abordările indirecte[24] şi asimetrice. Totuşi, această formă de război poate angaja întreaga gamă de acţiuni militare şi capacităţi, în scopul de a eroda puterea adversarilor, influenţa şi voinţa lor. Războiul neregulat, în mod normal, este unul de uzură, care erodează adversarii statali şi nonstatali regionali, şi poate avea ramificaţii şi conexiuni cu acţiuni transnaţionale, ca rezultat al globalizării politice, economice şi financiare. Scopul acestuia este de a câştiga legitimitatea acţiunilor şi de a influenţa populaţia. Tipuri diferite de forţe neregulate pot utiliza niveluri diferite ale acţiunilor violente şi nonviolente pentru a-şi exercita influenţa. Accesul la tehnologie va avea impact asupra operaţiilor forţelor neregulate. În contextul conflictului de tip hibrid, mai cu seamă la nivel tactic, acestea pot aplica tehnici, tactici şi proceduri comune forţelor regulate, dar vor utiliza mijloace şi aplicaţii asimetrice.

Componenta convenţională a ameninţării hibride, chiar şi în condiţiile înfrângerii, poate fi reactivată sau favorizată şi susţinută prin

intermediul desfăşurării acţiunilor neregulate, asimetrice. Operaţiile asimetrice vizează atacarea componentelor abstracte ale efortului adversarului, orientat împotriva ameninţării hibride, precum: motivaţia de a lupta şi încrederea soldaţilor şi a comandanţilor, deciziile politice şi diplomatice, opinia publică, interesele instituţiilor private, voinţa naţiunii de a lupta şi de a susţine efortul de război, voinţa şi implicarea colectivă a alianţelor şi coaliţiilor.

Unul dintre cele mai periculoase aspecte ale ameninţării hibride este abilitatea componentelor sale de a se transforma „în interior” şi „în afară” în forme extrem de variate. Forţe militare autohtone, de exemplu, îşi pot dezbrăca uniforma, însemnele şi alţi indicatori ai statului şi ai apartenenţei lor şi se pot amesteca şi ascunde în rândurile populaţiei locale. Forţele insurgente pot abandona armele şi pot protesta inocent în sens invers. Criminalii pot îmbrăca efectele şi harnaşamentul forţelor poliţiei locale pentru a obţine accesul în obiective importante. Ameninţările hibride vor beneficia de dificultăţile unei identificări certe a actorilor, situaţie care este în avantajul lor. Mediul operaţional abundă în actori executând activităţi împotriva intereselor statelor membre ale forţei de sprijin, dar fără o semnătură vizibilă, clară, a statutului lor ca ameninţare. Adesea, aceşti actori vor lăsa impresia amprentei similare forţelor oponente sau neutre.

În concluzie, oponenţii ameninţărilor hibride vor întâmpina dificultăţi serioase în ceea ce priveşte identificarea şi separarea „setului de probleme” specific fiecărui tip de ameninţare. Aceştia vor fi obligaţi să aplice măsuri privind realizarea economiei de forţe pentru a acoperi mai multe linii de operaţii, iar adversarul hibrid va continua să-şi mute efortul şi să evidenţieze permanent faptul că orice opţiune ar alege, aceasta este una nepotrivită.

## Concluzii

Din evaluarea riscurilor şi ameninţărilor convenţionale, neconvenţionale şi asimetrice, rezultă un nou concept, denumit „riscuri şi ameninţări de tip hibrid”, care se manifestă în mediul operaţional contemporan şi care presupune abordări complexe în plan informaţional, decizional şi acţional.

Din analiza caracteristicilor specifice riscurilor şi ameninţărilor care se manifestă atât în spaţiul fizic (riscuri şi ameninţări convenţionale, neconvenţionale şi asimetrice), cât şi în mediul virtual, rezultă faptul că acestea pot afecta securitatea naţională, regională sau globală, fapt care poate conduce la planificarea, pregătirea şi execuţia unor acţiuni militare de tip hibrid.

Marile puteri militare ale lumii – cum sunt SUA, Rusia sau o coaliţie de internaţională de state – se pot impune astăzi fără probleme împotriva unui oponent convenţional, însă provocarea majoră a zilelor noastre şi a viitorului predictibil nu este aceasta, ci modul în care potenţialul adversar se va organiza, se va adapta şi va lupta, dezvoltând capacităţi neconvenţionale, de tipul armelor de distrugere în masă sau asimetrice, criminalităţii şi terorismului ecologic, îndreptate împotriva omului şi mediului său de viaţă pentru a contrabalansa şi pentru a-şi îndeplini obiectivele strategice.

## NOTE:

1 *** *AJP-2(A), Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), Draft 2012, p. 1-2.

2 *** Training Circular No. TC 7-100, *Hybrid Threat*, Headquarters Department of the Army, Washington DC, July 2010.

3 Valerică Cruceru, *Războiul hibrid în gândirea militară americană (Monografie)*, Editura Universităţii Naţionale de apărare „Carol I”, Bucureşti, 2015, p. 28.

4 Ana Stan, „Rusia a ridicat războiul la rang de artă”, 02.09.2014, adev.ro/nb9y9f, accesat la 30.03.2015.

5 Valery Gherasimov, ”Tsennost nauki v predvidenii”, *Voyenno-Promysblennz Karyer*, 8(476), 27 februarie 2013, http://www.vpk-news.ru/articles/14632, accesat la 02.04.2014.

6 *** *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p.2-O-3

7 *** *Doctrina Armatei României*, Bucureşti, 2012, p. 173.

8 *** *AJP-01(D), Allied Joint Doctrine*, December 2010, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), pp. 2-7.

9 *** *Doctrina Armatei României*, Bucureşti, 2012, p. 121.

10 Teodor Frunzeti, „Convenţional şi neconvenţional în acţiunile militare”, în revista CSSAS *Impact strategic*, nr. 4[45]/2012, p. 8.

11 dexonline.ro, accesat la 28 iulie 2019.

12 *** T.C.-7-100, Department of the Army Training Circular No. 7-100, *Hybrid Threat*, p. 2-1.

13 *** *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p. 2-I-5.

14 Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2013, p. 20.

15 dexonline.ro, accesat la 28 iulie 2019.

16 ***AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p. 2-G-4.

17 Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2013, p. 20.

18 dexonline.ro, accesat la 28 iulie 2019.

19 Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2013, p. 21.

20 *** *Doctrina Armatei României*, Bucureşti, 2012, p. 134.

21 *** *AJP- 3(B), Allied Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 16 March 2011, pp. 1-17.

22 Călin Hentea, „Operaţiile informaţionale sau noile haine ale propagandei”, www.lumeamilitara.ro/, accesat la 25.04.2015.

23 Mihaiu Mărgărit, „Ucraina şi războiul hibrid, în tentativele Rusiei expansioniste ale Moscovei de revenire a ei la masa marilor decizii ce privesc geopolitica mondială”, *Pulsul Geostrategic*, Nr. 175, 20 septembrie 2014, http://www.ingepo.ro

24 ***Conducere militară planificare operaţională (Curs universitar), Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2009, p. 29.

## BIBLIOGRAFIE


***Conducere militară planificare operaţională (Curs universitar), Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2009.

***Doctrina Armatei României, Bucureşti, 2012.

*** *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012.

***AJP-01(D), Allied Joint Doctrine, December 2010, North Atlantic Treaty Organization, NATO Standardization Agency (NSA).

*** *AJP-2(A), Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), Draft 2012.

*** *AJP-3(B), Allied Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 16 March 2011.

*** Training Circular No. TC 7-100, *Hybrid Threat*, Headquarters Department of the Army, Washington DC, July 2010.

Cruceru Valerică, *Războiul hibrid în gândirea militară americană (Monografie)*, Editura Universităţii Naţionale de apărare „Carol I”, Bucureşti, 2015.

Cruceru Valerică, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2013.

Frunzeti Teodor, „Convenţional şi neconvenţional în acţiunile militare”, în revista CSSAS *Impact strategic* nr.4[45]/2012.

Gherasimov Valery, ”Tsennost nauki v predvidenii”, *Voyenno-Promysblennz Karyer*, 8(476), 27 februarie 2013, www.vpk-news.ru/

Hentea Călin, „Operaţiile informaţionale sau noile haine ale propagandei”, www.lumeamilitara.ro/

Mărgărit Mihaiu, „Ucraina şi războiul hibrid, în tentativele Rusiei expansioniste ale Moscovei de revenire a ei la masa marilor decizii ce privesc geopolitica mondială”, *Pulsul Geostrategic*, nr. 175, 20 septembrie 2014, http://www.ingepo.ro

Stan Ana, „Rusia a ridicat războiul la rang de artă”, 02.09.2014, adev.ro/

http://www.dexonline

# PLANIFICARE ȘI STILURI DE PREDARE ÎN EDUCAȚIA FIZICĂ MILITARĂ

## *PLANNING AND TEACHING STYLES IN MILITARY PHYSICAL EDUCATION*

## *STYLES DE PLANIFICATION ET D'ENSEIGNEMENT DE L'ÉDUCATION PHYSIQUE MILITAIRE*

**Lt.col.lect.univ.dr. Gabriel Constantin CIAPA***

Succesul însușirii informațiilor, teoretice sau practice, depinde în mare măsură de organizarea și structurarea lor pe perioade de timp bine definite, de cantitatea lor, de baza materială avută la dispoziție, dar și de calitatea și pregătirea specialistului în educație fizică militară și de felul în care informațiile sunt transmise. De aceea prezentul material este împărțit în două părți. Prima parte vizează, într-o manieră sintetică, principalele documente de planificare, organizare și conducere a activității de educație fizică militară, în unele situații apărând exemplificări, cu scopul facilitării înțelegerii și realizării lor. A doua parte a acestui articol este îndreptată spre stiluri de predare în educație fizică, spre modalitatea de transmitere a informațiilor prevăzute în documentele specifice educației fizice militare, orientare care are în vizor profesorul/specialistul/instructorul în această specialitate militară.

*The success of acquiring information, whether theoretical or practical, depends to a large extent on their organization and structuring over well-defined periods of time, on their quantity, on the material basis available, but also on the quality and training of the military physical education specialist and on the way in which information is transmitted. Therefore, this material is divided into two parts. The first part deals, in a synthetic way, with the main documents of planning, organization and management of the military physical education activity, in some cases appearing examples, in order to facilitate their understanding and performance. The second part of this article is directed to teaching styles in physical education, to the way of transmitting the information provided in the documents specific to military physical education, orientation that has in sight the teacher/specialist/trainer in this military specialty.*

*Une bonne assimilation des informations, qu'elles soient théoriques ou pratiques, dépend en grande partie de l'organisation et de la structuration des informations au cours de périodes bien déterminées, du volume des informations, de la base matérielle disponible, mais également de la qualité et de la formation du spécialiste de l'éducation physique militaire et du façon dont les informations sont transmises. Par conséquent, cet article est divisé en deux parties. La première partie traite, de manière synthétique, les principaux documents de planification, d'organisation et de gestion de l'activité d'éducation physique militaire, en donnant, dans certains cas, des exemples afin de faciliter leur compréhension et leur réalisation. La deuxième partie de l'article est consacrée aux styles d'enseignement de l'éducation physique, à la manière utilisée pour faire parvenir les informations contenues dans les documents spécifiques à l'éducation physique militaire, une orientation à l'intention de l'enseignant/du spécialiste/de l'instructeur de cette discipline militaire.*

**Cuvinte-cheie:** educație fizică militară; plan; stil; lecție; specialist; anticipare.
***Keywords:*** *military physical education; plan; style; lesson; specialist; anticipation.*
***Mots-clés:*** *éducation physique militaire; plan; style; leçon; spécialiste; prévision.*

Finalitatea unei instruiri colective sau individuale precise, de valoare, ancorată în realitatea câmpului de luptă, trebuie să se bazeze pe concretul acțiunilor de luptă desfășurate în teatrele de operații. Ori, și în cazul educației fizice militare, desăvârșirea instruirii este condiționată și de această realitate și de proiectarea în timp a informațiilor de transmis. Pentru a obține o finalitate pozitivă, este necesar ca specialistul în educație fizică militară să posede un bagaj de cunoștințe ridicat, nu doar în direcția execuției acțiunilor motrice, ci și în cea

***Academia Tehnică Militară***
e-mail: *ciapagabriel@yahoo.com*

concepției, planificării precise și reale, să înțeleagă fenomenul și, de asemenea, să aibă un interes crescut pentru această specialitate militară.

Dacă, pentru planificarea cunoștințelor de transmis, este nevoie de viziune și de proiecție în timp – în viziunea mea proiectarea înseamnă realizarea unei anticipări a acțiunilor motrice (în cazul educației fizice militare), pe care militarii trebuie să le parcurgă, și asigurarea cadrului informațional și didactic pentru îndeplinirea obiectivelor stabilite – pentru felul în care sunt transmise informațiile, este necesar un bagaj didactic pedagogic ridicat, experiență, deschidere la nou și, de ce nu, răbdare. Fiecare om este o entitate distinctă, cu personalitate aparte, cu posibilități de asimilare a cunoștințelor în ritmuri și la momente diferite.

**Planificarea în educaţia fizică militară**

În abordarea principalelor documente de planificare în educația fizică militară, plecăm de la certitudinea existenţei precizărilor privind necesitatea întocmirii principalelor documente de organizare, planificare şi conducere a educaţiei fizice militare.

După cum se ştie, planificarea este o activitate a unui om care urmăreşte atingerea unor obiective precise. Ea reprezintă una dintre cele mai importante activităţi, realizată de specialistul/instructorul de educaţie fizică militară, şi are „un grad ridicat de complexitate... determinat de o multitudine de variabile”[1]. Aceste variabile sunt: „perioada de timp pentru care se elaborează, concepţia de tip cibernetic, natura componentelor modelului de educaţie fizică şi sport, locul de desfăşurare a activităţii, componenţa grupurilor/claselor de subiecţi după criteriul sexului, componenţa grupurilor/claselor de subiecţi după criteriul nivelului de pregătire fizică şi motrică”[2]. Documentele în baza cărora specialistul consolidează ştiinţific procesul instructiv-educativ sunt: *planul tematic*, *planul calendaristic* şi *planul de lecţie/proiectul didactic* (pentru învăţământ) sau *planul de desfăşurare* (pentru instruire).

Primul document de planificare este *planul tematic*[3] anual. Conform Regulamentului educației fizice militare, acest document este obligatoriu. Se elaborează pentru o perioadă de un an de zile şi cuprinde componentele procesului instructiv-educativ (calităţile motrice, deprinderile şi priceperile motrice), numărul de lecţii în care sunt tratate acestea, dispunerea lor în anul de instruire, timpul alocat fiecărui component în parte. Unele lucrări de specialitate admit şi menţionarea probelor de control.

Completarea unui plan tematic anual se poate realiza având în vedere câteva aspecte: numărul de lecţii tematice poate fi mai mare sau mai mic, în funcţie de obiectivele generale de atins; într-o lecţie se pot aborda una, două (timpul alocat fiecărei teme este stabilit de specialist, în funcţie de scopul şi complexitatea lecţiei) sau trei teme (timpul este alocat, de regulă, în mod egal, dar şi aici complexitatea este cea care determină distribuirea lui); timpul menţionat nu este cel maxim al lecţiei, 50 sau 100 de minute, componentelor tematice acordându-li-se 60-70% din totalul minutelor, restul regăsindu-se în verigile de început (1, 2, 3) şi de sfârşit (7, 8).

Al doilea document, *planul calendaristic*[4], este şi cel mai discutat de către toţi marii specialişti. El se întocmeşte pentru o perioadă de timp mai scurtă, durată care poate varia, în funcţie de structura anului de instrucţie (trimestrial, semestrial etc.). Planul calendaristic este realizat pe baza planului tematic anual, componentele din planul tematic regăsindu-se şi în acesta. Diferenţa majoră dintre cele două este dată de *Anexa planului calendaristic*[5], document care înglobează toate sistemele şi mijloacele de acţionare (exerciţiile fizice) pentru fiecare subcomponentă tematică în parte: viteză, îndemânare, forţă etc., și de completarea codificată în planul calendaristic a acestor mijloace de acționare. Aceste sisteme de acţionare se iau şi se trec în *Anexă,* având ca surse de inspirație diferite manuale de specialitate reviste de specialitate și observarea altor specialişti. Pot fi menţionate şi utilizate şi alte mijloace, însă doar după ce ele au fost validate experimental, în raport cu sarcinile didactice.

Sistemele de acţionare trecute în *Anexa planului calendaristic* trebuie să fie foarte clar descrise, precizându-se: „denumirea actului sau acţiunii motrice; poziţia iniţială, intermediară sau finală a corpului executantului; distanţa, durata sau încărcătura efortului fizic; tempoul de execuţie; numărul de repetări; durata pauzei dintre repetări şi natura ei; formaţia de lucru şi modalitatea concretă de exersare”[6].

Mijloacele de acţionare pot fi *simple*: *forţă*, F1 (F1 reprezintă exercițiul numărul 1, precizat în *Anexa la planul calendaristic*, în grupa calităților

motrice) – din poziţia culcat sprijinit facial, flexia antebraţelor pe braţe, 2 x 20 de repetări, pauza pasivă 40 de secunde între serii, exersare frontal –, sau *complexe*: *fotbal*, Ft2 (Ft2 reprezintă exerciţiul numărul 2, precizat în *Anexa* la *Planul calendaristic*, în grupa deprinderi şi priceperi motrice specifice probelor şi ramurilor sportive), 1-2x, pauză pasivă 1 minut şi 30 de secunde; a) dribling în linie dreaptă pe distanţa de 25 m şi executarea de şut la poartă, tempo 60%, 3 x, pauză activă 20 de secunde; formaţia de lucru: două şiruri a câte patru elevi; b) dribling printre şase jaloane, amplasate în linie dreaptă la 2 m unul faţă de altul, pasă la un coleg aflat oblic înainte, la 5 m faţă de ultimul jalon, reprimirea mingii şi executarea unui şut la poartă; tempo 60%, 3 x, pauză activă 30 de secunde; formaţia de lucru: două şiruri a câte patru elevi.

*Planul calendaristic* se prezintă în două forme: *descriptiv* – se trece în clar fiecare mijloc de codificare în dreptul componentelor tematice – şi *grafic* – apare o codificare în dreptul componentelor tematice (1/2x, 3/4x etc.). Fie că vorbim de o modalitate sau alta de realizare a lui, planul calendaristic trebuie să conţină aceleaşi elemente ca planul tematic, la care se adaugă, obligatoriu, *sistemele de acţionare* codificate sau în clar şi *probele de control*. Este foarte important ca, în realizarea lui, la consemnarea mijloacelor de acţionare să se ţină cont de următoarele: timpul alocat prin planul tematic trebuie să fie epuizat cu mijloacele de acţionare şi să nu-l depăşească, modul de completare în căsuţe nu este standardizat – se poate opta pentru diferite formule de menţionare în scris –, să se planifice atâtea mijloace de acţionare, ca dozare, încât să acopere timpul alocat temei din planul tematic anual.

Al treilea document al educației fizice militare este *planul de lecţie / proiectul didactic / planul de desfăşurare* a procesului instructiv-educativ. Acest document este cel care permite realizarea obiectivelor operaţionale de lecţie, conducerea lecţiilor curente. Reprezintă materializarea gândirii detaliate a specialistului pentru îndeplinirea sarcinilor imediate de lecţie. Este o concretizare a capacităţii anticipative a specialistului pentru îndeplinirea obiectivelor de instruire, în timpul alocat lecţiei de educaţie fizică militară.

La întocmirea lui se urmăresc o serie de elemente esenţiale, logic structurate, în aceeaşi succesiune de fiecare dată.

*Primul element* vizează stabilirea obiectivelor, care trebuie să fie realiste, să se încadreze în timpul alocat, să respecte planurile de pregătire – obiectivele nu se adresează specialistului, ci îi vizează pe militari – trebuie să fie explicite şi să arate potenţiale modificări motrice la military, să urmărească o singură operaţie printr-o exprimare scurtă, să se încadreze într-o structură logică de pregătire generală. Pentru înţelegerea stabilirii obiectivelor, voi exemplifica, doar câteva dintre cuvintele cheie utilizate în educația fizică militară: să enumere, să enunţe, să descrie, să identifice, să coopereze, să acorde, să execute, să realizeze, dezvoltare, îmbunătăţirea, verificarea, însuşirea, consolidarea, perfecţionarea etc.

*Al doilea element* important se regăseşte în analizarea componentei umane aflat la dispoziţia specialistului (număr de militari, sex, nivel de pregătire), a condiţiilor de desfăşurare a procesului instructiv-educativ (materiale, geoclimaterice).

*Al treilea element* urmăreşte „elaborarea de strategii metodico-organizatorice: repartizarea timpului alocat lecţiei pentru fiecare verigă, stabilirea ordinii de abordare a temelor”[7], alegerea celor trei „M” (metode-materiale-mijloace) necesare realizării obiectivelor de lecţie, dozarea efortului, formaţii de lucru, tipuri de exersare.

Ultimul aspect, extrem de important, numit şi „evaluarea eficienţei activităţii curente”, vizează elaborarea unui sistem de evaluare a calităţii îndeplinirii sarcinilor didactice şi de militari, dar şi de conducătorul procesului instructiv. Însă, toate aceste aspecte ale planificării ar fi inutile, dacă ele nu s-ar materializa în concret, dacă nu s-ar pune în aplicare conținutul lor, dacă activitatea de predare nu ar mai avea loc.

**Stiluri de predare în educaţia fizică militară**

Predarea în educația fizică militară se defineşte ca fiind activitatea de transmitere a unui conţinut de învăţat, teoretic şi/sau practic, specific activităţii de învăţământ sau de instruire. Concret, ea presupune prezentarea conţinutului, explicarea aspectelor esenţiale ale noţiunilor, dezvoltarea de abilităţi practice şi teoretice, totul bazându-se pe obiective şi finalităţi ale acestei activităţi şi ale comenzii sociale.

Eficiența predării este condiționată și de stilul abordat de specialistul în educație fizică militară. Tipologia stilurilor de predare a fost realizată pentru

prima dată de către M. Mosston și Ashworth Sara, din dorința conceperii un ghid pentru profesorii din domeniu. Conform lor, spectrul este format din 11 stiluri, dintre care cinci sunt centrate pe specialist și șase, pe elev/student/militar. Stilurile de predare sunt absolut necesare, deoarece elevii/studenții/militarii trebuie să poată asimila ceea ce specialistul predă.

Totuși, alegerea stilurilor de predare poate depinde de specificul acțiunilor motrice, de omogenitatea grupului și a nivelului de pregătire a acestuia, de capacitatea de înțelegere a cunoștințelor, de obiectivele lecțiilor, de nivelul educațional și de experiența specialistului și, cel mai important, din punctul meu de vedere, de interesul și valoarea moral-socială a grupului pentru această formă de pregătire. Înțelegând că oamenii asimilează informații diferit, este evident că trebuie să existe stiluri de predare diferite pentru a se putea realiza adaptarea la stilurile de învățare.

„Stilul de predare reprezintă un set de comportamente selecţionate şi utilizate de specialist în vederea realizării obiectivelor educaţionale”[8]. Putem spune despre stilul de predare că este dat de modul individual-particular de realizare a procesului de predare. Stilul de predare utilizat în cadrul lecţiilor este pur alegerea specialistului. În enunţarea acestor stiluri de predare în educația fizică militară, avem în vedere două direcţii de analiză: în funcţie de abordarea activităţii, întâlnim *stilul comenzii, practic, reciproc, „verificare personală”*, *„incluziune”*; în funcţie de orientarea acţiunii, avem stilul direct şi cel indirect. La aceste stiluri, se mai pot adăuga și altele, pe care eu le încadrez într-o grupă, mai degrabă, de pseudostiluri, atunci când apare această modalitate de transmitere a informației în sistemul educației fizice. Aceste stiluri sunt cel democratic și cel neglijent.

*Stilul comenzii*[9]

Transmiterea cunoştinţelor se face unidirecţional, deciziile fiind luate numai de specialist, fără existenţa vreunui dialog între militari şi instructori, în mod autoritar, distant şi rece. Poate reprezenta abordarea celor nepregătiţi, încrezuţi, cu tendinţe de profesori. În această situaţie, numai militarii sunt de vină pentru lipsa însuşirii cunoştinţelor. Însă acest stil se impune și este necesar când militarii trebuie să răspundă prompt și rapid la comenzi, când siguranța executanților este primordială, când este căutată precizia. De exemplu, acest stil poate fi utilizat când este nevoie de o încălzire perfect sincronizată, în sporturi în care sincronizarea este o cerință pentru obținerea unui punctaj superior (înot sincron, arte marțiale, dans etc.), în festivități de deschidere sau de închidere a competițiilor sportive de mare anvergură, în marșuri și parade militare.

*Stilul practic*[10]

Specialistul demonstrează actul sau acțiunea motrică și stabilește oportunitatea pentru militari de a exersa și a-și dezvolta abilitățile în ritmul lor. Pe măsură ce militarii îndeplinesc sarcinile didactice, specialistul va circula printre ei, oferind feedback individual și de grup. De exemplu, specialistul demonstrează cum să efectuezi o tehnică de brațe din arte marțiale. Pe măsură ce elevii își însușesc tehnica, specialistul va merge și va oferi un răspuns legat de asimilarea acestei tehnici. Definitoriu pentru acest stil este practica individuală, chiar și în mod privat.

*Stilul reciproc*[11]

Trăsăturile definitorii pentru acest stil sunt reliefate de interacțiunea socială, ajutor reciproc, oferirea și primirea imediată de răspuns la acțiunile motrice realizate cu ajutorul unui partener. Rolul specialistului este de a indica ce trebuie executat, de a oferi răspunsuri și indicații în timpul realizării actului sau acțiunii motrice de către partenerii de lucru. Militarii vor lucra împreună, pe perechi, oferind în permanență un feedback despre ceea ce se realizează și ce nu. Sugestive pentru acest stil sunt exercițiile de gimnastică realizate cu ajutorul unui partener și, de asemenea, procedeele tehnice din diferitele sporturi de lupte.

*Stilul „verificare personală”*[12]

Este foarte asemănător stilului reciproc, doar că militarii vor desfășura activități motrice pe cont propriu. Acestora le sunt oferite criteriile de performanță, standarde de evaluare și un sumar al greșelilor pe care le pot realiza în executarea acțiuniilor motrice. Acest stil le permite militarilor să practice și să se autocorecteze în timpul lor și să-și evalueze propria învățare, să-și verifice propriile performanțe. În cadrul orelor, specialistul va lucra împreună cu elevii pentru a stabili ținte și obiective. Definitoriu pentru acest stil este autoevaluarea, bazată pe criterii specifice. Acest tip se

regăsește în sporturi precum baschet, tir cu arcul, golf, escaladă, surfing, skateboard, în diferite exerciții realizate în sala de forță.

*Stilul „incluziune”*[13]

Specialistul planifică și stabilește o varietate de sarcini care au niveluri de dificultate diferențiate. Astfel, militarii decid care sarcină este cea mai potrivită pentru abilitățile, aspirațiile și motivațiile lor. Acest stil oferă o abordare personalizată și de dezvoltare a învățării. Important pentru acest stil este faptul că militarii pot selecta aceeași sarcină didactică, dar cu un nivel de dificultate ridicat, care îi pot face să evolueze mai rapid. Nivelurile de dificultate sunt create de specialist, în funcție de grupul care trebuie instruit. De asemenea, acesta ajustează în permanență nivelul de lucru și verifică performanța atinsă de militari în cadrul procesului de instruire, conform criteriilor și standardelor stabilite în actul planificării. Acest stil se poate adopta în cadrul lecțiilor cu teme din arte marțiale, atunci când nivelul de dificultate al proceedelor tehnice poate fi crescut sau scăzut, în funcție de membrii colectivului de instruit.

*Stilul direct*[14] este orientat pe acţiunea instructorului. Prin abordarea acestui stil creşte eficienţa exersării, se reduc şansele de eroare în execuţia actelor şi acţiunilor motrice, cresc şansele unei coordonări şi conduceri mai bune a grupului participant la instruire. Acest procedeu are şi neajunsuri care constau în: lipsa posibilităţii de a aborda diferenţiat militarii şi „orientarea asupra rezultatelor învăţării, şi nu asupra procesului care are loc”[15]. Un exemplu logic de înşiruiri de acţiuni pentru acest stil de predare poate fi: explicarea conţinutului de învăţat şi demonstrarea lui, executarea acţiunilor motrice de militari, corectarea eventualelor greşeli, prezentarea indicaţiilor metodice, din nou corectarea greşelilor şi apoi reluarea executării actelor motrice.

*Stilul indirect*[16] este orientat spre acţiunea militarilor. În cadrul acestui stil se consideră că ei au posibilitatea de a alege calea pentru îndeplinirea sarcinilor didactice, de unde rezultă o mai bună implicare a acestora în actul didactic. Stilului indirect i se pot atribui şi două mari dezavantaje: un timp mai mare pentru realizarea sarcinilor şi lipsa controlului asupra grupului de pregătit.

*Stilul neglijent* aparţine celui dezinteresat de roadele muncii sale, celui căruia îi lipseşte motivaţia pentru actul educaţional. Acesta va accepta orice propunere din partea celor de instruit, este pasiv în lecţiile de educaţie fizică militară, nu este exigent, susţine un nivel de pregătire slab, sub potenţialul real al militarilor.

*Stilul democratic* are la bază cooperarea foarte bună dintre militar şi instructor, stimularea iniţiativei, motivaţia puternică şi încrederea acordată celor de instruit. Însă în unele cazuri acest stil poate conduce la neglijarea indicaţiilor instructorului și chiar la tentativa de a nu realiza acțiunea motrică. Este considerat un stil benefic pentru actul socializării și evoluției motrice, însă, din punctul meu de vedere, nu trebuie utilizat ca stil fundamental, permanent, în această specialitate militară.

Din punctul meu de vedere, specialistul în educație fizică militară nu trebuie să adopte doar unul dintre stiluri şi să-l folosească doar pe acesta în actul de predare. El trebuie să îmbine elementele pozitive ale acestora, să le adapteze grupului căruia i se adresează și să conducă întreaga activitate în funcție de obiectivele și de sarcinile de îndeplinit. De altfel, calitatea de specialist/ instructor în educație fizică militară se dobândeşte prin instruire adecvată, ca urmare a participării la forme de pregătire în instituţii specializate, şi necesită un sumar de competenţe psihopedagogice, profesionale, didactice şi de comunicare, care au ca finalitate orientarea lor spre atingerea obiectivelor actului de învăţare, în folosul celor instruiţi şi instituţiei militare.

**Concluzii**

Proiectare, planificare, predare sunt trei concepte şi, totodată, activităţi definitorii pentru finalitatea actului de instruire. Fără o viziune clară şi în lipsa anticipării acţiunilor la care militarii pot fi supuşi în situaţii reale de luptă, pregătirii din educaţia fizică militară îi va lipsi adaptarea conţinutului instruirii la cerinţa fundamentală a armatei: de îndeplinire a misiunilor de luptă. Materializarea proiecţiei conţinutului instruirii în documentele de planificare reprezintă un pas important în atingerea obiectivelor educaţiei fizice militare, o direcţie raţională şi normală, în cele din urmă, pentru specialiştii din acest domeniu.

Transpunerea conţinutului instruirii în cadrul lecţiei, realizarea actului de predare în sine reprezintă etapa esenţială prin care se face transferul de cunoştinţe de la specialist la militar. Cum se realizează acest transfer? Cantitatea şi calitatea cunoştinţelor de specialitate şi a celor pedagogice, atinse anterior actului predării, experienţa pedagogică şi de viaţă, calitatea proceselor cognitive superioare, a celor care conduc activitatea, capacitatea de interacţiune socială, dorinţa de a atinge obiectivele stabilite cu orice preţ, perseverenţa sunt doar câteva puncte de referinţă şi motive cu ajutorul cărora specialistul de educaţie fizică îşi construieşte propria modalitate, propriul stil de predare. Expunerea acestor câteva motive ne îndeamnă să credem, totodată, că un specialist în educaţie fizică militară nu se construieşte de la o zi la alta.

**NOTE:**

1 Gh. Cârstea, *Teoria şi metodica educaţiei fizice şi sportului*, Editura AN-DA, Bucureşti, 2000, p. 137.
2 *Ibidem*.
3 Gh. Cârstea, *Educaţia fizică: teoria şi bazele metodicii*, Editura ANEFS, Bucureşti, 1997, p. 197.
4 *Ibidem*, p. 201.
5 *Ibidem*, p. 207.
6 Gh. Cârstea, *Teoria şi metodica educaţiei fizice şi Sportului*, Editura AN-DA, Bucureşti, 2000, p. 144.
7 A. Dragnea şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Editura FEST, Bucureşti, 2006, p. 185.
8 *Ibidem*, p. 163.
9 Mosston M., Ashworth S., *Teaching Physical Education*, First Online Edition, Spectrum Teaching and Learning Institute, SUA, 2008, p. 76.
10 *Ibidem*, p. 94.
11 *Ibidem*, p. 116.
12 *Ibidem*, p. 141.
13 *Ibidem*, p. 156.
14 A. Dragnea şi colab., *op.cit.*, p. 163.
15 *Ibidem*.
16 *Ibidem*, p. 164.

## BIBLIOGRAFIE

Cârstea Gh., *Teoria şi metodica educaţiei fizice şi sportului*, Editura AN-DA, Bucureşti, 2000.

Ciapa G.C., *Pregătirea fizică a militarilor din armata României în conflictele moderne,* Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2018.

Ciapa G.C., *Educaţia fizică militară – formă de pregătire pentru luptă.* Raport de cercetare nr. 1, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2015.

Dragnea A. şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Editura FEST, Bucureşti, 2006.

Epuran M., Horghidan V., *Psihologia educaţiei fizice*, ANEFS, Bucureşti, 1994.

Mosston M., Ashworth S., *Teaching Physical Education*, First Online Edition, Spectrum Teaching and Learning Institute, SUA, 2008.

http://www.academia.edu

http://www.cognifit.com

http://www.education.cu-portland.edu

http://www.thepeproject.com

# PRINCIPII ȘI METODE DE INSTRUIRE ÎN EDUCAȚIA FIZICĂ MILITARĂ

## *PRINCIPLES AND METHODS OF TRAINING IN MILITARY PHYSICAL EDUCATION*

## *PRINCIPES ET MÉTHODES DE FORMATION EN ÉDUCATION PHYSIQUE MILITAIRE*

**Lt.col.lect.univ.dr. Gabriel Constantin CIAPA***

Legătura dintre teorie și aplicarea cunoștințelor teoretice în practica educației fizice militare se realizează, în unele situații, cu destul de multă ambiguitate și dificultate. Rezultatul acestei sincope se va regăsi imediat în nivelul de pregătire al celor instruiți. O cauză a acestei sincope o poate reprezenta trecerea în plan secund a unor cunoștințe teoretice fundamentale de specialitate, absolut necesare actului educațional. De aceea, în prima parte a acestui material, voi aborda principiile de instruire specifice subdomeniului educației fizice militare, cu scopul realizării unei interpretări a acestora, necesară atât înțelegerii, cât și importanței lor în actul instruirii în sistemul militar de specialitate.

A doua parte a acestui material este dedicată metodelor clasice de instruire în educația fizică. În întregimea lui, prezentul material își propune o reiterare a celor două fundamente ale educației fizice militare, realizarea unei sinteze a acestora și, eventual, o completare a literaturii militare de specialitate.

*The connection between theory and the application of theoretical knowledge in the practice of military physical education, is realized in some situations with quite an ambiguity and difficulty. The result of this syncope will be found immediately in the training level of the trained persons. A cause of this syncope can be represented by the passage in the second plane of certain fundamental theoretical specialized knowledge, absolutely necessary for the educational act. Therefore, in the first part of this material, I will approach the training principles specific to the sub-domain of military physical education, in order to achieve an interpretation of them, necessary both for their understanding and for their importance in the act of training in the specialized military system.*

*The second part of this material is dedicated to the classical methods of training in physical education. As a whole, this material aims at a reiteration of the two fundamentals of military physical education, providing a synthesis of them and, possibly, a supplement of the specialized military literature.*

*La relation entre la théorie et sa mise en pratique dans l'éducation physique militaire s'établit, dans certains cas, avec beaucoup d'ambiguïté et de difficultés. Le résultat de cette syncope se reflétera à l'instant au niveau de formation des apprentis. Une des causes de cette syncope pourrait être le passage de certaines connaissances théoriques fondamentales de spécialité, absolument nécessaires à l'acte éducatif, en arrière-plan. Par conséquent, dans la première partie de cet article, on va traiter les principes de formation spécifiques au sous-domaine de l'éducation physique militaire, afin de parvenir à une interprétation de ces principes, qui est nécessaire pour comprendre à la fois leur rôle et leur importance pour le processus de formation dans le système militaire spécialisé. La deuxième partie de l'article est consacrée aux méthodes classiques d'entraînement en éducation physique. Le présent document vise, dans l'ensemble, à rappeler les deux fondements de l'éducation physique militaire, à en faire une synthèse et, éventuellement, à compléter la littérature militaire spécialisée.*

**Cuvinte-cheie:** educație fizică militară; principii; metode; instruire; exersare.
***Keywords:*** *military physical education; principles; methods; training; practice.*
***Mots-clés:*** *l'éducation physique militaire; principes; méthodes; instruction; pratique.*

***Academia Tehnică Militară***
e-mail: *ciapagabriel@yahoo.com*

Subsistemul educației fizice militare trebuie să fie într-o permanentă modificare și adaptare la noile condiții cerute de sistemul militar. De aceea se impune o aplecare profundă spre toate posibilitățile reale care pot conduce la găsirea de soluții pentru îmbunătățirea atât a activității în sine, cât și a produsului finit – a se înțelege militarul/luptătorul. Fie că ne îndreptăm atenția asupra bazei materiale, fie asupra unor resurse teoretice științifice, acestea trebuie să conveargă și să se regăsească în calitatea celui instruit.

Aplicarea cunoștințelor teoretice din educația fizică militară în practica instruirii nu va face decât să faciliteze însușirea acțiunilor motrice sau formarea deprinderilor și priceperilor motrice, în condițiile unei pregătiri pentru luptă a militarilor în mod constant, lucid, real, riguros, unei desfășurări ritmice a activităților specifice, evaluării și controlului permanent.

Educația fizică militară, ca subsistem al educației generale, presupune funcționarea după reguli clare, având funcții și obiective precise, metodologie și terminologie proprie. De asemenea, educația fizică militară utilizează o serie de cunoștințe fundamentale, care au ca finalitate realizarea acțiunilor motrice. Unele dintre aceste fundamente ale instruirii în această specialitate militară sunt principiile de instruire și metodele de instruire în educația fizică.

**Principiile de instruire în educaţia fizică militară**

Procesul instructiv-educativ al educaţiei fizice militare este o activitate care se desfăşoară sub semnul normelor, dispoziţiilor, regulilor sau diferitelor cerinţe de instruire. Necesitatea acestor reguli sau cerinţe pleacă din nevoile de instruire ale armatei, pentru atingerea scopurilor de pregătire a acesteia. Unele dintre ele poartă numele de *principii de instruire*[1], principii care s-au statornicit ca necesar și obligativitate în pregătirea specifică acestui domeniu, fiind recunoscute şi respectate de toţi marii specialişti ai educaţiei fizice militare. Aceste principii sunt: al participării active şi conştiente, intuiției, accesibilității, sistematizării și continuităţii, legării instruirii de cerinţele activităţii practice, însuşirii temeinice.

*Principiul participării active şi conştiente*[2]

Din enunţul acestui principiu, se poate înţelege că el urmăreşte două direcţii de analiză a participanţilor la procesul de instruire: prima direcţie este dată de cerinţa implicării active a militarilor în instruire, iar cea de-a doua vizează conştientizarea lor în ceea ce priveşte pregătirea. Respectarea celor două direcţii trasate de acest principiu solicită îndeplinirea mai multor sarcini de către participanţii la instruire, instructorii şi militarii de instruit.

Un prim aspect este furnizat de obiectivele procesului instructiv-educativ, în sensul înţelegerii lor, de ce trebuie să participe la aceste programe de pregătire. Rolul instructorilor este determinant în crearea factorului motivaţional corect şi realist la militari pentru practicarea exerciţiilor fizice.

Al doilea punct de interes urmăreşte succesiunea logică a actelor şi acţiunilor motrice pe care militarii trebuie să le înveţe. Această succesiune trebuie înţeleasă, memorată şi aplicată atunci când este cazul. Un rol extrem de important îi revine instructorului, care, prin planificarea şi structurarea materialului de învăţat, poate contribui la uşurarea sau îngreuierea însuşirii sau dezvoltării structurilor motrice. De asemenea, el trebuie să cunoască elementele cheie din structura metodică a procedeelor de învăţat.

Al treilea aspect pe care acest principiu îl urmăreşte este de a crea o atitudine corespunzătoare de sensibilizare şi de responsabilizare a militarilor pentru învăţarea materialului didactic. Ei trebuie încurajaţi în a lucra independent, trebuie să li se ofere posibilitatea de a alege dintre soluţiile oferite de instructori, trebuie stimulaţi şi încurajaţi în a adopta o atitudine obiectivă faţă de procesul de instruire, faţă de modalităţile de predare.

Ultima latură a acestui principiu urmăreşte formarea la militari a capacităţii de autoapreciere şi de autoevaluare obiectivă a execuţiilor actelor şi acţiunilor motrice, precum şi a rezultatelor, obţinute ca urmare a instruirii. Aproape întotdeauna este „altul” de vină pentru lipsa performanţei proprii, găsindu-se justificări, uneori de-a dreptul penibile, pentru rezultatele slabe şi pentru lipsa participării la instruire.

*Principiul intuiţiei*[3]

Principiul acesta evidenţiază importanţa primul sistem de semnalizare uman: cel senzorial. „Intuiţia presupune o cunoaştere a realităţii cu ajutorul simţurilor, analizatorilor, receptorilor organismului uman”[4]. Şi în subsistemul educaţiei fizice militare,

principiul intuiţiei vizează stimularea a cât mai multor analizatori (vizual, auditiv, tactil). Accesarea acestora ca un tot unitar se poate reflecta în rapiditatea şi în calitatea însuşirii materialului de învăţat. Evident, militarii cu deficienţe ai acestor analizatori, deşi nu ar trebui să existe la instruire în sistemul militar, au de suferit în a recepţiona şi în a învăţa actele motrice. Pentru obţinerea de rezultate, se încearcă stimularea analizatorilor prin cele trei metode clasice de instruire: demonstraţia, prezentarea de materiale iconografice şi observarea altor militari, metode de instruire pe care le voi aborda în a doua parte a acestui material. Principiul intuiţiei impune ca materialul de transmis să poată fi văzut şi accesat de toţi cei prezenţi la instruire; de asemenea, principiul solicită stimularea şi celui de-al doilea sistem de semnalizare al organismului uman.

*Principiul accesibilităţii*[5]

Acest principiu evidenţiază importanţa desfăşurării procesului instructiv-educativ în funcţie de vârstă, de sex şi de nivel de pregătire. Accesibilitatea nu trebuie înţeleasă ca un minim de efort şi obiective pe care militarii trebuie să le îndeplinească în cadrul procesului instructiv-educativ, ci ca pe o cerinţă, care, pentru a fi îndeplinită, trebuie să depună efort fizic, trebuie să muncească, dacă doresc să evolueze.

Pentru a respecta acest principiu, instructorii militari trebuie să urmărească: „selecţionarea cu atenţie a stimulilor, a exerciţiilor fizice cu precădere; stabilirea unei dozări corespunzătoare a efortului fizic; folosirea unor reglatori metodici pentru a accelera procesul de însuşire a unor acte sau acţiuni motrice de către subiecţi; adaptarea metodelor şi procedeelor metodice de instruire şi educaţie la nivelul de înţelegere şi de dezvoltare psiho-motrică a subiecţilor; diferenţierea evaluării subiecţilor”[6] (conform *Regulamentului educaţiei fizice militare*, 2012, evaluarea acestora se realizează pe grupe de vârstă, de învăţământ sau de instrucţie).

Pentru a aplica acest principiu, este necesar ca instructorul să cunoască militarii participanţi la instruire, să creeze un ritm de lucru, raportat la reacţia militarilor la stimuli, şi să aplice următoarele reguli didactice: de la uşor la greu, de la simplu la complex şi de la cunoscut la necunoscut.

*Principiul sistematizării şi continuităţii*[7]

Acest principiu este relevant din prisma planificării activităţii şi întocmirii corecte a documentelor de conducere a lecţiilor de educaţie fizică militară. Elementele centrale ale sale, sistematizarea şi continuitatea, sunt condiţii esenţiale pentru atingerea obiectivelor educaţiei fizice militare.

Pentru ca principiul sistematizării şi continuităţii să se regăsească în activitatea de educaţie fizică militară, trebuie respectate următoarele exigenţe: ordonarea şi programarea logică a conţinuturilor de transmis în cadrul aceluiaşi ciclu de pregătire; conţinuturile noi de învăţat trebuie să se bazeze pe cele vechi, existente deja, ele devenind, la rândul lor, sprijin pentru cunoştinţele următoare; fondul procesului instructiv-educativ trebuie structurat şi programat în aşa fel încât să ofere posibilitatea legăturilor logice dintre anii de instrucţie sau anii de învăţământ; obligativitatea participării militarilor la instruire în mod constant – absenţele pot conduce la pierderea cunoştinţelor însuşite sau pot crea lacune în pregătire.

*Principiul legării instruirii de cerinţele activităţii practice*[8]

Pentru mulţi specialişti de educaţie fizică militară, acest principiu nu reprezintă o prioritate, el trecând în plan secund. Principiul reliefează importanţa ancorării pregătirii în realitatea luptei armate. Cu alte cuvinte, ceea ce se învaţă trebuie să fie util în potenţialele situaţii ale luptei armate, să capete cu adevărat valoare practică, iar cunoştinţele să fie adaptabile cerinţelor luptei.

Sunt multe situaţii în procesul instructiv-educativ în care conţinutul este transmis doar pentru a bifa un material de învăţat, şi nimic mai mult. Acest fapt se întâmplă tocmai ca urmare a lipsei cunoştinţelor de specialitate, a necunoaşterii cerinţelor luptei armate şi a promovării an de an a aceloraşi conţinuturi învechite, lipsite de relevanţă pentru practica vieţii. Literatura de specialitate mai denumeşte acest principiu şi al modelării, al cărui scop este acela de a crea posibilităţi de generalizare a materialului didactic însuşit, de a aplica cunoştinţele învăţate în condiţii total noi, imprevizibile, altele decât cele în care a avut loc desfăşurarea procesului instructiv-educativ.

*Principiul însuşirii temeinice*[9]

Principiul durabilităţii, cum mai este numit în literatura de specialitate, este condiţionat celorlalte principii. Durabilitatea conţinuturilor învăţate este condiţionată de: numărul mare de repetări, asigurate actelor şi acţiunilor motrice în cadrul procesului de instruire; programarea, de preferat, a unui volum mic din conţinutul de învăţat într-o anumită perioadă – se asigură condiţiile, ca buget de timp, pentru un număr mai mare de repetări numai dacă s-ar planifica un volum mare de învăţat, în aceeaşi unitate de timp; cunoaşterea stadiului pregătirii militarilor şi a nivelului cunoştinţelor însuşite de aceştia.

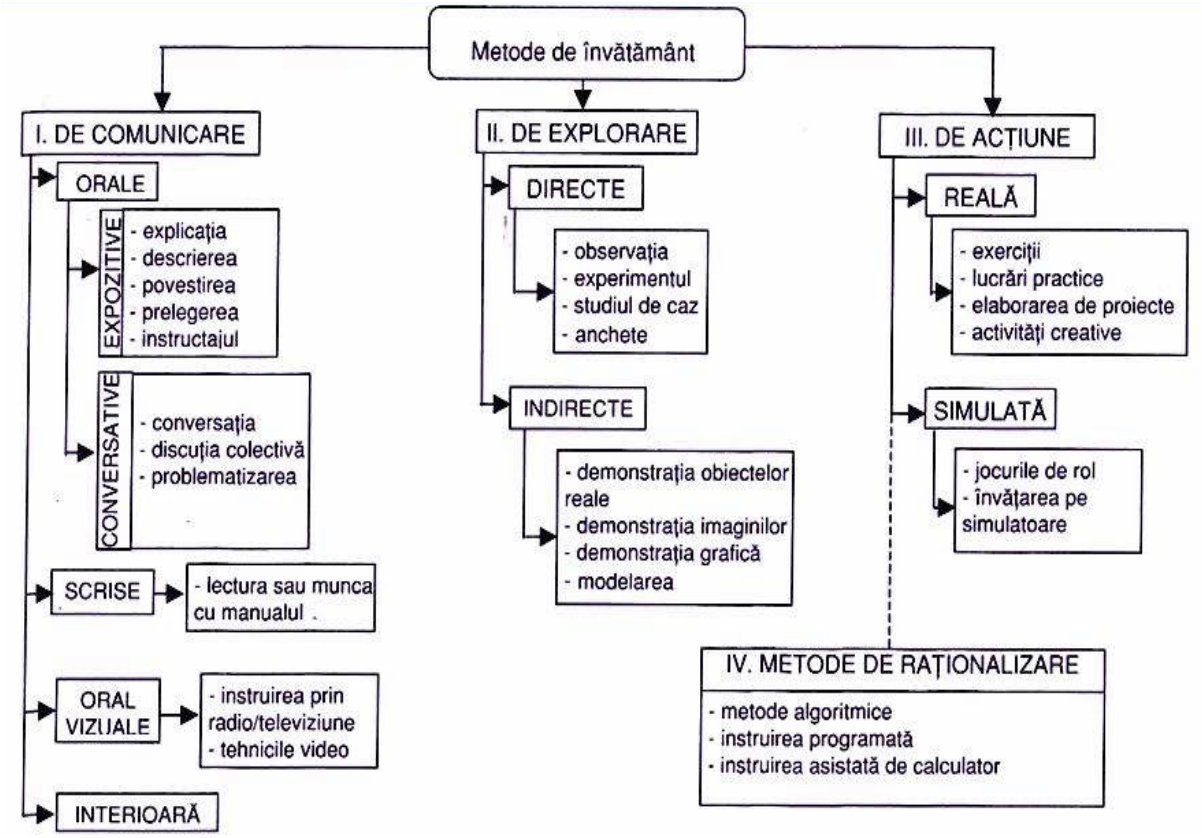



**Figura 1** *Clasificarea metodelor de învăţământ*[10]

**Metode de instruire în educaţia fizică militară**

Pedagogia numeşte metoda ca fiind *drumul spre* atingerea obiectivelor o modalitate de lucru. Această noţiune va stârni întodeauna tendinţe de definire, din partea tuturor specialiştilor. În viziunea mea, metoda reprezintă totalitatea elementelor didactice folosite pentru atingerea obiectivelor educaţiei fizice militare sau a obiectivelor operaţionale de lecţie prin intermediul unor acţiuni logice proiectate în timp. Alegerea metodelor de instruire şi utilizarea lor în cadrul lecţiilor de educaţie fizică militară ţin numai de ştiinţa celor care conduc activitatea. Aceste metode de instruire sunt strâns legate de mijloacele de realizare a scopurilor lecţiilor şi de atingere a obiectivelor stabilite. Metoda şi mijlocul sunt indisolubil legate şi se intercondiţionează reciproc. Un suport solid de cunoştinţe teoretice şi practice va uşura alegerea metodelor de instruire necesare actului instructiv-educativ.

În decursul anilor, specialiştii în domeniu au încercat mai multe clasificări, după diferite criterii. În cele din urmă, în fiecare dintre acestea se regăsesc aceleaşi metode.

În Figura 1 exemplificăm o astfel de clasificare, urmând a o dezvolta pe cea consacrată în acest domeniu.

În viziunea unora dintre specialiştii în educaţie fizică, metodele de instruire sunt verbale (explicaţia, expunerea, povestirea etc.) şi nonverbale (exersare, evaluare practică, demonstraţie etc.). Însă majoritatea specialiştilor din domeniu acceptă cu mai multă uşurinţă abordarea clasică a metodelor de instruire. Aceste metode se aplică şi subsistemului educaţiei fizice militare. Conform abordării clasice, avem metode de instruire verbale, intuitive

şi metoda practică. Metodele verbale se bazează pe capacitatea conducătorilor actului educaţional de transmitere a cunoştinţelor prin limbaj. Aceste metode verbale sunt: *prelegerea* – metodă care se aplică în învăţământul superior, mai ales, şi se bazează pe argumente ştiinţifice şi pe terminologie de specialitate adecvată; *explicaţia* – este cea mai folosită metodă şi de unii instructori singura, din păcate. Explicaţia trebuie să fie logică, precisă, clară şi să intervină la momentul potrivit. În cadrul procesului instructiv-educativ, explicaţia poate să preceadă demonstraţia, poate să intervină după demonstraţie sau concomitent cu aceasta (utilizarea acestor două metode simultan este mai greu de realizat şi nerecomandată, în cazul însuşirii procedeelor tehnice dificile).

Alte metode sunt: *povestirea* – se adresează copiilor, în principal, iar transmiterea informaţiilor şi asimilarea lor sunt ajutate de referirile legate de elementele din viaţa de zi cu zi şi cunoscute de către cei mici; *descrierea* – se efectuează printr-un conţinut al limbajului potrivit grupului de instruit; *conversaţia* – evidenţiază necesitatea existenţei dialogului permanent între militari şi instructorii sportivi; *studiul individual* – se realizează prin trasarea de sarcini didactice militarilor de către instructori şi îndrumarea lor spre studierea bibliografiei de specialitate; *brainstormingul* – nu este des folosită, însă ea stimulează implicarea militarilor în mod activ în desfăşurarea instruirii. Potrivit acestei metode, se exprimă puncte de vedere argumentate, care sunt şi acceptate, dar nu sunt definitivate ca soluţii pentru sarcinile didactice. Peste un timp relativ scurt, de câteva zile, se aduce în discuţie sarcina didactică nesoluţionată, se emit din nou păreri argumentate, şi sub îndrumarea specialistului, se admit soluţiile cele mai eficiente.

Prima metodă intuitivă este *demonstraţia* – alături de explicaţie şi exersare este cea mai folosită în educaţia fizică militară. Pentru a fi eficientă, ea trebuie realizată la nivel de model fie de către specialist (se mai numeşte şi demonstraţie nemijlocită), fie de către un alt militar din grupul de instruit, a cărui pregătire tehnică îi permite acest lucru (poartă numele şi de demonstraţie mijlocită). A doua metodă intuitivă este *observarea execuţiei altor militari* – este o alegere a instructorului, prin care se materializează şi sunt evidenţiate aspectele negative sau pozitive ale execuţiilor colegilor. Ultima metodă intuitivă este cea prin care se folosesc „materiale iconografice”[11] (schiţe, desene, kinograme[12], materiale video, grafice etc.). Se utilizează atunci când nu există posibilitatea realizării demonstraţiei la nivel de model sau ca o completare a acesteia.

A treia grupă de metode de instruire, cele practice, este formată, de fapt, dintr-una singură, general acceptată: *metoda exersării*. Metoda exersării implică executarea conţinutului de învăţat în mod conştient, sistematizat. Ea urmează în logica învăţării, în educaţia fizică militară, metodelor verbale şi a celor intuitive. Se adresează în totalitate militarilor care trebuie să se instruiască, sub conducerea şi sub supravegherea instructorului.

Gheorghe Cârstea numeşte şase tipuri de exersări[13]: „exersarea pentru formarea deprinderilor şi priceperilor motrice; exersarea pentru dezvoltarea, educarea calităţilor motrice; exersarea pentru optimizarea dezvoltării fizice corporale (se realizează, în special, în cadrul verigii a treia a lecţiei de educaţie fizică militară – influenţarea selectivă a aparatului locomotor, prin exerciţii specifice gimnasticii de bază); *exersarea pentru formarea capacităţii de organizare* (se realizează în fiecare lecţie, datorită folosirii mijloacelor specifice gimnasticii de bază, a exerciţiilor de front şi formaţii, dezvoltându-se capacitatea de autoorganizare şi autoconducere a militarilor); *exersarea pentru formarea capacităţii de practicare autonomă a exerciţiilor fizice* (înţelegerea structurii lecţiei de educaţie fizică militară, precum şi a mijloacelor folosite îi poate determina pe militari să lucreze liber anumite secvenţe din lecţie, sub supravegherea instructorului); *exersarea pentru formarea capacităţii de practicare independentă a exerciţiilor fizice* (în lecţiile de educaţie fizică militară se pun bazele teoretice şi practice necesare practicării exerciţiilor fizice în timpul liber)”.

În formarea deprinderilor şi a priceperilor motrice, metoda exersării poate îmbrăca următoarele forme[14]: „*exersarea grupată* – repetările urmăresc doar o deprindere motrică, înainte de a trece la următoarea; *exersarea separată* – militarul nu realizează sarcini identice în încercări succesive; *exersarea variabilă* – se însuşeşte actul sau acţiunea motrică, indiferent de parametrii săi (direcţie, viteză, tempo etc.).

Se poate exemplifica prin faptul că militarilor le va fi foarte uşor să facă transferul de informaţii motrice spre a realiza o aruncare cu grenada

la precizie, la o distanţă de 25 m, dacă ei s-au pregătit în prealabil la distanţe de 15 m, 20 m, 30 m; *exersarea constantă* – doar un parametru se modifică în timpul execuţiilor (de exemplu, direcţia de deplasare sau viteza de reacţie); *exersarea mentală* – vizează realizarea şi repetiţia mentală a succesiunii exerciţiilor de executat, imaginarea actului sau acţiunii motrice poate constitui un avantaj în învăţarea sarcinilor motrice; *exersarea analitică* – urmăreşte descompunerea procedeelor tehnice dificile în unităţi de învăţat mai mici şi lucrul pentru însuşirea acestora (nu trebuie insistat pentru folosirea acestei forme, pentru că se pot crea stereotipuri dinamice greşite şi se pot explica prin lipsa cursivităţii în execuţia integrală a procedeelor tehnice, a vitezei de execuţie a acestora etc.); *exersarea globală* – vizează executarea integrală a deprinderii motrice şi se poate utiliza şi de sine stătătoare, în cazul deprinderilor foarte simple, în care învăţarea se poate produce prin imitarea acţiunilor instructorului”.

Exersarea, analitică sau globală, în formarea deprinderilor motrice poate avea ca efecte „precizia mişcărilor, siguranţă, rapiditate în execuţie, consum redus de energie, cu condiţia să existe un control judicios al programului de instruire”[15].

M. Epuran prezintă avantajele și efectele exersării: „scurtarea treptată a timpului de îndeplinire a sarcinilor; specializarea treptată (dobândirea de deprinderi și priceperi motrice noi, în timp); înlăturarea treptată a mișcărilor inutile și încordării musculare (prin formarea automatismelor dispar mișcările grosiere și se obține chiar o relaxare musculară în execuția procedeelor tehnice, acestea devenind foarte precise); fixarea de noi combinații de mișcări; diminuarea sensibilității față de diferitele piedici externe; tendința de a transfera atenția de la proces asupra rezultatului (în timpul executării mișcărilor, militarii nu mai sunt concentrați asupra modului de execuție a tehnicii, ci asupra rezultatului acesteia); reducerea oboselii (prin exersare se întârzie apariția oboselii, ca urmare a programării și dirijării efortului în cadrul procesului instructiv-educativ); selectarea și interpretarea mai bună a indicatorilor externi și interni (aprecierea parametrilor spațio-temporali este un bun exemplu); reducerea treptată a erorilor de execuție (ca urmare a repetării într-un număr suficient de mare a unei acțiuni motrice, se poate înlătura orice greșeală în realizarea procedeului sau a tehnicii în sine); unificarea acțiunilor parțiale (în cazul procedeelor tehnice în etapa învățării sau formării deprinderilor motrice dificile, ca urmare a exersării analitice și însumării gesturilor motrice, treptat, se poate ajunge la manifestarea acțiunii motrice ca un tot unitar)”[16]. Toate aceste efecte ale exersării se regăsesc, într-un final, în calitatea militarilor instruiți.

**Concluzii**

Plecând de la nevoia de a înțelege teoria specialității militare educație fizică militară, de a aplica aceste cunoștințe în practică, prezentul material pledează în favoarea însușirii și aplicării cunoștințelor fundamentale ale acestui subsistem al educației generale, pledează pentru formarea abilităților de a conduce activitățile de instruire specifice acestui domeniu, bazate, simultan, pe teorie și practică, întărește ideea necesității ca activitățile de instruire să fie conduse de specialiști, în condițiile unei atitudini corecte față de bazele teoretice.

De asemenea, acest material militează pentru conștientizarea importanței cunoștințelor teoretice de specialitate, a respectului față de specialiști și a calității acestora, cu atât mai mult cu cât acest domeniu poate fi considerat un fundament pentru dezvoltarea celorlalte specialități militare.

**NOTE:**

1 Gh. Cârstea, *Teoria şi metodica educaţiei fizice şi Sportului*, Editura AN-DA, Bucureşti, 2000, p. 77.

2 *Ibidem*, p. 78.

3 *Ibidem*, p. 79.

4 *Ibidem*, p. 80.

5 *Ibidem*.

6 *Ibidem*, p. 81.

7 *Ibidem*.

8 *Ibidem*, p. 82.

9 *Ibidem*, p. 83.

10 I. Cerghit, *Metode de învăţământ*, Ediţia a III-a, Editura Didactică şi Pedagogică RA, Bucureşti, 1998, p. 98.

11 *Ibidem*, p. 88.

12 Reprezentare grafică succesivă şi logică a mişcărilor de bază care compun un procedeu sau un element tehnic.

13 Gh. Cârstea, *Teoria şi metodica educaţiei fizice şi Sportului*, Editura AN-DA, Bucureşti, 2000, p. 89.

14 Dragnea, A., şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Editura FEST, Bucureşti, 2006, p.152.

15 Ciapa G.C.,”Self-defense–physical and psychological support in military modern conflicts, Strategic changes in secuity and international relations”, revista *Strategii XXI*, vol. 3, Bucureşti, 2015, p. 299.

16 M. Epuran, V. Horghidan, *Psihologia educaţiei fizice*, ANEFS, Bucureşti, 1994, p. 180.

## BIBLIOGRAFIE

Cârstea Gh., *Teoria şi metodica educaţiei fizice şi Sportului*, Editura AN-DA, Bucureşti, 2000.

Cerghit I., *Metode de învăţământ*, Ediţia a III-a, Editura Didactică şi Pedagogică RA, Bucureşti, 1998.

Ciapa G.C., *Pregătirea fizică a militarilor din armata României în conflictele moderne,* Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2018.

Ciapa G.C., „Self-defense – physical and psychological support in military modern conflicts, Strategic changes in secuity and international relations”, revista *Strategii XXI*, vol. 3, Bucureşti, 2015.

Dragnea A. şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Editura FEST, Bucureşti, 2006.

Epuran M., Horghidan V., *Psihologia educaţiei fizice*, ANEFS, Bucureşti, 1994.

# SECURITATEA CIBERNETICĂ A INFRASTRUCTURILOR CRITICE ÎNTR-O LUME DIN CE ÎN CE MAI CONECTATĂ

## *THE CYBER SECURITY OF CRITICAL INFRASTRUCTURES IN A WORLD THAT'S INCREASINGLY CONNECTED*

## *CYBERSÉCURITÉ DES INFRASTRUCTURES CRITIQUES DANS UN MONDE DE PLUS EN PLUS CONNECTÉ*

**Lt.col.dr.ing. Vasile Florin POPESCU***

Într-o lume din ce în ce mai conectată, infrastructurile critice au devenit mai vulnerabile ca niciodată la amenințările de securitate cibernetică, fie că provin din state naționale, organizații criminale sau persoane fizice. Această nouă vulnerabilitate este cauzată de schimbările fundamentale ale sistemelor tehnologice ale organizațiilor guvernamentale și private. În acest sens, infrastructura critică virtuală a oricărei organizații/națiuni reprezintă o arenă în care securitatea este imperativă. Protecția cibernetică a devenit crucială în fiecare sector de activitate, iar absența unor măsuri pentru protecția infrastructurilor critice amenință să producă daune imense în funcționarea societății.

*In an increasingly connected world, critical infrastructures have become more vulnerable than ever to cyber security threats, whether they come from national states, criminal organizations or individuals. This new vulnerability stems from fundamental changes in the technological systems of organizations (government and private). In this regard, the Virtual Critical Infrastructure of any organization / nation represents an arena where security is absolutely imperative. Cyber protection has become crucial in every sector of activity, and the absence of measures to protect critical infrastructures threatens to cause huge damage to the functioning of the company.*

*Dans un monde de plus en plus connecté, les infrastructures critiques sont devenues plus vulnérables que jamais aux menaces de cybersécurité, qu'elles proviennent d'États nationaux, d'organisations criminelles ou d'individus. Cette nouvelle vulnérabilité est le résultat des changements fondamentaux des systèmes technologiques des organisations (gouvernementales et privées). À cet égard, l'Infrastructure critique virtuelle de toute organisation/nation représente une arène où la sécurité est absolument essentielle. La cybersécurité est devenue indispensable dans tous les secteurs d'activité et l'absence des mesures de protection des infrastructures critiques peut beaucoup nuire au fonctionnement de la société.*

**Cuvinte-cheie:** infrastructuri critice; spațiu cibernetic; amenințări cibernetice; vulnerabilități; sisteme de tehnologie informațională și operațională.

***Keywords:*** *critical infrastructures; cyber space; cyber threats; vulnerabilities, information and operational technology systems.*

***Mots-clés:*** *infrastructures critiques; cyberespace; cybermenaces; vulnérabilités; technologies de l'information et systèmes opérationnels.*

Avioane deturnate de la cursul normal. Garnituri de metrou blocate în tunelele de sub orașe. Baraje sparte care inundă orașe. Pene de electricitate. Telecomunicații blocate. Apeluri de urgență 112 inutilizabile. Aceste momente de haos și panică și alte consecințe potențiale ale atacurilor la adresa infrastructurii critice pot, în cel mai bun caz, să provoace doar astfel de inconveniente, iar în cel mai rău caz, pot duce la pierderi de vieți omenești sau la distrugeri la scară largă.

* ***Ministerul Apărării Naționale***
e-mail: *popescuveve@gmail.com*

Astăzi, aproximativ jumătate din populația lumii trăiește în zone urbane și se presupune că procesul de urbanizare se va accentua, astfel încât doar o treime dintre locuitorii planetei va locui în afara

zonelor urbane până în 2050[1]. Această dezvoltare ridică o serie de provocări care influențează și infrastructurile, a căror funcționare fiabilă și eficientă va determina modul în care orașele sunt capabile să răspundă cerințelor calității vieții[2]. Unele dintre aceste infrastructuri sunt numite „critice”, întrucât bunăstarea societății se bazează fundamental pe fiabilitatea lor. Ele pot fi înțelese ca elemente fundamentale ale sustenabilității societății, siguranței și securității aprovizionării. Infrastructurile critice oferă oamenilor acces la o gamă largă de mărfuri, a căror disponibilitate[3] este esențială pentru rezistența comunităților[4].

Conform Oxford English Dictionary, structura morfematică a termenului *infrastructură* este o combinaţie a prefixului „infra”, cu înţelesul de „sub”, și a rădăcinii cuvântului, purtătoare a semnificației lexicale, anume, „structura”, arată cum este construit un mecanism. Asocierea termenului „critic” celui de „infrastructură” definește acel tip de infrastructură, care, perturbată, poate conduce la pagube majore.

Caracterul critic al infrastructurilor este dat de următoarele:

- unicitatea lor;
- caracterul vital în funcţionarea sistemelor economice, sociale, politice, militare, informaţionale etc.;
- sensibilitatea la schimbări;
- vulnerabilitatea ridicată la ameninţările din mediul extern.

În funcţie de importanţa lor în funcţionalitatea sistemelor și proceselor, infrastructurile se împart în trei categorii[5]:

- infrastructuri obişnuite;
- infrastructuri speciale;
- infrastructuri critice.

Infrastructurile critice sunt împărţite în două categorii importante[6]:

- *fizice*:
  - internaţionale;
  - ale economiei statelor;
  - ale diferitelor sectoare industriale;
  - ale întreprinderilor/companiilor;
  - ale proiectelor;
  - ale transportului aerian, feroviar, naval;
  - ale sistemului financiar;
  - ale locuinţei, localităţii, ţării, continentului;
  - militare;
  - ale sistemului de ordine publică;
  - ale sistemului informaţional şi de siguranţă a statului;
  - ale sistemului sanitar şi de protecţie a cetăţeanului, familiei şi comunităţii
- *virtuale*:
  - ale sistemelor de comunicaţii;
  - ale reţelelor şi bazelor de date;
  - ale spaţiului cibernetic.

Într-o lume din ce în ce mai conectată, infrastructurile critice au devenit mai vulnerabile ca niciodată la amenințările de securitate cibernetică, fie că provin din state naționale, organizații criminale sau persoane fizice. Această nouă vulnerabilitate este cauzată de schimbările fundamentale ale sistemelor tehnologice ale organizațiilor guvernamentale și private. Astfel de organizații – armată, poliție, pompieri, furnizori de servicii medicale și utilități, sisteme bancare, sisteme de transport etc. – acționează cu două tipuri de sisteme tehnologice: sisteme de tehnologie informațională și sisteme de tehnologie operațională.

Sistemele de tehnologie informațională asigură funcțiile de bază ale biroului, cum ar fi comunicarea prin e-mail, salarizare, resurse umane etc., în timp ce sistemele de tehnologie operațională controlează echipamentele fizice și personalul necesar îndeplinirii misiunii lor.

În trecut, sistemele de tehnologie operațională constau din sisteme de sine stătătoare, care le făceau sigure. Acum, sistemele de tehnologie operațională rulează pe aceleași platforme software și hardware cunoscute, ca și sistemele IT. Aceste sisteme sunt bine cunoscute de hackeri și, prin urmare, sunt semnificativ mai puțin sigure.

Ce a dus la această convergență a sistemelor de tehnologie informațională cu sistemele de tehnologie operațională? Iată câteva exemple:

Un proprietar de casă reglează de la distanță termostatul la reședința sa, pentru a scădea temperatura, în timp ce este în vacanță. Un medic vizualizează consumul de insulină al pacienților pe un computer din birou. Companiile monitorizează de la distanță starea și locația trenurilor, autobuzelor și camioanelor, fluxul de petrol și gaze prin conducte, sau consumul de apă ori de energie electrică, pentru a gestiona aceste servicii în mod eficient.

În timp ce tehnologiile din aceste exemple ne îmbunătățesc viața, ele ne pot face în același timp vulnerabili.

Menționez asta, deoarece, pe măsură ce numărul dispozitivelor interconectate continuă să crească, numărul potențialelor puncte de acces pentru hackeri care perturbă infrastructura critică crește și el.

În acest sens, Infrastructura critică virtuală a oricărei organizații/națiuni reprezintă o arenă în care securitatea este imperativă. Protecția cibernetică a devenit crucială în fiecare sector de activitate, iar absența unor măsuri pentru protecția infrastructurilor critice amenință să producă daune imense în funcționarea societății în ansamblu.

Spațiul virtual sau cibernetic reprezintă un set de mijloace și proceduri, bazate pe tehnologia informației și comunicațiilor (TIC) și este format din hardware, software, Internet, servicii de informare și sisteme de control, devenind o infrastructură critică esențială pentru activitatea socioeconomică a oricărei națiuni, organizaţii sau proiect transnațional. Diferite dicționare și enciclopedii definesc spațiul cibernetic astfel:

• Spațiul cibernetic este o rețea de calculatoare formată dintr-o rețea mondială de rețele de calculatoare care folosește protocoale de rețea TCP/IP, pentru a facilita schimbul de date (sursa: Dicționarul Român Online);

• Spațiul cibernetic este mediul electronic de rețele de calculatoare, în care are loc comunicarea online[7].

• O metaforă pentru a descrie terenul nonfizic creat de sistemele informatice: Sistemele online creează un spațiu cibernetic în care oamenii pot comunica unul cu altul, fac cercetări sau, pur și simplu, cumpără[8].

• Spațiul cibernetic este un domeniu caracterizat de utilizarea dispozitivelor electronice și spectrului electromagnetic pentru a stoca, a modifica și a schimba date prin intermediul sistemelor de rețea și infrastructurilor fizice asociate. De fapt, spațiul cibernetic poate fi considerat ca interconectarea dintre ființele umane prin intermediul calculatoarelor și telecomunicațiilor, indiferent de poziţia geografică[9].

Guvernul SUA definește spațiul cibernetic ușor mai larg: Directivele prezidențiale de securitate națională nr. 23 şi 54 definesc spațiul cibernetic ca fiind rețeaua interdependentă a infrastructurilor de tehnologia informației, care include Internetul, rețelele de telecomunicații, sistemele informatice, utilizatorii, precum și cei care controlează industriile critice. Utilizarea comună a termenului se referă, de asemenea, la mediul virtual de informații și la interacțiunile dintre oameni.

Definițiile oferite de Webster, Wikipedia sau Dicționarul Oxford nu sunt absolute și suficient de cuprinzătoare. Conceptul de spațiu virtual s-a extins între timp, incluzând comerțul, finanțele, energia, Bursele de Valori etc.

Obiectivele atacurilor din mediul virtual pot fi clasificate în trei grupe majore:

• sectorul public, agenţiile guvernamentale;

• sectorul privat, în principal, operatorii de infrastructuri critice;

• cetățenii.

Atacurile cibernetice la adresa infrastrucurii critice virtuale pot fi clasificate, în funcție de sursă și de impactul acestora, astfel:

• *Atacurile sponsorizate de state*

Lumea reală şi conflictele fizice s-au extins în lumea virtuală a spațiului cibernetic. În ultimii ani, au fost detectate atacurile cibernetice împotriva infrastructurilor critice ale diferitelor țări și obiectivelor specifice. Câteva exemple cunoscute publicului larg sunt: atacul cibernetic din Estonia, în 2007, care a dus la dezactivarea temporară în mare parte a infrastructurilor critice ale țărilor baltice, atacul cibernetic lansat de Rusia împotriva Georgiei, în 2008, ca un preludiu la invazia terestră, cazul Stuxnet, cu atacuri cibernetice împotriva sistemelor SCADA, cazul Duqu, cu atacuri cibernetice împotriva organizațiilor industriale, atacurile cibernetice suferite de rețelele clasificate ale Guvernului Statelor Unite, comise de către hackeri de pe teritoriul chinez etc.

În ultimii ani, unele state au investit importante resurse economice, tehnice și umane în dezvoltarea amenințărilor avansate persistente (AAP), care atacă agresiv și aleg obiective foarte specifice, în scopul de a menține o prezență constantă în cadrul rețelelor posibilelor victime. Atacurile AAP sunt foarte dificil de detectat, din cauza faptului că utilizează tehnici și componente care sunt special proiectate pentru a se infiltra și rămâne în rețea fără a fi detectate.

• *Atacurile sponsorizate de către organizații private*

Obiectivul multor organizații private este de a obține secrete industriale și economice de la alte organizații competitoare, acest tip de atac fiind de multe ori executat cu sprijin guvernamental.

• *Terorismul, extremismul politic și/sau ideologic*

Terorismul și grupurile extremiste folosesc spațiul cibernetic pentru a planifica și a publica acțiunile lor și pentru a racola adepți care să le efectueze. Aceste grupuri recunosc importanța strategică și tactică a spațiului cibernetic pentru interesele lor, rețelele social media și forumurile devenind principalul instrument utilizat.

• *Atacurile grupurilor de crimă organizată*

Bandele de crimă organizată, cunoscute şi sub numele de bande informatice, au început să își desfășoare activitatea în spațiul cibernetic, exploatând posibilitatea anonimatului pe care acest domeniu o oferă. Obiectivul acestor tipuri de bande este de a obține informații sensibile pentru utilizarea, ulterioară, a acestora frauduloasă și pentru câștiguri economice semnificative.

• *Hackerii*

Odată cu apariţia Internetului, dar mai ales în ultimii ani, activităţile hackerilor au devenit una dintre cele mai mari ameninţări la adresa guvernelor și organizațiilor de orice natură. Principiile acestei agresiuni sunt anonimatul și distribuirea gratuită de informații în spațiul cibernetic, în esență, prin intermediul Internetului. Misiunea lor este de a „ataca” spațiul cibernetic, reprezentat de persoane sau de organizațiile care încalcă oricare dintre principiile sau intereselor lor. Acest lucru implică faptul că spațiul cibernetic al guvernelor din majoritatea țărilor din întreaga lume, al băncilor, al companiilor de telecomunicații, al furnizorilor de infrastructură critică, al furnizorilor de servicii de Internet, în ansamblu, tot spațiul cibernetic, sunt susceptibile de a fi hackuite cu obiectivul principal de a fura informații sensibile.

• *Atacurile personalului cu acces privilegiat (cei din interior)*

Aceste grupuri reprezintă una dintre cele mai mari ameninţări la adresa securității spațiului cibernetic al națiunilor, deoarece ele sunt, de cele mai multe ori, parte integrantă a tuturor atacurilor menționate anterior, putând fi emise de un spion sau de un angajat care lucrează pentru bande de teroriști sau infractori cibernetici, de angajați nemulțumiți etc.

**Concluzii**

Necesitatea de a stimula apărarea cibernetică pentru infrastructurile critice este clară. Dar întrebarea devine acum: Cum ajungem acolo? În acest sens, am dezvoltat câteva recomandări pentru a contribui la acțiuni colective eficiente.

• Elaborarea unei strategii naționale de educație cibernetică: pentru a proteja cu adevărat infrastructura critică, trebuie să avem persoane calificate. Prin urmare, este necesar ca educația cibernetică să devină o prioritate în procesul educațional. România nu are o strategie de educație în domeniul cibersecurității care să alimenteze și să finanțeze centre naționale de excelență în domeniu.

• O altă recomandare este mentoratul transorganizațional și transferul de cunoștințe. Organizațiile cu mai puțină experiență de securitate cibernetică sau echipele mai mici de cibersecuritate pot învăța de la colegii lor mai experimentați. Organizațiile mai mari ar trebui, de asemenea, să-și încurajeze experții să participe la asociații din industrie, în cadrul unor parteneriate public-private și organizații regionale, care să ofere toate oportunitățile de formalizare a îndrumării interorganizaționale și ale transferului de cunoștințe.

• Crearea unor strategii mai bune de partajare a informațiilor între sectorul guvernamental/de stat și sectorul privat: experții în securitate cibernetică par, în mare măsură, să fie de acord cu faptul că, pentru un nivel optim de securitate în toate sectoarele, cooperarea este esențială.

• Efectuarea de exerciții de scenarii pentru potențiale crize: când vine vorba despre infrastructură critică, un dezastru real nu este cadrul propice care să ne determine să învățăm din greșeli. O astfel de pregătire trebuie să aibă loc în avans, în exerciții de scenarii la crize care să simuleze modul în care o echipă de răspuns ar face față unui incident neașteptat.

**NOTE:**

1 M. Rizea et al., UN (United Nations), *World Urbanization Prospects: The 2018 Revision, Key Facts*, 2018, https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf, accesat la 10 noiembrie 2018.

2 S. Riffat, R. Powell, D. Aydin, *Future cities and environmental sustainability. Future Cities Environ*, 2016.

3 A.H. Hay, S. Willibald, *Making Resilience Accessible. Access: An Enabler of Community Resilience*, Southern Harbour, 2017, https://www.southernharbour.net/assets/docs/SH_Access%20WhitePaper_2017_0307%C6%92.pdf, accesat la 14 ianuarie 2019.

4 A. Hay, *Surviving catastrophic events: Stimulating community resilience. In Infrastructure Risk and Resilience*, Transportation, IET, Stevenage, UK, 2013, pp. 41-46.

5 G. Alexandrescu, Gh. Văduva, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2006.

6 G. Alexandrescu, Gh. Văduva, *op.cit.*

7 http://en.wikipedia.org/wiki/Cyberspace

8 http://www.webopedia.com/TERM/C/cyberspace.html

9 http://searchsoa.techtarget.com/definition/cyberspace

## BIBLIOGRAFIE

Alexandrescu G., Văduva Gh., *Infrastructuri critice. Pericole, ameninţări la adresa acestora. sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2006.

Hay A., *Surviving catastrophic events: Stimulating community resilience. In Infrastructure Risk and Resilience*, Transportation, IET, Stevenage, UK, 2013.

Hay A.H., Willibald S., *Making Resilience Accessible. Access: An Enabler of Community Resilience*, Southern Harbour. 2017, https://www.southernharbour.net/assets/docs/SH_Access%20WhitePaper_2017_0307%C6%92.pdf

Riffat S., Powell R., Aydin D., *Future cities and environmental sustainability. Future Cities Environ*, 2016.

Rizea M. et al., *UN (United Nations). World Urbanization Prospects: The 2018 Revision*, Key Facts. 2018, https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf

http://en.wikipedia.org/wiki/Cyberspace

http://searchsoa.techtarget.com/definition/cyberspace

http://www.webopedia.com/TERM/C/cyberspace.html

# FORME DE MANIFESTARE A TERORISMULUI CIBERNETIC

## *WAYS OF CYBERTERRORISM*

## *FORMES D'ACTION DU CYBERTERRORISME*

**Cdor.prof.univ.dr. Sorin TOPOR***

Atacurile cibernetice, în prezent, devin tot mai complexe, mai frecvente şi cu efecte distructive tot mai mari. Indiferent de tipul sau dimensiunea unei organizaţii, aceasta afectează informaţiile infrastructurilor publice şi private.

Terorismul contemporan, care urmărește comiterea de acţiuni cu obiective clare, desfășurate o singură dată sau în serie, având, ca motivaţii, rezistenţa la schimbarea de ordin politic, economic sau social, efecte asupra informaţiilor globale, utilizează și metode de atac cibernetic prin implementarea noilor tehnologii informaționale.

În acest articol mi-am propus ca, pornind de la analizarea principalilor factori de insecuritate publică și de dezordine socială, pe care îi consider ca determinanți în dezvoltarea unor forme moderne de terorism, să formulez conținutul conceptului de terorism cibernetic, în raport cu care să evidențiez acele aspecte relevante pentru înțelegerea modalităților sale de aplicare.

*Cyber attacks are now becoming more and more complex, more frequent and with increasing destructive effects. Regardless of the type or value of an organization, it affects information of public and private infrastructures.*

*In this context, the terrorism aims to execute actions, driven only once or in series, motivating as resistance to political, economic or social changes and producing global information effects. It is well known the development of terrorism is favored by the development of information technology. Last but not least, the social factor and the arms proliferation determine the adapt of objective aspect of terrorism, often the modeling of terrorist ideology based on issues of population discontent with the ease of acquisition of weapons, munitions and destructive materials through various forms of trade.*

*In this work we propose to determine the content of the concept of cyber terrorism, starting from the analysis of the main factors of public insecurity and social disorder that facilitate the development of modern forms of terrorism. In this order we propose to underline the base aspects to understand the ways of its application.*

*Les cyberattaques sont, à l'heure actuelle, de plus en plus complexes, de plus en plus fréquentes et de plus en plus destructrices. Quelle que soit la nature ou la dimension d'une organisation, elles portent préjudice aux informations des infrastructures publiques et privées.*

*Le terrorisme contemporain, qui cherche à engager des actions ponctuelles ou successives, avec des objectifs bien définis, ayant pour motivation la résistance aux changements politiques, économiques ou sociaux, ayant des effets sur les informations globales, utilise également des méthodes de cyberattaque par la mise en œuvre de nouvelles technologies de l'information.*

*À partir de l'analyse des principaux facteurs d'insécurité publique et de désordre social, considérés, à mon avis, comme déterminants pour le développement des formes modernes du terrorisme, j'ai l'intention, dans cet article, d'établir le contenu du concept de cyberterrorisme, par rapport auquel je devrais souligner les aspects pertinents pour comprendre ses modalités de mise en pratique.*

**Cuvinte-cheie:** terorism; terorism cibernetic; spionaj cibernetic; fraude cibernetice; e-propaganda; e-instruire; radicalizare.

***Keywords:*** *terrorism; cyber terrorism; cyber spying; cyber frauds; e-propaganda; e-training; radicalization.*

***Mots-clés:*** *terrorisme; cyberterrorisme; cyber-espionnage; cyber fraude; e-propagande; e-learning; radicalisation.*

**** Universitatea Națională de Apărare „Carol I”***
e-mail: *sorin.topor@yahoo.com*

În prezent, în cadrul societății informațiile circulă extrem de rapid prin capabilitățile moderne oferite de tehnologia informațională. Astfel, mass-media își consolidează funcția de instrument de bază pentru analiza, transmiterea, formarea curentelor de opinii, pentru stabilirea sau pentru corectarea unor agende de lucru ale factorilor decizionali etc., toate acestea având, ca principal obiectiv, „comerțul cu informații”. De aceea informațiile vândute trebuie să fie frumos prezentate, în imagini sugestive, dacă este vorba despre o situație materială și/sau cu însușiri carismatice, dacă acestea provin din situații specifice vieții socioumane. Pentru aceasta, au apărut adevărate „științe”, așa cum sunt neuromarketingul, consilierea de imagine, consultanța vestimentară etc.

Putem aprecia că toate aceste caracteristici ale cotidianului au, ca scop principal, captarea atenției unui public, devenind „ținta” lui de interes, fie acesta instruit ori nu, educat sau nu. Se observă că, pentru atingerea acestui obiectiv, în prezent nu mai pot fi utilizate doar metodele tradiționale de comunicare. Pentru ca o agenție mediatică să aibă succes, va trebui ca publicul vizat să fie „sedus” cu informații. Iar pentru a ajunge la sufletul oamenilor, sunt necesare tehnici și tehnologii moderne care să permită optimizarea abilităților de comunicare la nivel global. Mă refer la accesul facil la serviciile Internet, la servicii de știri, furnizate prin diverse canale TV, radio și presă scrisă, la alte servicii de comunicare, la comunicații de tip satelitar, la telefonia celulară etc.

Organizațiile teroriste, promovând violența extremă, au și acestea publicul lor. Persoanelor care formează acest segment de public le sunt stimulate percepțiile pentru a considera că dețin un nivel ridicat de „psiho-putere” asupra altor indivizi. Numai așa se explică de ce acest tip de public ascultă şi susţine mesajul transmis de liderii organizațiilor teroriste.

Cele mai elocvente exemple provin din spaţiile actuale de conflict, şi anume: din Afganistan, din Orientul Mijlociu, din Africa etc., zone unde se încurajează reacția armată prin stimularea percepţiei populației că războiul, declanșat de SUA, se desfășoară împotriva islamului; din zona Palestina – Israel, unde se promovează ideea de aplicare discreţionară a politicilor de acordare a drepturilor cetăţeneşti ori a modului de eliberare a vizelor, pe fondul situaţiei extrem de complexe a migraţei dinspre zonele controlate de ISIS/Daesh; din alte zone din arealul global, caracterizate printr-o puternică „rezistenţă socială”, manifestată de grupări anarhiste şi de justiţiari care militează, prin violență, pentru o așa-zisă „apărare a drepturilor omului”, violența fiind considerată singura formă de reacție față de abuzurile serviciilor de informaţii şi instituțiilor guvernamentale (de exemplu, lupta vestelor galbene în Franța, în anul 2018).

Apreciez că obiectivul nemijlocit al terorismului este de obţinere sau de menţinere a unei stări de insecuritate publică şi de dezordine socială în spații tot mai întinse. Iar dacă în societatea informațională, atribut tot mai des folosit pentru a caracteriza actualul stadiu de evoluție socială, informația a devansat celelalte dimensiuni sociale și organizațiile teroriste suferă transformări, fiind nevoite să își adapteze metodele de comunicare la cerințele consumatorilor de informații. Bazându-mă pe aceste particularități, „terorismul cibernetic” devine metoda cea mai atractivă pentru organizațiile teroriste contemporane, foarte bine adaptată mediului informațional contemporan. Astfel, Internetul devine un suport de furnizare de informații controlate de organizații teroriste, efectele asimilării lor de către publicul vizat fiind de amplificare a pericolului terorist, perceput de populație. Mai mult decât atât, rețeaua Internet a devenit un instrument de control și de manipulare, persoana manipulată emoțional fiind încurajată să ucidă, să provoace rănirea altor persoane, să se autodistrugă sau să provoace distrugeri materiale.

Apreciez că această metodă este mult mai complexă decât hacktivismul și infracționalitatea cibernetică, fiind exploatată de organizațiile teroriste pentru propagandă, pentru obținerea de sprijin financiar, de informaţii și pentru comunicare între membrii organizaţiilor lor[1].

Gabriel Weimann[2] a identificat cel puţin şase moduri diferite de utilizare a spaţiului cibernetic în scopuri teroriste:

1. *ca instrument al războiului psihologic* – se cunosc imaginile difuzate în scopul provocării terorii în rândul populaţiei ţintă (imagini cu ostatici executaţi prin decapitare şi care aparţineau unei naţionalităţi sau erau angajaţii unei corporaţii);

2. *ca instrument de propagandă* – organizaţiile teroriste pot face publicitate acţiunilor lor prin emisiuni în direct, oriunde în lume. Difuzarea de informaţii le facilitează popularizarea realizărilor şi diminuarea greşelilor lor;

3. *ca instrument financiar* – se cunoaște că Al-Qaeda a primit ajutor financiar, graţie averii lui Bin Laden şi contribuţiei mai multor organizaţii neguvernamentale, prin diverse metode de sponsorizare. În prezent, experţi, precum Jimmy Gurule, atrag atenţia asupra Bitcoin, ca reprezentând un mijloc potrivit pentru acordarea sprijinului financiar unei organizaţii teroriste[3]. Activităţile specifice crimei organizate, desfăşurate de Daesh, și ne referim, aici, la contrabanda cu benzină, pot fi încadrate acestui tip de sponsorizare, dacă plăţile se efectuează cu moneda cibernetică;

4. *ca instrument de recrutare* – folosind Internetul, Daesh şi-a înmulţit numărul de luptători străini, în comparaţie cu Al-Qaeda. Distribuirea masivă, în rândul populaţiei, a imaginilor şi videoclipurilor care arată viaţa „corectă” a mujahedinilor, precum şi succesul acţiunilor Daesh împotriva duşmanilor nonmusulmani (inclusiv execuţiile umane) au ajutat la deschiderea de birouri de informare şi de recrutare în întreaga lume. Succesul acestor metode, aşa cum era de aşteptat, a trezit un real interes printre tinerii musulmani;

5. *ca instrument de ascundere/disimulare a sistemului organizaţional şi conducerii sale* – practic, modelul de organizare și ierarhia structurilor unei grupări teroriste au putut fi ascunse prin stabilirea unor reţele multiple de posturi de comunicare. Astfel, importanţa elementelor de conducere, tradiționale unei ierarhii verticale, a fost estompată de conducerea în rețea, pe orizontală. Membrii sau grupările teroriste s-au putut sprijini reciproc, şi-au putut coordona şi planifica atacurile etc. într-un mod mai ieftin şi mai sigur. În Al-Qaeda, pentru ca liderii să nu poată fi detectaţi, s-a făcut apel către toţi „fraţii în jihad” să folosească serviciul PalTalk;

6. *ca depozit de documente* – oricine poate găsi în paginile web numeroase manuale şi ghiduri referitoare la fabricarea explozivelor, la lupta în mediul urban, la tactici de gherilă şi de supravieţuire etc.

Aspectele pe care le consider ca fiind definitorii pentru activitatea terorismului cibernetic, pe care le-am identificat prin analiza celor mai frecvente evenimente teroriste contemporane, le-am grupat în patru forme de manifestare, descrise în continuare. Având în vedere că majoritatea provin din surse deschise, unde informațiile nu prezintă întotdeauna un grad mare de credibilitate, precizez că această clasificare se bazează pe informații identificate în unele surse bibliografice și pe interpretarea personală a unor posibilități ipotetice de atac ale teroriștilor cibernetici.

**Spionaj cibernetic**

Apreciez că spionajul cibernetic este una dintre cele mai importante şi alarmante probleme internaţionale ale societăţii contemporane, prin aspectele pe care le voi prezenta succint în continuare.

Realitatea actuală ne confirmă că un sistem informaţional nu trebuie să mai fie protejat doar de cei identificaţi sau autointitulaţi „băieţi răi”, ci de oricine, care, în mod voit sau întâmplător, intră în „zona de confort” a ţintei. De aceea una dintre cele mai mari probleme care dă multe bătăi de cap guvernanţilor este definirea spionajului cibernetic. Multe organizații și-au creat propriile definiţii, care, de regulă, se rezumă la factorii care pot produce distrugeri de date și de informații, pe timpul unui atac, într-o rețea informatică, ori care ascund identitatea atacatorului sau felul în care au fost utilizate informaţiile furate etc.

În analiza de față, avem, ca reper, definiţia din Manualul Tallinn, care, sub regula 32, precizează că spionajul cibernetic reprezintă „orice act executat clandestin sau utilizarea de false pretenţii prin folosirea capabilităţilor cibernetice, în intenţia de a obţine informaţii”[4]. Aparent, nu ar trebui să abordăm această definiție atunci când analizăm terorismul cibernetic ca formă de manifestare a războiului asimetric. Însă Manualul Tallinn ne prezintă și unele concluzii ale grupului de experţi, potrivit cărora atacul Al-Qaeda, din 11 septembrie 2001, asupra SUA, este asimilat, sub aspect juridic internaţional, dreptului la autoapărare în faţa unui atac armat[5], situație care îmi permite utilizarea acesteia în continuare.

Plecând de la aceste opinii, analiza mea se complică, atunci când suprapun definiției speţa ”Snowden”, în care Edward Snowden a demonstrat că practic oricine poate spiona, Internetul oferind un mare nivel de anonimat. O multitudine de date şi de informaţii pot fi procurate din dispozitivele mobile conectate la diversele servicii de Internet, aşa cum sunt ipaduri, tablete, telefoane mobile, smartphone-uri etc. Toate aceste dispozitive electronice pot fi simultan în relații multiple, în diverse reţele cibernetice şi în rețele de comunicaţii.

Deşi există norme legislative care prevăd sancţiuni pentru interceptarea apelurilor telefonice celulare de către unele structuri guvernamentale, s-a dovedit că și structurile de crimă organizată pot intercepta și monitoriza convorbirile de pe un telefon mobil. Când telefonul emite, o rețea de telefonie digitală permite urmărirea dispunerii geografice a acelui dispozitiv. Identificat ca abonat, sub un număr de telefon celular, emisiile acestuia permit stabilirea activității desfășurate pe timpul deplasării între site-urile celulare şi prin Internet.

Având aceste oportunități, oferite de tehnologie, nimic nu îi împiedică pe teroriști să utilizeze tehnicile de interceptare și de monitorizare a unor emisii a dispozitivelor pe care le consideră de interes. Prin urmare, spionajul cibernetic poate fi utilizat și în sprijinul săvârşirii de acte teroriste. Acesta asigură: facilitarea accesului neautorizat; interceptarea pachetelor de date; virusarea sistemelor informatice; blocarea procesului de comunicare a datelor; piratare software; clonarea mijloacelor electronice de plată; activităţi de inginerie socială; identificarea de activități planificate prin aplicațiile de management al proiectelor, aplicații existente în orice telefon celular; alte particularităţi comportamentale ale ţintei.

În general, din perspectiva securității, riscurile şi implicaţiile unui atac major de securitate cibernetică, cu origini teroriste, pot fi comparabile celor din perioada Războiului Rece. Extrapolând aceste riscuri la un nivel mult mai mare asupra interesului național ori asupra interesului comun într-o alianță internațională, vom observa că, procedural, nu se schimbă cu nimic. Spre exemplu, infrastructurile reţelelor de transport al energiei electrice, instalaţiile de tratare a apei, nodurile de management feroviar şi rutier, facilităţile aeroportuare etc., toate sunt vulnerabile spionajului cibernetic și altor amenințări informaţionale. Spionajul cibernetic poate pregăti lovirea directă a unor ţinte, poate procura informaţii în sprijinul acțiunilor maliţioase și care nu vizează executarea unui atac direct, ori poate extrage informaţii, în scopul șantajării țintei și obținerii de fonduri.

Este evident că, pentru un astfel de efort de realizare a spionajului prin și cu dispozitive cibernetice, este nevoie de o forţă reală, de o capabilitate specializată, despre care nu avem cunoștință că ar exista în organizarea niciunei structuri teroriste contemporane. Însă, lipsa acestor infomații nu trebuie să ne „încurajeze” prea mult. Lecțiile învățate, în urma acțiunilor contrateroriste, ne atenționează că, atunci când un lider puternic al unei organizaţii teroriste dispune de fonduri suficiente, poate achiziționa de pe piaţa neagră cam tot ce își propune. Având bani, pot cumpăra serviciile unor indivizi recunoscuți ca având reale performanțe în activitatea infracțională pe Internet, ori a unor simpatizanţi ai ideologiilor teroriste, buni specialişti în utilizarea instrumentelor de spionaj cibernetic, iar stimulându-le orgoliile, să-și „rezolve” toate obiectivele informaționale propuse.

**Fraude cibernetice, comise în sprijinul activităţii teroriste**

Potrivit Codului penal din România, frauda informatică reprezintă „introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane”[6]. După cum se observă, în această definiție nu se face legătura cu terorismul. Definiția face trimitere către o zonă specifică infracţionalităţii.

În prezent, tot mai mulți infractori, în vederea comiterii de activităţi infracţionale, în afara graniţelor fizice sau administrative, exploatează viteza, confortul şi anonimatul oferit de mediul informatic, afectând grav victima prin atacurile cibernetice efectuate sau prin exercitarea de ameninţări asupra oricărei persoane aflate oriunde în lume.

Deşi nu există o definiţie universală şi recunoscută pentru infracțiuni cibernetice, pe baza cazuisticii penale privind infracţiunile legate de Internet, clasific activitatea infracțională specifică în:

• infracţionalitate informatică avansată (sau infracţiuni înalt tehnologizate) – cuprind atacuri sofisticate împotriva componentelor şi programelor informatice;

• infracţionalitate cu caracter informatic – cuprind infracţiuni „tradiţionale” care au suferit „modernizări”, odată cu apariţia Internetului. Între acestea, includem infracţiunile împotriva copiilor, infracţiuni financiare şi chiar acele activități infracționale din zona terorismului.

Încă o dată doresc să subliniez că, oricât de schimbătoare este natura infracţionalităţii

informatice, determinată de aceste noi tendinţe în dezvoltarea sistemelor şi reţelelor informatice, nu toate activităţile din Internet, specifice crimei organizate, reprezintă terorism cibernetic.

În general, activitatea recunoscută ca fiind desfăşurată de structurile de crimă organizată se orientează în vederea maximizării profitului, în cel mai scurt timp. Dintre acestea, amintim furtul, frauda, jocurile ilegale, vânzarea de medicamente contrafăcute etc.[7] Am considerat necesar să fac aceste precizări pentru a înţelege că structurile poliţiei sunt angajate în neutralizarea tuturor fraudelor informatice, pentru combaterea organizaţiilor teroriste, primind sprijin şi de la alte structuri specializate în combaterea activităţilor logistice sau financiare destinate susţinerii terorismului. De altfel, miniştrii de interne din cadrul G7 au solicitat, în cadrul întâlnirii de la Ischia, Italia, în octombrie 2017, partajarea informaţiilor, din platforma globală, despre aşa-anumiţii „luptători teroriști străini” (”foreign terrorist fighters – FTFs”) pe timpul schimbului de date şi analizei activităţii preponderent extremiste. În finalul acestui summit, miniştrii de interne au susţinut, printr-o declaraţie comună, că vor „sprijini rolul INTERPOL ca platformă globală pentru schimbul de informaţii despre documentele de călătorie pierdute şi furate, precum şi pentru examinarea sistematică a călătorilor internaţionali, incluzând schimbul de informaţii biometrice şi de date colectate în spaţiul de luptă. Nu în ultimul rând se angajează să încurajeze toate statele să intensifice utilizarea bazelor sale de date”[8]. De altfel, INTERPOL a fost pionierul schimbului de informaţii pentru sprijinul juridic al acţiunilor militare încă din anul 2005, prin Proiectul Vennlig, în Irak şi, ulterior, prin Proiectul Hamah, în Afganistan. Informaţiile furnizate prin INTERPOL permit subminarea activităţilor grupărilor teroriste, interzicerea deplasării luptătorilor-teroriști care urmăresc întoarcerea în zonele de conflict, evaluarea nivelurilor de risc şi sprijinirea investigaţiilor necesare executării arestărilor conexe.

De ce toate aceste alarme? Pentru că, începând cu anul 2018, pe baza evoluţiilor îngrijorătoare a ameninţărilor geopolitice, ideologice şi tehno-logice, care fac ca prevenirea fraudelor cibernetice să fie o problemă preponderent de protecţie a afacerilor împotriva noilor forme şi a celor emergente de infracţionalitate financiară, se observă şi o serie de efecte asupra stării de securitate naţională a unui stat. Astfel, în perioada 20-24 noiembrie 2017, printr-o iniţiativă EMMA (European Money Mule Action), îndreptată împotriva spălării banilor transnaţionali, s-a reuşit identificarea unor transferuri ilegale de fonduri legate de crimina-litatea informatică[9], în valoare de aproximativ 31 de milioane de dolari. Conform EMMA, 90% dintre aceşti bani puteau fi destinaţi sprijinirii activităţii teroriste a unor grupări, precum Boko Haram, Statul Islamic şi Hezbollah. Aceste fonduri proveneau din aşa-numitele transporturi de bani şi criptofonduri, transporturi despre care autorităţile afirmă că sunt esenţiale pentru operaţiunile care fac ca activitatea să treacă de la scopuri infracţionale la terorism.

Mai mult decât atât, în cazul operaţiilor militare de destabilizare a puterii militanţilor din Irak, din Siria, din Somalia etc., grupările extremiste par să se orienteze către infracţionalitatea financiară online, prin eforturi de finanţare a radicalizării[10], pentru recrutare din interiorul naţiunilor occidentale şi, nu în ultimul rând, pentru achiziţionarea de arme de foc necesare executării de atacuri individuale şi locale, cu obiective limitate. Se estimează că, în viitor, extremiştii din ţările occidentale ar putea dezvolta diverse metode de obţinere de venituri prin infracţiuni cibernetice pentru testarea de noi tehnologii, dintre care cele vizate sunt dronele încărcate cu exploziv[11]. De altfel, cele mai frecvente obiective ale fraudelor informatice pe care se sprijină activitatea teroristă sunt cele destinate achiziţionării online de diverse materiale, de componente explozive, chimice şi/sau biologice, închirierii de maşini şi apartamente.

Organizaţiile teroriste şi sponsorii lor pot folosi Internetul pentru finanţarea acestor activităţi. Modul în care teroriştii utilizează Internetul pentru strângerea de fonduri şi pentru achiziţionarea de resurse poate fi clasificat în patru categorii generale (indicare sursă a clasificării):

- cererea directă – se referă la utilizarea site-urilor web, grupurilor de chat, mesageriei electronice şi comunicărilor direcţionate pentru a solicita donaţii de la adepți;
- comerţul electronic – după cum se cunoaşte, în cadrul Internetului se poate desfăşura comerţ electronic, existând site-uri web care pot fi organizate ca magazine online cu diverse produse şi unde se pot oferi

susţinătorilor cărţi, înregistrări audio şi video, alte articole;

- exploatarea instrumentelor de plată online – dispozitivele de plată online oferă servicii specializate prin intermediul site-urilor dedicate sau al platformelor de comunicaţii, facilitează transferul fondurilor electronic între părţi;
- sponsorizare din partea unor organizaţii caritabile – transferurile de fonduri sunt adesea efectuate prin transfer bancar electronic, card de credit sau facilităţi alternative de plată, disponibile prin intermediul serviciilor, precum PayPal sau Skype.

„Spălarea banilor” este o altă activitate a crimei organizate, importantă pentru sprijinul organizaţiilor teroriste. Un exemplu în acest sens este cazul hackerului Younis Tsouli, care, în Marea Britanie, a spălat câştiguri ilicite, obţinute prin furtul din carduri bancare, în scopul finanţării unor acte de terorism[12]. Pentru aceasta, el a apelat la mai multe metode, inclusiv la transferul prin intermediul conturilor electronice de plată online, fondurile fiind direcţionate prin mai multe ţări, înainte de a ajunge la destinaţia dorită. Banii astfel spălaţi au fost utilizaţi atât pentru a plăti înregistrarea de către Tsouli a 180 de site-uri, unde se difuzau videoclipuri de propagandă ale Al-Qaeda, cât şi pentru a achiziţiona echipamente necesare activităţilor teroriste, în mai multe ţări. Se pare că au fost utilizate circa 1.400 de carduri de credit, care au generat aproximativ 1,6 milioane de lire sterline, în fonduri ilicite pentru finanţarea terorismului.

**E-propaganda, educaţia şi radicalizarea**

Exploatând Internetul, grupările teroriste pot „beneficia” de promovarea propriilor ideologii în vederea incitării la ură şi la violenţă, ori pentru pregătirea atentatelor teroriste, pentru atragerea de simpatizanţi, pentru instruire asistată etc. Reţelele informaţionale ale utilizatorilor casnici, ale firmelor şi ale instituţiilor, care permit conectarea diverselor tehnologii informaţionale, pot fi programate să execute simultan un atac în spaţiul cibernetic, din diverse zone ale lumii, asupra unui serviciu sau unei reţele conectate la Internet.

Una dintre cele mai cunoscute metode de atac pe Internet este difuzarea de materiale de propagandă. În general, propaganda prin Internet adoptă forma comunicărilor multimedia prin care se pune la dispoziţie cititorului o mulţime de informaţii care constituie instrucţiuni ideologice sau practice, explicaţii, justificări, sau care promovează aspecte specifice vieţii într-o organizaţie teroristă. Acestea pot include mesaje virtuale, prezentări, reviste, tratate, fişiere audio, video şi jocuri video, realizate de organizaţiile teroriste sau de simpatizanţi. Cu toate acestea, spre deosebire de abordarea legitimă a unui punct de vedere, ceea ce constituie propaganda teroristă este adesea o evaluare subiectivă a tuturor aspectelor prezentate.

Difuzarea propagandei nu este o activitate interzisă. Unul dintre principiile de bază ale dreptului internaţional privind protecţia drepturilor omului include dreptul la libertatea de exprimare. Aceasta garantează unei persoane dreptul de a împărtăşi o opinie sau de a distribui un conţinut, care, în mod normal, poate fi sau nu acceptat de către alte persoane (sub rezerva anumitor excepţii limitate).

Una dintre excluderile general acceptate în ceea ce priveşte acest drept este interzicerea distribuirii anumitor materiale cu conţinut sexual explicit, interdicţie considerată a fi în interesul public pentru protejarea grupurilor vulnerabile. Alte excluderi, prevăzute de lege şi dovedite a fi necesare, se referă la mesaje care, în mod vădit, sunt dăunătoare protecţiei securităţii naţionale şi internaţionale, precum şi la cele de natură să incite la acte de violenţă împotriva indivizilor sau anumitor grupuri de persoane.

Aşa după cum se cunoaşte, promovarea violenţei este o temă comună în propaganda legată de terorism. Acesta este unul dintre motivele principale care explică de ce un mesaj distribuit prin Internet, care se referă la terorism, creşte exponenţial audienţa, publicul fiind afectat emoţional. Propaganda pe Internet poate include conţinut, cum ar fi înregistrări video ale unor acte de terorism violente sau simulări ale acestora, încurajând utilizatorul să se angajeze prin joc virtual pentru a acţiona ca un terorist.

Promovarea retoricii extremiste, care încurajează actele violente, este o altă tendinţă comună, identificată în cadrul platformelor informatice care găzduiesc conţinut extremist pe Internet. Este evident că acest conţinut poate fi distribuit ulterior publicului şi personal, şi prin mijloace media fizice, aşa cum sunt CD-urile şi DVD-urile. Însă, de bază rămâne Internetul, spaţiul

care oferă o gamă largă de instrumente constând în site-uri web dedicate, camere de video-chat şi forumuri de discuţii, reviste on-line, platforme de socializare în reţea, aşa cum sunt Twitter şi Facebook, site-uri video populare şi de partajare a fişierelor media, de tipul YouTube, Rapidshare etc.

Propaganda teroristă are ca principale obiective recrutarea de simpatizanţi, radicalizarea şi incitarea la violenţă. Mesajele difuzate vor căuta să transmită factori incitanţi de mândrie, de realizare şi de dedicare scopurilor extremiste. Acestea pot fi utilizate pentru a demonstra eficienţa atacurilor teroriste, angajamentul şi corectitudinea faţă de cei care au oferit sprijinul financiar.

Alte obiective ale propagandei teroriste pot include folosirea manipulării psihologice, în scopul subminării credinţei unui anumit individ în valorile sale sociale sau promovării sentimentelor de anxietate, frică sau panică în rândul populaţiei sau al unui segment al acesteia. Aceasta se poate realiza prin diseminarea dezinformării, prin zvonuri, prin ameninţări cu violenţă sau prin imagini legate de acte de violenţă. Audienţa vizată poate include spectatori direcţi şi/sau public afectat de publicitatea potenţială, generată de astfel de materiale.

Internetul este locul idel pentru stabilirea de conexiuni şi pentru relaţionarea cu cei interesaţi, tinerii reprezentând victimele ideale, adesea, prinşi în mrejele teribilismului, ale reacţiunii faţă de ce e perimat şi haterismului. Mai mult decât atât, pe baza abilităţile lor de utilizare a Internetului, tinerii pot dezvolta o publicitate implicită prin redifuzarea conţinutului online, prin discuţii şi mesaje în care îşi comunică părerile faţă de administratorii site-ului sau/şi cu ceilalţi membri. Grupurile teroriste au recunoscut „puterea” acestui instrument şi au început să-l folosească cu abilitate. Astfel, acestea difuzează pe aceleaşi platforme mesaje şi programe de îndoctrinare a tineretului cu mesaje radicale.

Deşi nu se poate măsura amploarea succesului acţiunii lor, se recunoaşte că Internetul riscă să devină un instrument performant de recrutare şi de radicalizare. Pentru aceasta, Daesh prezintă diverse aspecte care ţin de oportunităţile profesionale, de viaţa de familie sau de apartenenţa la o comunitate. Această metodă nu vizează doar tinerii sau persoanele deja intrate în procesul de recrutare, ci pe oricine intră în contact cu produsele lor propagandistice, fie printr-un link redirecţionat, fie prin notificări de tip ”push”. Mesajele utilizate nu sunt simple naraţiuni, ci ele sunt atent fabricate pentru a realiza o influenţare psihologică cu efecte graduale. Modalitatea în care acestea vor fi recepţionate este influenţată de mai mulţi factori, dintre care enumerăm: educaţie, vârstă, ocupaţie, mediu relaţional, modalitate de abordare etc.

Radicalizarea unei persoane depinde de contextul familial, emoţional, politic, financiar etc. al individului la acel moment. Nizar Trabelsi, acuzat că a amplasat o bombă într-o unitate militară din Belgia, în numele Al-Qaeda, pe timpul interogatoriului din cadrul anchetei penale a afirmat că elementul iniţial care l-a determinat să adere la cauza teroristă a fost prezentarea de către recrutori a unei fotografii cu o fetiţă ucisă în Fâşia Gaza, în anul 2001[13].

**Instruire asistată prin sisteme informatice**

Observăm că organizaţiile teroriste utilizează Internetul și pentru diseminarea informaţiilor. Dintre produsele lor, enumerăm o serie de ghiduri practice, sub formă de manuale online, clipuri audio şi video, informaţii şi alte sfaturi pe platforme online, toate asigurând o platformă de instruire asistată prin calculator. Mai mult decât atât, aceste platforme cibernetice pun la dispoziţie instrucţiuni detaliate, într-o formă extrem de facilă, mai mult intuitivă (adesea, în format multimedia, în limbi de circulaţie preponderent locală, dar şi internaţională), pe teme diverse, precum: particularităţile construirii unui dispozitiv exploziv improvizat; modalităţi ale uzului armelor de foc, armelor albe sau altor arme improvizate; modalităţile de combinare a unor substanţe, în mod curent, nepericuloase şi transformarea lor în otrăvuri sau în alte elemente periculoase; particularirăţile planificării şi organizării atacurilor teroriste etc.

Prin urmare, platformele de instruire cibernetică, astfel constituite, pot fi considerate tabere virtuale de instruire, urmând ca antrenarea fizică să se execute în mod individual, cu sau fără asistenţă de specialitate. De asemenea, aceste platforme pot fi folosite pentru discuţii sau pentru distribuirea observaţiilor identificate în cadrul experimentelor, pentru comunicarea lecţiilor învăţate despre metodele, tehnicile sau cunoştinţele operaţionale specifice executării de acţiuni teroriste.

De exemplu, revista online *Inspire*, despre care se presupune că este publicată de Al-Qaeda, are ca obiectiv iniţial declarat instruirea musulmanilor pentru jihad. Acestă publicaţie conţine o cantitate mare de materiale ideologice, destinate încurajării terorismului, inclusiv declaraţii atribuite lui Osama Bin Laden, Sheikh Ayman al-Zawahiri, altor persoane reprezentative ale organizației Al-Qaeda.

Elementele de instruire, disponibile online, includ, printre altele, instrumente necesare activităţilor contrainformative, activităților de protecție și celor de hacking, instrumente pentru îmbunătăţirea securităţii legăturilor de comunicaţii şi a altor activităţi de menținere a legăturii online, instrumente de selectare, de propunere a unor metode de criptare şi tehnici de ascundere a identității. Se pare că natura interactivă a platformelor digitale în spațiul cibernetic ajută la consolidarea acelor sentimente de comuniune dintre indivizii aflați în diverse locaţii şi dispuneri geografice, încurajând, astfel, crearea de reţele de schimb de materiale instructive şi tactice. Mai mult decât atât, Internetul poate fi folosit nu numai ca mijloc de a publica retorica extremistă și videoclipuri, ci și ca o modalitate de dezvoltare a relațiilor, o modalitate de a solicita sprijinul celor responsabili cu propaganda orientată etc.

Demn de remarcat în ceea ce privește pericolul radicalizării prin Internet este că spațiul cibernetic poate constitui un mediu eficient de recrutare și de instruire a minorilor, cunoscut fiind faptul că această categorie este semnificativă pentru o mare parte a utilizatorilor. Propaganda făcută în scopul recrutării minorilor poate lua forma unor desene animate, a unor videoclipuri muzicale populare sau a unor jocuri pe suport informatic. De regulă, produsele propagandistice, difuzate pe site-urile web aflate sub controlul teroriștilor sau afiliaţilor acestora, au ca scop vizionarea lor de către minori. De aceea ele includ un melanj de desene animate şi de povestioare cu mesaje care promovează şi glorifică diverse acte de terorism, așa cum este martiriul și atacurile suicidare.

Alte structuri teroriste creează și promovează jocuri digitale. Caracterul lor online le transformă în reale instrumente de recrutare şi de instruire. Astfel de jocuri pot promova violenţa de orice fel, îndreptată împotriva unui stat sau unui individ marcant pentru un partid politic, pot stabili scale de valori și alte recompense pentru „succesul” parcurgerii etapelor virtuale, putând fi oferite unui public tot mai larg, adesea fiind traduse în mai multe limbi de circulație pentru spațiul geografic de interes.

Pe baza celor prezentate, putem observa că și atacul lui Brenton Tarrant ar putea fi încadat ca făcând parte dintr-o etapă de instruire online. Imaginile video, difuzate simultan în rețeaua Facebook, *atenție*, imagini produse și postate în direct de atacator printr-o cameră video, aflată în permanență deschisă, îl arăta cum, la data de 08.03.2019, conducea o mașină spre o moschee, cum intra în clădire și cum deschidea focul asupra celor aflați înăuntru, în mod nediscriminatoriu. Ulterior, îl prezenta cum îi executa pe cei răniți căzuți în stradă, cum își schimba arma, cum trăgea asupra curioșilor de pe stradă, mascat fiind de parbrizul mașinii și de faptul că nu a deschis geamul acesteia în timpul mersului.

Este clar că evenimentul a fost un atac terorist, fiind susținut și de „manifestul”, publicat pe Internet, în care îi denunța pe imigranți ca invadatori. Legat de Internet, Facebook, Twitter și Google au permis susținerea a numeroase discuții și difuzarea de materiale cu conținut extremist în cadrul platformelor lor, ca urmare a distribuirii imaginilor video și a filmelor rezultate din acest eveniment. *Daily Mail*, citându-l pe Clement Thibault, analist la platforma globală a piețelor financiare Investing.com, remarca că „streaming-ul live al filmărilor din Noua Zeelandă va aduce cu siguranță mai multe întrebări privind regulile și controlul asupra Facebook. Aceasta a oferit o platformă pentru atacul oribil de astăzi și, fără îndoială, va fi pusă sub semnul întrebării pentru facilitarea răspândirii acestui eveniment”[14].

**Concluzii**

După cum se observă, terorismul cibernetic trebuie considerat ca o etapă a evoluţiei infracţiunilor cibernetice, adaptată scopurilor teroriste. Este evident că resursele oferite de spaţiul cibernetic şi mecanismele de comitere a acţiunilor informatice se întrepătrund, ele fiind exploatate la maximum de către cei proveniţi atât din zona criminalităţii informatice, cât şi din zona terorismului.

Din punctul de vedere al dezvoltării terorismului cibernetic, apreciez că pot fi identificate trei scenarii de bază, ale căror diferenţe provin din raporturi diferite de cauzalitate. Nu exclud

posibilitatea existenţei şi altor scenarii, pe care le consider derivate sau soluţii adoptate, în funcţie de resursele avute la dispoziţie şi de instruirea în domeniu.

Cele trei scenarii de dezvoltare a terorismului cibernetic sunt:

*Scenariul 1* – instruirea unor teroriști tradiționali în hacktivism;

*Scenariul 2* – angajarea unor hackeri pentru organizarea și executarea unor atacuri teroriste cu sprijin informatic și informațional, dat de Internet, atacuri similare modelului „mercenarilor cibernetici”;

*Scenariul 3* – hackeri simpatizanţi, care împărtăşesc ideologiile organizaţiei teroriste şi, ulterior, devin membri activi ai acesteia.

Principalele metode utilizate în sfera criminalităţii informatice și care ar putea fi exploatate în scopul desfăşurării unui atac terorist sunt: atacurile prin parolă; atacuri prin accesarea reţelei şi interceptarea pachetelor de date; atacuri care exploatează accesul liber (trusted access); atacuri prin IP (IP spoofing); atacuri prin inginerie socială; atacuri cu predicţia numărului secvenţei; atacuri cu deturnarea sesiunii; atacuri care exploatează slăbiciunile tehnologiei; atacuri care exploatează bibliotecile partajate etc. Toate aceste metode pot configura un scop infracţional, din care să se aprecieze motivaţia pentru care ele au fost lansate.

Concluzionez că nu este nicio diferenţă între cunoştinţele necesare şi setul de instrumente folosite de către hackeri şi teroriști cibernetici, efectele finalizării atacului şi motivaţia lui fiind singurele elementele care le diferenţiază. Sinergia măsurilor terorismului convenţional şi ale războiului informaţional se constituie într-un element foarte periculos şi, totodată, avantajos pentru teroriști, deoarece acesta combină scopurile letale cu obiectivul major de generare de frică.

Pentru teroriştii cibernetici, adoptarea acestor măsuri informaţionale permite o acţiune liberă în diverse spaţii geografice, cu încălcarea graniţelor convenţionale fizice ale statelor contemporane. În acelaşi timp, teroriştii tradiţionali pot folosi războiul informaţional pentru a limita costul unui atac de acest tip, în comparaţie cu cel al unui atac convenţional.

De asemenea, războiul informaţional furnizează anonimatul atacatorului și obţine un efect sporit propagării schizofreniei în cadrul ţintei, fără limitarea capacităţilor teroriste de a spori efortul pe timpul atacului. Astfel, raportul „cost scăzut/efecte sporite” este de departe mult mai atractiv pentru teroriştii care utilizează războiul informaţional, faţă de cei care se opun acestui fapt.

Trebuie acceptat că terorismul cibernetic este o realitate care a depășit de mult domeniul strict limitat al propagandei pe Internet. Însă, prin sintagma că întărirea terorismului tradiţional se va realiza prin alegerea și dezvoltarea tehnicilor și metodelor specifice războiului informaţional, nu trebuie să înţelegem că au apărut noi tipuri de teroriști.

Terorismul cibernetic nu este război informaţional și nici un cumul de infracțiuni cibernetice. Este ceva nou, extrem de versatil, care se confundă cu alte forme sociocibernetice și care are un mare potențial de dezvoltare. Cum se va adapta cerințelor tradiționale ale terorismului clasic rămâne doar o opțiune a managementului organizației teroriste respective. Vom vedea...

**NOTE:**

1 Manuel R. Torres Soriano, ”Guerras por delegación en el ciberespacio – Proxy wars in cyberspace”, *IEEE* – Revista institutului spaniol de studii strategice –, nr. 9, 2017.

2 Gabriel Weimann, ”Special Report”, United States Institute of Peace, martie 2004, https://www.usip.org/sites/default/files/sr116.pdf, accesat la 14.09.2018.

3 Apud. Jimmy Gurule, în Dru Stevenson, ”Effect of the national security paradigm on criminal law”, https://law.stanford.edu/wp-content/uploads/2018/03/stevenson.pdf, accesat la 16.10.2018.

4 Michael N. Schmitt (general editor), Liis Vihul (managing editor), *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, University Press, Cambridge, 2017, p. 168.

5 *Ibidem*, p. 345.

6 https://legeaz.net/noul-cod-penal/art-249, accesat la 15.02.2019.

7 Uptin Saiidi, ”Inside Interpol’s Singapore cybercrime-fighting complex”, https://www.cnbc.com/2017/05/17/inside-interpols-singapore-cybercrime-fighting-complex.html, accesat la 16.02.2019.

8 *** *G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL*, https://www.interpol.int/News-and-media/News/2017/N2017-144, accesat la 16.02.2019.

9 Liam Tung, ”Australia helps EU in latest crack down on money mules”, https://www.cso.com.au/article/630544/australia-helps-eu-latest-crack-down-money-mules/, accesat la 12.01.2019.

10 Timothy L. Quintero, ”The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime”, https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/, accesat la 12.01.2019.

11 *** *Threat Lens 2018 Annual Forecast*, https://worldview.stratfor.com/article/threat-lens-2018-annual-forecast-excerpt, accesat la 12.01.2019.

12 Michael Jacobson, ”Terrorist Financing and the Internet”, *Studies in Conflict & Terrorism*, https://www.tandfonline.com/doi/pdf/10.1080/10576101003587184, accesat la 10.11.2018.

13 Melodie Bouchaud, ”Belgium Condemned Over Unlawful Extradition of Terrorist to the US”, https://news.vice.com/en_us/article/3kegx3/belgium-condemned-over-unlawful-extradition-of-terrorist-to-the-us, accesat la 03.11.2018.

14 https://www.dailymail.co.uk/news/article-6814269/Facebook-shares-drop-execs-quit-Christchurch-live-stream-shooting-stirs-outrage.html, accesat la 15.04.2019.

## BIBLIOGRAFIE


*** „Anders Breivik, autorul atacurilor din Norvegia, ar putea primi «impresionanta» pedeapsă de 30 de ani de închisoare!”, http://www.ghimpele.ro

*** ”Cyber-attack: US and UK blame North Korea for WannaCry”, https://www.bbc.com

*** *Decret nr. 212, din 31 octombrie 1974, pentru ratificarea Pactului internațional cu privire la drepturile economice, sociale și culturale și Pactului internațional cu privire la drepturile civile și politice*, publicat în B.Of. nr. 146/20 1974, http://www.cdep.ro

*** „Efectul Breivik: Circa o sută de norvegieni vor să devină «teroriști solitari», http://www.financiarul.ro

*** ”Facebook shares drop execs quit Christchurch live stream shooting stirs outrage”, https://www.dailymail.co.uk

*** ”G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL”, https://www.interpol.int

*** ”Hacked: The Bangladesh Bank Heist”, https://www.aljazeera.com

*** *Noul cod penal*, https://legeaz.net

*** *Threat Lens 2018 Annual Forecast*, https://worldview.stratfor.com

Bălan George, „Noua concepţie internaţională de acţiune doctrinară şi practică în combaterea terorismului”, http://fs.legaladviser.ro

Bouchaud Melodie, ”Belgium Condemned Over Unlawful Extradition of Terrorist to the US”, https://news.vice.com

Bumiller Elisabeth, Thom Shanker, ”Panetta Warns of Dire Threat of Cyberattack on US”, https://www.nytimes.com

Fedotov Yury, ”Taking action where we can to stop cybercrime”, https://www.unodc.org

Flynn Matthew J., *Is There a Cyber War?*, Excelsior College, National Cybersecurity Institute Journal, vol. 1, Issue 2, 2014.

Jacobson Michael, ”Terrorist Financing and the Internet”, *Studies in Conflict & Terrorism*, https://www.tandfonline.com

Jurj-Tudoran Remus, „Instigarea publică la săvârșirea unei infracțiuni de terorism și libertatea de exprimare în practica Curții Europene a Drepturilor Omului”, http://revistaprolege.ro

Quintero Timothy L., ”The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime”, https://www.insightcrime.org

Saiidi Uptin, ”Inside Interpol’s Singapore cybercrime – fighting complex”, https://www.cnbc.com

Schmitt Michael N. (general editor), Liis Vihul (managing editor), *Tallinn Manual 2.0,* On the International Law Applicable to Cyber Operations, Cambridge, University Press, 2017.

Soriano Manuel R. Torres, ”Guerras por delegación en el ciberespacio – Proxy wars in cyberspace”, *IEEE* – Revista institutului spaniol de studii strategice –, nr. 9, 2017.

Stevenson Dru, ”Effect of the national security paradigm on criminal law”, https://law.stanford.edu

Tanasă Remus, „Benedict Anderson şi destinul «Comunităţilor imaginate»”, https://www.lapunkt.ro

Tung Liam, ”Australia helps EU in latest crack down on money mules”, https://www.cso.com.au

Weimann Gabriel, ”How modern terrorism uses the Internet, United States Institute of Peace”, https://www.usip.org

# FILE DIN ISTORIA UNIVERSITĂŢII NAŢIONALE DE APĂRARE „CAROL I”

## *FILES FROM THE HISTORY OF ”CAROL I” NATIONAL DEFENCE UNIVERSITY*

## *DES PAGES DE L’HISTOIRE DE L’UNIVERSITÉ DE DÉFENSE NATIONALE ”CAROL Ier”*

**Dr. Laura-Rodica HÎMPĂ***

Instituţie unică prin vechime, structură şi organizare, Universitatea Naţională de Apărare „Carol I” s-a evidenţiat, de-a lungul timpului, la nivelul organizaţiilor militare de învăţământ superior românesc, prin amploarea activităţilor sale de formare şi informare a ofiţerilor. Articolul redă aspecte din elementele constitutive ale Şcolii Superioare de Război (denumirea iniţială, din anul 1889), cu scurte opriri asupra anilor 1919, 1937 şi 1939, ilustrate cu documente de arhivă.

Cercetarea se bazează pe documentele studiate la Arhivele Naţionale Militare, Serviciul Arhivelor Naţionale Istorice Centrale, Biblioteca Academiei Române şi Biblioteca Universităţii Naţionale de Apărare „Carol I”.

*Unique institution through seniority, structure and organization, the ”Carol I” National Defense University has stood out over time at the level of the military organizations of higher education in Romania, through the scope of its activities of training the officers in theory and practice. The article gives aspects of the constituent elements of the Superior War School (the initial name from 1889), with brief stops on the years 1919, 1937 and 1939, illustrated with archival documents.*

*The research is based on the documents studied at the National Military Archives, the Service of the Central National Historical Archives, the Library of the Romanian Academy and the Library of the National Defense University “Carol I”.*

*Institution unique par son ancienneté, sa structure et son organisation, l’Université de Défense Nationale ”Carol Ier” s’est distinguée, au fil du temps, parmi d’autres organisations militaires d’enseignement supérieur en Roumanie, par la portée de ses activités de formation et d’information des officiers. L’article décrit des aspects sur les éléments constitutifs de l’École supérieure de guerre (comme était dénommée, au début, en 1889), avec de brefs arrêts sur les années 1919, 1937 et 1939, illustrés par des documents d’archives.*

*La recherche est basée sur les documents étudiés aux Archives Militaires Nationales, au Service des Archives Centrales d’Histoire Nationale, à la Bibliothèque de l’Académie Roumaine et à la Bibliothèque de l’Université de Défense Nationale ”Carol Ier”.*

**Cuvinte-cheie**: Şcoala Superioară de Război; Universitatea Naţională de Apărare „Carol I”; Buletinul Universităţii Naţionale de Apărare „Carol I”.

***Keywords:*** *Superior War School; ”Carol I” National Defense University; Bulletin ”Carol I” National Defense University.*

***Mots clés****: École supérieure de guerre; Université de Défense Nationale ”Carol Ier”; Bulletin de l’Université de Défense Nationale ”Carol Ier”.*

Cercetarea de faţă îşi propune să surprindă câteva momente importante din evoluţia de peste un secol a Universităţii Naţionale de Apărare „Carol I”, din perspectiva documentelor de arhivă. Etapele surprinse aici ilustrează liniile de fond ale ideilor în jurul cărora s-au articulat direcţiile care au influenţat de-a lungul timpului învăţământul superior militar şi, implicit, eşaloanele de conducere ale Armatei României.

Limitările impuse de dimensiunile rezonabile ale unui articol ştiinţific au condus la surprinderea retrospectivă a câtorva evenimente decisive: 1889, anul înfiinţării; apoi anul 1919, care a adus înfiinţarea Şcolii de Intendenţă; 1937, anul în care

***Universitatea Naţională de Apărare „Carol I”***
e-mail*: l.himpa@gmail.com*

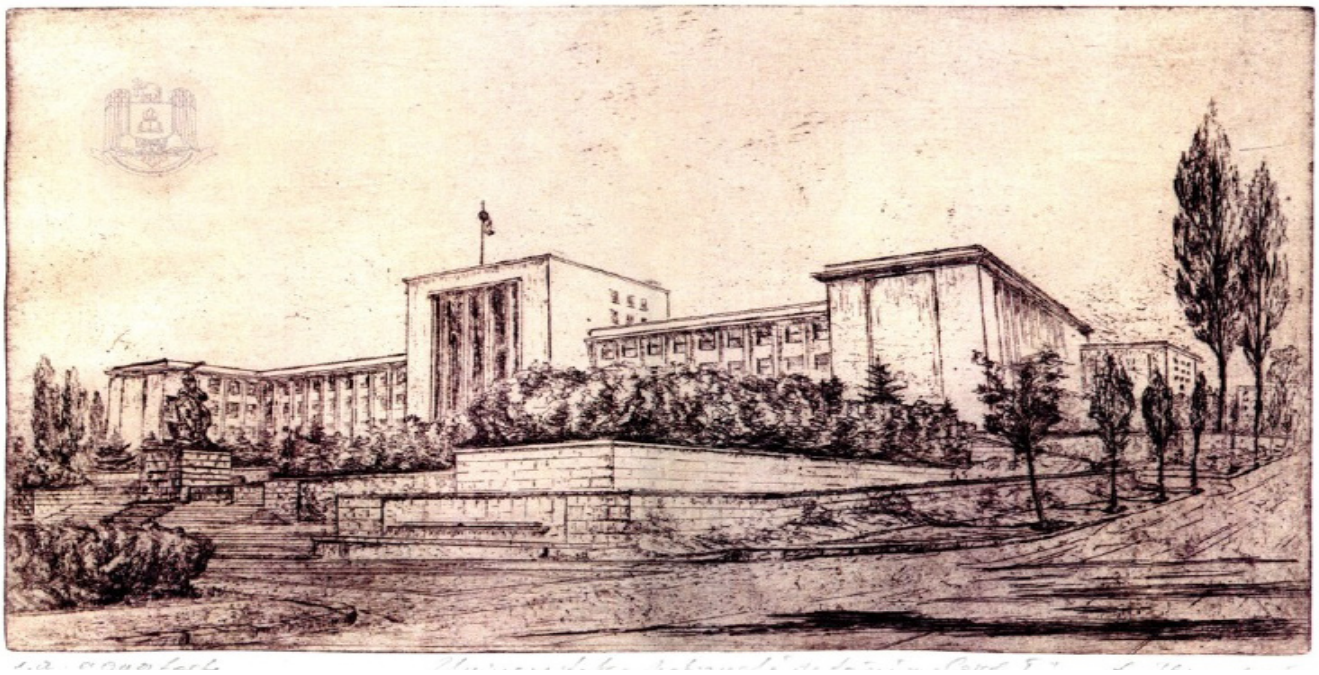
a luat fiinţă Buletinul Universităţii Naţionale de Apărare „Carol I”; 1939, anul în care s-a inaugurat actualul sediu şi în care s-au aniversat primii 50 de ani de activitate.

Momentul apariţiei Şcolii Superioare de Război a venit într-un context în care nevoia de formare a personalului militar superior era văzută ca o prioritate naţională. Până în anul 1889, ofiţerii de rang înalt erau trimişi la studii în marile capitale europene, la universităţi militare de renume (Torino, Bruxelles, Paris, Berlin, Viena). Acest mod de educare asigura o pregătire elitistă prin contactul direct cu civilizaţia şi cultura europeană.

Înfiinţarea Şcolii Superioare de Război, ca intermediar şi formator pentru doctrina armatei române, a constituit o necesitate odată cu crearea „Matei Basarab”, „Mihai Viteazul”, „Gheorghe Şincai”, „Spiru Haret”, „Sfântul Sava”, „Titu Maiorescu”, „Iulia Haşdeu”, Biblioteca Academiei Române, Casa Monopolurilor Statului, Universitatea Naţională de Apărare „Carol I”, Consiliul de Miniştri, Palatul Ministerului Transporturilor, Ministerul Justiţiei, Institutul Agronomic, Palatul Regal, Palatul Patriarhiei etc.[2]

Printre realizările regelui Carol I, se numără la loc de cinste şi Şcoala Superioară de Război, înfiinţată prin Înalt Decret Regal nr. 2073, emis la data de 8/20 august 1889.

În primul articol al legii, a fost stabilit scopul instituţiei: pregătirea ofiţerilor de stat major şi răspândirea în armată a înaltelor cunoştinţe militare. Cursurile ţineau doi ani, iar condiţiile



*Universitatea Naţională de Apărare „Carol I”*

Gravură realizată de Eugen Ilina, Uniunea Artiştilor Plastici din România

Statului Major General, la 12 noiembrie 1859, prin Înaltul Ordin de Zi nr. 83, semnat de Alexandru Ioan Cuza. Ofiţerii care alcătuiau acest organism erau recrutaţi din rândul celor care absolviseră şcoli de război în străinătate şi care „posedau cunoştinţe speciale militare dobândite prin studii sistematice”[1], însă fără a avea o gândire militară românească proprie.

Ctitor al României moderne, regele Carol I a avut în vedere să se construiască, în Bucureşti şi aproape în toate oraşele reşedinţă de judeţ, clădiri administrative, tribunale, biserici, cinematografe, Biblioteca Centrală Universitară „Carol I”, liceele: pe care candidaţii trebuiau să le îndeplinească, enumerate în articolul cinci, erau următoarele: să fi deţinut gradul de locotenent, să fi lucrat „cel puţin doi ani în serviciu efectiv la trupă, să aibă o bună conduită sub toate raporturile şi să fie de o bună constituţie fizică, recunoscut sănătoasă”. Un medic militar trebuia să dea un aviz din care să reiasă „constituţiunea fizică a candidatului, în special vederea şi auzul” (Anexa nr. 1).

După anul 1919, având în vedere situaţia creată prin noile alianţe, încheiate în urma Primului Război Mondial, colaborarea României s-a limitat la Şcolile Superioare de Război de la Torino şi Paris.

De asemenea, este recunoscut oficial faptul că, după Războiul de Întregire (1914-1916), România a preluat doctrina Armatei Franceze[3].

Pornind de la discursul de inaugurare a Şcolii Superioare de Război, rostit de întemeietorul acesteia, generalul Ştefan Fălcoianu[4], în noiembrie 1889, potrivit căruia „Necesitatea creării unei Şcoli Superioare de Război a fost mult simţită şi solicitată cu stăruinţă de Marele Stat Major al Armatei. (...) Vom pune toate silinţele noastre spre a ne achita cu cel mai viu interes de această îndatorire; vom reclama, şi suntem siguri că vom dobândi concursul camarazilor noştri cei mai luminaţi şi, astfel, sperăm că, cu toţii împreună, vom face ca această importantă instituţiune să dea roadele ce Armata aşteaptă de la dânsa”[5], putem concluziona acum, la ceas aniversar, după 130 de ani de efervescentă activitate, după schimbări şi transformări de nume[6], că vorbele mai sus amintite şi-au atins, an după an, adevăratul sens.

*Portretul lui Ştefan Fălcoianu*

Gravură realizată de Nicolae Grigorescu,
Biblioteca Academiei Române

Din evoluţia Statului Major General, de la formele iniţiale până la structura complexă de astăzi, de concepţie şi pregătire doctrinară, toate dominate de un caracter naţional specific, un pas hotărâtor a fost apariţia, în 1889, a Şcolii Superioare de Război, care a pus amprenta pe educaţia ofiţerilor de rang înalt, încurajând totodată cooperarea cu celelalte armate, cercetarea şi inovarea, toate conducând la maximizarea capacităţii operative şi deci la eficientizarea întregii armate.

Astfel, menirea prestigioasei instituţii de învăţământ superior militar românesc a fost ţinută vie şi şi-a atins scopul, slujită cu devotament şi înalte sentimente de patriotism atât de ofiţerii superiori ai Armatei Române pe care i-a format, cât şi de nume importante ale culturii române, pornind de la Nicolae Iorga, Grigore Alexandrescu, Simion Mehedinţi, Dimitrie Gusti, Henri H. Stahl, Dimitrie Caracostea.

Nevoia de modernizare, perfecţionare şi aliniere la cerinţele vremii a dus la o extindere permanentă a domeniilor de formare a ofiţerilor studenţi.

Astfel, în anul 1919, regele Ferdinand a emis Înaltul Decret Regal nr. 4729/1919, prin care a luat fiinţă „Secţia de intendenţă pe lângă Şcoala Superioară de Război”[7], cu o durată de doi ani.

„(...) Este absolut necesar ca, pe lângă ceilalţi factori care contribuie la câştigarea bătăliilor, să existe şi exponentul organismului economic, care, prin pregătirea sa de specialitate, să organizeze şi să dirijeze economia războiului de care depinde în mare parte soarta bătăliilor. Şcoala Superioară de Război, dând importanţa cuvenită acestui principiu suveran în pregătirea marelui organism Armata, prin înfiinţarea şi funcţionarea Secţiei de Intendenţă sub acelaşi acoperiş şi sub impulsiunea aceleiaşi direcţiuni, a completat golul atât de simţit în conducerea şi structura armatei”[8].

Erau studiate domenii ca: matematica financiară, dreptul comercial, economia politică şi naţională, finanţe, statistică, chimie industrială şi alimentară, legislaţia şi administraţia militară etc. (Anexa nr. 2). Până în anul 1939, au absolvit 19 promoţii (348 de absolvenţi) Şcoala Superioară de Intendenţă.

Participantă activă la cele mai importante evenimente din istoria României de după 1889 şi până în prezent, Şcoala Superioară de Război a format promoţii de ofiţeri de Stat Major şi a impus, datorită profesorilor şi comandanţilor săi, cunoştinţele militare de care a fost nevoie pentru a-şi duce până la capăt misiunea, a ştiut să ţină pasul cu timpul şi a trecut, uneori chiar cu sacrificii umane, peste cele două Războaie Mondiale şi peste Revoluţia din 1989. Candelă vie pentru eroii căzuţi la datorie este prezentă în Holul de Onoare, iar numele acestora este gravat în marmură albă pentru amintirea lor veşnică.

Anul 1937 rămâne în istoria Şcolii Superioare de Război atât prin apariţia „Buletinului Şcolii Superioare de Războiu”, prima titulatură a publicaţiei, (Anexa nr. 5), cât şi prin demararea lucrărilor pentru construirea noului sediu din Şoseaua Panduri.

Desprins din pleiada publicaţiilor periodice militare ale perioadei interbelice, Buletinul Universităţii Naţionale de Apărare „Carol I” a rămas revista cu cea mai lungă existenţă, împlinind, în luna aprilie 2019, 82 de ani de tradiţie şi valoare[9].

Primul număr al Buletinului Universităţii Naţionale de Apărare „Carol I” a apărut în anul 1937, aprilie–mai, cu aprobarea şi la iniţiativa Marelui Stat Major, nr. 2872/23, ianuarie 1937, fapt de o importanţă deosebită, meţionat şi în Regulamentul Şcolii Superioare de Război din acel an.

Nu numai rezistenţa în timp este de remarcat în cazul de faţă, ci şi menţinerea rolului de tribună a spaţiului celor mai înalte idei, aflată în slujba celei mai importante instituţii de învăţământ superior militar din România.

În Regulamentul „Şcolii Superioare de Război” din anul 1937, au fost expuse atât menirea, cât şi mijloacele de realizare a obiectivelor instituţiei. Au fost subliniate două idei centrale: educaţia la nivel superior a ofiţerilor militari şi asigurarea unei baze de pregătire dintre cele mai moderne „în vederea comandei şi conducerii Marilor Unităţi şi în vederea alegerii ofiţerilor de Stat-Major”[10].

Dintre metodele de îndeplinire a obiectivelor propuse iniţial, în primul rând a fost menţionată activitatea ofiţerilor absolvenţi, „cu ocazia serviciului lor la trupă sau la comandamente (...), procedeu aşa de lent faţă de rapiditatea de astăzi a progresului ştiinţei militare”, riscând ca doctrina abia primită în armată să devină perimată. Ineficacitatea provenea şi din lipsa de experienţă şi de autoritate a celor care nu reuşeau să impună cunoştinţele dobândite.

În al doilea rând, a fost subliniat rolul avut de „publicaţiunea prin care se obţinea difuzarea noilor idei, mult mai rapid, în acelaşi timp cu predarea cursurilor în Şcoală şi ţinerea la curent a comandamentelor cu un material intelectual oficial, verificat prin numeroase dezbateri, foarte necesar documentării lor, pentru aplicarea doctrinei în armată”[11]. Un alt avantaj foarte important subliniat în Regulament a fost şi stabilirea unei comunităţi de vederi între comandamente şi ofiţerii de stat major, ceea ce contribuia de la început la o încredere reciprocă şi la o colaborare mult mai fructuoasă.

În urma celor expuse mai sus, Şcoala Superioară de Război, ca organ oficial de înaltă cultură militară al Marelui Stat Major şi cu aprobarea acestuia, a luat iniţiativa imprimării unui „Buletin”, menit nu numai să înlăture neajunsurile primului procedeu, dar în acelaşi timp să-l şi completeze.

Văzut ca un mijloc de propagandă a celor mai avansate cunoştinţe în comunitatea militară academică şi de formare a unei unităţi de doctrină în armată, în fiecare Buletin erau expuse diferite subiecte pentru a fi, astfel, mai bine urmărite şi aplicate: defensiva, ofensiva, cavaleria, infanteria, artileria, geniul, mijloacele mecanizate etc.

Apariţia Buletinului a fost considerată unul dintre cele mai importante obiective ale Şcolii Superioare de Război în rolul ei de răspândire a cunoştinţelor militare superioare în armată, despre care directorul de atunci, generalul adjutant Paul Teodorescu, a spus: „Păşim cu încredere în greaua misiune pe care, din dragostea de a servi instituţia, ne-o asumăm”[12].

Modificările continue la nivelul învăţământului superior militar din România şi, mai ales, cele produse în diseminarea informaţiilor au afectat mijloacele de comunicare şi de utilizare la nivelul cunoaşterii umane. Schimbările politice, economice şi sociale, produse de-a lungul timpului, au avut o puternică influenţă şi asupra modului de informare a specialiştilor militari implicaţi în procesul de învăţământ.

Noile tehnologii ale informării şi fenomenele sociale, generate de mass-media în vederea informării şi comunicării tuturor generaţiilor, au dus la noi practici de comunicare, la o revoluţie în practica muncii intelectuale, conducând invariabil la preeminenţa folosirii unui text în defavoarea lecturii tradiţionale. În acest context, Buletinul Universităţii Naţionale de Apărare „Carol I” reprezintă, în prezent, un forum de dezbatere şi analiză pentru mediile academice şi profesionale, revista fiind deschisă, în egală măsură, cadrelor didactice, cercetătorilor, doctoranzilor şi postdoctoranzilor, studenţilor, personalului militar şi civil din instituţii aparţinând domeniului apărării, ordinii publice şi securităţii naţionale.

Au fost permanent analizate importanţa şi rolul publicaţiei în dezvoltarea demersului de învăţare şi cercetare şi au fost aplicate soluţii care includ, în prezent, pe lângă publicarea în mediul online, şi apariţia unui număr în limba engleză, cu periodicitate trimestrială, sub titlul: ”Bulletin of Carol I National Defence University”, ambele publicaţii fiind disponibile la adresa http://buletinul.unap.ro/.

Începând din anul 2011, Buletinul Universităţii Naţionale de Apărare „Carol I” este o publicaţie cu prestigiu recunoscut în domeniul „Ştiinţe militare, informaţii şi ordine publică” al Consiliului Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare, indexat şi în baze de date internaţionale.

Evoluţia spectaculoasă a tehnologiilor a declanşat valul schimbărilor şi în ceea ce priveşte nivelul comunicaţiilor şi rolul jucat de acestea în societatea contemporană. Tematica Buletinului a cunoscut o extindere spre zone rezervate până acum specialiştilor din alte domenii, şi conţinutul articolelor a fost în permanenţă reconsiderat.

Modalitatea de învăţare instituţională, dar şi cea individuală în cadrul armatei sunt esenţiale în momentul de faţă, asigurând abilităţile necesare accesului în lumea structurilor infodocumentare din mediul digital. Cele mai vizibile sunt cele care privesc tipologia documentelor în era digitală, provocări la care oamenii trebuie să fie dispuşi şi capabili să se adapteze în permanenţă. De exemplu, e-learning este considerată o oportunitate de învăţare care duce la evoluţia capacităţii de efectuare a muncii independente, dar şi la capacitatea de fi parte a unei echipe în care Buletinul Universităţii Naţionale de Apărare „Carol I” răspunde „prezent la apel” prin varianta sa online.

Atributele necesare funcţionării la standarde ridicate, menite să facă faţă rapid schimbărilor organizaţionale, se regăsesc în modul actual de prezentare a Buletinului: flexibilitate, creativitate, lucru în echipă, colaborare, capacitate de sinteză, curiozitate intelectuală şi experienţa culturală semnificativă a celor 82 de ani parcurşi.

Apariţia trimestrială a început din anul 1956 şi continuă până în prezent. Denumirea a fost schimbată de-a lungul vremii, în strânsă legătură cu titulatura oficială a instituţiei, astfel că, în anul 1991, numele a fost schimbat în „Buletinul Academiei de Înalte Studii Militare”[13], apoi, în anul 2003, în „Buletinul Universităţii Naţionale de Apărare”[14], iar, din anul 2005, poartă actuala denumire: „Buletinul Universităţii Naţionale de Apărare «Carol I»”[15].

Din documentele păstrate în arhive şi din mărturiile contemporanilor la evoluţia şi transformarea instituţiei de la Şcoala Superioară de Război la Universitatea Naţională de Apărare „Carol I”, am selectat şi anul 1939, care a fost dedicat celei de-a 50-a aniversări de existenţă a sa, prilej cu care a fost inaugurat cu fast, la 6 decembrie, sediul actual al instituţiei, deşi cel de-al Doilea Război Mondial începuse deja în Europa.

Momentul a fost pregătit începând cu doi ani în urmă, în anul 1937, cu apelul, repetat timp de doi ani în ziare, la radio, în Monitorul Oastei (nr. 1 – 12/1938), făcut foştilor studenţi şi profesori pentru strângerea materialului documentar necesar alcătuirii unui album al absolvenţilor, o carte a amintirilor, a unei statistici a activităţii şcolii, pentru alcătuirea unui muzeu cu obiecte, documente şi fotografii etc. (Anexele nr. 3, 4).

În urma demersurilor făcute a fost publicată o operă unică: „Cartea amintirilor absolvenţilor 1889 - 1939”, din păcate într-un singur exemplar, care se află la Muzeul Militar din Bucureşti.

Izvor incontestabil de informaţii deosebit de preţioase pentru împlinirile şi avatarurile primilor 50 de ani din viaţa instituţiei, de interes pentru mediul academic, dar şi pentru publicul larg, „Cartea amintirilor absolvenţilor 1889-1939” reprezintă o lucrare pentru care s-ar impune o lărgire a gradului de accesibilitate, de ce nu, o ediţie anastatică a acestei lucrări, ca un omagiu pentru cei care au slujit aici, atunci, şi ca un bun exemplu pentru urmaşi.

Anul 1939 rămâne ca un moment de bilanţ al primilor 50 de ani de activitate ai Şcolii Superioare de Război, ani în care au fost scrise 3.270 de lucrări de specialitate, dintre care 309 lucrări de istorie militară, 258 de tactica infanteriei, 196 de tactica artileriei etc.[16]

Anii 1919, 1937 şi 1939, asupra cărora am aruncat aceste câteva priviri, reprezintă etape de dezvoltare în lungul şir de evenimente care au marcat cei 130 de ani de existenţă ai Universităţii Naţionale de Apărare „Carol I”.

Am ilustrat cu imagini de arhivă acest mic tablou, pentru a simţi întru câtva parfumul epocii trecute şi pentru a reprezenta aşa cum se cuvine aceste piese de puzzle, care alcătuiesc acum tabloul vieţii noastre cotidiene, a celor care ducem mai departe cu mândrie mottoul instituit de regele Carol I: *LABOR IMPROBUS OMNIA VINCIT!*

*Ad multos annos*, Universitate Naţională de Apărare „Carol I”!

## ANEXE

**Anexa nr. 1**

## DECRETUL DE ÎNFIINŢARE A ŞCOLII SUPERIOARE DE RĂZBOI

*Înalt Decret 2073/8 august 1889*
*CAROL I,*
*Prin graţia lui Dumnezeu şi voinţa naţională, rege al României, la toţi de faţă şi viitori, sănătate.*

*Având în vedere articolul 4 al legii din martie 1883, asupra serviciului de stat major, asupra raportului ministrului nostru secretar de stat la Departamentul de Război nr. 14.498, am decretat şi decretăm:*

*Art. 1. Se înfiinţează pe lângă Marele Stat Major o Şcoală Superioară de Război, destinată a forma ofiţeri de stat major.*

*Art. 2. Recrutarea ofiţerilor elevi pentru această şcoală se va face conform legii, prin concurs între locotenenţi şi căpitani de toate armele, care vor avea cel puţin doi ani de serviciu efectiv la o trupă, cu o bună conduită şi o constituţie fizică sănătoasă.*

*Art. 3. Numărul elevilor ce se vor admite va fi acum, la început, de zece. Ofiţerii elevi vor fi detaşaţi de la corpurile lor şi vor purta uniforma armei lor.*

*Art. 4. Examenul de admitere va fi scris, oral şi practic. El va consta din patru probe: proba scrisă, compusă din două compoziţii, din care una în limba franceză sau germană, proba orală asupra materiilor din program, proba practică constând într-o ridicare cu planşeta de recunoaştere pe teren şi proba de echitaţie.*

*Art. 5. Materiile concursului vor fi următoarele: legislaţia şi administraţia militară, arta şi istoria militară, artileria, fortificaţia, geografia, topografia, regulamnetele de infanterie, cavalerie şi artilerie.*

*Art. 6. Cursurile şcolii vor fi de doi ani. Vor începe în fiecare an la 1 noiembrie şi se vor termina la 1 iunie anul viitor, la de la 1 iunie la 1 octombrie, elevii vor fi exercitaţi pe teren la lucrări topografice, călătorii de stat major, călătorii pe graniţă şi participare la manevrele anuale.*

*Art. 7. Examenele vor avea loc în fiecare an, pe cursuri, îndată ce unul este terminat, iar examenul general va avea loc în luna octombrie a anului al 2-lea de studiu, asupra tuturor materiilor predate în şcoală şi înaintea juriului compus cum se va prescrie mai jos.*

*Afară de examene elevii vor fi supuşi la interogaţiuni asupra cursurilor şi vor executa în fiecare lună cel puţin o compoziţie scrisă la materiile hotărâte de direcţia studiilor.*

*Elevii vor fi exercitaţi la exerciţiul tactic al celor trei arme.*

*Exerciţiul pe teren se va face cu unităţi de garnizoană.*

*Art. 8. Toate cursurile vor fi obligatorii şi următoarele:*

### Anul I

| | |
|---|---|
| *Istoria militară* | *30 lecţii* |
| *Tactica infanteriei* | *24 lecţii* |
| *Tactica cavaleriei* | *12 lecţii* |
| *Mobilizarea* | *14 lecţii* |
| *Geografia militară generală* | *20 lecţii* |
| *Artileria şi tactica sa* | *25 lecţii* |
| *Fortificaţia* | *20 lecţii* |
| *Limba franceză* | *20 lecţii* |
| *Limba germană* | *20 lecţii* |

**Anul al II-lea**

| | |
|---|---|
| *Istoria militară* | *30 lecţii* |
| *Tactica şi strategia generală* | *15 lecţii* |
| *Geografia militară a României* | *10 lecţii* |
| *Telegrafia militară* | *10 lecţii* |
| *Căi ferate* | *10 lecţii* |
| *Serviciul de stat major* | *25 lecţii* |
| *Fortificaţia* | *15 lecţii* |
| *Administraţia* | *20 lecţii* |
| *Dreptul internaţional* | *15 lecţii* |
| *Limba germană* | *20 lecţii* |
| *Limba franceză* | *20 lecţii* |

*Programele analitice se vor face de profesorii respectivi şi se vor aproba în prealabil de Comitetul Consultativ de Stat Major.*

*Art. 9. Profesorii acestei şcoli se vor numi de ministrul de Război, după propunerea Comitetul Consultativ de Stat Major.*

*Art. 10. Juriul de examinare, atât pentru admitere în şcoală, cât şi pentru absolvire, se va compune din trei ofiţeri superiori, brevetaţi din cele trei arme, şi doi membri din Comitetul Consultativ de Stat Major, din care unul preşedinte.*

*Juriul de examinare pentru admitere în şcoală va constata, după memoriile şi recomandările ofiţerilor candidaţi, conduita şi aptitudinea lor militară, şi un medic superior militar va da avizul său asupra constituţiei fizice a candidaţilor. Cei recunoscuţi improprii vor fi eliminaţi de la concurs.*

*Şeful Statului Major General va avea supravegherea atât asupra mersului, cât şi asupra examenelor în general.*

*Art. 11. La finele anului întâi, ofiţerii elevi, care se vor dovedi prin examenele parţiale că nu pot urma mai departe, se vor aduce înaintea juriului examinator, care se va pronunţa în mod definitiv şi, după raportul şefului Statului Major General, se vor trimite la corpurile lor.*

*De asemenea, la finele anului al II-lea, ofiţerii elevi care nu vor lua examenul de absolvire vor fi trimişi la corpurile lor.*

*Repetări de clase nu se vor admite sub niciun motiv.*

*Art. 12. Ofiţerii absolvenţi ai Şcolii Superioare de Război vor fi clasaţi pe rând de merit*[17]*, se va primi brevetul de stat major şi vor fi trimişi a face un stagiu de instrucţie de câte un an în corpuri de trupă, la o altă armă decât aceea de unde au venit, şi acolo vor comanda cel puţin timp de 6 luni o companie, baterie sau escadron.*

*Art. 13. După stagiul de instrucţie la trupă, ofiţerii brevetaţi vor fi chemaţi, în rândul clasării lor de merit, a face stagiul de stat major 2 ani la Marele Stat Major şi 1 an în statele majore de corp de armată şi divizie.*

*Dacă în timpul stagiului la trupă şi în serviciile succesive de stat major se va constata că unii din ofiţerii brevetaţi nu corespund condiţiilor de aptitudine cerute, acei ofiţeri, după propunerea şefului de Stat Major General şi avizul Comitetului Consultativ de Stat Major, vor fi înapoiaţi la armele lor.*

*Art. 14. Un regulament interior al şcolii se va elabora de ministrul nostru secretar de stat la Departamentul de Război, care este însărcinat cu executarea decretului de faţă.*

*Dat în Castelul Peleş, la 8 august 1889.*

*CAROL*

*Ministru de Război*
*General Gheorghe Manu*

Monitorul Oastei nr. 55/ 19 august 1889, pp. 891-894.

**Anexa nr. 2**

# DECRETUL DE ÎNFIINŢARE A „SECŢIEI DE INTENDENŢĂ” ÎN CADRUL ŞCOLII SUPERIOARE DE RĂZBOI, 6 NOIEMBRIE 1919

Anexa Nr. 2.-
50

FERDINAND I

Prin graţia lui Dumnezeu şi voinţa naţională, Rege al României,

La toţi de faţă şi viitori, sănătate :

Asupra raportului Ministrului Nostru Secretar de Stat la Departamentul de Războiu, sub Nr.1298,

AM DECRETAT SI DECRETAM :

Art.1. Se înfiinţează pe lângă Scoala Superioară de Războiu "O secţie de intendenţă" cu scopul :

a) A pregăti ofiţerii de diferite arme şi servicii cari doresc să intre în serviciul intendenţei.

b) In mod excepţional şi pentru ca scopul dela litera a) să poată fi pus în practică, a cpmpleta cunoştinţele generale şi tehnice speciale ale actualilor ofiţeri de intendenţă spre a fi utili comandamentelor în ceea ce priveşte organizarea, mobilizarea şi conducerea serviciilor administrative.

Art.2. Admiterea la Scoala Superioară de Războiu "secţia intendenţei" se va face prin concurs. Epoca examenului de admitere şi condiţiunile vor fi aceleaşi ca pentru ofiţerii combatanţi cari intră în şcoala Superioară de Războiu.

Pentru anul acesta se vor putea prezenta la concursul de admitere toţi intendanţii căpitani şi maiori cari nu trec vârsta de ani la 1 Ianuarie 1920.

Art.3. Concursul de admitere atât pentru anul acesta cât şi pentru viitor, va consta dintr'o probă scrisă şi una orală, referitoare la cunoştinţe generale şi cunoştinţe tehnice speciale, după cum urmează :

a) Cunoştinţe generale: Istoria şi Geografia generală, Noţiuni de drept civil, comercial, constituţional şi administrativ, Noţiuni de finanţe şi economie politică.

b) Cunoştinţe militare, speciale tehnice : Legislaţie şi administraţie militară cum şi toate legile şi regulamentele în legătură cu acestea ; organizarea şi funcţionarea serviciului de subzistenţă ; Noţiuni de chimie alimentară; citirea hărţilor.

Art.4. Durata cursurilor va fi de doi ani, urmându-se regimul prevăzut în regulamentul Scoalei Superioare de Războiu.

Art.5. Numărul ofiţerilor ce se va admite în şcoală se va hotărî anual prin decizie ministerială, potrivit cu nevoile serviciului administrativ al armatei şi cu rezultatul concursului.

·/.

57

Art.6. Anul acesta concursul de admitere va avea loc la M.St.M. (Scoala Superioară de Războiu) în prima jumătate a lunei Decemvrie.

Cererile de admitere la concurs,înaintate prin corpurile de trupă,comandamentele şi serviciile respective însoţite de aprecierile tuturor şefilor erarhici,vor trebui să sosească la M.St.M. (Scoala Superioară de Războiu),cel mai târziu la 1 Decemvrie 1919.

Pentru viitor admiterea la concurs se va face potrivit dispozitiunilor ce se vor prevedea în regulamentul Scoalei Superioare de Războiu (pentru secţia Intendenţei).

Art.7. Toate dispoziţiunile de detaliu relative la : funcţionarea secţiei de intendenţă,profesori,personalul de cadre al şcoalei,cursuri,programe,sisteme de cotare,examene, etc. se vor stabili într'un regulament special,ce va forma o anexă a regulamentului Scoalei Superioare de Războiu.

Art.8. Ministru Nostru Secretar de Stat la Departamentul de Războiu este însărcinat cu executarea decretului de faţă.

Dat la Castelul Peleş, la 6 Noemvrie 1919.

FERDINAND.

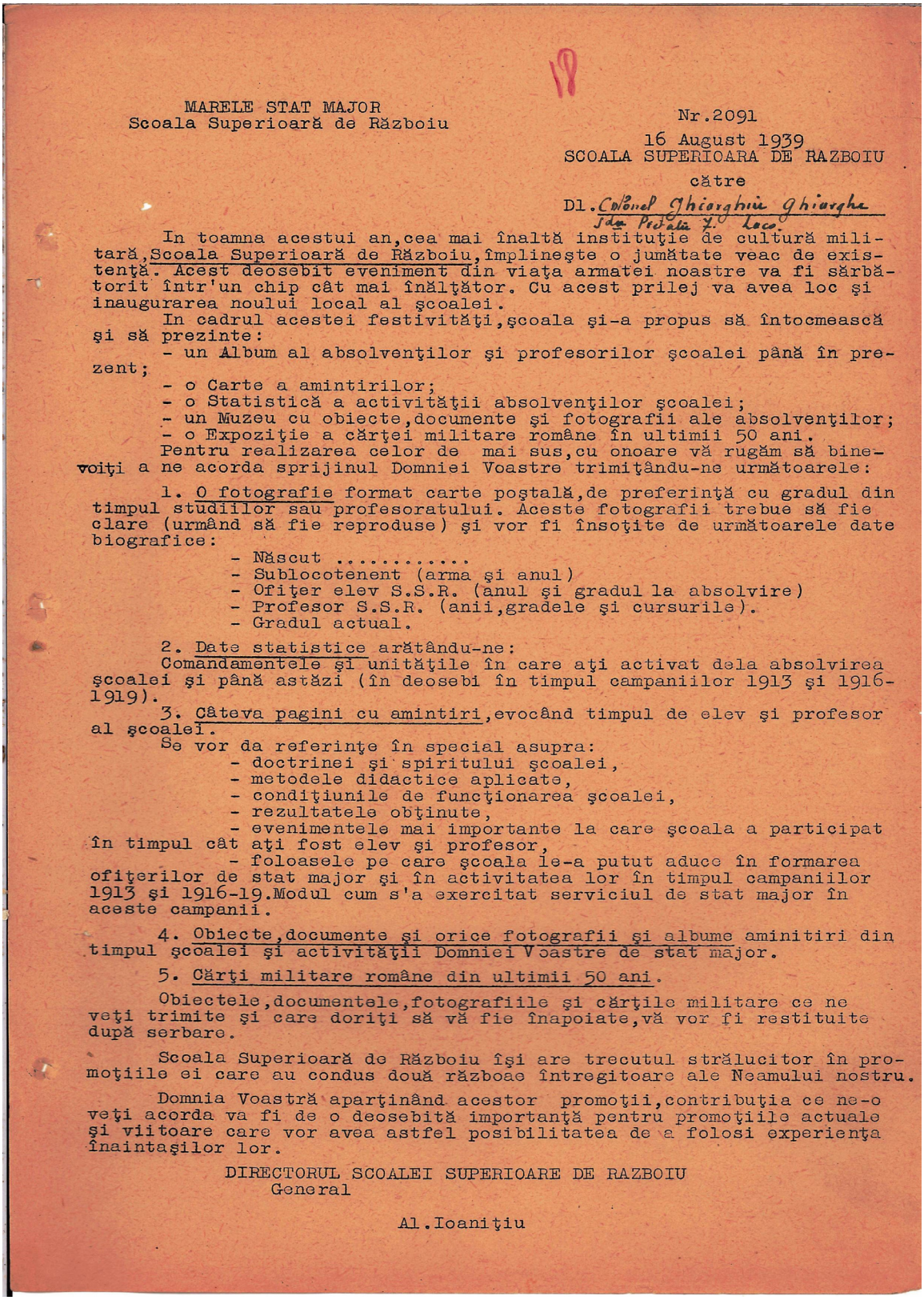
MINISTRU DE RAZBOIU
GENERAL DE BRIGADA
Ion Răşcanu

Nr. 4729

Arhivele Militare Naţionale Române, Fond Şcoala Superioară de Război, dosar nr. 417, fila 50-51.

**Anexa nr. 3**

# APELUL PENTRU STRÂNGEREA MATERIALULUI DOCUMENTAR LA 50 DE ANI DE EXISTENȚĂ A ŞCOLII SUPERIOARE DE RĂZBOI, DIN ANUL 1937



MARELE STAT MAJOR
Scoala Superioară de Războiu

Nr.2091
16 August 1939
SCOALA SUPERIOARA DE RAZBOIU

către

Dl. Colonel Ghiorghiu Ghiorghe
Ida Prefata 7. Loco.

In toamna acestui an, cea mai înaltă instituţie de cultură militară, Scoala Superioară de Războiu, împlineşte o jumătate veac de existenţă. Acest deosebit eveniment din viaţa armatei noastre va fi sărbătorit într'un chip cât mai înălţător. Cu acest prilej va avea loc şi inaugurarea noului local al şcoalei.

In cadrul acestei festivităţi, şcoala şi-a propus să întocmească şi să prezinte:

- un Album al absolvenţilor şi profesorilor şcoalei până în prezent;
- o Carte a amintirilor;
- o Statistică a activităţii absolvenţilor şcoalei;
- un Muzeu cu obiecte, documente şi fotografii ale absolvenţilor;
- o Expoziţie a cărţei militare române în ultimii 50 ani.

Pentru realizarea celor de mai sus, cu onoare vă rugăm să binevoiţi a ne acorda sprijinul Domniei Voastre trimiţându-ne următoarele:

1. O fotografie format carte poştală, de preferinţă cu gradul din timpul studiilor sau profesoratului. Aceste fotografii trebue să fie clare (urmând să fie reproduse) şi vor fi însoţite de următoarele date biografice:
   - Născut .....
   - Sublocotenent (arma şi anul)
   - Ofiţer elev S.S.R. (anul şi gradul la absolvire)
   - Profesor S.S.R. (anii, gradele şi cursurile).
   - Gradul actual.
2. Date statistice arătându-ne:
   Comandamentele şi unităţile în care aţi activat dela absolvirea şcoalei şi până astăzi (în deosebi în timpul campaniilor 1913 şi 1916-1919).
3. Câteva pagini cu amintiri, evocând timpul de elev şi profesor al şcoalei.
   Se vor da referinţe în special asupra:
   - doctrinei şi spiritului şcoalei,
   - metodele didactice aplicate,
   - condiţiunile de funcţionarea şcoalei,
   - rezultatele obţinute,
   - evenimentele mai importante la care şcoala a participat în timpul cât aţi fost elev şi profesor,
   - foloasele pe care şcoala le-a putut aduce în formarea ofiţerilor de stat major şi în activitatea lor în timpul campaniilor 1913 şi 1916-19. Modul cum s'a exercitat serviciul de stat major în aceste campanii.
4. Obiecte, documente şi orice fotografii şi albume aminitiri din timpul şcoalei şi activităţii Domniei Voastre de stat major.
5. Cărţi militare române din ultimii 50 ani.

Obiectele, documentele, fotografiile şi cărţile militare ce ne veţi trimite şi care doriţi să vă fie înapoiate, vă vor fi restituite după serbare.

Scoala Superioară de Războiu îşi are trecutul strălucitor în promoţiile ei care au condus două războae întregitoare ale Neamului nostru.

Domnia Voastră aparţinând acestor promoţii, contribuţia ce ne-o veţi acorda va fi de o deosebită importanţă pentru promoţiile actuale şi viitoare care vor avea astfel posibilitatea de a folosi experienţa înaintaşilor lor.

DIRECTORUL SCOALEI SUPERIOARE DE RAZBOIU
General

Al. Ioaniţiu

Arhivele Militare Naţionale Române, Fond Şcoala Superioară de Război, dosar nr. 413, f. 18.

**Anexa nr. 4**

# REVENIRE LA PRIMUL APEL (CEL DIN ANUL 1937) PENTRU OMAGIEREA ŞCOLII SUPERIOARE DE RĂZBOI, ÎN ANUL 1939

32

MARELE STAT MAJOR
Scoala Superioară de Războiu.

SEMICENTENARUL SCOALEI
SUPERIOARE DE RAZBOIU.
1889 - 1939

A P E L
către
Absolvenţii şi Profesorii Scoalei Superioare de Războiu şi Scoalei Superioare de Intendenţă.

In toamna acestui an, cea mai înaltă instituţie de cultură militară, Scoala Superioară de Războiu, împlineşte o jumătate veac de existenţă. Acest deosebit eveniment din viaţa armatei noastre va fi sărbătorit într'un chip cât mai înălţător. Cu acest prilej va avea loc şi inaugurarea noului local al şcoalei.

In cadrul acestei festivităţi, Scoala şi-a propus să întocmească şi să prezinte :

- un Album al absolvenţilor şi profesorilor şcoalei până în prezent;
- o Carte a amintirilor;
- o Statistică a activităţei absolvenţilor şcoalei;
- un Muzeu cu obiecte,documente şi fotografii ale absolvenţilor;
- o Expoziţie a cărţei militare române în ultimii 50 ani.

Pentru realizarea celor de mai sus, sunteţi rugaţi a ne acorda sprijinul trimiţându-ne imediat următoarele :

1. O fotografie format carte postală,de preferinţă cu gradul din timpul studiilor sau profesoratului. Aceste fotografii să fie clare urmând să fie reproduse; vor fi însoţite de următoarele date biografice:
   - Născut .....
   - Sublocot.(arma şi anul)
   - Ofiţer elev S.S.R.(anul şi gradul la absolvire)
   - Profesor S.S.R.(anii , gradele şi cursurile),
   - Gradul actual.

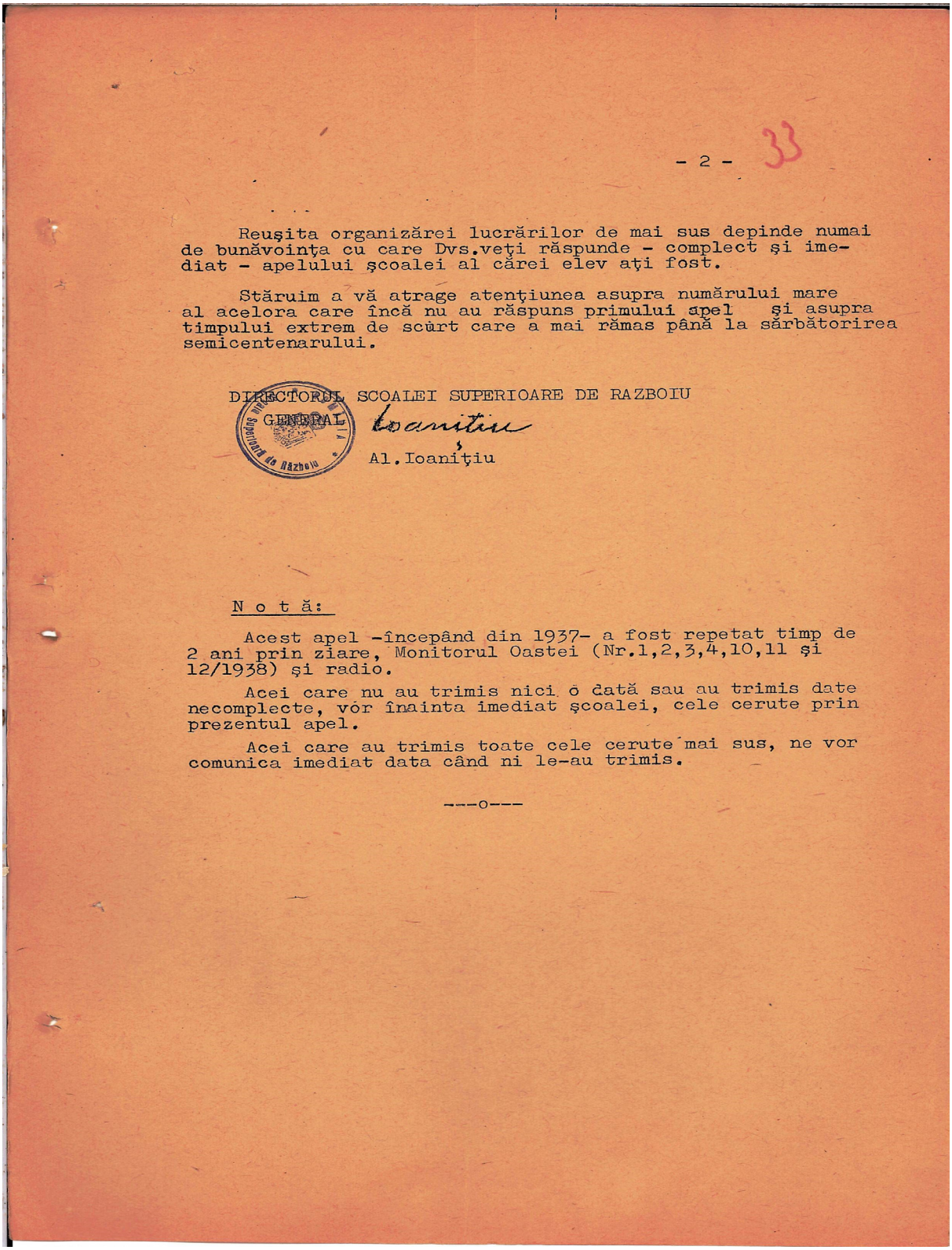
2. Date statistice arătându-ne :
Comandamentele şi unităţile în care aţi activat dela absolvirea şcoalei şi până astăzi (în deosebi în timpul campaniilor 1913 şi 1916-1919).

3. Câteva pagini cu amintiri,evocând timpul de elev şi profesor al şcoalei.
Se vor da referinţe în special asupra :
- doctrinei şi spiritului şcoalei,
- metodele didactice aplicate,
- condiţiunile de funcţionarea şcoalei,
- rezultatele obţinute,
- evenimentele mai importante la care şcoala a participat în timpul cât aţi fost elev şi profesor,
- foloasele pe care şcoala le-a putut aduce în formarea ofiţerilor de stat major şi în activitatea lor în timpul campaniilor 1913 şi 1916-19. Modul cum s'a exercitat serviciul de stat major în aceste campanii.

4. Obiecte, documente şi orice fotografii şi albume amintiri din timpul şcoalei şi activităţei Dvs.de stat major.

5. Cărţi militare române din ultimii 50 ani.

./.



- 2 - 33

Reuşita organizării lucrărilor de mai sus depinde numai de bunăvoinţa cu care Dvs.veţi răspunde - complect şi imediat - apelului şcoalei al cărei elev aţi fost.

Stăruim a vă atrage atenţiunea asupra numărului mare al acelora care încă nu au răspuns primului apel şi asupra timpului extrem de scurt care a mai rămas până la sărbătorirea semicentenarului.

DIRECTORUL SCOALEI SUPERIOARE DE RAZBOIU
GENERAL
Ioanitiu
Al.Ioaniţiu

N o t ă:

Acest apel -începând din 1937- a fost repetat timp de 2 ani prin ziare, Monitorul Oastei (Nr.1,2,3,4,10,11 şi 12/1938) şi radio.

Acei care nu au trimis nici o dată sau au trimis date necomplecte, vor înainta imediat şcoalei, cele cerute prin prezentul apel.

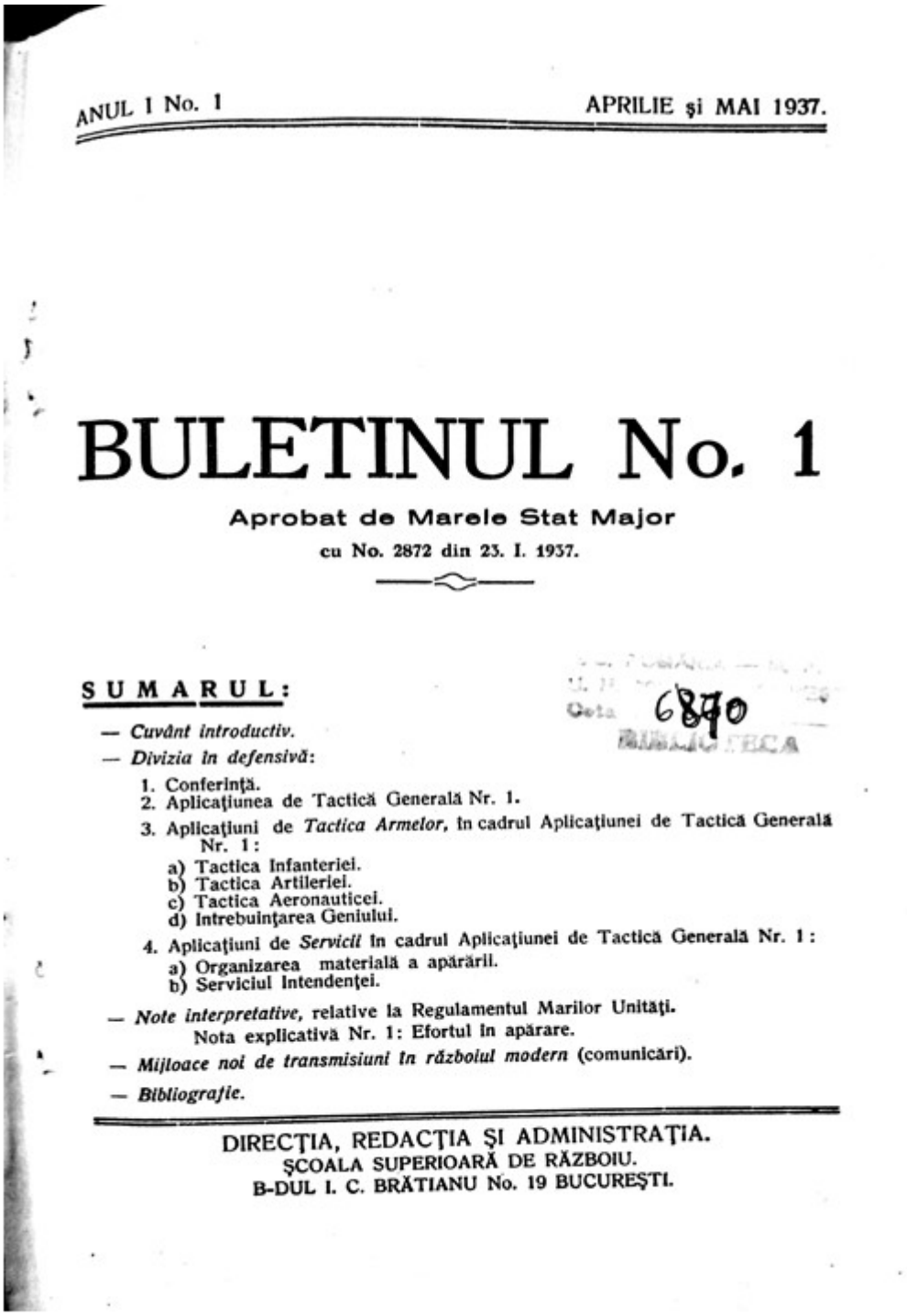
Acei care au trimis toate cele cerute mai sus, ne vor comunica imediat data când ni le-au trimis.

---o---

Arhivele Militare Naţionale Române, Fond Şcoala Superioară de Război, dosar nr. 413, f. 32-33.

**Anexa nr. 5**

## PRIMUL NUMĂR AL BULETINULUI ŞCOLII SUPERIOARE DE RĂZBOI, APRILIE - MAI 1937



ANUL 1 No. 1 — APRILIE şi MAI 1937.

# BULETINUL No. 1

**Aprobat de Marele Stat Major**
**cu No. 2872 din 23. I. 1937.**

**SUMARUL:**





DIRECŢIA, REDACŢIA ŞI ADMINISTRAŢIA.
ŞCOALA SUPERIOARĂ DE RĂZBOIU.
B-DUL I. C. BRĂTIANU No. 19 BUCUREŞTI.

# Cuvânt înainte.

*Regulamentul Şcoalei Superioare de Război, la art. 1, defineşte scopul Şcoalei astfel:*

*a) a răspândi în armată cunoştinţele militare superioare;*

*b) a procura ofiţerilor de toate armele o bază de pregătire în vederea comandei şi conducerii Marilor Unităţi, şi în vederea alegerii ofiţerilor de Stat-major.*

*Primul postulat regulamentar poate fi adus la îndeplinire prin două procedee, şi anume:*

***Unul,** cel deja practicat, prin ofiţerii absolvenţi ai Şcoalei, cu ocazia serviciului lor la trupă sau la comandamente.*

*Procedeul acesta este aşa de lent faţă de rapiditatea de astăzi a progresului ştiinţei militare, încât se riscă ca doctrina de abia răspândită în armată să devină perimată.*

*Ineficacitatea lui mai provine şi din faptul că ofiţerii tineri de Stat-major, neavând nici autoritatea necesară, nici experienţă suficientă, nu pot să impună cunoştinţele primite în Şcoală; deci răspândirea lor, şi din această cauză, lasă de dorit.*

*Trebue însă recunoscut că acest sistem are un avantaj incontestabil, acela de a se servi de elemente vii, care pot să acţioneze direct, să aplice noile idei, să convingă şi să însufleţească, pe cel cu care vin în contact.*

***Un alt** procedeu este publicaţiunea. Prin aceasta se obţine:*

*— difuzarea noilor idei, mult mai rapid, ea având loc în acelaş timp cu predarea cursurilor în Şcoală;*

*— ţinerea la curent a comandamentelor cu un material intelectual oficial, verificat prin numeroase dezbateri, foarte*

**Anexa nr. 6**

**ISTORICUL ŞCOLII SUPERIOARE DE RĂZBOI,
BUCUREŞTI 1889-1939**



# ISTORICUL

## ŞCOALEI SUPERIOARE DE RAZBOIU

## 1889–1939.


BUCUREŞTI

1939

## NOTE:

1 *Istoria Statului Major General Documente 1859 - 1947*, p. 5.

2 Ioan Scurtu, *Civilizaţia românească interbelică (1918-1940)*, Editura Fundaţiei România de Mâine, Bucureşti, 2008, p. 24.

3 Şcoala Superioară de Război, *Istoricul Şcoalei Superioare de Război 1889-1939*, Bucureşti, 1939, p. 376. Din 1919 până în 1939 au fost trimişi să studieze marea artă a războiului la Paris 49 de ofiţeri români şi la Torino, 8 ofiţeri. La acelaşi bilanţ de activitate ştiinţifică, s-a subliniat şi vasta literatură militară românească „materializată prin studii profunde şi îmbunătăţiri materiale de tot felul”.

4 Serviciul Arhivelor Naţionale Istorice Centrale (în continuare SANIC), Fond Familia Fălcoianu, dosar nr. 4, fila 1 - 4. Ştefan Fălcoianu (06.06.1835 – 22.01.1905) a absolvit Şcoala de Stat Major de la Paris în 1862, ataşat al Armatei Franceze până în anul 1864; între anii 1870 - 1877 a fost director general al Telegrafelor şi Poştelor; în anul 1876 a fost numit membru al Academiei Române, apoi a ocupat funcţia de vicepreşedinte; din 20.10.1877 a fost numit Şef de Stat Major şi a luat parte la acţiunile Armatei Române de la Plevna şi Vidin; de la 20.10.1883 a fost director al Căilor Ferate din România; la 10.03.1883 a fost avansat în gradul de general de brigadă; între 23.06.1883 şi 13.01.1886 a fost ministru de război şi inspector general al şcolilor militare în cabinetul Ion Brătianu; la 10.05.1892 a fost avansat în gradul de general de divizie; la 08.06.1894 a fost numit comandant al Corpului I al Armatei Române; la 12.06.1894 a demisionat din armată.

5 „Revista Armatei”, nr. 21-22/1889, pp. 764-765.

6 Academia Militară, Academia Militară Generală, Academia de Înalte Studii Militare, Universitatea Naţională de Apărare, Universitatea Naţională de Apărare „Carol I”, denumire primită prin Hotărârea de Guvern nr. 969/ 25 august 2005.

7 Şcoala Superioară de Război, *Istoricul Şcoalei Superioare de Război 1889-1939*, Bucureşti, 1939, p. 299.

8 *Ibidem*, p. 304.

9 Vezi articolul „80 de ani în slujba comunităţii academice militare: Buletinul Universităţii Naţionale de Apărare «Carol I» între tradiţie şi modernitate”, Laura-Rodica Hîmpă, *Buletinul Universităţii Naţionale de Apărare „Carol I”*, vol. IV, nr. 2/2017, pp. 9 - 16, www.buletinul.unap.ro

10 „Regulamentul Şcoalei Superioare de Război”, în: *Buletinul Şcolii Superioare de Război*, 1937, nr. 1, aprilie–mai, p. 5. Apariţia Buletinului a fost aprobată de Marele Stat Major, nr. 2872/23 ianuarie 1937.

11 *Ibidem*, p. 6.

12 *Ibidem*.

13 Hotărârea Guvernului României nr. 305/23 aprilie 1991.

14 Hotărârea Guvernului României nr. 1027/28 august 2003.

15 Hotărârea Guvernului României nr. 969/25 august 2005.

16 Mircea Mureşan, *Universitatea Naţională de Apărare, scurt istoric*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2004, p. 11.

17 În ordinea mediilor obţinute.

## BIBLIOGRAFIE


*** *Arhivele Naţionale Militare Române*, Fond Şcoala Superioară de Război.

*** *Arhivele Naţionale Române*, Fond Ştefan Fălcoianu.

*** *Buletinul Arhivelor Militare Române 1998-2019.*

*** *Buletinul Şcolii Superioare de Război 1937-1948.*

*** *Buletinul Universităţii Naţionale de Apărare „Carol I”.*

*** *Monitorul Oficial 1872-2019.*

*** *Monitorul Oastei 1872-1948.*

*** *Revista Armatei 1877-1948.*

*** *Revista de Istorie Militară 2010-2019.*

*** *Revista Fundaţiilor Regale 1934-1948.*

*** *Istoria Statului Major General Român. Documente 1859-1947*, Editura Militară, Bucureşti, 1994.

*** *Istoricul Şcoalei Superioare de Război, Bucureşti 1889-1939*, Tipografia Şcolii Superioare de Război, Bucureşti, 1939.

Caracostea Dumitru, *Aspectul psihologic al războiului*, Editura „Cartea Românească”, Bucureşti, 1922.

Iorga Nicolae, *Istoria învăţământului românesc*, Editura Didactică şi Pedagogică, Bucureşti, 1971.

Iorga Nicolae, *Istoria armatei româneşti*, Editura Ministerului de Război, vol. I, II, Bucureşti, 1931.

Iorga Nicolae, *Stări sufleteşti şi războaie. Lecţii la Şcoala Superioară de Război în 1938*, Tipografia Şcolii Superioare de Război, Bucureşti, 1939.

Mureşan Mircea, *Universitatea Naţională de Apărare, scurt istoric*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2004.

Scurtu Ioan, *Civilizaţia românească interbelică (1918-1940)*, Editura Fundaţiei România de Mâine, Bucureşti, 2008.

Redactor-şef: Laura MÎNDRICAN
Redactor: Irina TUDORACHE
Corectori: Mariana ROŞCA
Carmen-Luminița IACOBESCU
Tehnoredactor: Gabriela CHIRCORIAN
Coperta: Andreea GÎRTONEA

ISSN (on line) 2065 - 8281

Lucrarea conține 114 pagini.

EDITURA UNIVERSITĂŢII NAŢIONALE DE APĂRARE „CAROL I”
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
e-mail: *buletinul@unap.ro*
Tel. 319.48.80/0215; 0453

AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2015-2020
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2015-2020

BIROUL EXECUTIV AL CONSILIULUI ARACIS
EXECUTIVE BUREAU OF ARACIS

Președinte / President
Prof. univ. dr. Peiroșcu Iordan

Vicepreședinte / Vice President
Prof. univ. dr. Ghițulică Cristina

Director Departament de Evaluare Externă a Calității / Director of the Evaluation Department
Prof. univ. dr. Popa Ion

Director Departament de Acreditare / Director of the Acreditation Department
Prof. univ. dr. ing. Lache Simona

Secretar General / General Secretary
Prof. univ. dr. Stan Vasilica

Data eliberării / Release date: 29.10.2015

Nr. 129/2015

IEP
EUA-Institutional Evaluation Programme

Institutional Evaluation Programme
Performance in Research, Performance in Teaching – Quality, Diversity and Innovation in Romanian Universities Project

"CAROL I - NATIONAL DEFENCE UNIVERSITY"
BUCHAREST-ROMANIA



**Publicație științifică indexată în bazele de date internaționale CEEOL și GOOGLE SCHOLAR.**

Șoseaua Panduri, nr. 68–72, sector 5, București
e-mail: buletinul@unap.ro
Tel.: 021-319.59.69; 021-319.48.80/0215; 0453




EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
(Editură cu prestigiu recunoscut de Consiliul Național de Atestare a Titlurilor,
Diplomelor şi Certificatelor Universitare)

ISSN 1584 - 1928