GÂNDIREA MILITARĂ ROMÂNEASCĂ

FONDATĂ ÎN ANUL 1864 SUB TITLUL „ROMÂNIA MILITARĂ”
- SERIE NOUĂ, ANUL XXXI -

3/2020

REVISTĂ DE ȘTIINȚĂ MILITARĂ ȘI STUDII DE SECURITATE EDITATĂ DE STATUL MAJOR AL APĂRĂRII

ADRESA REDACȚIEI
București, str. Izvor nr. 110, sector 5
Cod poștal: 050564
Telefon: +4021.410.40.40/1001731;1001732
Tel./fax: +4021.319.56.63
E-mail: gmr@mapn.ro
Web: gmr.mapn.ro

Tiparul a fost executat
la Centrul tehnic-editorial al armatei
sub comanda __/2020 B ___

EDITOR
STATUL MAJOR AL APĂRĂRII

ÎNALTUL DECRET REGAL NR. 3663 PRIN CARE „ROMÂNIA MILITARĂ" DEVINE REVISTA OFICIALĂ A MARELUI STAT MAJOR

„Art. I - Se înființează la Marele Stat Major, cu începere de la 1 Ianuarie 1898, revistă oficială sub denumirea de „România Militară", în care toți ofițerii din armată vor găsi studii militare, care să intereseze instrucțiunea lor.

Prin organul acestei reviste toți ofițerii, de toate armele, aflați în activitate de serviciu, își vor putea publica lucrările lor personale și cari interesează armata".

Carol - Regele României
Dat în Bucuresci la 8 decembre 1897

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Revistă de ştiinţă militară şi studii de securitate
editată de Statul Major al Apărării

Fondată în anul 1864 sub titlul „România Militară”
– serie nouă, anul XXXI –

ISSN Print: 1454-0460
ISSN Online: 1842-8231

Revista *Gândirea Militară Românească* este revistă ştiinţifică
cu prestigiu recunoscut din domeniul
„Ştiinţe militare, informaţii şi ordine publică”, potrivit evaluării
făcute de către Consiliul Naţional de Atestare a Titlurilor,
Diplomelor şi Certificatelor Universitare în anul 2011
(http://www.cnatdcu.ro/wp-content/uploads/2011/11/reviste-militare1.pdf)

Revista *Gândirea Militară Românească* este inclusă în bazele de date
INDEX COPERNICUS INTERNATIONAL, EBSCO,
domeniul International Security & Counter-Terrorism Reference Center,
și Catalogul ROAD

Responsabilitatea pentru conţinutul materialelor publicate
revine în exclusivitate autorilor, în conformitate cu prevederile
Legii nr. 206 din 27.05.2004

O MOȘTENIRE DE LA 1864

Drumul spre modernitate al Oștirii Române a început în 1859, odată cu instituirea Corpului de Stat Major General al Principatelor Unite, actualmente Statul Major al Apărării.

La numai câţiva ani, în 1864, un grup de nouă căpitani, absolvenţi ai celei dintâi promoţii a Şcolii de cadeţi din Bucureşti, a avut iniţiativa creării unei *„reviste de ştiinţă, artă şi istorie militară”*, cu denumirea *„România Militară”*.

Iniţiatorii acestui demers publicistic – **G. Slăniceanu** (căpitan, şeful Batalionului de Geniu), **A. Gramont** (căpitan de stat major), **G. Borănescu** (căpitan de geniu), **G. Anghelescu** (căpitan de stat major), **A. Anghelescu** (căpitan de artilerie), **E. Arion** (căpitan de artilerie), **E. Boteanu** (căpitan de stat major), **E. Pencovici** (căpitan de stat major) şi **C. Barozzi** (căpitan de geniu) –, educaţi nu doar în România, ci şi în străinătate, erau animaţi de necesitatea dezvoltării, şi în Armata Română, a unei activităţi teoretice consistente.

Programul[1] revistei, inclus încă din primul număr, apărut la 15 februarie 1864, conţinea idei şi demersuri novatoare, cu scopul de:

„- a lucra la organizarea sistemului nostru militar, ce Camera legiuitoare este chemată în curând a-l hotărî;

- a aduna şi a cerceta instituţiile vechi militare ale Patriei, instituţii ce au făcut atâtea veacuri gloria României şi ne-au asigurat existenţa;

- a trata, în lipsă de orice uvraje militare, tot ce se raportă la instrucţia Oastei, baza cea mai solidă a armatei;

- a întreţine pe Oşteanul Român cu cunoştinţa evenimentelor militare ce se petrec în lume;

- a veni să lucrăm împreună şi din toată inima la înălţarea şi consolidarea edificiului ce este menit să asigure viitorul patriei noastre”[2].

Publicaţie independentă, dar aflată sub egida Ministerului de Război, *„România Militară”* şi-a încetat apariţia în 1866, din lipsă de fonduri şi de abonaţi. Va reapărea după un sfert de veac, în 1891, tot la iniţiativa unui grup de ofiţeri din Marele Stat Major, care îşi propuneau *„reproducerea studiilor serioase de organizare, de strategie, de arta de a conduce trupele în orice circumstanţe”*[3]. La scurt timp, prin Înaltul Decret Regal nr. 3663 din 8 decembrie 1897, *„România Militară”* a devenit, de la 1 ianuarie 1898, *„organul oficial de publicitate al Marelui Stat Major”.*

C. Barozzi
(căpitan de geniu)

E. Pencovici
(căpitan de stat major)

E. Boteanu
(căpitan de stat major)

G. Borănescu
(căpitan de geniu)

G. Anghelescu
(căpitan de stat major)

G. Slăniceanu
(căpitan, şeful Batalionului de Geniu)

E. Arion
(căpitan de artilerie)

A. Anghelescu
(căpitan de artilerie)

---

[1] *Din trecutul României Militare cu prilejul aniversării a 75 de ani de la apariţia ei în viaţa armatei. 1864-1939*, Bucureşti, 1939, p. 31.

[2] *Ibidem*, p. 32.

[3] *România Militară*, nr. 1, 1891, p. 6.

Premiile revistei GÂNDIREA MILITARĂ ROMÂNEASCĂ se acordă în fiecare an, de către Statul Major al Apărării, celor mai valoroase lucrări din domeniul ştiinţei militare, editate în anul precedent

Premiul „General de brigadă Constantin Hîrjeu“

Premiul „Locotenent-colonel Mircea Tomescu“

Premiul „General de divizie Ștefan Fălcoianu“

Premiul „General de corp de armată Ioan Sichitiu“

Premiul „Mareșal Alexandru Averescu“

CUPRINS

EDITORIAL	Gheorghiță VLAD	6	REZILIENȚA SOCIETĂȚII ÎN CONTEXTUL PANDEMIEI COVID-19 ȘI ROLUL ARMATEI ÎN ACEST PROCES
SECURITATE ÎN CONTEXT PANDEMIC	Petre SCÎRLET Cristian ICHIMESCU	10	CONFLICTELE/OPERAȚIILE INFORMAȚIONALE ALE FEDERAȚIEI RUSE ÎN CONTEXTUL *SARS-COV-2*
	Alba I.C. POPESCU	24	ARME BIOLOGICE ȘI VECTORI PANDEMICI
ȘTIINȚĂ MILITARĂ	Răzvan GRIGORAȘ	54	PROSPECTIVA SECURITĂȚII – IZVOR AL GÂNDIRII MILITARE ROMÂNEȘTI –
	Lucian Valeriu SCIPANOV	68	POSIBILE SOLUȚII DE REALIZARE A UNEI STRATEGII NAȚIONALE DE SECURITATE. IDENTIFICAREA LOCULUI STRATEGIEI MARITIME
	Cătălin CHIRIAC	88	DESIGNUL OPERAȚIEI LA NIVEL TACTIC
	Romică CERNAT	98	RĂZBOIUL CIBERNETIC ȘI TERORISMUL CIBERNETIC. TRĂSĂTURI ȘI RĂSPUNSURI LA ACESTE AMENINȚĂRI
INFORMAȚII ȘI SECURITATE	Gheorghe BOARU Iulian Marius IORGA	116	SECURITATEA INFORMAȚIILOR ȘI A SISTEMELOR INFORMAȚIONALE MILITARE
	Marian-Valentin BÎNĂ Cristian DRAGOMIR	148	UTILIZAREA MASS-MEDIEI CA INSTRUMENT AL RĂZBOIULUI HIBRID
	Viorica Ionela TRINCU	164	CAMPANIILE DE DEZINFORMARE – COMPONENTE IMPORTANTE ALE RĂZBIULUI HIBRID –
OPINII	Mădălina Virginia ANTONESCU	178	PROTECȚIA MEDIULUI ÎN CAZUL CONFLICTELOR ARMATE
	Vasile BOGDAN Viorel MIHALCEA	200	DESPRE EUROREGIUNILE DE COOOPERARE TRANSFRONTALIERĂ ALE ROMÂNIEI
	Sorina-Georgiana RUSU	222	NEVOIA PREGĂTIRII ORAȘELOR PENTRU DESFĂȘURAREA OPERAȚIILOR MILITARE
ISTORIE MILITARĂ	Ion RÎȘNOVEANU	230	APĂRAREA FIXĂ MARITIMĂ ÎN SECTORUL ROMÂNESC AL MĂRII NEGRE ÎN PERIOADA INTERBELICĂ ȘI ÎNCEPUTUL CELUI DE-AL DOILEA RĂZBOI MONDIAL
	Sorin APARASCHIVEI	246	NICOLAE ȘTEFĂNESCU – ÎN SERVICIUL STATULUI ȘI AL NAȚIUNII ROMÂNE –
	Dan-Dragoș SICHIGEA	274	MISIUNEA NAVALĂ FRANCEZĂ ÎN ROMÂNIA – EFORTURI PENTRU SEMNAREA UNOR CONTRACTE DE ÎNZESTRARE NAVALĂ LA ÎNCHEIEREA PRIMULUI RĂZBOI MONDIAL –

REZILIENȚA SOCIETĂȚII ÎN CONTEXTUL PANDEMIEI COVID-19 ȘI ROLUL ARMATEI ÎN ACEST PROCES

General-maior Gheorghiță VLAD
Locțiitorul pentru operații și instrucție al șefului Statului Major al Apărării

Lumea se confruntă, de la începutul anului 2020, cu o criză medicală – pandemie care ar putea fi clasificată în categoria known knowns – pericole cunoscute. Istoria omenirii a mai înregistrat astfel de situații. Ne sunt cunoscute, deoarece au fost imortalizate prin artă, literatură sau filme – atât din perspective istorice, cât și futurist-distopice. De asemenea, au existat avertismente de-a lungul timpului, din partea organizațiilor internaționale din domeniul sănătății, despre un astfel de risc privind securitatea medicală. Cu toate acestea, pandemia generată de coronavirusul SARS-CoV-2, care determină boala COVID-19, este scenariul de securitate pentru care omenirea, în general, a fost foarte puțin pregătită.

Încadrarea unei pandemii ca problemă de securitate nu înseamnă „este timpul să intrați în panică", nici că o pandemie ar trebui să fie echivalată cu un război sau cu o problemă militară. Cu toate acestea, este, cu siguranță, o problemă de securitate. Ca atare, gestionarea situației necesită minți lucide și cele mai bune informații posibile, deseori în condițiile în care datele sunt incomplete sau insuficiente. Acest tip de criză

GÂNDIREA MILITARĂ ROMÂNEASCĂ

ilustrează natura complexă a securității, în care sunt implicați mai mulți actori, iar o bună cooperare civil-militară este esențială pentru înțelegerea imaginii de ansamblu.

Pandemia COVID-19 nu face parte din provocările care se încadrează în mod obișnuit în securitatea militarizată (utilizarea forței), dar ne-a dovedit că ar putea, totuși, destabiliza societăți întregi.

Prin urmare, nu este o mare surpriză faptul că, atunci când lucrurile au devenit cu adevărat complicate, armata a fost implicată. Acest lucru nu este fără precedent. Ori de câte ori apare un dezastru natural sau provocat de om, forțele armate devin una dintre soluțiile de bază pentru guverne în generarea răspunsului lor. Majoritatea țărilor au o legislație în vigoare care permite utilizarea forțelor armate pentru a sprijini autoritățile civile în crize și situații de urgență non-militare.

Armata română a sprijinit autoritățile centrale și locale prin instalarea a trei spitale ROL 2 în București, Constanța și Timișoara, instalarea a peste 50 de unități de triaj epidemiologic în spitalele militare și civile din țară, efectuarea a aproximativ 25.000 de teste pentru depistarea COVID-19, asigurarea conducerii temporare a trei spitale județene din Suceava, Deva și Focșani. De asemenea, militarii au acționat, pe perioada stării de urgență, în aproximativ 100.000 de misiuni, au fost alături de oamenii aflați în dificultate, au distribuit aproximativ 4.000 de pachete cu produse alimentare și de igienă veteranilor și văduvelor de război în 10 județe. Militarii din Forțele Aeriene Române au efectuat peste 20 de misiuni prin care au asigurat transportul aerian a aproximativ 270 de tone de echipamente de protecție medicală, precum și evacuarea unor cetățeni români din străinătate. Cercetătorii militari au realizat, într-un timp record, o izoletă care a fost omologată și a intrat în producția de serie, precum și un demonstrator tehnologic pentru un ventilator mecanic, două produse extrem de utile sistemului medical. Nu în ultimul rând, întrucât, în astfel de momente, este nevoie, mai mult ca oricând, de solidaritate, compasiune și unitate, specialiști și cadre medicale militare au fost cooptate în echipele dislocate pentru a sprijini efortul autorităților din Republica Moldova și SUA privind gestionarea pandemiei.

Așadar, confruntându-se cu deficiențe critice în capacitățile instituțiilor civile în timpul unui dezastru major, guvernele apelează în mod firesc la capabilitățile militare. De ce reușesc militarii să gestioneze mai eficient o situație de criză, este o întrebare la care se poate răspunde cu câteva argumente ce stau la baza existenței și funcționării sistemului militar.

În primul rând, un leadership puternic este esențial. Trecerea la condiții de război necesită lideri în permanență pregătiți pentru asta, nu decidenți care neagă realitatea. Ca organizații, sistemele militare sunt configurate în mod unic pentru a face față celor mai dure condiții de război, o situație care testează, stresează și întinde limita tuturor facultăților umane – fizice, psihice și mentale. Aceasta include un spectru de capacități și capabilități pe care foarte puține alte organizații le implementează – de la comandă și control la logistică și managementul resurselor, de la asistență medicală și protecție CBRN la transport și inginerie, de la informații și supraveghere la comunicații strategice și chiar cercetare internă și dezvoltare și așa mai departe.

În al doilea rând, informațiile fac diferența. Deși nu este întotdeauna completă sau pe deplin exactă, informația stă la baza luării tuturor deciziilor militare. Navigarea prin „ceața războiului" este imposibilă fără informații. Multe autorități au ignorat semnalele de avertizare timpurie ale pandemiei, iar unele guverne nu au reușit să lanseze eforturile necesare pentru a colecta o imagine completă a răspândirii infecției în interiorul granițelor lor.

În al treilea rând, militarii sunt instruiți să considere timpul o resursă critică, ce nu poate fi recuperată atunci când este pierdută. În astfel de condiții, disponibilitatea presupune o planificare permanentă și riguroasă, care ajustează constant cursurile de acțiune și alocarea de resurse, deoarece o situație dinamică evoluează rapid și incertitudinea crește exponențial. Prin urmare, viteza de reacție și o abordare proactivă contează foarte mult. Odată ce răspândirea pandemiei a dat startul unei creșteri exponențiale în multe țări, autoritățile respective s-au aflat constant în spatele curbei, au pierdut timp prețios ca urmare a implementării unor jumătăți de măsură, fiind nevoite astfel să reacționeze mai degrabă decât să modeleze evenimentele.

În altă ordine de idei, pentru militari, „logistica este componenta care asigură succesul în luptă". Unii observatori au comparat situația medicilor lipsiți de resurse cu trimiterea trupelor militare în luptă fără armament și echipament de protecție. Militarii sunt educați în gestionarea logisticii de război și au avantajul că învață multe din istoria militară și, nu de puține ori, chiar din propria experiență. De asemenea, în mentalul militarilor, stocurile de rezervă sunt foarte importante. Ei știu că trebuie să dispună de rezerve pentru absolut orice, deoarece pierderile vor avea loc în mod inevitabil și vor trebui înlocuite rapid.

Nu în ultimul rând, pregătirea mentală și moralul sunt aspecte pe care se pune mare accent. Printr-o varietate de tehnici și practici, structurile militare își propun să mențină coeziunea unităților și moralul indivizilor aflați sub spectrul războiului. Aceste tehnici pot, în anumite cazuri, să fie replicate la nivelul societății în timpul crizelor, cum ar fi pandemia în curs de desfășurare. Un exemplu în acest sens este principiul că „nimeni nu este lăsat în urmă", care stă la baza moralului militarilor în luptă. Multe guverne și societăți au îmbrățișat această tehnică în fața pandemiei coronavirusului – nimeni nu a rămas fără sprijin în urma închiderii granițelor, persoanele în vârstă nu au fost lăsate abandonate în auto-izolare, echipe de voluntari au distribuit alimente celor aflați în nevoie etc. Acesta a fost un mesaj extrem de puternic, care a contribuit la gestionarea pandemiei, astfel încât efectul acesteia să fie cât mai limitat.

Concluzia este că organizațiile militare și membrii acestora internalizează multe elemente de rezistență în situații limită ca parte a muncii și vieții lor și, prin urmare, pot inspira, îndruma și susține societățile părinte în perioadele de nevoie, dacă li se solicită sprijinul. Dar, așa cum militarii știu bine, drumul către reziliență începe cu mult înainte de a izbucni ostilitățile războiului și se bazează adesea pe capacitatea de a menține o atenție sănătoasă asupra scenariilor pentru cele mai grave situații, chiar și atunci când vremurile sunt relaxate și pașnice.

Din actuala pandemie reiese clar că, pentru a gestiona crizele, trebuie să ne gândim critic la rolul abordărilor cuprinzătoare care implică mai mulți actori, începând de la guverne, societate civilă, sector privat, armată și poliție și, nu în ultimul rând, cetățenii din comunitățile lor.

CONFLICTELE/OPERAȚIILE INFORMAȚIONALE ALE FEDERAȚIEI RUSE ÎN CONTEXTUL *SARS-CoV-2*

Maior Petre SCÎRLET
Universitatea Națională de Apărare „Carol I”, București

Lect. univ. dr. Cristian ICHIMESCU
Universitatea Națională de Apărare „Carol I”, București

Evenimentele de mare impact global, precum pandemia Covid-19, apar foarte rar – probabil de câteva ori în decursul unui secol – și produc, printre altele, schimbări majore la nivel geopolitic, vizând alianțe, blocuri politice, regiuni, state și zone de influență.

Pandemia Covid-19 a afectat într-un timp scurt întreaga lume, iar libertatea personală a miliarde de oameni a fost îngrădită într-un mod fără precedent. Cu toate acestea, pandemia nu a înghețat diferendele existente între diverse state ale lumii.

Deși este nevoie de un răspuns global împotriva crizei coronavirusului SARS-CoV-2, Federația Rusă nu consideră că este în interesul său să contribuie în acest demers – și, de fapt, Kremlinul se folosește de criză pentru a destabiliza și mai mult lumea.

Astfel, concomitent cu virusul, cu aceeași repeziciune, se extinde în întreaga lume și o cantitate enormă de date și informații, multe dintre acestea fiind parte a unei ample campanii de influențare a opiniei publice prin conflicte/operații informaționale planificate și executate de autoritățile ruse.

Cadrul global creat prin extinderea pandemiei a reprezentat momentul operativ identificat de Kremlin pentru a pune în aplicare, din nou, mașinăria complexă reprezentată de conflictele informaționale/operațiile informaționale, care au devenit, astfel, cea mai complexă formă de confruntare modernă.

Cuvinte-cheie: activități informaționale, Covid-19, dezinformare, infodemie, operații cibernetice.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

CE SUNT CONFLICTELE/OPERAȚIILE INFORMAȚIONALE CONTEMPORANE?

Doctrina operațiilor informaționale – S.M.G.-66 – din anul 2017 definește noțiunea de *operații informaționale* ca reprezentând *„o funcție de stat major destinată analizei, planificării, evaluării și integrării tuturor activităților informaționale în vederea obținerii efectelor dorite asupra voinței, capacității de înțelegere, percepției și capabilităților adversarilor, potențialilor adversari și a audiențelor țintă aprobate de Consiliul Suprem de Apărare a Țării, în sprijinul îndeplinirii obiectivelor militare”*[1].

În anul 2009, NATO, în cadrul doctrinei AJP-3.10, *Allied Joint Doctrine for Information Operations*, a definit *operaţiile informaţionale* ca fiind *„o funcţie a statului major de a analiza, a planifica, a evalua şi a integra activităţi informaţionale pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor adversarilor, potenţialilor adversari şi audienţelor aprobate de NAC în sprijinul obiectivelor misiunii Alianţei”*[2].

NATO, în cadrul doctrinei Allied Joint Doctrine for Information Operations, a definit operaţiile informaționale ca fiind „o funcție a statului major de a analiza, a planifica, a evalua şi a integra activități informaționale pentru a crea efectele dorite asupra voinței, înțelegerii şi capabilităților adversarilor, potențialilor adversari şi audiențelor aprobate de NAC în sprijinul obiectivelor misiunii Alianței”.

Analizând definițiile prezentate, putem remarca o serie de similitudini. În viziunea celor două doctrine, operațiile informaționale se identifică prin *efectele* produse asupra a trei categorii distincte: voința; capacitatea de înțelegere și percepția; capabilități. În plus, din studierea doctrinelor menționate[3], operațiile informaționale se pun în practică prin executarea unor tipuri de activități, respectiv activități de influențare, activități împotriva conducerii și capabilităților de comandă și activități de protecție informațională.

În viziunea unor autori, pentru Federația Rusă, conceptul de conflict informațional implică *„operații în rețelele de calculatoare împreună cu operațiile psihologice, comunicare strategică, influențare”*[4]

[1] S.M.G.-66, *Doctrina operațiilor informaționale,* București, 2017, p. 15.
[2] AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009, p. 1-3. (în original: *„is a staff function to analyze, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives”*).
[3] AJP-3.10, *op. cit.*, p. 1-7, și S.M.G.-66, *op. cit.*, p. 21.
[4] Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, p. 7.

și *„informații, contrainformații, măsuri active, dezinformare, război electronic”*[5].

Putem sesiza, astfel, diferența dintre cele două accepțiuni (NATO/România vs. Federația Rusă) în sensul complexității conceptului abordat de către Kremlin, care reprezintă un concept extins, ce acoperă o gamă amplă și diversă de acțiuni. Astfel, observăm că, pentru Federația Rusă, toate domeniile formează o unitate sub conceptul de *information warfare (conflictul informațional)*, în timp ce NATO abordează conceptul *information operations (operații informaționale)*. Pe parcursul acestui articol, vom utiliza conceptul *conflictele/operațiile informaționale* pentru a caracteriza acțiunile informaționale ale Federației Ruse.

Pe tot parcursul Războiului Rece, strategia sovietică a apelat la o serie de așa-zise „măsuri active”, care descriu acțiuni și strategii menite să influențeze deciziile unui stat, populația acestuia și evenimentele politice, militare și sociale importante din statul respectiv.

O trăsătură a conflictelor/operațiilor informaționale derulate de Federația Rusă este caracterul ofensiv, care s-a regăsit în toate campaniile informaționale derulate de acest stat de-a lungul timpului împotriva diverșilor actori statali. În continuare, vom prezenta o scurtă istorie a conflictelor/operațiilor informaționale puse în practică de Federația Rusă prin utilizarea unor domenii importante, cum ar fi cel al dezinformării și al măsurilor active.

ISTORIA RUSEASCĂ A CONFLICTELOR/OPERAȚIILOR INFORMAȚIONALE

Ideile de bază pe care se susțin o parte din formele conflictelor/operațiilor informaționale derulate de Federația Rusă nu sunt noi, având origini încă din perioada Războiului Rece. Pe tot parcursul Războiului Rece, strategia sovietică a apelat la o serie de așa-zise *„măsuri active”*, care descriu acțiuni și strategii menite să influențeze deciziile unui stat, populația acestuia și evenimentele politice, militare și sociale importante din statul respectiv.

Afirmațiile conform cărora Statele Unite au comis atacuri cu arme biologice au fost acuzații comune din partea unor adversari precum URSS sau Cuba, prin care s-a încercat acreditarea ideii, la nivelul comunității internaționale, potrivit căreia Statele Unite au încălcat Convenția privind armele biologice.

[5] Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 martie 2011, http://www.rferl.org/articleprintview/2345202.html, accesat la 12 martie 2020, apud Keir Giles, *op. cit.*, p. 7.

În timp ce multe acuzații legate de arme biologice au pornit de la Kremlin, acestea au fost adesea amplificate de surse media din țările aliate ale URSS. Mass-media cubaneză a afirmat constant că Statele Unite au răspândit o varietate de maladii în perioada anilor 1970-1980. În paralel, autoritățile ruse au acuzat SUA de implicare în dezvoltarea pe teritoriul Pakistanului a unor specii deosebit de periculoase de țânțari, care urma să fie folosite pentru răspândirea rapidă a armelor biologice[6].

Acuzațiile aduse la adresa Statelor Unite în privința folosirii armelor biologice au fost o practică des utilizată de către adversarii din timpul Războiului Rece, însă cele mai insidioase două campanii au fost cele referitoare la Războiul din Coreea[7] și campania de dezinformare SIDA[8].

Se poate observa că, în perioada Războiului Rece, luând ca bază teoretică definiția NATO a operațiilor informaționale, URSS a utilizat preponderent *activități informaționale pentru a crea efectele dorite asupra înțelegerii și capabilităților diferitelor audiențe*. De asemenea, observăm planificarea și executarea în special a activităților de influențare și a activităților de protecție informațională.

În perioada Războiului Rece, luând ca bază teoretică definiția NATO a operațiilor informaționale, URSS a utilizat preponderent activități informaționale pentru a crea efectele dorite asupra înțelegerii și capabilităților diferitelor audiențe.

Acuzațiile privind armele biologice din jurul actualei pandemii cu virusul SARS-CoV-2 continuă linia specifică a conflictelor/operațiilor informaționale desfășurate de Uniunea Sovietică în timpul Războiului Rece, însă capacitățile de confruntare și obiectivele urmărite sunt mult mai complexe.

Federația Rusă conduce, în prezent, poate unele dintre cele mai ample și complexe conflicte informaționale din ultimii ani, care integrează secvențe de operații mass-media, manipulare, dezinformare, propagandă – albă, neagră și gri, operații în rețele sociale, operații cibernetice și cu implicarea întregului arsenal

[6] Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, vol. 57:205-227, ianuarie 2012, https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618, accesat la 11 aprilie 2020.

[7] Pentru mai multe detalii, Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 aprilie 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/, accesat la 11 aprilie 2020.

[8] Vezi Douglas Selvage, Christopher Nehring, *Operation „Denver”: KGB and Stasi Disinformation regarding AIDS*, 22 iulie 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids, accesat la 11 aprilie 2020, și Filippa Lentzos, *The Russian disinformation attack that poses a biological danger*,19 noiembrie 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/, accesat la 11 aprilie 2020.

de instrumente specifice conflictului informațional, dintre care am aminti: acuzarea adversarului pentru săvârșirea unor atrocități, propaganda sau discreditarea propagandei adversarului, amplificarea exagerată a anumitor mize, invocarea protecției etc.

Toate capacităţile de confruntare enumerate sunt utilizate, dar dimensiunea dezinformării, alături de cea cibernetică, se detaşează faţă de celelalte forme.

CORONAVIRUSUL DEZINFORMĂRII – NOUL CONFLICT INFORMAȚIONAL RUS –

În această perioadă, un număr mare de oameni sunt închiși în case și petrec o mare parte din timp pe social media. Potrivit datelor, la sfârșitul lunii martie a.c., existau mai mult de trei miliarde de postări și peste 100 de miliarde de interacțiuni asupra *#covid19*, *#coronavirus* și similare[9].

Organizația Mondială a Sănătății a avertizat că lumea se confruntă în paralel cu două epidemii: una generată de noul coronavirus SARS CoV-2 și o a doua referindu-se la o așa-zisă „infodemie”, descriind acest fenomen ca o supra-abundență de știri mai mult sau mai puțin exacte.

Încă din data de 2 februarie a.c., Organizația Mondială a Sănătății (OMS) a avertizat că lumea se confruntă în paralel cu două epidemii[10]: una generată de noul coronavirus SARS CoV-2 și o a doua referindu-se la o așa-zisă *„infodemie”*, descriind acest fenomen ca o supra-abundență de știri mai mult sau mai puțin exacte.

Narațiunea propusă de vectorii Federației Ruse se referă, în principal, la alterarea spațiului public al țintelor vizate prin injectarea de dezinformare și propagandă. Concomitent, un alt pilon este acela al lobby-ului prin care se urmărește influențarea publicului-țintă prin idei vehiculate în spațiul public de către purtători de mesaj legitimi și credibili.

Nu în ultimul rând, se apelează la operații psihologice elaborate în care contează atât informaţia răspândită, cât, mai ales, efectul creat de informaţie în cadrul publicului-ţintă, respectiv naşterea şi crearea sau accentuarea fricilor, crearea emoţiilor colective, pregătirea publicului pentru a reacţiona la viitoare evenimente într-o formulă dirijată.

Fluxurile narațiunii Federației Ruse

Narațiunile rusești pot fi împărțite în trei categorii: o așa-zisă dezinformare de bază, dezinformarea complexă și propaganda elaborată.

[9] Faruk Zorlu, *Covid-19: Infodemic spreads faster than pandemic*, 31.03.2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381, accesat la 13 aprilie 2020.

[10] OMS a ridicat nivelul epidemiei Covid-19 la rangul de pandemie la data de 11 martie 2020.

Dezinformarea de bază constă în cele mai puțin sofisticate tipuri de dezinformare. Aceste abordări vizează publicul cel mai puțin informat din masele rusești și nu numai, printre care sentimentul anti-american este puternic din punct de vedere istoric și ușor de inflamat. Instrumentele utilizate includ platforme de dezinformare, bloggeri, precum și conturi utilizate de către rușii care trăiesc în SUA, Canada și UE. Pentru acest public-țintă, propagandiștii ruși folosesc în mod deliberat un limbaj nesofisticat și argumente primitive, dar convingătoare, simple[11].

Dezinformarea complexă promulgă idei similare, dar îmbrăcate diferit. Această abordare se bazează pe teorii ale conspirației elaborate, care au ca scop crearea așa-numitei realități alternative și încercarea de a promova neîncrederea în rândul publicului străin. Platformele de informare din Rusia folosesc *„dovezi”* pseudoștiințifice că virusul a fost creat într-un laborator american pentru a opri creșterea economică a Chinei[12].

Dezinformarea complexă promulgă idei similare, dar îmbrăcate diferit. Această abordare se bazează pe teorii ale conspirației elaborate, care au ca scop crearea așa-numitei realități alternative și încercarea de a promova neîncrederea în rândul publicului străin.

Iar cea de-a treia categorie prezintă un exemplu de *propagandă elaborată*, concepută pentru cercuri foarte înguste din afara Federației Ruse. În acest caz, statul rus se bazează pe oameni de știință proeminenți proprii și, uneori, apelează și la surse străine (în principal, chineze). Potrivit teoriilor acestora, *„coronavirusul ... a devenit sfârșitul lumii moderne”*[13]. Se susține faptul că ordinea mondială stabilită după Războiul Rece se prăbușește acum și face loc unei noi perioade, în care vor apărea noi lideri.

„Dezinformarea se joacă cu viețile oamenilor. Dezinformarea poate să ucidă” – susținea, într-o conferință de presă, în a doua decadă a lunii martie a.c., Josep Borrell, directorul Serviciului European de Acțiune Externă. Acest joc periculos a debutat la începutul anului curent și s-a dezvoltat gradual.

[11] *NATO uses COVID-19 to mobilise Western military forces against Russia*, 19.03.2020, Interviu cu Alexander Artamonov, realizat de Agenția de știri Novorossia, https://novorosinform.org/808651, accesat la 13 aprilie 2020.

[12] Vicky Peláez, *Scientists: coronavirus would be a weapon of biological warfare*, 13.02.2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/, accesat la 14 aprilie 2020.

[13] Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 05.04.2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship, accesat la 14 aprilie 2020 (în original, *„Coronavirus... has become the end of the modern world”).*

Prima dezinformare înregistrată pe tema Covid-19 a apărut în *Sputnik News*, pe 22 ianuarie[14], când a fost publicat un articol potrivit căruia virusul a fost creat de om, o armă creată de NATO[15].

Potrivit unui studiu efectuat de EUvsDisinf[16], analizând articolele publicate în mass-media străine între 22 ianuarie și 25 martie a.c. pe tema Covid-19, ținta predilectă rămân SUA, 39 de articole fiind îndreptate către acestea, articole în care se susține că SUA au creat virusul SARS-CoV-2. A doua cea mai comună narațiune, cu 26 de articole publicate, este că UE nu reușește să facă față crizei și, ca urmare, se dezintegrează, împreună cu spațiul Schengen. În special, această narațiune a eșecului și a lipsei de solidaritate a UE este în trend după acordarea ajutorului rusesc în Italia. Narațiunea că virusul este folosit ca o armă împotriva Chinei și economia sa vine pe locul al treilea, cu 24 de articole. Pe locul patru este narațiunea că întreaga criză coronavirus este un plan secret al elitei globale, cu 17 articole[17].

În domeniul militar, dezinformarea a vizat exercițiul multinațional *Defender Europe 2020*. Conducerea rusă a criticat exercițiul ca fiind un *„scenariu anti-rus”* ofensiv[18], dar apoi a folosit propaganda pentru a răspândi teoria potrivit căreia, prin desfășurarea exercițiului, s-ar putea facilita răspândirea virusului SARS-CoV-2 în Europa din cauza sosirii și mișcării unui număr mare de trupe.

În domeniul militar, dezinformarea a vizat exercițiul multinațional „Defender Europe 2020”. Conducerea rusă a criticat exercițiul ca fiind un „scenariu anti-rus” ofensiv, dar apoi a folosit propaganda pentru a răspândi teoria potrivit căreia, prin desfășurarea exercițiului, s-ar putea facilita răspândirea virusului SARS-CoV-2 în Europa din cauza sosirii și mișcării unui număr mare de trupe.

Canale utilizate

Pentru atingerea obiectivelor, Moscova dispune de o serie de vectori de propagare a mesajelor, care pot fi împărțiți astfel:

1. Mass-media tradițională (trustul *Russia Today*, care deține și postul de televiziune *Russia Today* și proiectul *Sputnik*, *Pervy Kanal*);

[14] *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/, accesat la 14 aprilie 2020.

[15] *A new Chinese coronavirus was likely elaborated in NATO biolabs*, https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/, accesat la 14 aprilie 2020.

[16] *EuvsDisinfo*, din cadrul East StratCom Task Force, este proiectul Serviciului European de Acțiune Externă. Aceasta a fost înființată în 2015, pentru a răspunde campaniilor de dezinformare ale Federației Ruse care afectează Uniunea Europeană. Pentru mai multe informații, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en, accesat la 14 aprilie 2020.

[17] *Ibidem.*

[18] *The US Defender 2020 military manoeuvre is explicitly directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia, după Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen*, https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title, accesat la 14 aprilie 2020.

2. Mediul virtual (armata de troli a Kremlinului) – structuri specializate în activități pe platforme de blog, producție de știri, crearea de imagini și conținut denigrator pentru subminarea unei anumite ținte, producția de conținut video și redactarea de comentarii pro-Kremlin postate în medii virtuale. Conform unui raport pregătit pentru Global Engagement Center[19] din cadrul Departamentului de Stat al SUA, s-a observat utilizarea unor conturi controlate de statul rus și utilizate inițial pentru influențarea evenimentelor specifice conflictului din Siria și grevelor extinse din Franța, pentru a posta, în prezent, mesaje legate de pandemia coronavirus.
   Potrivit Departamentului de Stat, în momentul în care mass-media rusă a început să difuzeze articole și interviuri antioccidentale despre originile virusului SARS-CoV-2, conturile ruse au început să le promoveze pe plan mondial, acoperind peste 20 de limbi – de la engleză la rusă și de la sârbă la arabă.
3. Implicarea unor personaje influente din Federația Rusă, formatori de opinie aserviți Kremlinului. Evident, în acest tablou nu putea lipsi unul dintre cei mai influenți gânditori geopolitici ai Federației Ruse, Alexander Dughin, un naționalist rus și un susținător foarte activ al Bisericii Ortodoxe, care a avansat ideea că, atunci când virusul își va termina marșul victoriei pe întreaga planetă, va fi distrusă ordinea mondială existentă. Este de notorietate faptul că mesajele acestuia se înscriu în agenda propagandei ruse, intens promovată în ultimii ani, fiind unul dintre principalele instrumente pe care aceasta construiește, promovează și dezvoltă elementele constitutive ale unei imagini de marcă a Federației Ruse.
4. ONG-uri, think-tank-uri și alte platforme de discuții al căror scop este de a disemina propaganda rusă.
5. Și, nu în ultimul rând, am aminti implicarea serviciilor de informații ruse în promovarea de mesaje în sprijinul politicii externe ruse la nivelul țărilor membre ale UE. Acestea folosesc jurnaliști independenți, ziariști, ONG-uri și institute de cercetare.

Conform unui raport pregătit pentru Global Engagement Center din cadrul Departamentului de Stat al SUA, s-a observat utilizarea unor conturi controlate de statul rus și utilizate inițial pentru influențarea evenimentelor specifice conflictului din Siria și grevelor extinse din Franța, pentru a posta, în prezent, mesaje legate de pandemia coronavirus.

[19] Lea Gabrielle, *Briefing on Disinformation and Propaganda Related to COVID-19*, https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19, accesat la 14 aprilie 2020.

Dacă, în privința americanilor, conflictele informaționale derulate de Federația Rusă urmăresc destabilizarea și discreditarea Statelor Unite pe plan european, profitând de incapacitatea SUA de a-și ajuta aliații, pentru Uniunea Europeană agenda este una mai complexă, vizând subminarea coeziunii prin cultivarea unor concentrări a activităților informaționale asupra unor țări membre ale UE.

În acest context, Moscova a încercat anihilarea mișcărilor de imagine ale Chinei de a trimite ajutor Italiei și Spaniei și a acționat pentru a revendica toată publicitatea și beneficiile.

Din Rusia, cu dragoste...

Ajutorul Moscovei pentru Italia în legătură cu coronavirusul a fost acoperit pe scară largă, atât în presa internațională[20], cât și în cea rusă. Italia a salutat cu recunoștință sosirea unui avion chinez – în prezența președintelui italian și a ambasadorului chinez –, care a transportat medici și echipamente. Mass-media de stat rusă a prezentat situația din Italia în contextul luptei pe care această țară o poartă pentru limitarea răspândirii coronavirusului, în moduri diferite.

La Radio Vesti FM, controlat de Kremlin, publicului i s-a spus că epidemia coronavirusului va forța Italia să părăsească UE. Anterior, Sputnik, controlat tot de Kremlin, a promovat teoria conspirației conform căreia coronavirusul ar fi putut fi creat pentru a limita povara economică a cetățenilor pensionați din bugetul Italiei.

La *Radio Vesti FM*, controlat de Kremlin, publicului i s-a spus că epidemia coronavirusului va forța Italia să părăsească UE[21]. Anterior, *Sputnik*, controlat tot de Kremlin, a promovat teoria conspirației conform căreia coronavirusul ar fi putut fi creat pentru a limita povara economică a cetățenilor pensionați din bugetul Italiei[22].

Sputnik i-a acuzat, de asemenea, pe membrii Parlamentului European că doresc să lanseze o campanie împotriva ajutorului rusesc pentru Italia, când, în realitate, au cerut să analizeze campaniile de dezinformare și utilizarea geopolitică a ajutorului.

Totodată, în mass-media rusă a fost intens promovat un videoclip în care un cetățean italian a înlocuit steagul Uniunii Europene cu cel al Rusiei, vehiculând, în mod fals, ideea că acest curent este unul

[20] Potrivit unei analize efectuate de cotidianul italian *La Stampa*, aproximativ 80% din proviziile trimise de Rusia sunt *„inutile”*, Jacopo Iacoboni, *La Stampa*, 25 martie 2020, *Coronavirus, la telefonata Conte-Putin agita il governo: „Più che aiuti arrivano militari russi in Italia”*, https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327, accesat la 15 aprilie 2020.

[21] *Coronavirus: BBC Challenges Pro-Kremlin Reporting from Italy*, 1 aprilie 2020, https://euvsdisinfo.eu/coronavirus-bbc-challenges-pro-kremlin-reporting-from-italy/, accesat la 15 aprilie 2020.

[22] *Ibidem*.

generalizat. Un reporter al televiziunii britanice *BBC* a contactat respectivul cetățean italian pentru solicitarea unui punct de vedere în care a precizat că a decis ridicarea mai multor steaguri ale Federației Ruse în afara magazinului pe care îl deține pentru a-și exprima recunoștința față de Rusia!

Un alt videoclip care a fost distribuit în presa pro-Kremlin arată imnul Federației Ruse intonat în Italia. Printre publicațiile rusești care au transmis videoclipul s-au numărat rețeaua controlată de stat *Rossiya 1* și canalul de televiziune pro-Kremlin *REN TV*, a cărui poveste a fost prezentată online sub titlul: *„Imnul Rusiei a sunat pe străzile Italiei”*[23].

Mass-media rusă nu a explicat nici că muzica din videoclip apare din interiorul biroului unei organizații pe care articolul *BB*C o descrie ca *„neofascistă”* și nici că persoana din spatele videoclipului este un activist care are legături cu Rusia.

În articolul său, *BBC* a demonstrat că două videoclipuri diferite cu imnul Rusiei, care au circulat în mass-media rusă, sunt, de fapt, înregistrări ale aceluiași eveniment, dar din unghiuri diferite.

Concomitent cu ajutorul acordat, Italia a fost și ținta unor atacuri cibernetice, ca, de altfel, întreaga Europă.

Infractorii cibernetici profită de timpul tot mai mare pe care oamenii îl petrec online din cauza noilor măsuri luate de statele membre pentru a opri răspândirea virusului.

Operațiile cibernetice ruse

Operațiile cibernetice reprezintă unul dintre cele mai importante domenii din cadrul conflictului informațional pe care Federația Rusă îl desfășoară pe fondul pandemiei cu virusul *SARS-CoV-2*.

Președintele Comisiei Europene, Ursula von der Leyen, a avertizat, în data de 24 martie a.c., despre creșterea semnificativă a criminalității informatice din UE, în contextul extinderii pandemiei *Covid-19*[24]. Infractorii cibernetici profită de timpul tot mai mare pe care oamenii îl petrec online din cauza noilor măsuri luate de statele membre pentru a opri răspândirea virusului.

Primul grup de hackeri sponsorizat de Kremlin care a fost angajat pe acest front a fost grupul *Hades*[25], despre care există indicii

[23] *На улицах итальянских городов прозвучал гимн России*, 26 martie 2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii, accesat la 15 aprilie 2020.

[24] *EU Commission Warns of Increased Cybercrime During Coronavirus Crisis*, VOA News, 24 martie 2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus, accesat la 15 aprilie 2020.

[25] Cătălin Cîmpanu, *State-sponsored hackers are now using coronavirus lures to infect their targets*, 13 martie 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/, accesat la 16 aprilie 2020.

că funcționează în afara Federației Ruse, și o legătură cu gruparea APT28, unul dintre cele mai renumite grupări de spionaj cibernetic ale Federației Ruse. Potrivit companiei chineze de securitate cibernetică QiAnXin, hackerii Hades au desfășurat o campanie la jumătatea lunii februarie, când au ascuns un virus troian în documente care conțineau cele mai noi știri despre *Covid-19*. Documentele au fost trimise către ținte din Ucraina, deghizate în e-mailuri provenite de la Centrul de Sănătate Publică al Ministerului Sănătății din Ucraina[26].

În perioada pandemiei cu virusul SARS-CoV-2, luând ca bază teoretică definiția NATO a operațiilor informaționale, Federația Rusă a utilizat preponderent activități informaționale pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor diferitelor audiențe. De asemenea, observăm planificarea și executarea activităților de influențare, a activităților împotriva conducerii și capabilităților de comandă, precum și a activităților de protecție informațională.

Și un raport al Europol[27] din cursul lunii martie confirmă cele deja enumerate, evidențiind faptul că, în această perioadă, infracțiunile cibernetice au crescut semnificativ. Europol monitorizează încă de la început impactul pandemiei *Covid-19* asupra peisajului criminalității informatice și a publicat o evaluare actualizată a amenințărilor cu privire la potențialele evoluții ulterioare în acest domeniu al criminalității.

Principalele constatări din această evaluare sunt: impactul pandemiei cu virusul *SARS-CoV-2* asupra criminalității informatice a fost cel mai vizibil în comparație cu alte activități infracționale; infractorii activi în domeniul criminalității informatice au fost capabili să se adapteze rapid și să valorifice anxietățile și temerile victimelor lor; campaniile de *phishing* și *ransomware* sunt lansate pentru a exploata criza actuală și se preconizează că vor continua să crească în domeniul de aplicare și la scară largă; atât organizațiile criminale, statele, cât și actorii susținuți de stat încearcă să exploateze criza sănătății publice pentru a promova interesele geopolitice[28].

Se poate observa că, în perioada pandemiei cu virusul *SARS-CoV-2*, luând ca bază teoretică definiția NATO a operațiilor informaționale, Federația Rusă a utilizat preponderent *activități informaționale pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor* diferitelor audiențe. De asemenea, observăm planificarea și executarea activităților de influențare, a activităților împotriva conducerii și capabilităților de comandă, precum și a activităților de protecție informațională.

[26] *Ibidem.*

[27] *Catching the virus cybercrime, disinformation and the COVID-19 pandemic*, 3 aprilie 2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, accesat la 16 aprilie 2020.

[28] *Ibidem.*

GÂNDIREA MILITARĂ ROMÂNEASCĂ

CONCLUZII

Deși amenințarea generată de amploarea acestei pandemii este una reală și deloc de neglijat, Federația Rusă vede în această catastrofă o oportunitate de a promova și dezvolta planurile de executare a unor conflicte/operații informaționale împotriva Occidentului pe fondul pandemiei *Covid-19.*

Răspândirea virusului *SARS-CoV-2* a oferit un nou câmp de luptă, în care conflictele/operațiile informațiile constituie cea mai avansată armă, în prezent acestea beneficiind de o viteză de propagare mult mai rapidă, precum și de o rază de acțiune mare, contribuind decisiv la modelarea și influențarea rapidă atât a opiniilor, cât și a acțiunilor audiențelor țintă.

Răspândirea virusului SARS-CoV-2 a oferit un nou câmp de luptă, în care conflictele/ operațiile informațiile constituie cea mai avansată armă, în prezent acestea beneficiind de o viteză de propagare mult mai rapidă, precum și de o rază de acțiune mare, contribuind decisiv la modelarea și influențarea rapidă atât a opiniilor, cât și a acțiunilor audiențelor țintă.

O miză pentru Federația Rusă în acest context o reprezintă relaționarea cu Italia, care vine într-un moment în care această țară este vulnerabilă. Interesul tot mai mare al Federației Ruse în UE și oferirea ajutorului către Italia reprezintă elemente concrete de punere în practică a unor conflicte/operații informaționale împotriva UE și a țărilor membre.

Din analiza comparată a modului de punere în practică a domeniilor conflictelor/operațiilor informaționale din perioada Războiului Rece cu perioada specifică pandemiei cu virusul *SARS-CoV-2* se poate observa trecerea de la utilizarea parțială a unor activități informaționale specifice Războiului Rece la folosirea tuturor activităților informaționale *pentru a crea efectele dorite asupra voinţei, înţelegerii şi capabilităţilor* diferitelor audiențe. Tipologia mesajelor utilizate nu este una nouă, însă, ce este diferit acum este executarea conflictelor/operațiilor informaționale din ce în ce mai intruzive și utilizarea acestora nu doar pentru destabilizarea SUA, ci și a Uniunii Europene.

De asemenea, considerăm că este probabil ca acțiunile subsumate conflictelor/operațiilor informaționale, derulate de Federația Rusă, *să se intensifice și să se dezvolte*, căutând să identifice noi vulnerabilități, având în vedere măsurile de contracarare deja întreprinse de autoritățile Uniunii Europene, precum și de către SUA.

În contextul în care Federația Rusă investește masiv în programe de cercetare privind inteligența artificială, specialiștii în securitate descriu deja noul concept de *știri false*, care va fi inițiat de capacitatea tehnologică a inteligenței artificiale de a reproduce fidel vocea individului, ca ființă umană, ca fiind un nou domeniu al conflictelor/ operațiilor informaționale ale viitorului.

BIBLIOGRAFIE:

1. ***, AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
2. ***, S.M.G.-66, *Doctrina operațiilor informaționale*, București, 2017.
3. Cătălin Cîmpanu, *State-sponsored hackers are now using coronavirus lures to infect their targets*, 13 martie 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/
4. Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 5 aprilie 2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship
5. Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 aprilie 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/
6. Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016.
7. Jacopo Iacoboni, *La Stampa*, 25 martie 2020, *Coronavirus, la telefonata Conte-Putin agita il governo: "Più che aiuti arrivano militari russi in Italia",* https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327
8. Filippa Lentzos, *The Russian disinformation attack that poses a biological danger*, 19 noiembrie 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/
9. Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, vol. 57:205-227, https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618
10. Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 martie 2011, http://www.rferl.org/articleprintview/2345202.html
11. Vicky Peláez, *Scientists: coronavirus would be a weapon of biological warfare*, 13 februarie 2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/
12. Douglas Selvage, Christopher Nehring, *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*, 22 iulie 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids
13. Faruk Zorlu, *Covid-19: Infodemic spreads faster than pandemic*, 31 martie 2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381

14. *A new Chinese coronavirus was likely elaborated in NATO biolabs,* https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/
15. *Catching the virus cybercrime, disinformation and the COVID-19 pandemic*, 3 aprilie 2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
16. *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/
17. *EU Commission Warns of Increased Cybercrime During Coronavirus Crisis,* VOA News, 24 martie 2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus
18. *На улицах итальянских городов прозвучал гимн России*, 26 martie 2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii
19. *NATO uses COVID-19 to mobilise Western military forces against Russia*, 19 martie 2020, Interviu cu Alexander Artamonov, realizat de Agenția de știri Novorossia, https://novorosinform.org/808651
20. *The US Defender 2020 military manoeuvre is explicitly directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia după Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen,* https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title.

ARME BIOLOGICE ȘI VECTORI PANDEMICI

*Dr. Alba I.C. POPESCU**

Universitatea Națională de Apărare „Carol I”, București

Războiul biologic nu este o invenție a epocii moderne. El a fost practicat încă din Antichitate, când hitiții au trimis bolnavi de ciumă în taberele egiptene pentru a-și decima dușmanii înainte de luptă. Diferența dintre epoci este făcută doar de tehnologia actuală, capabilă să multiplice, să selecteze, să diversifice și să hibridizeze vectorii războiului biologic. Astfel, în prezent, o bacterie, crescută într-o cămară transformată în laborator, poate fi mai letală decât orice armă chimică. Întrucât, în epoca modernă a accesului public la informații, limita între pandemia spontană, naturală și atacul biologic urmat de izbucnirea unei pandemii este tot mai îngustă, vectorii unei pandemii naturale pot oricând deveni, în ochii opiniei publice, vectorii unui atac biologic. Dar și invers, până la descoperirea „pacientului zero” – la nivelul căruia s-au produs mutațiile genomice naturale –, orice armă biologică poate fi considerată „mutație naturală” responsabilă de declanșarea unei pandemii cu efecte devastatoare. Prin urmare, care sunt caracteristicile unei arme biologice? Care sunt principalele categorii de arme biologice? Care sunt principalii vectori pandemici?

Cuvinte-cheie: pandemie, război biologic, vectori pandemici, fitoagenți, Covid-19.

* A absolvit Universitatea de Medicină și Farmacie *„Carol Davila”* din București, deține un master în sănătate publică și a lucrat mai mulți ani în Africa, unde s-a dedicat combaterii epidemiilor de HIV, TBC și malarie.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Motto: „Virusurile gripei s-au răspândit mereu foarte rapid ..., acesta este un dezastru care stă să se întâmple”.
Peter C. Doherty, imunolog,
laureat al Premiului Nobel pentru Medicină

INTRODUCERE

Războiul biologic nu este o invenție a epocii moderne. El a fost practicat încă din Antichitate, când hitiții au trimis bolnavi de ciumă în taberele egiptene pentru a-și decima dușmanii înainte de luptă. Diferența dintre epoci este făcută doar de tehnologia actuală, capabilă să multiplice, să selecteze, să diversifice și să hibridizeze vectorii războiului biologic. Astfel, în prezent, o bacterie, crescută într-o cămară transformată în laborator, poate fi mai letală decât orice armă chimică. De aceea, nu întâmplător, arma biologică mai este numită și *„bomba nucleară a săracului”*[1]. Întrucât, în epoca modernă a accesului public la informații, limita între pandemia spontană, naturală și atacul biologic urmat de izbucnirea unei pandemii este tot mai îngustă, vectorii unei pandemii naturale pot oricând deveni, în ochii opiniei publice, vectorii unui atac biologic. Dar și invers, până la descoperirea *„pacientului zero”* – la nivelul căruia s-au produs mutațiile genomice naturale –, orice armă biologică poate fi considerată *„mutație naturală”* responsabilă de declanșarea unei pandemii cu efecte devastatoare. Prin urmare, *care sunt caracteristicile unei arme biologice? Care sunt principalele categorii de arme biologice? Care sunt principalii vectori pandemici?*

Întrucât, în epoca modernă a accesului public la informații, limita între pandemia spontană, naturală și atacul biologic urmat de izbucnirea unei pandemii este tot mai îngustă, vectorii unei pandemii naturale pot oricând deveni, în ochii opiniei publice, vectorii unui atac biologic.

CE SUNT MICROORGANISMELE?

Conform *Dicționarului Enciclopedic*, *microorganismele* sunt *„organisme animale sau vegetale de dimensiuni microscopice (...) foarte răspândite în aer, apă, sol și cu rol important în circuitul*

[1] *The myth of biological weapons as the poor man’s atomic bomb*, în *Bulletin of the Atomic Scientist*, 18 martie 2015, https://thebulletin.org/roundtable_entry/the-myth-of-biological-weapons-as-the-poor-mans-atomic-bomb/, accesat la 21.04.2020.

substanțelor în natură”[2], care, în funcție de efectele pe care le produc asupra oamenilor, animalelor și plantelor, pot fi:

- saprofite – benefice, alcătuiesc microflora și microfauna din sol și intervin în homeostazia mediului în care se dezvoltă, unele fiind utilizate în industria alimentară, farmaceutică (prepararea aluatului, fabricarea vinului, oțetului etc., prepararea iaurturilor, a antibioticelor și vitaminelor etc.) și în ingineria genetică;
- patogene – provoacă boli ale plantelor, animalelor și oamenilor.

Microorganismele alcatuiesc un grup foarte vast și eterogen de organisme microscopice, cu morfologie și activitate biologică diferite, structurat în următoarele domenii, regnuri sau încrengături[3]:

- *Bacterii* – microorganisme procariote din domeniul *Bacteria*, cu lungime de câțiva micrometri, cu morfologie diversă (sferică, alungită, spiralată, polimorfă). Întrucât nu prezintă membrană nucleară și nucleoli, având un nucleiod în loc de nucleu, care îi limitează capacitatea de supraviețuire independentă, trăiesc în relații de simbioză sau de parazitism cu oamenii, plantele și animalele. Pot fi eubacterii/bacterii adevărate, cu perete celular fin, gram-negative sau cu perete celular gros, gram-pozitive și micoplasme, lipsite de perete celular (micoplasme);
- *Arhee* – microorganisme unicelulare, anucleate, care aparțin domeniului *Archaea*. Se găsesc în numeroase habitate, în sol, oceane (archea planctonului), în colonul uman sau ombilicul uman. Nu se cunosc arhee patogene;
- *Fungi microscopici* (mucegaiuri și levuri) – sunt microorganisme eucariote din regnul *Fungi*, unul dintre cele trei mari regnuri ale domeniului *Eukaryota*. Au nucleu complet, pot fi saprofite, parazite sau simbiotice cu plantele (micoriză) sau cu alge albastre-verzi (licheni);

[2] Marcel D. Popa și colab., *Dicționar Enciclopedic*, Editura Enciclopedică, 1993-2009, https://dexonline.ro/definitie/microorganism, accesat la 10.04.2020.

[3] Valeria Firă, Maria Năstăsescu, *Zoologia nevertebratelor*, Editura Didactică și Pedagogică, București, 1977.

- *Microalge* sau *microfite* – microorganisme eucariote unicelulare prezente în sistemele de apă dulce și marine, inclusiv în sedimente. Pot exista individual, în lanțuri sau în grupuri și pot atinge dimensiuni de la câțiva micrometri la câteva sute de micrometri. Capabile de fotosinteză, produc aproximativ jumătate din oxigenul atmosferic. Nu se cunosc microalge patogene;
- *Protozoare* – cele mai simple organisme eucariote unicelulare din subregnul *Protozoa*, fac legătura între plante și animale. Traiesc în mediul acvatic/lichidian, unele pot atinge dimensiuni vizibile, de ordinul centimetrilor. 40 de specii de protozoare sunt patogene pentru om;
- *Virusuri* – sunt entități acelulare, exclusiv parazitare și patogene, aflate la limita dintre viu și neviu. Sunt alcătuite din material genetic (ADN sau ARN), invizibil la microscopul optic, fără capacitate de autoreproducere în afara unei celule parazitate;
- *Agenții infecțioși* (viroizi, prioni) – nu sunt considerați microorganisme, sunt agenți infecțioși de natură proteică, lipsiți de orice tip de acid nucleic.

Bacteriile, fungii, protozoarele, virusurile și agenții infecțioși subvirali sunt patogeni pentru oameni, plante și animale, bolile produse de micro-organismele patogene numindu-se boli infecțioase.

Precum putem deduce din clasificarea de mai sus, doar bacteriile, fungii, protozoarele, virusurile și agenții infecțioși subvirali sunt patogeni pentru oameni, plante și animale, bolile produse de microorganismele patogene numindu-se *boli infecțioase*.

Agentul microbian patogen prezintă o serie de proprietăți, precum[4]:

- **Patogenitatea**: capacitatea unui microorganism de a produce o boală infecţioasă într-o gazdă receptivă. Infecțiile generate de microorganismele patogene asupra regnului animal se numesc *zoonoze*, atunci când afectează animalele, și *antroponoze*, atunci când afectează oamenii. Atunci când infecțiile se transmit de la animale la oameni, infecțiile se numesc *antropozoonoze*.

[4] *Noțiuni generale de patogenitate și virulență*, https://www.scribd.com/doc/270695407/Notiuni-Generale-de-Patogenitate-Si-Virulenta, accesat la 10.04.2020.

- **Virulenţa**: cantitatea minimă de microorganism sau de produs al acestuia capabilă să genereze îmbolnăvirea sau moartea sistemului biologic de testare.

Reprezintă un indicator cantitativ al patogenității, dependent de trei caracteristici ale agentului microbian, respectiv:

1. ***Infecțiozitate*** – capacitatea microorganismului patogen de a pătrunde, a se localiza și multiplica în organismul gazdă, în ciuda atacurilor sistemului imun, și de a produce un focar primar de infecție;
2. ***Invazivitate*** sau *agresivitate*, respectiv capacitatea micro-organismului patogen de a depăși, prin mijloace proprii, barierele epiteliale și de a pătrunde și a se multiplica în țesuturile gazdei;
3. ***Toxigenitate*** – capacitatea agentului microbian de a produce toxine. Este o proprietate esențială a mecanismului patogenic bacterian.

Există trei niveluri de virulență:

- *virulenţa crescută*, specifică tulpinilor microbiene care produc infecții cu evoluţie clinică gravă;
- *virulenţa diminuată*, specifică tulpinilor microbiene care produc forme uşoare de boală;
- *virulenţa atenuată*, specifică tulpinilor utilizate în prepararea de vaccinuri.

Din multitudinea de microorganisme patogene, foarte puține sunt pasibile de a declanșa pandemii, ca urmare a proprietăților de virulență și patogenitate și, mai ales, ca urmare a dezvoltării mecanismelor de apărare a organismelor gazdă. De obicei, pandemiile[5] sunt generate de microorganisme capabile să genereze tulpini noi, cu patogenitate și virulență crescute. În general, cele mai pasibile a dezvolta natural astfel de tulpini capabile să declanșeze pandemii sunt virusurile de tip *ARN*, la care frecvența mutațiilor genetice crește cu fiecare multiplicare în nucleul celulei gazdă.

[5] Epidemie prezentă pe minimum cinci continente.

Cu toate acestea, există și posibilitatea intervenției umane, în laborator, asupra genoamelor microbiene, cu amplificarea acestor trăsături și transformarea microorganismelor în arme biologice.

Există și alte criterii de clasificare a vectorilor patogeni, în funcție de:

- regnul țintă: fitoagenți (care acționează asupra regnului vegetal – plante, arbuşti şi arbori) şi zoo/antropoagenți (care acţionează asupra regnului animal – om, animale, păsări, insecte);
- efectele la nivelul organismului gazdă: agenți hemolitici, citolitici, necrotici etc.;
- calea de transmitere: digestivi, aerieni, hematologici etc.

ARME BIOLOGICE

Care sunt caracteristicile unei arme biologice?

Conform definiției agreate de Organizația Mondială a Sănătății, *„armele biologice reprezintă microorganisme precum virusurile, bacteriile, ciupercile sau alte toxine, care sunt produse (în laboratoare) și sunt eliberate în mod deliberat pentru a provoca boli și moarte la om, animale sau plante”*[6]. Ele se constituie în provocări dificile pentru serviciile de sănătate publică, economie, societate prin numărul mare de decese/distrugeri de șeptel, recoltă, pe care le generează într-o perioadă scurtă de timp.

Conform definiției agreate de Organizația Mondială a Sănătății, „armele biologice reprezintă microorganisme precum virusurile, bacteriile, ciupercile sau alte toxine, care sunt produse (în laboratoare) și sunt eliberate în mod deliberat pentru a provoca boli și moarte la om, animale sau plante”.

Armele biologice reprezintă o categorie a unei clase mai mari de arme, denumite *Arme de Distrugere (Nimicire) în Masă*, din care mai fac parte armele chimice, armele nucleare și cele radiologice.

Microorganismele transformate în arme biologice **sunt multiplicate prin biotehnologie,** iar **manipularea genetică** le induce **trăsături pe care nu le aveau inițial,** respectiv:

- patogenitate mult crescută;
- infecțiozitate mult crescută;
- virulenţă mult crescută;
- rezistenţă multiplă la antibiotice, antivirale sau antimicotice;

[6] *Biological weapons,* World Health Organization, https://www.who.int/health-topics/biological-weapons#tab=tab_1, accesat la 10.04.2020.

- perioadă de incubaţie asimptomatică puternic contagioasă;
- acţiune asupra a numeroase sisteme şi aparate ale organismului uman;
- durată crescută de viaţă a microorganismului în afara organismului rezervor;
- durată de acţiune limitată în timp (pentru a permite invazia ulterioară a teritoriului respectiv depopulat);
- tropism selectiv al agentului biologic faţă de anumiţi receptori specifici unor grupe populaţionale etc.

Ce mai trebuie reținut este faptul că, în cazul unei arme biologice, niciodată nu se poate identifica *„pacientul zero”*, în organismul căruia s-a produs mutația letală. *Identificarea „cazului zero” reprezintă dovada de necontestat că un sinistru pandemic a izbucnit natural.* Cu toate acestea, deși este posibil, nu este obligatoriu ca *„pacientul zero”* să fie identificat în cazul unei pandemii naturale, situație care poate genera suspiciuni privind originea ei. Pe cale de consecință, există o limită foarte îngustă între pandemiile naturale și cele produse prin atacuri biologice, limită spulberată doar prin identificarea *„cazului zero”*.

Spre deosebire de celelalte arme de nimicire în masă, o armă biologică poate fi fabricată în spații mici, este ușor de transportat, imposibil de detectat, întrucât este incoloră, insipidă și invizibilă.

Impactul produs de aceste microorganisme asupra populației umane/animale depinde de mai mulți factori, respectiv:

- perioada de incubaţie, în care organismul devine rezervor asimptomatic şi contagios, trebuie să fie cât mai lungă;
- calea de transmitere, care poate fi digestivă, aeriană, hematologică;
- existența sau nu a antidoturilor sau a tratamentelor eficiente;
- costurile şi durata tratamentelor;
- rata de deces în primele 24-72 de ore de la declanșarea bolii.

Căile de transmitere cele mai periculoase, prin numărul mare de indivizi care pot fi afectați într-o perioadă scurtă de timp, sunt cea digestivă și cea aeriană.

Spre deosebire de celelalte arme de nimicire în masă, o armă biologică poate fi fabricată în spații mici, este ușor de transportat, imposibil de detectat, întrucât este incoloră, insipidă și invizibilă.

În cantități egale, armele biologice sunt mult mai ucigătoare decât cele chimice. De exemplu, doza letală de toxină botulinică ingerată este de 0,1 micrograme, iar inhalată este de 5 micrograme. Doza letală inhalată de *VX Lethal Nerve Agent*, cel mai toxic agent neuroparalizant, este de 1.000 de micrograme, fiind de 200 de ori mai mare decât cea de toxină botulinică[7]. În plus, proliferarea acestor tipuri de arme se realizează natural, fiind vorba despre organisme vii.

Prin urmare, o armă biologică performantă poate declanșa, cu ușurință, o pandemie globală, cu efecte în plan demografic, economic, social, politic greu de gestionat, surclasând, prin complexitatea consecințelor, orice altă armă de nimicire în masă.

Deși perfecționarea, producția și stocarea armelor biologice sunt interzise prin *Convenția din 10 aprilie 1972*[8], realitatea a demonstrat continuarea cercetărilor și a producției în domeniu chiar și în laboratoare improvizate, cum a fost cazul sectei japoneze *Aum Shinrikyo*, condusă de Shoko Asahara, care începuse producția de bacil antracic[9], în scopuri teroriste. În acest sens, terorismul biologic sau ***„bioterorismul*** *reprezintă utilizarea sau amenințarea cu utilizarea de arme biologice – microorganisme sau toxine biologice, capabile să producă îmbolnăvirea sau decesul ființelor umane, animalelor, insectelor și plantelor – în scopul îndeplinirii unor obiective politice/economice”*[10].

[7] Eric Croddy, James J. Wirtz, *Weapons of Mass Destruction: Chemical and biological weapons*, ABC CLIO, 2005, p. 54.

[8] *CONVENȚIE din 10 aprilie 1972 cu privire la interzicerea perfecționării, producției și stocării armelor bacteriologice (biologice) și cu toxine și la distrugerea lor*, http://legislatie.just.ro/Public/DetaliiDocument/28190, accesat la 29.05.2020.

[9] *Aum Shinrikyo: The Japanese cult behind the Tokyo Sarin attack*, BBC News, 06.07.2018, https://www.bbc.com/news/world-asia-35975069, accesat la 29.05.2020

[10] Alba Iulia Catrinel Popescu, *Jucătorul din Umbră*, Editura Militară, București, 2016, p. 229.

Care sunt principalele categorii de arme biologice?

1. Armele biologice care acţionează asupra sănătăţii umane

Centers for Disease Control and Prevention Atlanta (C.D.C. Atlanta)[11] – *Centrul pentru Controlul și Prevenirea Bolilor din Atlanta* a clasificat armele biologice care acționează asupra omului în trei categorii, în funcție de patogenitate, morbiditate, mortalitate și ușurința procurării, producerii și diseminării în mediul înconjurător, după cum urmează:

- *clasa A* (uşor diseminabile şi transmisibile de la om la om, foarte patogene, mortalitate foarte ridicată, pot genera panică publică şi insubordonare civică, având impact major asupra serviciilor de sănătate publică, economiei, relaţiilor sociale, stabilităţii politice):
  - transmitere aeriană: *Bacillus anthracis* (antrax), *Variola major* (variolă), *Yersinia pestis* (ciumă), *Francisella tularensis* (tularemie), *filoviridae* (febrele hemoragice Ebola şi Marburg), *arenaviridae* (febrele hemoragice Lassa şi Argentiniană);
  - transmitere digestivă: neurotoxină de *Clostridium botulinum* (botulism);
- *clasa B* (relativ uşor de diseminat, morbiditate moderată şi mortalitate scăzută, pot genera şi ele panică publică, având impact major asupra serviciilor de sănătate publică şi a economiei, dar şi efecte asupra celorlalte sectoare ale societăţii):
  - cu transmitere aeriană: *Brucella sp.* (bruceloza), *Coxiella burnetti* (febra Q), *Rickettsia prowazekii* (tifos exantematic), *alphaviridae* (encefalitele virale), *Burkholderia mallei* (morva), toxina de *Ricinus communis (*diaree hemoragică*)*, toxina epsilon de *Clostridium perfringens* (toxiinfecţii, gangrene gazoase), enterotoxina B de *Staphylococcus aureus* (septicemie);

[11] Centers for Disease Control and Prevention (C.D.C.) Classification of Bioterrorism Microorganisms, Part 3 of 5, Johns Hopkins Bloomberg School of Public Health, 2006, http://ocw.jhsph.edu/courses/Biological AgentsOfWaterAndFoodborneBioterrorism/PDFs/WaterFoodTerror3.pdf, accesat la 29.10.2015.

  - cu transmitere digestivă: *Salmonella sp.* (salmoneloze), *Vibrio cholerae* (holera), *Shigella dysenteriae* (dizenterie), *Cryptosporidium* (criptosporidiaza), *Escherichia coli O157: H7* (infecţie entero-hemoragică), *Noroviridae* (gastroenterita virală);
- *clasa C* (uşor de procurat, de produs şi de diseminat, morbiditate şi mortalitate înalte, cu impact major asupra populaţiei): *bacil Koch* rezistent la terapia antituberculoasă (tuberculoză), *Nipah viridae* (encefalita virală), *hantaviridae* (sindrom cardio-pulmonar), *Flaviviridae* (febra galbenă), viruşi ai febrelor hemoragice şi ai encefalitelor, transmişi prin înţepătură de căpuşă.

Deversarea unor bacterii, cum sunt cele care produc dizenteriile, febra tifoidă și, mai ales, botulismul, în sistemul de alimentare cu apă potabilă al unei metropole sau diseminarea aeriană prin avioane, drone sau dispozitive tip aerosoli, de microorganisme precum cele care produc gripa, variola sau antraxul, pot genera epidemii greu de stăpânit.

Deversarea unor bacterii, cum sunt cele care produc dizenteriile, febra tifoidă și, mai ales, botulismul, în sistemul de alimentare cu apă potabilă al unei metropole sau diseminarea aeriană prin avioane, drone sau dispozitive tip aerosoli, de microorganisme precum cele care produc gripa, variola sau antraxul, pot genera epidemii greu de stăpânit.

Un astfel de episod epidemic, cu care ne-am confruntat deja, când se punea foarte serios problema transformării sale într-o sursă de arme biologice pentru rețelele teroriste, s-a întâmplat în anul 2014, în vestul Africii. Atunci, în Guineea, Liberia și Sierra Leone a făcut ravagii epidemia de febră hemoragică *Ebola* (inclusă de *C.D.C. Atlanta* în rândul agenților biologici de clasa A). Principalele temeri au fost legate de eventualitatea ca structuri jihadiste să procure tulpini virale din secrețiile provenite de la bolnavi sau să-și transforme militanții infectați în vectori biologici, trimiși ulterior, pe calea rețelelor de migrație ilegală, în mijloace de transport în comun, gări și aeroporturi internaționale sau în mari aglomerări urbane occidentale[12]. Îngrijorările au fost amplificate de starea de panică și de insubordonare civică a populației afectate de dezastru, precum și de incapacitatea guvernelor africane de a gestiona eficient situația. În aceste condiții, pe fondul

[12] Bruce Dorminey, *Ebola As ISIS Bio-Weapon?,* Forbes, 05.10.2014, http://www.forbes.com/sites/brucedorminey/ 2014/10/05/ebola-as-isis-bio-weapon/, accesat la 26.09.2015.

riscului major de multiplicare și de extindere a cazurilor de îmbolnăvire spre alte state vest-africane, SUA au decis trimiterea în Liberia a peste 2.500 de militari aparținând *101 Airborne Division – Divizia 101 Aeropurtată*, în cadrul operațiunii *United Assistence,* de ajutor acordat administrațiilor locale implicate în contracararea epidemiei. Misiunile militarilor americani au vizat contenția focarelor de infecție și contracararea panicii localnicilor, precum și sprijinirea activității personalului medical și paramedical din cadrul *United States Agency for International Development* (U.S.A.I.D.) – *Agenția pentru Dezvoltare Internațională a SUA.* În cursul misiunii desfășurate pe durata a cinci luni, între 25 octombrie 2014 și 27 februarie 2015, au fost construite centre de tratament, s-au înființat laboratoare mobile și peste 1.500 de lucrători sanitari locali au participat la cursuri de specializare ținute de cadre militare americane[13,14].

Arma biologică nu se adresează doar omului. Ea poate ataca şi restul ecosistemului, de la plante la animale, păsări, peşti şi insecte, în acest caz, scopul fiind cu precădere unul economic, de distrugere a surselor de hrană.

Dar, arma biologică nu se adresează doar omului. Ea poate ataca și restul ecosistemului, de la plante la animale, păsări, pești și insecte, în acest caz, scopul fiind cu precădere unul economic, de distrugere a surselor de hrană.

2. Fitoagenţii

Distrugerea recoltelor și a rezervelor alimentare a reprezentat o tactică străveche militară, utilizată și în epoca modernă, Războiul din Vietnam (1955-1975) fiind un exemplu în această privință. Efectele unei infestări masive se contabilizează în mii de hectare de culturi distruse, foamete, distrugerea ecosistemului prin dispariția unor verigi trofice, distrugerea șeptelului, instabilitate internă, mari costuri economice, umane și animale, mai ales atunci când o astfel de molimă apare pe fondul unei secete prelungite sau în regiuni suprapopulate, vulnerabilizarea țării în fața unui eveniment neprevăzut sau a unui conflict.

[13] Anthony P. Cardile, Clinton K. Murray, Christopher T. Littell, Neel J. Shah, Matthew N. Fandre, Dennis C. Drinkwater, Brian P. Markelz, Todd J. Vento, *Monitoring Exposure to Ebola and Health of U.S. Military Personnel Deployed in Support of Ebola Control Efforts – Liberia*, October 25, 2014-February 27, 2015, *Morbidity and Mortality Weekly Report (MMWR)*, Centers for Disease Control and Prevention, 03.07.2015, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6425a2.htm, accesat la 29.10.2010.

[14] Alba Iulia Catrinel Popescu, *op. cit*, pp. 229-231.

Fitoagenții pot fi microorganisme sau insecte: lăcuste, gândaci de Colorado, albine sălbatice, viespile japoneze, specii de fluturi etc.

Un exemplu clasic de fitoagent microbian îl reprezintă ciuperca *Prycularia oryzae cavara*, numită și *agentul orezului*, responsabilă de boala numită *„febra orezului”*[15]. Apărută într-un lan, în decurs de câteva ore, prin intermediul sporilor, infestează întreaga zonă, ducând la moartea tuturor plantelor. De exemplu, un astfel de atac, de tip *agroterorist*, concentrat asupra orezăriilor din Asia sau Australia, poate determina moartea prin înfometare a milioane de oameni, explozia prețurilor produselor alimentare și mari dezechilibre financiare globale.

Actualmente, există peste 200 de astfel de fitoagenți, specializați pe câte un tip de plantă: cerealieră, leguminoasă, fructe, arbori, arbuști etc.

3. Zooagenţii

Zooagenţii au ca organisme ţintă atât omul, cât şi celelalte mamifere, păsările, insectele sau peştii.

Zooagenții au ca organisme țintă atât omul, cât și celelalte mamifere, păsările, insectele sau peștii. Sunt extrem de numeroși și diversificați. Anual, apar specii noi, cu rezistență crescută la antibiotice, antivirale sau antimicotice, iar efectele lor sunt devastatoare asupra sănătății publice și economiei, putând genera pandemii cu consecințe demografice uriașe și implicații directe asupra marii majorități a componentelor puterii naționale, ducând la vulnerabilizarea statelor afectate și la instabilitate zonală. Când infestează șeptelul, rezerva piscicolă sau păsăretul, au drept consecință epizootii care, mai ales în regiuni improprii culturilor agricole, duc la apariția foametei, cu tot cortegiul de manifestări sociale conexe.

Rinderpesta sau **ciuma bovinelor** este o epizootie generată de virusul Rinder, înalt patogen, care afectează atât bovinele, cât și alte ierbivore rumegătoare. Ca și în cazul ciumei/pestei porcine, boala se poate transmite foarte ușor, putând afecta întreg șeptelul unei țări în câteva zile.

Consecințele economice ale unei epizootii extinse, chiar și fără a avea caracteristicile de armă biologică, sunt de ordinul zecilor de milioane de dolari. De exemplu, **pesta porcină africană** sau boala

[15] *Rice-Detailed Study of Diseases*, http://www.ikisan.com/links/ap_riceDetailedStudyofDiseases.shtml, accesat la 01.01.2016.

lui Montgomery, boală virală hemoragică febrilă, contagioasă și severă, a produs pagube enorme, fiind de ajuns să amintim:

- episodul din SUA, din 1975, soldat cu pierderi de aproximativ 65 de milioane de dolari;
- focarele apărute în 2007, în România, care au costat compania Smithfield în jur de 12 milioane de dolari;
- epizootia din 2018-2019, care a dus la distrugerea unor combinate de creştere a porcilor şi stoparea unor programe naţionale de revigorare a raselor româneşti de porcine Bazna şi Mangaliţa.

Iată cum o epizootie poate determina prăbușirea economică a unei regiuni și stoparea unor programe naționale, mai ales atunci când ea devine recurentă.

Gripa aviară reprezintă prima pandemie/ epizootie care a demonstrat că semnalele de alarmă trase de Organizația Mondială a Sănătăţii nu sunt doar discuţii lipsite de conținut.

Alte exemple clasice de epizootii sunt **boala vacii nebune** sau **encefalopatia spongiformă bovină,** care s-a soldat cu pierderi de vieți omenești și dezastre economice prin sacrificarea în masă a șeptelului din zonele învecinate unui caz dovedit, și binecunoscuta **gripă aviară**, care a produs pierderi economice uriașe, inclusiv la noi în țară, prin sacrificarea masivă a populației de păsări din regiuni întinse ale țării.

Gripa aviară reprezintă prima pandemie/epizootie care a demonstrat că semnalele de alarmă trase de Organizația Mondială a Sănătății (OMS) nu sunt doar discuții lipsite de conținut. Modul de transmitere a bolii, prin intermediul păsărilor călătoare, care pot parcurge mii de km în cursul unui voiaj, amintește de sistemul de transport aerian, prin care un bolnav, rezervor activ de microbi, poate ajunge în câteva ore pe un alt continent, unde poate transmite boala.

Faptul că Organizația Națiunilor Unite (ONU) l-a desemnat, în data de 29 septembrie 2005, pe Dr. David Nabarro[16] în funcția de *Coordonator al Sistemului ONU pentru Gripa Aviară și Umană*[17]

[16] *WHO expert to work with the UN system on avian and human influenza,* World Health Organization, https://www.who.int/mediacentre/news/releases/2005/pr45/en/, accesat la 01.04.2020.

[17] Sistem care reunește organizații internaționale precum FAO/OIE – supravegherea sănătății animalelor, WHO – epidemiologie și sănătatea oamenilor, UNEP – monitorizarea migrației păsărilor sălbatice, UNICEF – campanii de informare publică, OCHA/WFP/UNHCR – planificare, avertizare și asistență umanitară, UNDP – asigurarea planificării guvernamentale multi-sectoriale.

a demonstrat preocuparea privind riscul izbucnirii unei pandemii, ale cărei consecințe ar fi implicat, pe lângă potențialele pierderi de vieți omenești, consecințe economice și ecologice, prin antrenarea unor lanțuri trofice și ecosisteme de pe traseele migrației păsărilor.

Potrivit fostului director general al Organizației Mondiale a Sănătății, Margaret Chan, *„nicio țară nu este pregătită pentru eventualitatea unei pandemii de gripă aviară. Nu vor exista suficiente rezerve, nici de medicamente, nici de material sanitar de genul măștilor (...), iar rata de atac ar putea atinge 20% din populație”*[18]. Declarația, datată noiembrie 2007, este pe deplin valabilă și astăzi, când coronavirusul Covid-19 face ravagii.

VECTORII PANDEMICI

Care sunt cei mai comuni vectori pandemici?

a) Virusuri

Gripa umană. Episodul pandemic de la începutul secolului trecut, cunoscut sub numele de *gripa spaniolă*, a generat peste 400 de milioane de îmbolnăviri și 50 de milioane de decese, cea mai afectată fiind grupa de vârstă între 20 și 40 de ani. Explicația este legată de faptul că această grupă de vârstă este cea implicată în activitățile sociale, știut fiind că virusul gripal se transmite prin tuse, strănut sau contact cu fluide ale corpului până la o distanță de 10 metri de rezervor. Practic, într-un an, 1918, numărul victimelor acestei pandemii a fost mai mare decât pierderile de vieți omenești din conflagrația mondială care abia se încheiase, iar costurile economice induse de pandemie, cumulate cu distrugerile post-conflict, au contribuit la declanșarea recesiunii din anii ’20. Ulterior, în anii 1957 și 1968 au mai existat două episoade pandemice, cunoscute sub numele de *gripa rusească* și *gripa de Hong-Kong*. În fața acestei realități, OMS a dezvoltat programul anual de vaccinare preventivă împotriva gripei. Trebuie menționat că virusul gripal suferă mutații de la un an la altul, prin urmare este obligatorie imunizarea anuală, corespunzătoare noului genotip viral.

[18] Vezi https://www.who.int/mediacentre/influenzaAH1N1_presstranscript_20090611.pdf, accesat la 05.04.2020; Alexandra Sandru, *Pericolul aviar: Crezi că ne vom confrunta cu o pandemie? (sondaj),* ziare.com, 29.11.2007, http://www.ziare.com/social/capitala/pericolul-aviar-crezi-ca-ne-vom-confrunta-cu-o-pandemie-sondaj-185674, accesat la 05.04.2020.

Responsabilii OMS au atras atenția, în nenumărate rânduri, că este foarte posibilă declanșarea unei noi pandemii gripale cu un virus hibrid aviaro-uman, ușor transmisibil la om, apărut prin combinație nucleică într-un organism uman care a suferit dublă infectare[19]. Aceste virusuri mutante sunt extrem de periculoase, pentru că iau elemente de patogenitate de la virusurile originare, nici oamenii și nici animalele nu au imunitate față de ele și nu există vaccinuri pregătite pentru o astfel de situație. În acest sens, reprezentanții OMS afirmau că, *„dacă virusul va suferi mutații care îi vor conferi abilitatea de a se răspândi de la o persoană la alta, este dificil să găsim o comparație istorică cu ceea ce va urma”.* Iată că pandemia actuală, cu coronavirus Covid-19, începe să împlinească *„profeția”* specialiștilor OMS.

Virusurile mutante sunt extrem de periculoase, pentru că iau elemente de patogenitate de la virusurile originare, nici oamenii și nici animalele nu au imunitate față de ele și nu există vaccinuri pregătite pentru o astfel de situație.

Sindromul Acut Respirator Sever-SARS este o cunoștință relativ recentă a medicilor aflați în prima linie a luptei contra marilor dezastre epidemice, mai mult sau mai puțin apărute natural. În anul 2002, în provincia Guandong din sudul Chinei, au fost identificate o serie de infecții respiratorii, cu evoluție rapidă spre deces, prin pneumonie rebelă la orice tratament. Nici până în prezent nu se cunoaște specia rezervor a acestui virus mutant. Faptul că această epidemie nu a dobândit proporții globale se datorează medicilor din organizații internaționale precum OMS sau *Médecins Sans Frontières (Medici fără Frontiere)*, care au reușit, în 2003, stoparea acestui flagel. Circa 800 de oameni au murit în urma epidemiei de SARS, printre victime numărându-se și medici veniți să stopeze dezastrul[20].

Enteroviroza cu virus intestinal 71. În luna mai a anului 2008, în China a izbucnit o epidemie care a afectat, în mare parte, copiii sub șase ani. Infecția a fost numită boala *„mână-picior-gură”*, ca urmare a erupțiilor herpetice din regiunea gurii și a eczemelor de pe mâini și picioare. Însoțită de febră mare și diaree, această enteroviroză

[19] *OMS atrage atenția asupra riscului unei pandemii de gripă*, Rompres, 17.10.2007, http://www.romedic.ro/stiri-medicale/Stiri_generale_0341/OMS_atrage_atentia_asupra_riscului_unei_pandemii_de_gripa_04178.html, accesat la 08.01.2009; Neeti Mittal, Bikash Medhi, *The Bird Flu: A New Emerging Pandemic Threat and Its Pharmacological Intervention*, în *International Journal of Health Sciences*, 2007, iulie, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3068632/, accesat la 10.04.2020.

[20] *Feature: Colleagues and patients honor doctor killed by SARS (2),* http://www.highbeam.com/doc/1P2-13415220.html, accesat la 02.04.2020.

este extrem de gravă prin patogenitate și infecțiozitate. Nici până acum cercetătorii nu au reușit să descopere mecanismul patogenic al acestui virus[21].

Infecția HIV-SIDA. S-au scris tomuri întregi despre această infecție, s-au alocat sume uriașe pentru descoperirea virusului implicat în apariția acestei boli, pentru găsirea unui tratament, pentru campanii de informare, pentru industria de *safety*, s-au făcut filme, s-au ridicat monumente, într-un cuvânt, această infecție a fost emblema ultimului secol, boală care a isterizat omenirea și care a adus cele mai mari profituri industriilor de consumabile medicale și sanitare de unică folosință. Continentul cel mai afectat a fost cel african, locul multor orori și spațiu de confruntare a marilor interese economice globale în materie de petrol, minereuri strategice, diamante, uraniu etc. Cu toate că cele mai potente organizații caritabile se implică financiar în combaterea acestui flagel și mari companii multinaționale își comercializează cu mare succes ultimele minuni tehnice în identificarea și evaluarea infecției cu înspăimântătorul virus, rezultatele din teren sunt încă negative.

Continentul cel mai afectat de infecția cu HIV-SIDA a fost cel african, locul multor orori și spațiu de confruntare a marilor interese economice globale în materie de petrol, minereuri strategice, diamante, uraniu etc.

În cursul uneia dintre multele conferințe care au loc anual pe tema infecției cu retrovirusul imunodeficienței umane dobândite, reprezentanții *Médecins Sans Frontières* au făcut publice câteva realități de la fața locului, spunând că: *„o infirmieră în Malawi ține în viață 400 de pacienți acordându-le tratamentul, dar ea nu este plătită decât cu trei dolari pe zi”* – declarație aparținând dr. Moses Massaquoi, coordonator al organizației umanitare în Malawi[22] – și că *„este devastator să stai și să vezi cum oamenii se îmbolnăvesc tot mai rau – și cum mor uneori – în timp ce așteaptă săptămâni și chiar luni înainte de a fi tratați, pur și simplu pentru că nu există suficienți lucrători în domeniul sănătății”*, iar aceia care există sunt *„supraîncărcați de muncă, prost plătiți și subevaluați”* – afirmația dr. Mit Philips privind

[21] C. Chi, Q. Sun, S. Wang, Z. Zhang, X. Li, C.J. Cardona, Y. Jin, Z. Xing, *Robust antiviral responses to enterovirus 71 infection in human intestinal epithelial cells*, May 16, 2013, US National Library of Medicine National Institutes of Health, https://www.ncbi.nlm.nih.gov/pubmed/23685430, accesat la 10.03.2020.

[22] *Mind the Deadly Gaps: Health Care Worker Shortages in Southern Africa Causing Fatal Delays in Bringing AIDS Care to Those in Urgent Need*, https://www.internationalbudget.org/wp-content/uploads/2011/04/newsletter46.pdf, accesat la 02.04.2020.

situația medicilor și a cadrelor medicale din statele cu prevalență mare a bolii, citat de AFP. Într-adevăr, flagelul secolului nu este nici pe departe limitat sau ținut sub control. Zilnic, se produc noi îmbolnăviri, boala a depășit dimensiunile continentale, devenind pandemia cea mai *„de succes”* care a afectat, deopotrivă, lumea occidentală, precum și pe cea asiatică sau africană. Faptul că această boală a afectat simultan și pe cei bogați, frumoși și celebri, ca și pe cei săraci a demonstrat, încă o dată, faptul că, în fața bolii și a morții, cu toții suntem egali și că un microorganism, rod al nu se știe cărei conjuncturi, ajunge să-și ia tributul, indiferent de numele purtat de victima sa.

Raport OMS: 39 de noi boli infecțioase din 1967 până în prezent, printre care infecțiile cu HIV-SIDA, SARS, Ebola, enterovirus 71 etc. și a peste 1.100 de episoade epidemice în regiuni diferite ale globului.

În raportul anual al OMS, dat publicității în 2007[23], se atrăgea atenția că riscul apariției unor epidemii globale este tot mai mare. În raport se menționează faptul că, *„în lumea noastră, din ce în ce mai interconectată, noi boli apar cu o frecvență fără precedent, de multe ori având posibilitatea de a traversa granițele și a se răspândi rapid”*, responsabilii instituției amintind de apariția a **39 de noi boli infecțioase din 1967 până în prezent**, printre care infecțiile cu HIV-SIDA, SARS, Ebola, enterovirus 71 etc. și a peste 1.100 de episoade epidemice în regiuni diferite ale globului. De asemenea, se menționează că, *„având în vedere că aproximativ 2,1 miliarde de persoane se deplasează anual prin intermediul liniilor aeriene, riscul declanșării unei epidemii globale este foarte ridicat”*. Totodată, oficialii OMS au cerut statelor lumii să-și asigure stocuri suficiente de vaccinuri și medicamente de urgență destinate combaterii unor eventuale epidemii. Din păcate, apelul lor a rămas fără ecou. În anul 2020, omenirea este la fel de expusă riscurilor descrise de specialiștii OMS precum era înainte de 2007.

În anul 2020, omenirea este la fel de expusă riscurilor descrise de specialiștii OMS precum era înainte de 2007.

Variola a omorât, numai în secolul al XX-lea, între 300 și 500 de milioane de persoane. În anul 1967 s-au înregistrat 15 milioane de îmbolnăviri și două milioane de decese. În același an, OMS a demarat o campanie intensă de vaccinare și de informare a opiniei publice cu privire la această boală, astfel că, 10 ani mai târziu, variola a fost total eradicată. Din acel moment, nu s-a mai semnalat niciun caz, variola

[23] *The world health report 2007 – A safer future: global public health security in the 21st century,* WHO, https://www.who.int/whr/2007/en/, accesat la 02.04.2020.

fiind singura boală contagioasă ai cărei germeni, *orthopox viridae*, au fost total eliminați din mediul înconjurător. Este foarte contagioasă, se transmite prin contact direct sau prin obiecte contaminate. După o perioadă relativ lungă de incubație asimptomatică, de 12-14 zile, declanșează febra ridicată, cefaleea, durerile violente lombare și exantemul pustulos. Vaccinarea și izolarea bolnavilor stopează rapid boala. Întrucât vaccinul anti-variolic conține germeni atenuați, nu se justifică vaccinarea anticipată, deoarece se poate produce îmbolnăvirea dacă organismul este slăbit. Mortalitatea variază între 20% și 50% din cazuri. Variola a fost instrumentul biologic al genocidului din 1763, când colonizatorii englezi au lichidat triburile amerindiene din Ottawa. Nativilor americani li s-au dat cadou pături infectate cu variolă. În două săptămâni, mii de nativi au murit[24].

Febrele hemoragice (Lassa, Ebola) sunt, probabil, marea spaimă a instituțiilor cu atribuții în asigurarea securității naționale. Primele cazuri oficiale de Ebola au fost înregistrate în regiunea cu același nume, din actuala R.D. Congo, în anii 1970-1980, când s-au descoperit numeroase cadavre de primate și de oameni, cu sângele șiroind din zeci și zeci de răni. Încă nu s-au descoperit, cu certitudine, organismele rezervor, chiar dacă unii incriminează liliecii frugivori. Nu se cunoaște niciun fel de tratament eficient și nu se pot stabili nici măsuri profilactice active. La ora actuală, se știe sigur că virusul Ebola se transmite prin contactul cu dejecțiile și fluidele umane ale persoanelor infectate. Cu toate acestea, din fericire, atât Ebola, cât și Lassa nu ar putea fi arme biologice prea eficiente în mâinile unor teroriști, întrucât bolnavii mor atât de repede, încât nu mai au timp să transmită maladia[25]. Caracteristica acestor boli o reprezintă febra ridicată, durerile musculare intense și microhemoragiile care afectează vasele capilare din întregul organism, motiv pentru care febra Ebola a mai fost numită *„boala celor un milion de tăieturi”*. Mortalitatea atinge ușor 90% din cazuri în primele două săptămani.

Ebola și Lassa nu ar putea fi arme biologice prea eficiente în mâinile unor teroriști, întrucât bolnavii mor atât de repede, încât nu mai au timp să transmită maladia.

[24] Patrick J. Kiger, *Did Colonists Give Infected Blankets to Native Americans as Biological Warfare?,* History, 25.11.2019, https://www.history.com/news/colonists-native-americans-smallpox-blankets, accesat la 03.04.2020.

[25] L. Borio, T. Inglesby, C.J. Peters et al, *Hemorrhagic fever viruses as biological weapons: medical and public health management,* 2002, May 8, https://www.ncbi.nlm.nih.gov/pubmed/11988060, accesat la 02.04.2020.

Virusul Nipah este o descoperire de dată recentă a microbiologilor. În 1999, în regiunea Nipah din Malaezia, a izbucnit o epidemie de encefalită care a omorat 105 oameni, fără ca cineva să poată stabili cauza bolii. Virusologii au reușit să izoleze virusul Nipah, dar nu au putut stabili rezervorul. Se pare că este o zoonoză care afectează oamenii și porcii, se transmite prin contact direct cu fluidele infectate ale oamenilor și animalelor, are o perioadă de incubație de 4-18 zile și, după un prodrom de tip gripal, produce inflamarea creierului, urmată de comă și deces. Nu există tratament[26]. Este inclus în categoria armelor biologice de tip B.

Virusurile Himera sunt rodul laboratoarelor militare aflate în căutarea armei perfecte. Sunt denumite astfel după personajul mitic cu același nume, Himera, monstrul tricefal cu un cap de șarpe, unul de leu și unul de țap. Asemenea Himerei, aceste virusuri sunt obținute prin combinarea materialului genetic aparținând celor mai agresive virusuri existente la ora aceasta. În anii '90, Dr. Ken Alibek, cercetător în cadrul programului sovietic *Chimera*, a defectat în SUA și a declarat, în fața Congresului, că URSS a dezvoltat un virus care combină patogenitatea a două dintre cele mai letale microorganisme: Ebola și variola[27]. Ulterior, Alibek și-a publicat o parte din cunoștințele în domeniu în cartea *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told from Inside by the Man Who Ran It*[28] *(Biohazard: Povestea adevărată și înfiorătoare a celui mai mare program secret de arme biologice din lume – Povestit din interior de omul care l-a condus).*

Se cunoaște că unele armate au stocuri de virus variolic combinat cu virusul encefalitei venezuelene și se discută intens, deocamdată la nivel de teorie a conspirației, despre caracterul artificial, de laborator, al virusului HIV, precum și despre posibilitatea apariției **unui virus hibrid de HIV și gripă, transmisibil pe cale aeriană**. Bineînțeles

[26] *Nipah virus infection,* WHO, https://www.who.int/csr/disease/nipah/en/, accesat la 02.04.2020.
[27] Vezi http://www.house.gov/jec/hearings/intell/alibek.htm, accesat la 02.04.2009.
[28] Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told from Inside by the Man Who Ran It*, Delta; Reprint edition (April 11, 2000).

că prima întrebare care se naște într-un astfel de caz este legată de consecințele deversării în libertate, chiar și accidental, a unei astfel de arme. În ce s-ar transforma omenirea, cum ar putea supraviețui fără echipament de protecție chiar și cei care finanțează și plănuiesc asemenea monstruozități? Un prim răspuns îl avem chiar acum, când Covid-19 face ravagii în rândul populației vârstnice și a paralizat economia mondială.

b) Bacterii

Ciuma, morbul care a înspăimântat omenirea de-a lungul câtorva mii de ani, este generată de o bacterie, *Yersinia pestis*, și se poate manifesta sub două forme clinice: *ciuma bubonică* și *ciuma pulmonară*. Calea de transmitere a bolii este prin contactul cu fluide corporale infectate și prin ciupiturile insectelor hematofage, precum puricii și păduchii. În lipsa tratamentului, în primele 24 de ore de la infectare, mortalitatea este de 70%-90%, ceea ce face din acest microb o armă bacteriologică însemnată. Ciuma, tifosul exantematic și mai recenta pancardită infecțioasă cu *Bartonella rochalimae*[29] sunt afecțiuni transmise de insectele care parazitează șobolanii, rozătoare al căror număr, în unele aglomerări urbane din state asiatice, africane și nu numai, depășește numărul oamenilor. Marca bolii o reprezintă un ganglion axilar infectat. Dacă abcesul ganglionar drenează, bolnavul scapă, dacă nu, în absența unui tratament antibiotic adecvat, moare prin septicemie.

Antraxul reprezintă o afecţiune determinată de o bacterie, Bacillus anthracis, care poate rezista în praf, sub formă de spori, până la 40 de ani, aspect extrem de important în evaluarea eficacităţii pe termen lung a unei astfel de arme. Calea de transmitere este aeriană, cutanată şi digestivă, forma pulmonară a bolii fiind mortală 100%.

Antraxul sau **dalacul** reprezintă o afecțiune determinată de o bacterie, *Bacillus anthracis*, care poate rezista în praf, sub formă de spori, până la 40 de ani, aspect extrem de important în evaluarea eficacității pe termen lung a unei astfel de arme. Calea de transmitere este aeriană, cutanată și digestivă, forma pulmonară a bolii fiind mortală 100%. Marca bolii este așa-numita *„bubă neagră"*, care apare în antraxul cutanat la locul inoculării, unde se creează o zonă de necroză responsabilă de culoarea închisă a tegumentului. Moartea survine

[29] *Scientists discover 21st century black plague that spreads from rats to humans*, Daily Mail, 24.11.2008, https://www.dailymail.co.uk/health/article-1088887/Scientists-discover-21st-century-black-plague-spreads-rats-humans.html, accesat la 02.04.2020.

prin septicemie în câteva ore de la inoculare, patogenitatea sa fiind atât de ridicată, încât, și în cazul unui tratament aplicat rapid, mortalitatea este de 75%.

Cercetările militare în privința acestui microb datează din anii ’80, când atât armata sovietică, dar și armata americană au acumulat stocuri de rachete cu nucleu de antrax. În contextul atacurilor teroriste din 2001, Biroul Federal de Investigații (FBI) a dat publicității o informație privind o posibilă legătură între atacurile cu antrax din 2001 și persoane având conexiuni cu un centru militar american[30].

Cunoscută drept boala iepurilor, tularemia a făcut numeroase victime în timpul celui de-al Doilea Război Mondial, când armata germană și cea sovietică s-au acuzat reciproc că au folosit iepuri infectați drept arme biologice.

Tularemia. Bacteria *Francisella tularensis* este una dintre cele mai infecțioase, putându-se transmite atât pe cale aeriană, digestivă, sangvină, cât și prin contact cu fluide animale contaminate. Cunoscută drept *boala iepurilor*, tularemia a făcut numeroase victime în timpul celui de-al Doilea Război Mondial, când armata germană și cea sovietică s-au acuzat reciproc că au folosit iepuri infectați drept arme biologice. Perioada de incubație de 3-5 zile, timp în care omul infectat devine rezervor, face ca periculozitatea bolii să crească. Această bacterie este inclusă în categoria armelor biologice. În anii ’50, SUA, URSS, Marea Britanie și Canada au dezvoltat unități de producție de astfel de arme, iar în 1990, cercetătorii suedezi au izolat o tulpină extrem de periculoasă, rezistentă la antibiotice[31]. Întrucat este sensibilă la radiațiile solare, specialiștii în contra-bioterorism susțin că un atac terorist cu o tulpină de *Francisella* ar putea fi eficient numai în spații întunecoase și foarte aglomerate, cum ar fi stațiile de metrou sau pasajele pietonale subterane[32].

Botulismul este o boală paralitică foarte gravă, cauzată de neurotoxina bacteriei *Clostridium botulinum*. Bacteria este comună și foarte răspândită în natură, fiind prezentă în stare latentă, de spori, în

[30] *A Study of The 2001 Anthrax Terror Attacks and the History of Biological Warfare,* 01.04.2015, https://www.fasebj.org/doi/abs/10.1096/fasebj.29.1_supplement.735.3, accesat la 02.04.2020.

[31] Kristy Young Johnson, Paul Matthew Nolan, *Biological Weapons: Recognizing, Understanding, and Responding to the Threat*, Hoboken, NJ: Wiley, 2016, p. 98, https://books.google.ro/books?id=O4ebCgAAQBAJ&pg=PA98&lpg=PA98&dq=tularemia+Russia+2005+biological+weapon&source=bl&ots=d90NA_Zxoc&sig=ACfU3U3M16f5YjFVnmHFhqwaNfJv_hUHjQ&hl=ro&sa=X&ved=2ahUKEwiEgpqMndfoAhULHcAKHdFqBO04ChDoATAAegQICxAq#v=onepage&q=tularemia%20Russia%202005%20biological%20weapon&f=false, accesat la 02.04.2020.

[32] *Ibidem*.

sedimentele din sol și ocean. Dacă ajunge în medii anaerobe, cum ar fi, de exemplu, conservele, rănile adânci sau tractul intestinal, sporii germinează în bacterii active, care se înmulțesc și produc toxină. Clostridium botulinum produce opt tipuri de toxine (de la A până la H), considerate a fi printre cele mai puternice toxine cunoscute în acest moment. De exemplu, o formulă mult diluată de toxină botulinică A este utilizată clinic sub denumirea de Botox și o formulă multdiluată de toxină botulinică B este utilizată clinic sub numele de Myobloc[33]. Netratat, botulismul produce paralizia mușchilor striați, inclusiv a musculaturii respiratorii, urmată de deces în 24-72 de ore. Faptul că această bacterie se transmite pe cale aeriană, cutanată (dacă există o rană adâncă) și alimentară face ca periculozitatea ei să fie maximă. Toxinele botulinice se înscriu printre cele mai eficiente arme biologice, deoarece:

- sunt extrem de puternice și letale, fiind necesare cantităţi infinitesimale pentru uciderea unui adult de 70 kg (inhalarea a 0,7-0,9 µg de toxină botulinică aerosolizată);
- unele dintre ele sunt relativ ușor de produs și de transportat;
- bolnavii de botulism necesită îngrijiri intensive, chestiune care paralizează sistemul de asistenţă medicală[34].

Netratat, botulismul produce paralizia mușchilor striaţi, inclusiv a musculaturii respiratorii, urmată de deces în 24-72 de ore. Faptul că această bacterie se transmite pe cale aeriană, cutanată (dacă există o rană adâncă) și alimentară face ca periculozitatea ei să fie maximă.

Holera este o afecțiune extrem de gravă și contagioasă, generată de *Vibrio Cholerae.* Este o boală diareică acută severă, însoțită de vomismente abundente, care determină exicoza – deshidratarea rapidă a bolnavului prin pierdere masivă de electroliți. Mortalitatea depășește 85% din cazuri, la izbucnirea epidemiei. Calea de transmitere a vibrionului este digestivă, fecal-orală. În condiții naturale, este o epidemie hidrică specifică sărăciei și subdezvoltării, fiind transmisă fie prin apa de băut infectată cu fecale ca urmare a sanitației deficitare, fie prin consumul de pește infectat și/sau de apă provenită din ape curgătoare sau stătătoare infectate. La începutul secolului trecut, marele savant român, doctorul Ion Cantacuzino (1863-1934), a izolat

[33] *Botulinum Toxin (Botulism*), UPMC Center for Health Security, 2014, 26.02.2014, http://www.centerforhealthsecurity.org/our-work/publications/botulinum-toxin-botulism-fact-sheet, accesat la 02.04.2020.

[34] *Botulinum Toxin (Botulism), op. cit.*

vibrionul și a produs primul vaccin antiholeric, pe care l-a administrat trupelor române aflate pe front în timpul celui de-al Doilea Război Balcanic (16 iunie 1913 – 18 iulie 1913), salvându-le de la extincție și schimbând radical soarta războiului[35]. Transformat în armă, vibrionul holeric își sporește contagiozitatea, virulența și patogenitatea, fiind inclus în categoria armelor biologice de categoria B.

Infecțiile alimentare globale. Încă din 2006, autorul lucrării *The Omnivore's Dilemma: A Natural History of Four Meals*[36] *(Dilema Omnivorului: O Istorie Naturală a celor Patru Mese)*, jurnalistul american Michael Pollan[37] a atras atenția opiniei publice asupra riscului unor pandemii cu *Salmonella* și *Colibacil* ca urmare a consumului hranei comercializate, la nivel global, de marile corporații din industria alimentară. Aceste corporații au ajuns să monopolizeze întreg lanțul de fabricație, de la producție și până la desfacere. În acest sens, Pollan amintește că, în 2007, SUA s-au confruntat cu infecții digestive severe cauzate de consumul de conserve de spanac infectate cu Salmonella. De asemenea, anul 2008 a fost anul roșiilor infectate cu același enterobacil și menționează că *„80% din carnea de vită din SUA provine din fermele deținute de patru companii, alte două procesează frunzele de salată de pe piață, iar 30% din lapte este procesat de către o singură companie"*. În acest mod, un agent patogen insinuat în linia de producție a alimentelor de tip *fast food*, semipreparate sau conserve poate ajunge, fără nicio dificultate, în orice regiune a globului. Ulterior, cazurile de toxiinfecții grave cu botulism declanșate de consumul unor conserve de chili insuficient preparate termic (cazul Castleberry's Food Company din 2007) sau alertele epidemice privind anumite produse alimentare (castraveții contaminați cu bacteria E-coli în 2011) confirmă temerile jurnalistului american.

[35] Raluca Bajenaru, *Prof. Dr. Ioan Cantacuzino, fondatorul școlii române de microbiologie*, 08.02.2012, https://medicaacademica.ro/prof-dr-ioan-cantacuzino-fondatorul-scolii-romane-de-microbiologie/, accesat la 01.04.2020.

[36] Michael Pollan, *The Omnivore's Dilemma: A Natural History of Four Meals*, Penguin Books; First edition (April 11, 2006).

[37] Alex Koppelman, *What's wrong with our food?,* Salon, 07.12.2006, http://www.salon.com/news/feature/2006/12/07/pollan_bad_food/, accesat la 10.03.2020.

Pandemia globală a rezistenței la antibiotice este un alt subiect care incită îngrijorarea specialiștilor în sănătate publică. Ramuri medicale precum marea chirurgie, chimioterapia oncologică, transplantul de organe, terapiile bolilor degenerative au început să se confrunte cu creșterea rezistenței bacteriene la antibiotice, consecință a abuzului de medicamente. În aceste condiții, ritmul de perimare a antibioticelor a depășit cu mult ritmul descoperirii altora noi și eficiente. Este de notorietate revenirea în forță, pe plan mondial, a tuberculozei multidrog-rezistente, precum și apariția, în anii '90, a stafilococilor rezistenți la meticilină (penicilină sintetică, antibiotic de elecție în infecții stafilococice sistemice), ca urmare a abuzului de antibiotice. În general, dacă o infecție este depistată înainte ca germenii să pătrundă în sânge, este ușor rezolvabilă medicamentos, prin antibioterapie țintită. Dar, dacă s-a produs bacteriemia/septicemia, singurele antibiotice care mai pot distruge germenele sunt cele de rezervă, denumite astfel, întrucât reprezintă ultima variantă de tratare a infecției respective. Problema este extrem de gravă, deoarece apariția tulpinilor bacteriene cu rezistență multiplă este mai rapidă decât ritmul descoperirilor de noi antibiotice, fiind o chestiune de timp până când vor apărea stafilococi sau alte bacterii letale prin rezistența dobândită la orice tip de antibiotic[38].

Ramuri medicale precum marea chirurgie, chimioterapia oncologică, transplantul de organe, terapiile bolilor degenerative au început să se confrunte cu creşterea rezistenţei bacteriene la antibiotice, consecință a abuzului de medicamente.

c) Protozoare

Malaria este, fără doar și poate, unul dintre marii ucigași ai omenirii. În 2018, malaria a afectat 228 de milioane de oameni, dintre care peste 405.000 au murit[39]. Este endemică în regiunile tropicale și subtropicale din Africa, Asia, America Centrală și de Sud, unde mediul umed și cald, aflat în bălțile, mlaștinile și sistemele de canalizare colmatate din marile aglomerări urbane, creează condițiile ideale dezvoltării țânțarilor anofeli. Cauza acestei parazitoze sangvine o reprezintă un protozoar, *Plasmodium malariae,* cu cele patru subtipuri ale sale, dintre care

[38] *Antimicrobial resistance*, 15.02.2018, WHO, https://www.who.int/news-room/fact-sheets/detail/antimicrobial-resistance, accesat la 03.04.2020.

[39] *World malaria report 2019*, World Health Organization, 4 december 2019, https://www.who.int/publications-detail/world-malaria-report-2019, accesat la 01.04.2020.

cele mai frecvente sunt *Plasmodium vivax* și *Plasmodium falciparum*. În unele regiuni din Africa Subsahariană, prevalența bolii depășește 90% din populație. Pe lângă pierderile de vieți omenești, malaria are și un impact economic major prin:

- incapacitatea de muncă indusă de accesele febrile recurente;
- costul tratamentelor, al spitalizărilor;
- frecvenţa anomaliilor genetice precum siclemia sau talasemia, provocate de infecţia plasmodică;
- scăderea activităţilor de turism şi a activităţilor economice conexe etc.

Se consideră că impactul economic al malariei asupra Africii depășește 12 miliarde de dolari anual[40], iar în țări cu prevalență mare, poate costa peste 40% din cheltuielile pentru asistență publică. Nu trebuie uitat faptul că, în Africa, infecția HIV, tuberculoza și infecțiile digestive sunt endemice, aceste boli debilizante favorizând recurențele atacurilor de malarie. Practic, în viitor, pe fondul agravării crizei economice și al alterării condițiilor de viață în regiunile mai sus-amintite, ne putem aștepta la o creștere a numărului de victime ale acestui flagel și la o împovărare economică suplimentară a statelor afectate.

Insectele sunt soldaţi exemplari, care pot ajunge neobservaţi în liniile inamice şi pot transmite cu repeziciune maladii letale.

Insecte folosite ca vectori de transmitere a bolilor. În anul 2008, entomologul american Jeffrey A. Lockwood a publicat cartea intitulată *Six-Legged Soldiers: Using Insects as Weapons of War*[41] *(Soldatul cu șase picioare: Folosirea insectelor ca arme de război)*, în care afirmă, așa cum reiese din titlu, că insectele sunt soldați exemplari, care pot ajunge neobservați în liniile inamice și pot transmite cu repeziciune maladii letale. Un astfel de exemplu de maladie letală transmisă de insecte este *Febra Văii Riftului*, denumită astfel după valea cu același nume din Kenya. Acolo, în estul Africii, în anul 1931, a izbucnit o epidemie neobișnuită, care a ucis oameni și animale, deopotrivă.

[40] B.M. Greenwood, K. Bojang, C.J. Whitty, G.A. Targett, *Malaria,* Lancet 365: 1487-1498, 2005, doi:10.1016/S0140-6736(05)66420-3. PMID 15850634, https://www.ncbi.nlm.nih.gov/pubmed/15850634, accesat la 02.04.2020.

[41] Jeffrey A. Lockwood, *Six-Legged Soldiers: Using Insects as Weapons of War*, Oxford University Press, SUA, October 10th, 2008.

Ulterior, microbiologii au identificat agentul patogen în persoana unui virus transmis prin contact direct cu fluidele organice infectate sau prin ciupitura de țânțari. Această zoonoză poate avea forme de manifestare diferite, meningo-encefalitică, hemoragică sau oculară și, netratată, determină decesul persoanei infectate. Un alt exemplu îl reprezintă virusurile *Febrei Galbene* (a ficatului) și *Febrei Dengue*, transmise prin ciupitura țânțarului Aedes. În acest context, profesorul Lockwood a susținut că grupările teroriste ar putea declanșa foarte ușor un atac bioterorist cu ajutorul insectelor infectate transportate în valize, pe care teroriștii le-ar putea introduce, fără probleme, pe teritoriul statelor țintă, declarând că *„teroriștilor le-ar fi mult mai ușor să folosească insectele decât să dezvolte o armă nucleară sau chimică pentru că materia primă se găsește în curtea casei”*[42]. Afirmațiile lui Lockwood sunt cât se poate de serioase și de logice. Este suficient să ne imaginăm ce s-ar întâmpla dacă țânțari Aedes infectați ar fi eliberați într-o regiune în care populația nu a fost imunizată? Ar urma un val uriaș de îmbolnăviri și de decese, știut fiind că nu există tratament pentru niciuna dintre aceste maladii. La fel cum reintroducerea țânțarilor anofeli într-o regiune precum Delta Dunării, unde aceste insecte au existat în trecut, ar crea o situație epidemiologică foarte serioasă.

Și, nu în ultimul rând, trebuie să amintim căpușele, vectorii bolii Lyme. Subiectul instrumentalizării militare a căpușelor a reizbucnit în forță în *mass-media* americană în cursul anului 2019, când Congresul SUA, în urma unui amendament depus de congresman-ul republican de New Jersey, Chris Smith, a solicitat o anchetă care să stabilească dacă există vreo legătură între răspândirea bolii Lyme și un presupus experiment militar al Pentagonului. Smith și-a argumentat amendamentul spunând că a fost inspirat de *„o serie de cărți și articole care sugerează că s-au făcut cercetări importante în facilitățile guvernamentale americane, inclusiv în Fort Detrick, Maryland și Plum Island, New York, pentru a transforma căpușele și… insectele în arme*

[42] Stephen Adams, *Terrorists could use insect based biological weapon*, *The Telegraph*, 05.01.2009, https://www.telegraph.co.uk/news/earth/wildlife/4123782/Terrorists-could-use-insect-based-biological-weapon.html, accesat la 02.04.2020.

biologice”[43]. Una dintre cărțile la care făcea referire Smith este *Bitten: The Secret History of Lyme Disease and Biological Weapons*[44] *(Mușcat: Istoria secretă a bolii Lyme și a armelor biologice)*, scrisă de Kris Newby, cercetător la Universitatea Stanford, el însuși bolnav de Lyme. În cartea respectivă, se afirmă că entomologul Willy Burgdorfer (1925-2014), cel care a descoperit agentul etiologic al bolii, spirocheta *Borrelia burgdorferi*, ar fi spus că epidemia Lyme, care a afectat populația SUA în anii ’60, ar fi fost un experiment militar nereușit. Mai mult, spune Newby, Willy Burgdorfer, fost cercetător în biotehnologii militare pentru armata americană, ar fi afirmat că a avut misiunea de a crește și înmulți purici, căpușe, țânțari și alte insecte hematofage pe care le-a infectat cu agenți patogeni ai unor boli umane. Programul militar amintit are rădăcini în perioada Germaniei naziste, prin doctorul Erich Traub (1906-1985), cel care ar fi fost implicat în cercetări militare privind *febra aftoasă*, *Rinderpesta*, *pseudorabia*, *enteroviroza cu virus intestinal 71* și *Borelia*[45]. Traub ar fi fost șeful *Insel Riems*, un laborator secret nazist din regiunea baltică, unde a avut misiunea de a produce arme biologice menite să distrugă șeptelul Uniunii Sovietice[46]. Ajuns în SUA după război, Traub a lucrat ca cercetător în laboratorul din Fort Detrick, Frederick, Maryland. Boala Lyme, produsă de mușcătura unei capușe infectate cu *Borelia burgdorferi,* este cunoscută pentru eritemul mobil, însoțit de febră, paralizie facială, artrită, dureri intermitente la nivelul tendoanelor, mușchilor, articulațiilor și oaselor, inflamarea creierului și a măduvei spinării, dureri severe de cap și rigiditate a gâtului, care duc, în final, la deces.

Boala Lyme, produsă de mușcătura unei capușe infectate cu Borelia burgdorferi, este cunoscută pentru eritemul mobil, însoțit de febră, paralizie facială, artrită, dureri intermitente la nivelul tendoanelor, mușchilor, articulațiilor și oaselor, inflamarea creierului și a măduvei spinării, dureri severe de cap și rigiditate a gâtului, care duc, în final, la deces.

[43] Julian Borger, *House orders Pentagon to review if it exposed Americans to weaponised ticks*, *The Guardian*, 16.07.2019, https://www.theguardian.com/us-news/2019/jul/16/pentagon-review-weaponised-ticks-lyme-disease, accesat la 03.04.2020.

[44] Kris Newby, *Bitten: The Secret History of Lyme Disease and Biological Weapons*, Harper Wave; 1 edition (May 14, 2019).

[45] Karl Grossman, *Lyme Disease and Biowarfare*, Counter Punch, 14.08.2019, https://www.counterpunch.org/2019/08/14/lyme-disease-and-biowarfare/, accesat la 03.04.2020.

[46] *Ibidem*.

ÎN LOC DE CONCLUZII

Din păcate, pericolele pandemic și bioterorist au fost trecute, în mod constant, pe un plan secund al preocupărilor decidenților politici, dovada stând modul în care statele lumii au gestionat primele luni ale actualei pandemii cu coronavirus. Cu toate acestea, efectele devastatoare, multisectoriale, ale acestei pandemii la nivel statal au demonstrat, încă o dată, că agentul microbian poate fi acel *„David”* care îl poate pune la pământ pe *„Goliath”.*

În cazul mutației naturale a agentului patogen, efectele pandemice pot fi cataclismice, pentru că *„noutatea”* genomică aduce cu sine patogenitate și virulență neobișnuite, tratamente care nu mai funcționează, panica, suprasolicitarea sistemului medical, închiderea economiei și numeroase victime umane sau animale.

În cazul unei arme biologice, întrucât producătorul trebuie să dețină și un antidot, pentru a nu-și distruge și propria armată/propriul popor, situația este mai ușor de gestionat, tulpinile respective având *„un termen de valabilitate”* limitat, pentru a permite invazia teritoriului atacat biologic.

Și într-un caz, și în celălalt, cunoașterea acestor agenți patogeni, înțelegerea modului în care ei acționează și, mai ales, o justă pregătire și organizare a mijloacelor de contracarare și contenție a focarelor epidemice pot salva vieți, locuri de muncă, libertăți individuale, recolte, șeptel etc.

BIBLIOGRAFIE:

1. ***, *A Study of The 2001 Anthrax Terror Attacks and the History of Biological Warfare,* 01.04.2015, https://www.fasebj.org/doi/abs/10.1096/fasebj.29.1_supplement.735.3
2. ***, *Antimicrobial resistance*, 15.02.2018, WHO, https://www.who.int/news-room/fact-sheets/detail/antimicrobial-resistance
3. ***, *Biological weapons*, World Health Organization, https://www.who.int/health-topics/biological-weapons#tab=tab_1
4. ***, *Botulinum Toxin (Botulism*), UPMC Center for Health Security, 2014, 26.02.2014, http://www.centerforhealthsecurity.org/our-work/publications/botulinum-toxin-botulism-fact-sheet
5. ***, *Emerging Pandemic Threat And Its Pharmacological Intervention*, *International Journal of Health Sciences*, 2007, July, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3068632/

6. ***, *Feature: Colleagues and patients honor doctor killed by SARS (2),* http://www.highbeam.com/doc/1P2-13415220.html
7. ***, *Mind the Deadly Gaps: Health Care Worker Shortages in Southern Africa Causing Fatal Delays in Bringing AIDS Care to Those in Urgent Need*, https://www.internationalbudget.org/wp-content/uploads/2011/04/newsletter46.pdf
8. ***, *OMS atrage atenția asupra riscului unei pandemii de gripă*, Rompres, 17.10.2007, http://www.romedic.ro/stiri-medicale/Stiri_generale_0341/OMS_atrage_atentia_asupra_riscului_unei_pandemii_de_gripa_04178.html
9. ***, *Nipah virus infection,* WHO, https://www.who.int/csr/disease/nipah/en/
10. ***, *Rice-Detailed Study of Diseases*, http://www.ikisan.com/links/ap_riceDetailedStudyofDiseases.shtml
11. ***, *World malaria report 2019*, World Health Organization, 4 december 2019, https://www.who.int/publications-detail/world-malaria-report-2019
12. Stephen Adams, *Terrorists could use insect based biological weapon*, *The Telegraph*, 05.01.2009, https://www.telegraph.co.uk/news/earth/wildlife/4123782/Terrorists-could-use-insect-based-biological-weapon.html
13. Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World-Told from Inside by the Man Who Ran It*, Delta; Reprint edition, April 11, 2000.
14. Raluca Bajenaru, *Prof. Dr. Ioan Cantacuzino, fondatorul școlii române de microbiologie*, 08.02.2012, https://medicaacademica.ro/prof-dr-ioan-cantacuzino-fondatorul-scolii-romane-de-microbiologie/
15. Julian Borger, *House orders Pentagon to review if it exposed Americans to weaponised ticks*, *The Guardian*, 16.07.2019, https://www.theguardian.com/us-news/2019/jul/16/pentagon-review-weaponised-ticks-lyme-disease
16. L. Borio, T. Inglesby, C.J. Peters et al, *Hemorrhagic fever viruses as biological weapons: medical and public health management*, 2002 May 8, https://www.ncbi.nlm.nih.gov/pubmed/11988060
17. Anthony P. Cardile, Clinton K. Murray, Christopher T. Littell, Neel J. Shah, Matthew N. Fandre, Dennis C. Drinkwater, Brian P. Markelz, Todd J. Vento, *Monitoring Exposure to Ebola and Health of U.S. Military Personnel Deployed in Support of Ebola Control Efforts – Liberia*, 25 octombrie 2014-27 februarie 2015, Morbidity and Mortality Weekly Report (MMWR), Centers for Disease Control and Prevention, 03.07.2015, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6425a2.html
18. C. Chi, Q. Sun, S. Wang, Z. Zhang, X. Li, C.J. Cardona, Y. Jin, Z. Xing, *Robust antiviral responses to enterovirus 71 infection in human intestinal epithelial cells*, May 16, 2013, US National Library of Medicine National Institutes of Health, https://www.ncbi.nlm.nih.gov/pubmed/23685430
19. Eric Croddy, James J. Wirtz, *Weapons of Mass Destruction: Chemical and biological weapons*, ABC CLIO, 2005.
20. Bruce Dorminey, *Ebola As ISIS Bio-Weapon?,* Forbes, 05.10.2014, http://www.forbes.com/sites/brucedorminey/2014/10/05/ebola-as-isis-bio-weapon/
21. Karl Grossman, *Lyme Disease and Biowarfare*, Counter Punch, 14.08.2019, https://www.counterpunch.org/2019/08/14/lyme-disease-and-biowarfare/
22. Kristy Young Johnson, Paul Matthew Nolan, *Biological Weapons: Recognizing, Understanding, and Responding to the Threat*, Hoboken, NJ: Wiley, 2016, https://books.google.ro/books?id=O4ebCgAAQBAJ&pg=PA98&lpg=PA98&dq=tularemia+Russia+2005+biological+weapon&source=bl&ots=d90NA_Zxoc&sig=ACfU3U3M16f5YjFVnmHFhqwaNfJv_hUHjQ&hl=ro&sa=X&ved=2ahUKEwiEgpqMndfoAhULHcAKHdFqBO04ChDoATAAegQICxAq#v=onepage&q=tularemia%20Russia%202005%20biological%20weapon&f=false
23. Patrick J. Kiger, *Did Colonists Give Infected Blankets to Native Americans as Biological Warfare?*, History, 25.11.2019, https://www.history.com/news/colonists-native-americans-smallpox-blankets
24. Alex Koppelman, *What's wrong with our food?*, Salon, 07.12.2006, http://www.salon.com/news/feature/2006/12/07/pollan_bad_food/
25. Jeffrey A. Lockwood, *Six-Legged Soldiers: Using Insects as Weapons of War*, Oxford University Press, USA, October 10th 2008.
26. Kris Newby, Bitten: *The Secret History of Lyme Disease and Biological Weapons*, Harper Wave; 1 edition, May 14, 2019.
27. Michael Pollan, *The Omnivore's Dilemma: A Natural History of Four Meals*, Penguin Books; First edition, April 11, 2006.
28. Alba Iulia Catrinel Popescu, *Jucătorul din Umbră*, Editura Militară, București, 2016.
29. https://www.who.int/mediacentre/influenzaAH1N1_presstranscript_20090611.pdf, accesat la data de 05.04.2020; Alexandra Sandru, *Pericolul aviar: Crezi ca ne vom confrunta cu o pandemie? (sondaj)*, ziare.com, 29.11.2007, http://www.ziare.com/social/capitala/pericolul-aviar-crezi-ca-ne-vom-confrunta-cu-o-pandemie-sondaj-185674.

PROSPECTIVA SECURITĂȚII – IZVOR AL GÂNDIRII MILITARE ROMÂNEȘTI –

Lect. univ. dr. Răzvan GRIGORAȘ

Universitatea Națională de Apărare „Carol I”, București

În acest articol, am adus în discuție studierea viitorului pentru a înțelege care sunt schimbările esențiale ce vor influența securitatea națională. Principala contribuție a acestei lucrări este identificarea a cinci mari tendințe ale anului 2050 și prezentarea impactului pe care acestea îl au asupra gândirii militare românești. Scopul lucrării a fost îndeplinit cu ajutorul analizei tendințelor și a factorilor – metodă arhicunoscută pentru implementarea schimbării și a dezvoltării în organizații. În acest sens, concluzia fundamentală a articolului evidențiază faptul că problema prospectivei devine un mobil, prin care gândirea militară românească poate crea baza securitizării României anului 2050, deschizând drumul Armatei României spre adaptare.

Cuvinte-cheie: prospectivă strategică, ONU, previziunea securității, viitorul armatei, securitatea cibernetică.

Mulțumesc, pe această cale, conducerii Statului Major al Apărării și Comisiei de evaluare a lucrărilor selecționate pentru Premiile revistei *Gândirea Militară Românească*, pentru că au crezut în proiectul *Previziunea securității*, lucrare ce a primit, anul trecut, Premiul *„General de divizie Ștefan Fălcoianu”* al revistei *Gândirea Militară Românească*.

INTRODUCERE ASUPRA STUDIULUI VIITORULUI

Cunoașterea viitorului reprezintă o veche moștenire, pe care J.C. Glenn[1] o consideră a fi insuficient cercetată. Spre deosebire de prezent sau de trecut (ce pot fi cunoscute prin experiența proprie sau prin amintiri), viitorul nu poate face apel la certitudini. În fapt, verificarea rezultatelor anticipate o poate realiza numai trecerea timpului. Din acest motiv, ideea anticipării a fost cantonată, de-a lungul vremurilor, în sfera misticului și a miticului, elementul științific lipsind, în general, din ecuație.

Una dintre abordările coerente ce a determinat apariția caracterului științific al anticipării a fost cea a lui Bertrand de Jouvenel[2]. Acesta a introdus conceptul de *„viitori posibili”* – în esență, stări posibile viitoare care pleacă de la o situație unică și dau naștere unui con al posibilităților. Pe fundamentul acestui concept, s-au dezvoltat ulterior metodologiile specifice anticipării.

Bertrand de Jouvenel a introdus conceptul de „viitori posibili” – în esență, stări posibile viitoare care pleacă de la o situație unică și dau naștere unui con al posibilităților. Pe fundamentul acestui concept, s-au dezvoltat ulterior metodologiile specifice anticipării.

Astăzi, există două curente științifice care grupează cercetările din domeniu. Primul curent – *cel al studiilor prospective* – subsumează eforturile unor cercetători precum J.C. Glenn[3] și R. Popper[4]. Aceștia consideră că scopul anticipării este explorarea stărilor posibile viitoare pentru a îmbunătăți deciziile adoptate. Valoarea studiilor constă mai mult în a deschide mințile către noi posibilități și mai puțin în a analiza acuratețea produsului.

Al doilea curent – *cel al previziunii* – este reprezentat de eforturile unor cercetători precum van Steenbergen[5] sau Gold și Hines[6]. Aceștia consideră că scopul anticipării se concentrează mai mult pe procesul de planificare și pe exactitatea instrumentului de măsurare.

---

1 J.C. Glenn, *Futures Research Methodology Version 3.0.*, Washington D.C.: Millennium Project, 2014.

2 B.d. Jouvenel, *L'art de la conjecture*, Ed. du Rocher, Monaco, 1964.

3 J.C. Glenn, *op. cit.*

4 R. Popper, *Foresight Methodology*, 2008, în L. Georghiou, J. Cassingena, M. Keenan, I. Miles și R. Popper (eds.), *The Handbook of Technology Foresight*, Edward Elgar, Cheltenham, 2008, pp. 44-88.

5 B. Steenbergen, *Scenarios As a Powerful Tool for Public Policy*, în *Proceedings of the Prague Workshop on Futures Studies Methodology*, 2005.

6 J. Gold, A. Hines, *An organizational futurist role for integrating foresight into corporations. Technological Forecasting and Social Change*, 2014, DOI: 101. 10.1016/j.techfore.2014.04.003.

Cele două curente au dat naștere unor stiluri variate ce se găsesc la intersecția dintre previziune și prospectivă[7]. Din rândul preocupărilor lipsesc studiile referitoare la viitorul securității și apărării. Aceasta are loc, întrucât anticiparea în securitate și apărare a fost mai degrabă mobilul practicienilor. Aceasta este și situația **gândirii militare românești**, unde accentul s-a pus pe planificarea acțiunilor militare în raport cu determinarea cursurilor de acțiune ale inamicului.

TENDINȚE ALE ANULUI 2050

Lucrarea de față pune accentul pe implementarea produselor prospectivei strategice în domeniul securității și apărării (prima școală de gândire) și pe modul în care acestea pot fi utilizate de practicienii gândirii militare românești pentru crearea unei posturi strategice solide a României anului 2050.

Raportându-ne la taxonomia anterior descrisă, lucrarea de față pune accentul pe implementarea produselor prospectivei strategice în domeniul securității și apărării (prima școală de gândire) și pe modul în care acestea pot fi utilizate de practicienii gândirii militare românești pentru crearea unei posturi strategice solide a României anului 2050. Mai exact, în acest articol vom prezenta principalii *factori determinanți* care pot influența viitorul securității și apărării naționale[8].

Literatura de specialitate abundă în analize de acest tip, exemple fiind analiza lui Eberhard Sandschneider cu privire la implicațiile digitalizării asupra întregului Glob[9], cea a lui Al Gore cu privire la implicațiile schimbărilor climatice asupra oamenilor[10], analiza periodică pusă la dispoziția National Intelligence Council[11] și, bineînțeles, analiza Ministerul britanic al Apărării din anul 2018, ce poartă titlul de *Global*

[7] Aducem în discuție eforturile lui Godet ce aplică prospectiva strategică în domeniul planificării (M. Godet, *The Art of Scenarios and Strategic Planning: Tools and Pitfalls*, în *Technological Forecasting and Social Change*, 65, 3-22, 2000) și pe cele ale lui Georghiou, ce se concentrează pe dimensiunea socio-economică a previziunii (L. Georghiou, *Third Generation Foresight: Integrating the Socio-economic Dimension*, în *Technology Foresight – the approach to and potential for New Technology Foresight, Conference proceedings, NISTEP Research Material 77*, 2001). Alte eforturi au fost realizate de către E. Masini, care, încă din anul 1983, își punea problema aplicării prospectivei și a modului în care să se realizeze transferul cunoștințelor către planificare (a se vedea E. Masini, *Visions of desirable societies*, Oxford, Pergamon Press, 1983).

[8] În literatura de specialitate, analiza factorilor determinanți are mai multe forme, printre care analiza tendințelor, analiza driver-ilor, analiza semnalelor slabe și a evenimentelor de tip *lebădă neagră*. O detaliere a acestor forme se regăsește pe European Foresight Platform, la adresa http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/, consultat la 12 februarie 2020.

[9] E. Sandschneider, *Drivers of Global Change What Happens When Digital Disruption Meets Geopolitics?*, în *Richard C. Holbrooke Forum*, iunie 2017.

[10] Al Gore, *The Future: Six Drivers of Global Change,* New York, Random House, ed. 2013.

[11] ***, National Intelligence Council, *Global Trends 2030: Alternative worlds*, Washington D.C., 2012.

Strategic Trends: The Future Starts Today[12]. Pe baza lucrărilor mai-sus menționate, am selectat un număr de cinci factori pe care îi considerăm determinanți pentru securitatea României în anul 2050 și la care gândirea militară românească trebuie să reacționeze într-o manieră conjugată. Aceștia sunt: *(1) modelarea unei societăți post-petrol, (2) poluarea și accesul la resursele de apă, (3) impactul tehnologiilor moderne asupra înzestrării forțelor și modelarea spațiului cibernetic, (4) extinderea Consiliului de Securitate al ONU* și *(5) redefinirea sistemului mondial de alianțe.* Vom prezenta, în rândurile următoare, fiecare factor analizat.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Există un număr de cinci factori pe care îi considerăm determinanți pentru securitatea României în anul 2050 și la care gândirea militară românească trebuie să reacționeze într-o manieră conjugată: (1) modelarea unei societăți post-petrol, (2) poluarea și accesul la resursele de apă, (3) impactul tehnologiilor moderne asupra înzestrării forțelor și modelarea spațiului cibernetic, (4) extinderea Consiliului de Securitate al ONU și (5) redefinirea sistemului mondial de alianțe.

(1) Modelarea unei societăți post-petrol

O societate post-petrol reprezintă modalitatea de rezolvare a două probleme majore ale lumii noastre: (1) controlarea consumului de energie și (2) încetinirea poluării și a încălzirii globale. Aceste două elemente sunt interdependente, iar limitele lor se suprapun deseori, făcând dificilă analiza lor separată.

Multe studii se contrazic și creează inconsecvență în rândul decidenților, atunci când analizează consumul de energie. Spre exemplu, Ministerul britanic al apărării aduce în discuție creșterea consumului global de energie – cu până la 60%, până în 2050[13]. *International Futures* oferă o altă perspectivă – deschisă către mai multe posibilități, pe baza anumitor scenarii create (2020). Astfel, consumul global de energie din 2050 poate să scadă cu până la 30%, dar poate să și ia amploare cu până la 60%, așa cum reiese din *figura nr. 1*. Diferențele majore ale estimărilor nu sunt deloc îmbucurătoare și apar pe fondul interacțiunilor dintre doi factori cu efecte contrare: (1) dezvoltarea economiei bazate pe servicii în detrimentul industriilor și (2) implementarea conceptului de *Internet of Things (IOT)*. Primul factor scade consumul energetic, mutând presiunea acestuia către China, iar cel de-al doilea crește consumul, bazându-se pe disponibilitatea anumitor device-uri în cloud.

Totuși, există anumite certitudini. În primul rând, scăderea consumului de energie nu poate fi realizată decât într-o perspectivă ecologistă. În al doilea rând, consumul va fi cu certitudine influențat

[12] ***, Ministerul britanic al Apărării, *Global Strategic Trends: The Future Starts Today*, Londra 2018.

[13] *Ibidem*.

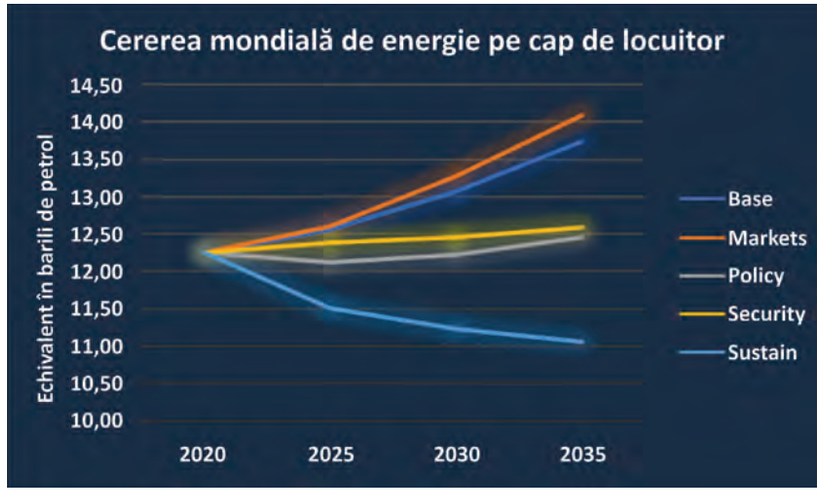

Figura nr. 1: Estimarea cererii de energie mondială în diverse scenarii[14]

* Scenariul Base continuă politicile din prezent, scenariul Markets pune accent pe intensificarea schimburilor economice, scenariul Policy pe politici publice, scenariul Security pe intensificarea măsurilor de securitate națională și scenariul Sustain pe implementarea politicilor ecologice.

Perspectiva unei societăți bazate pe protejarea mediului înconjurător și pe energia regenerabilă reprezintă vectorul controlării consumului de energie. Acest tip de societate este denumită „societatea post-petrol" și devine un mobil al activității economice mondiale.

de precaritatea resurselor. Prin urmare, perspectiva unei societăți bazate pe protejarea mediului înconjurător și pe energia regenerabilă reprezintă vectorul controlării consumului de energie. Acest tip de societate este denumită *societatea post-petrol* și devine un mobil al activității economice mondiale. Credem că apariția societății post-petrol este certă. În schimb, data exactă a apariției rămâne sub semnul întrebării, probabil după anul 2050. Aceasta se întâmplă din cauza apariției fracturării hidraulice și a exploatării gazelor de șist ce vor crea efecte la nivelul economiei americane. Potrivit estimărilor IHS Global Insight, făcute în 2013, gazele de șist vor reprezenta 60% din piața americană în 2035. Potrivit aceluiași raport, creșterea estimată va fi însoțită de un proces investițional ce va însuma peste 1,9 trilioane de dolari și va determina crearea a peste 1,6 milioane de locuri de muncă în anul 2035.

Acest factor influențează gândirea militară românească din două perspective. Prima perspectivă este cea a *adaptării tehnologice*. Aceasta se referă la eficientizarea consumului de energie al echipamentelor militare și la reducerea amprentei de carbon a acțiunilor militare. A doua perspectivă este cea a *securității energetice* a României

[14] Sursa: International Futures, 2020.

și are în vedere asigurarea independenței energetice naționale și protejarea infrastructurilor critice implicate în procesul de producere sau distribuire a energiei.

(2) Poluarea și accesul la resursele de apă

În anul 2015, marii lideri au semnat *Acordul de la Paris* – document care își propune limitarea creșterii temperaturii globale cu 1,5^0 C până în 2050[15]. Sunt multe de făcut în acest sens. Unul dintre elementele importante este scăderea utilizării cărbunelui cu 50% până în 2050 – un obiectiv ambițios –, ținând cont de faptul că International Energy Agency (IEA) prevede că, în anul 2050, lumea încă se va baza pe energia combustibililor fosili în procent de peste 70% (2017). Vom reuși, oare, să renunțăm la jumătate din 70%?

Utilizarea apei potabile aduce cu sine alte polemici. La nivel internațional, exploatarea și utilizarea apei potabile se realizează la cote maximale, conform estimărilor din raportul *Global Strategic Trends: The Future Starts Today*[16]. Pentru anul 2050, se anticipează creșteri masive ale utilizării apei dulci – cu 1,5 trilioane de m^3 de apă mai mult ca în 2010. În aceste condiții, **mai mult de jumătate din populația lumii** nu va avea acces la apă potabilă în anul 2050, potrivit aceleiași surse.

La nivel internațional, exploatarea și utilizarea apei potabile se realizează la cote maximale, conform estimărilor din raportul Global Strategic Trends: The Future Starts Today. Pentru anul 2050, se anticipează creșteri masive ale utilizării apei dulci – cu 1,5 trilioane de m^3 de apă mai mult ca în 2010. În aceste condiții, mai mult de jumătate din populația lumii nu va avea acces la apă potabilă în anul 2050, potrivit aceleiași surse.

La nivelul României, tendința de utilizare a apei este greu de identificat. Scenariile *International Futures* tind să identifice un punct de cotitură în jurul anului 2040. Eventuala scădere din anii 2040 va trebui susținută printr-o politică ecologică bine structurată, așa cum reiese din *figura nr. 2*. Conform estimărilor US National Intelligence Council, făcute în anul 2012, România se va afla într-o zonă **cu stres sever** în legătură cu accesul la apă, după anul 2035, ceea ce va conduce la noi riscuri și vulnerabilități în securitatea națională.

Acest factor influențează gândirea militară românească din perspectiva asigurării accesului la apă al populației și, implicit, al forțelor militare. Scăderea amprentei de carbon a acțiunilor militare va fi un punct sensibil pe agenda presei anului 2050. Nu în ultimul rând, precaritatea accesului la apă, ce se prefigurează începând cu 2035, poate conduce la revolte sociale și la încercarea de redistribuire forțată a acesteia.

[15] *Jurnalul Oficial al UE*, 2016.
[16] ***, Ministerul britanic al Apărării, *op. cit.,* pp. 17-28.

Figura nr. 2: Utilizarea apei pe cap de locuitor în România[17]

* Scenariul Base continuă politicile din prezent, scenariul Markets pune accent pe intensificarea schimburilor economice, scenariul Policy pe politici publice, scenariul Security pe intensificarea măsurilor de securitate națională și scenariul Sustain pe implementarea politicilor ecologice.

(3) Impactul tehnologiilor moderne asupra înzestrării forțelor și modelarea spațiului cibernetic

Tehnologiile moderne și impactul lor asupra acțiunilor militare sunt, astăzi, preocupări majore. Autori, precum M. L. Cummings, Stephan de Spiegeleire și Panwar, au analizat posibilitățile de utilizare a inteligenței artificiale (Artificial Intelligence/ AI) în domeniul militar.

Tehnologiile moderne și impactul lor asupra acțiunilor militare sunt, astăzi, preocupări majore. Autori, precum M.L. Cummings[18], Stephan de Spiegeleire et al[19] și Panwar[20], au analizat posibilitățile de utilizare a inteligenței artificiale (Artificial Intelligence/AI) în domeniul militar. Unele state importante – precum SUA – își propun militarizarea cloud-ului (Army Cloud Computing Strategy, 2015). Nu în ultimul rând, impactul *IoT* asupra conflictelor militare devine un punct-cheie în asigurarea inițiativei și a libertății de mișcare a forțelor, așa cum remarcă și M. Tonin într-un raport către oficialii NATO[21].

[17] Sursa: International Futures, 2020.

[18] M.L. Cummings, *Artificial Intelligence and the Future of Warfare*, The Royal Institute of International Affairs, Chatham House, 2017.

[19] Stephan de Spiegeleire et al., *Artificial Intelligence and The Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers*, The Hague Centre for Strategic Studies (HCSS), 2017.

[20] R.S. Panwar, *AI in Military Operations*, IDSA Strategic Comments, www.idsa.in, 2018, accesat la 12 februarie 2020.

[21] M. Tonin, *The Internet Of Things: Promises and Perils of a Disruptive Technology,* https://www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis, consultat la 10.02.2020.

RAND Europe și HCSS au sintetizat, într-un studiu, principalele teme tehnologice ale zilelor noastre, care pot influența înzestrarea forțelor. Acestea sunt: (1) senzorizarea și extinderea rețelelor; (2) machine learning și inteligență artificială; (3) globalizarea tehnologiei; (4) spațiul cosmic ca mediu operațional; (5) dezvoltarea umană; (6) energia regenerabilă și armele energetice[22].

RAND Europe și HCSS au sintetizat, într-un studiu, principalele teme tehnologice ale zilelor noastre, care pot influența înzestrarea forțelor. Acestea sunt: (1) senzorizarea și extinderea rețelelor; (2) machine learning și inteligență artificială; (3) globalizarea tehnologiei; (4) spațiul cosmic ca mediu operațional; (5) dezvoltarea umană; (6) energia regenerabilă și armele energetice.

Practica zilelor noastre mai aduce în discuție o altă problemă majoră: cea a securității și criminalității cibernetice. În anul 2016, anumiți actori nord-coreeni au organizat un jaf cibernetic ce a păgubit Banca Bangladesh-ului cu 81 de milioane de dolari[23]. Tot în același an, nord-coreenii au lansat ransomware-ul WannaCry, ce a produs efecte dramatice la nivel mondial[24]. În anul 2017, National Cybersecurity and Communications Integration Center (NCCIC) din Statele Unite ale Americii a dezvăluit publicului că, pe timpul unor acțiuni ale Federației Ruse în Ucraina, malware-ul NotPetya a sistat accesul unor zone la energie electrică. Pe lângă pagubele însemnate, de peste 10 miliarde de dolari, **NotPetya a reușit oprirea funcționării sistemului de monitorizare a radiațiilor Centralei Nucleare de la Cernobîl**[25].

Pornind de la aceste fundamente, este foarte dificil să anticipăm evoluțiile tehnologice specifice anului 2050 ce vor influența gândirea militară. **Câteva prospecții se pot face totuși**. Una dintre cele mai importante consecințe ale prezentului se referă la faptul că statele puternice vor putea folosi sisteme de armament cu încărcătură nucleară în spațiul cosmic până în 2050, fapt ce va conduce la definirea unui nou spațiu de luptă. O a doua prospecție se referă la calitatea datelor și a informațiilor. În raportul *Global Strategic Trends: The Future Starts Today*, Ministerul britanic al Apărării consideră că, pe măsură ce cantitatea de informații se va extinde, în special în spațiul virtual, va fi mai greu de făcut diferența între adevăr și fake-news[26]. Astfel, cine va avea acces la informații și la date direct de la sursele primare va fi mai puternic. Se preconizează că, până în anul 2050, anumiți actori non-statali vor avea acces la imagini satelitare cu o rezoluție înaltă ale întregului Glob, influențând fundamental balanța confruntărilor

[22] *European Defence Matters*, 2017.

[23] D.R. Coats, *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, United Stated Army War College, 2018.

[24] *Strategic Cyberspace Operations Guide*, 2018.

[25] M. Scott et al., *Cyberattack Hits Ukraine Then Spreads Internationally, New York Times*, 26 iunie 2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html, consultat la 10.02.2020

[26] ***, Ministerul britanic al Apărării, *op. cit.*, pp. 129-137.

militare. Unele entități statale și non-statale au dezvoltat deja algoritmi pentru analiza populației civile. Este de așteptat ca, la nivelul anului 2050, acestea să fie arhiutilizate în planificarea acțiunilor asimetrice de către actori non-statali. Rămâne de văzut cum va reuși gândirea militară românească să se raporteze la aceste problematici.

Principalul factor generator de riscuri în anul 2050 va fi criminalitatea cibernetică. Unii autori consideră că abilitatea de a controla spațiul cibernetic va fi viitoarea formă dominantă a puterii actorilor de orice natură.

Acțiunile cibernetice viitoare vor putea crea efecte asupra unor infrastructuri critice, facilități industriale și vor putea opri accesul la anumite servicii publice, mai ales pentru forțele militare angajate în acțiuni militare.

Totuși, principalul factor generator de riscuri în anul 2050 va fi criminalitatea cibernetică. Unii autori consideră că abilitatea de a controla spațiul cibernetic va fi viitoarea formă dominantă a puterii actorilor de orice natură. Acțiunile cibernetice viitoare vor putea crea efecte asupra unor infrastructuri critice, facilități industriale și vor putea opri accesul la anumite servicii publice, **mai ales pentru forțele militare angajate în acțiuni militare**. Conform Raportului *Global Strategic Trends: The Future Starts Today*, aceasta va impune dezvoltarea unui cadru legislativ și acțional mult mai adecvat protejării în fața atacurilor cibernetice[27].

(4) Extinderea Consiliului de Securitate al ONU

Organizația Națiunilor Unite este, conform exemplelor anterioare din istorie, organismul ce are ca scop prezervarea *statu-quoului* menționat de tratatele subsecvente unui război (în cazul de față, al celui de-al Doilea Război Mondial). ONU a reușit să își păstreze integritatea și să rămână un actor important în securitatea mondială, făcându-și prezentă filosofia de asigurare a păcii. Practica internațională și cercetătorii din domeniu aduc în discuție succesul organizației pe fondul capacității sale instituționale de reformă și de transformare, în special în aria Consiliului de Securitate. În esență, proiectul Consiliului de Securitate al ONU a rămas ancorat în situația anului 1945. De la prima sa reuniune, în anul 1952, componența membrilor permanenți a rămas neschimbată (cele cinci state câștigătoare ale războiului). Numărul membrilor nepermanenți a crescut de la șase la zece membri, fiind aleși pe un mandat de doi ani. Prin urmare, marea miză a reformelor vizează creșterea portofoliului membrilor permanenți, întrucât aceștia beneficiază de drept de veto. La nivel mondial, există mai multe grupuri de interes ce promovează reforma. Conform Ministerului Afacerilor Externe (2020), se pot identifica un număr de patru grupuri de state

[27] *Ibidem*.

și de interese implicate în procesul de reformă[28]. Ele sunt enumerate în *tabelul nr. 1.*

Grup de interes	Număr de membri	Membri permanenți suplimentari	Membri nonpermanenți suplimentari
G4 Germania, Brazilia, Japonia și India	25	*Nr. crește cu 6 membri:* 2 state africane 2 state asiatice 1 stat din America Latină 1 stat din vestul Europei	*Nr. crește cu 4 membri:* 1 stat african 1 stat asiatic 1 stat din SE Europei 1 stat din America Latină
Unitate pentru Consens Italia, Argentina, Pakistan și Mexic	35	Nu se modifică	*Nr. crește cu 20 membri:* 6 state africane 5 state asiatice 4 state din America Latină 3 state din vestul Europei 2 state din SE Europei
Uniunea Africană (Consensul de la Ezulwini)	26	*Nr. crește cu 6 membri:* 2 state africane 2 state asiatice 1 stat din America Latină 1 stat din vestul Europei	*Nr. crește cu 5 membri:* 2 state africane 1 stat asiatic 1 stat din SE Europei 1 stat din America Latină
Grupul celor 21	*Promovează numai revizuirea procedurilor.*		

Tabelul nr. 1: Grupuri de interes cu privire la revizuirea Consiliului de Securitate[29]

Credem că modificarea componenței membrilor cu drept de veto ai Consiliului poate crește percepția pozitivă despre ONU a actorilor internaționali și poate limita acțiunile lor revizioniste. **Acest factor influențează gândirea militară românească** dintr-o perspectivă fundamentală. Consiliul de Securitate al ONU reglează pulsul

[28] Cele patru grupuri au fost sintetizate conform datelor oficiale ale Ministerului Afacerilor Externe, disponibile în articolul *Reforma Consiliului de Securitate ONU*, vezi https://www.mae.ro/node/1589, consultat la 12 februarie 2020.

[29] Sursa: autorul.

și intensitatea intervențiilor și determină cadrul mondial de interpretare a securității la care România a aderat. Din acest motiv, lipsa consensului cu privire la organizarea Consiliului (în special a membrilor permanenți) va încuraja, cu certitudine, încercările revizioniste la adresa *statu-quoului* internațional. Prin urmare, asigurarea securității naționale va fi afectată direct, prin pășirea într-o nouă etapă, ce se îndreaptă către conflictualitate.

(5) Redefinirea sistemului mondial de alianțe

Sistemul mondial de alianțe asigură distribuirea puterii între actorii relațiilor internaționale, fiind un marker al păcii sau al conflictualității. Experiența istorică a două blocuri antagonice de aliați este grăitoare, în acest sens. De altfel, lumea zilelor noastre a depășit paradigma bipolară a Războiului Rece și se definește ca una de tip multipolar.

Sistemul mondial de alianțe asigură distribuirea puterii între actorii relațiilor internaționale, fiind un marker al păcii sau al conflictualității. Experiența istorică a două blocuri antagonice de aliați este grăitoare, în acest sens. De altfel, lumea zilelor noastre a depășit paradigma bipolară a Războiului Rece și se definește ca una de tip multipolar. Unii autori consideră această multipolaritate o etapă intermediară către o nouă bipolaritate și aduc în discuție creșterea Chinei sau a Indiei în raport cu SUA[30]. Acești autori poziționează China sau India într-un potențial challenger al SUA, după anul 2040. Din acest motiv, orice sistem de alianțe ce include China sau India devine, la rându-i, un marker al unei posibile conflictualități. Prin urmare, în anul 2050, este de dorit o repartiție echilibrată a puterii între SUA, China, Federația Rusă, India, Japonia și Uniunea Europeană. Transformarea proiectului Uniunii Europene într-unul mai solid, cu o mai mare substanță de tip federal, devine un laitmotiv al anilor 2050. Cultivarea schimbului de resurse umane, materiale și economice dintre state reprezintă un pansament al eventualelor elemente conflictuale. Peisajul anului 2050 aduce un *„no go area”* pentru o posibilă alianță dezvoltată pe axa **China – India – Federația Rusă** și o serie de *„milestone-uri”* referitoare la **întărirea Uniunii Europene și a Parteneriatului Transatlantic**. Atât extinderea Alianței, cât și a Uniunii Europene sunt elemente necesare fundamentării unei posturi strategice viabile în plan internațional

[30] Putem analiza aici lucrarea lui H.P. Pant, *Contemporary Debates in Indian Foreign and Security Policy*, New York: Palgrave Macmillan, 2008. Aceasta poziționează India într-un potențial challenger pentru SUA. Putem remarca și analiza lui G.J. Ikenberry, *The Future of the Liberal World Order: Internationalism after America*, *Foreign Affairs* 90(3), 2011, http://www.eastlaw.net/wp-content/uploads/2016/09/Future-of-Liberal-world-order-90ForeignAff56.pdf, consultat la 12 februarie 2020. Acesta vede China într-un potențial challenger pentru SUA. Această idee este împărtășită și de către H. Kissinger, în lucrarea *On China*, New York: The Penguin Press, 2011.

pentru toate țările ce fac parte din cele două proiecte. Jocul dual de politică externă al unor actori statali din cadrul acestor organizații nu poate avea consecințe pozitive pe plan internațional.

Acest factor influențează gândirea militară românească dintr-o perspectivă fundamentală. Redefinirea sistemului mondial de alianțe va determina, cu certitudine, schimbări în amploarea înzestrării tehnice, în procedurile, dar și în organizarea sistemului militar românesc. Poziția geografică a României a demonstrat, în cursul istoriei, că redefinirile apartenențelor la diverse sisteme de alianțe nu au avut un aport dinamic pozitiv asupra securității naționale. Din punctul de vedere al ieșirii la Marea Neagră, România devine un stat *sui-generis* al Alianței Nord-Atlantice și al Uniunii Europene. Pe fondul jocului criptic al Turciei în regiune, ca și al acțiunilor Federației Ruse, drumul României către 2050 trebuie să fie unul predictibil pentru actualii aliați, dar și mult mai consistent în privința unui proiect european durabil. Definirea unor proiecte regionale (cum ar fi B9) nu face decât să întărească postura strategică a țării noastre. Tehnica militară va trebui să țină pasul cu noile inovații din cercetarea științifică din comunitatea aliată. Acest fapt se va dovedi improbabil de atins la nivelul anului 2050, dacă inițiativele europene privind apărarea nu vor căpăta forță și UE nu va identifica modalitățile concrete de asigurare internă a furnizorilor.

Redefinirea sistemului mondial de alianțe va determina, cu certitudine, schimbări în amploarea înzestrării tehnice, în procedurile, dar și în organizarea sistemului militar românesc. Poziția geografică a României a demonstrat, în cursul istoriei, că redefinirile apartenențelor la diverse sisteme de alianțe nu au avut un aport dinamic pozitiv asupra securității naționale.

CONCLUZII CU PRIVIRE LA ADAPTAREA GÂNDIRII MILITARE ROMÂNEȘTI

În esență, problema prospectivei devine un mobil prin care gândirea militară românească poate crea baza securitizării României anului 2050. Chiar dacă securitatea va fi definită cu alte repere în 2050, ea va rămâne cupola sub care cetățenii vor reuși să își ducă traiul, simțindu-se în siguranță. Din acest motiv, Armata României va trebui să se adapteze și să găsească soluții pentru a-și îndeplini misiunile.

În acest articol au fost prezentați principalii factori ce vor avea impact asupra securității naționale în 2050, cu scopul de a trage câteva învățăminte pentru gândirea militară românească. Probabil, una dintre cele mai pregnante probleme ale României anului 2050 va fi determinată de trecerea către o societate ecologică (post-petrol), pe fondul poluării crescute și al precarității resurselor de apă potabilă. Interacțiunile celor doi factori vor crea premisele unor transformări profunde la nivel național, de la adaptarea tehnologică până la schimbarea modului de trai.

Gândirea militară românească va trebui să reacționeze și să susțină *securitatea energetică* a României. Totodată, va trebui să pregătească *adaptarea tehnologică militară* și eficientizarea consumului de energie al echipamentelor specifice. Efectul final va avea o structură tripartită, direcționată către: (1) asigurarea independenței energetice naționale, (2) protejarea infrastructurilor critice implicate în procesul de producere sau distribuire a energiei și (3) prevenirea unor revolte sociale pe fondul precarității resurselor de apă potabilă.

Din punctul nostru de vedere, inovațiile tehnologice reprezintă factorul disruptiv cel mai greu de anticipat în gândirea militară românească. Deși inovațiile vor transforma profund societatea noastră, nu este clar, în acest moment, când și dacă vor determina cu adevărat o **revoluție în afaceri militare**, așa cum a făcut-o, spre exemplu, **apariția mitralierei**.

Gândirea militară românească va trebui să reacționeze și să susțină securitatea energetică a României. Totodată, va trebui să pregătească adaptarea tehnologică militară și eficientizarea consumului de energie al echipamentelor specifice.

Este cert totuși că, în momentul de față, se fac pași serioși pentru aplicarea unui nou concept – cel de *Internet of Things* –, care **poate deveni motorul acestei revoluții**. Conectarea tuturor *device*-urilor la o platformă integratoare, bazându-ne pe viteze 5G, va crea fundamentul unor efecte în cascadă, atât pozitive, cât și negative. Oportunitățile majore ale binomului IOT-5G vor permite cunoașterea și senzorizarea crescută a mediului de luptă modern. Există și efecte negative, printre care se numără creșterea vulnerabilității în fața atacurilor cibernetice. Ținând cont că anumite entități au dezvoltat deja algoritmi pentru analiza populației civile și că vor avea și acces la hărți detaliate prin diverse platforme satelitare, aceasta îi va transforma în inamici de temut. Prin urmare, gândirea militară românească va trebui să găsească soluții pentru a face față extinderii rețelelor ce vor permite monitorizarea tuturor elementelor specifice mediului de instruire sau câmpului de luptă modern, de la performanțe individuale la amenințări detectate.

În același timp, gândirea militară românească va trebui să contracarareze noile **posibilități de proiectare a forței în acțiuni militare** (spațiul cosmic, spațiul cibernetic, spațiul aerian – cu referire la drone și roiuri de drone). Va fi nevoie de un echilibru între investițiile tehnologice militare și cultivarea unui sistem de alianțe specific. Din acest motiv, redefinirea sistemului mondial de alianțe sau a Consiliului de Securitate al ONU va determina, cu certitudine, schimbări în amploarea înzestrării tehnice, în procedurile aplicate în momente de criză, dar și în organizarea sistemului militar românesc. Integrarea acțiunilor cibernetice în operațiile curente reprezintă una dintre aceste schimbări.

BIBLIOGRAFIE:

1. ***, *Acordul de la Paris*, L 282/4 RO, *Jurnalul Oficial al Uniunii Europene* din data de 19.10.2016, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22016A1019(01)&from=RO
2. ***, *Disruptive defence innovations ahead, European Defence Matters*, No 17, 2017.
3. ***, *International Futures (IFs) modeling system*, Frederick S. Pardee Center for International Futures, Josef Korbel School of International Studies, Denver, CO: University of Denver, 2020, http://www.ifs.du.edu/ifs/frm_MainMenu.aspx
4. ***, Ministry of Defence UK, *Global Strategic Trends: The Future Starts Today*, London, 2018
5. ***, *Strategic Cyberspace Operations Guide*, United States Army War College, Center for Strategic Leadership, 2018, https://info.publicintelligence.net/USArmy-StrategicCO.pdf
6. ***, *The economic and employment contributions of shale gas in the United States*, IHS Global Insight, www.nic.gov
7. ***, National Intelligence Council, *Global trends 2030: Alternative worlds,* Washington D.C., 2012.
8. ***, US Army. *Army Cloud Computing Strategy*, 2015.
9. K. Bertolucci*, Taxonomy for the future: Organizing Futures Information into a New Hierarchical Structure*, *Future Research Quaterly*, 2004.
10. M.L. Cummings, *Artificial Intelligence and the Future of Warfare*, The Royal Institute of International Affairs, Chatham House, 2017.
11. J.C. Glenn, *Futures Research Methodology Version 3.0.* Washington D.C.: Millennium Project, 2014.
12. G.J. Ikenberry, *The Future of the Liberal World Order: Internationalism After America*, *Foreign Affairs* 90(3), 2011, http://www.eastlaw.net/wp-content/uploads/2016/09/Future-of-Liberal-world-order-90ForeignAff56.pdf
13. B. d. Jouvenel, *L'art de la conjecture*, Ed. du Rocher, Monaco, 1964.
14. H. Kissinger, *On China*, New York: The Penguin Press, 2011. Stephan de Spiegeleire Matthijs Maas Tim Sweijs, *Artificial Intelligence and The Future of Defense: Strategic Implications for Small and Medium-Sized Force Providers*, The Hague Centre for Strategic Studies (HCSS), 2017.
15. H.P. Pant, *Contemporary Debates in Indian Foreign and Security Policy*. New York: Palgrave Macmillan, 2008.
16. R.S. Panwar, *AI in Military Operations*, IDSA Strategic Comments, 2018, www.idsa.in
17. R. Popper, *Foresight Methodology*, 2008, în L. Georghiou, J. Cassingena, M. Keenan, I. Miles și R. Popper (eds.), *The Handbook of Technology Foresight*, Edward Elgar, Cheltenham.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

POSIBILE SOLUȚII DE REALIZARE A UNEI STRATEGII NAȚIONALE DE SECURITATE – IDENTIFICAREA LOCULUI STRATEGIEI MARITIME –

Dr. Lucian Valeriu SCIPANOV
Universitatea Națională de Apărare „Carol I”, București

Demersul identificării unei posibile soluții privind realizarea unei strategii naționale de apărare derivă din motivația extrinsecă de-a cuantifica acele obiective ale securității naționale care își găsesc reprezentativitate în strategii și doctrine. Strategia națională de apărare conține acele direcții, corespunzătoare obiectivelor naționale, privind manifestarea unor interese pe plan intern și internațional. Identificarea unui model care să realizeze o conexiune între finalități, căile de realizare și mijloacele necesare îndeplinirii obiectivelor naționale privind securitatea reprezintă un demers necesar nivelului teoretic al gândirii strategice din care gândirea practică își extrage fundamentele.

Noutatea acestui articol decurge din motivația intrinsecă de-a identifica locul și nivelul de reprezentativitate a unei strategii maritime în cadrul Strategiei naționale de apărare și al Strategiei militare. Prin intermediul acestui demers, mă adresez specialiștilor, celor care contribuie la realizarea unor documente strategice și doctrinare, studenților masteranzi și doctoranzi, ofițerilor cursanți, celor interesați de mecanismul dezvoltării unei strategii, pentru a avea la îndemână o posibilă soluție de realizare a strategiei naționale de apărare, dar și pentru a identifica legătura dintre elementele componente (obiective-căi-mijloace) și implicațiile acestora la nivelul strategiilor și doctrinelor secundare.

Cuvinte-cheie: strategie de securitate, strategie de apărare, strategie maritimă, putere maritimă, modelul Ends, Ways&Means.

INTRODUCERE

Termenul *strategie*, așa cum este el definit în *Dicționarul Limbii Române*, reprezintă *„partea componentă a artei militare care se ocupă cu problemele pregătirii, planificării și ducerii războiului și operațiilor militare”*[1].

Termenul își are originea în limba greacă, fiind compus din *stratos* (armată) și *agein* (conducere)[2]. În concepția greacă, *strategos* era denumit generalul, conducătorul armatei, *stratego*[3] reprezenta capacitatea de a comanda, de a fi comandant, de a fi general, împreună cu derivatele termenului, care acopereau, ca înțeles acceptat, funcţiile generalului sau calităţile acestuia.

În concepția greacă, „strategos” era denumit generalul, conducătorul armatei, „stratego” reprezenta capacitatea de a comanda, de a fi comandant, de a fi general, împreună cu derivatele termenului, care acopereau, ca înțeles acceptat, funcţiile generalului sau calităţile acestuia.

Chiar dacă am identificat foarte multe conotații militare ale termenului, am întâlnit și sensuri care fac referire la politici, planuri și direcții de acțiune în diferite domenii de aplicare: strategii de joc; strategii de dezvoltare; strategii economice etc. Astfel, în primă instanță, putem spune că strategia reprezintă un plan sistematizat, bine fundamentat, prin care se pun în aplicare anumite obiective planificate, utilizând mijloacele specifice avute la îndemână, și care să contribuie la îndeplinirea scopului pentru care a fost realizat.

În abordarea națională se menționează aspectul științific al termenului, strategia reprezentând *„știința conducerii luptei”*[4]. În alte abordări științifice se identifică faptul că strategia reprezintă *„arta de a folosi cu dibăcie toate mijloacele disponibile în vederea asigurării succesului într-o luptă”*[5]. La nivel politico-militar, strategia acoperă mult mai mult decât latura militară. În diferite situații, strategia acoperă domeniile securității (strategie de securitate), domeniul apărării (strategie de apărare), domeniul militar (strategie militară), domeniul maritim (strategie maritimă) etc.

[1] Conform dexonline.ro, accesat la 10.02.2020.
[2] Conform https://www8.gsb.columbia.edu/articles/ideas-work/von-clausewitz-war-six-lessons-modern-strategist, accesat la 22.02.2020.
[3] Vezi verbul *strategos*, adjectivul *strategikos*, substantivul *strategika* (pl.), n.a.
[4] *Dicționar de neologisme*, Editura Steaua Nordului, 2002.
[5] *Ibidem*.

Strategia a fost în atenția filozofilor, conducătorilor, istoricilor și scriitorilor, aceștia conferindu-i diferite sensuri și înțelesuri, astfel încât să acopere, în principiu, nevoia de înțelegere și utilizare a termenului.

Frederik cel Mare[6] a fost unul dintre cei care a înțeles importanța unei viziuni unitare privind conducerea statului și modul de abordare a apărării dintr-o perspectivă științifică. Afirmația lui, potrivit căreia *„Cel care încearcă să apere totul nu apără, de fapt, nimic”*[7], reprezintă acceptarea faptului că o strategie de apărare este o soluție privind un răspuns optim în ceea ce privește securitatea regatului (Prusiei).

Teoreticianul care a subliniat cel mai bine rolul strategiei din punct de vedere militar a fost Carl von Clausewitz, cel care menționa că *„Strategia este întrebuinţarea luptei în scopul războiului”*[8], oferind, astfel, o primă perspectivă militară modernă asupra termenului.

Toate aceste opinii conturează ideea că strategia este o știință, dar este și o artă.

„Strategia este ştiinţa războiului; ea schiţează planurile, are viziunea generală şi determină mersul acţiunilor militare, este, vorbind exact, ştiinţa generalilor-comandanţi”.

STRATEGIA ESTE ȘTIINȚĂ ȘI ARTĂ

„Strategia este ştiinţa războiului; ea schiţează planurile, are viziunea generală şi determină mersul acţiunilor militare, este, vorbind exact, ştiinţa generalilor-comandanţi”[9]. Fiind o știință, este accentuat caracterul teoretic al sensului: *„Strategia trebuie să studieze lupta în legătură cu rezultatele sale posibile, precum și cu forțele intelectuale și morale cele mai importante în folosirea ei”*[10].

Pe de altă parte, strategia *„este arta de a combina pregătirile pentru război și gruparea operațiunilor pentru a atinge scopul propus de război pentru forțele armate*”[11]. Strategia este arta bazată pe știința comandantului și intuiția sa, acea sclipire de geniu, greu de atins fără o experiență de arme. Se diferențiază, în acest context, teoreticienii de practicieni: *„Cercetătorul care, pornind de la acest succes de ansamblu,*

[6] Frederic al II-lea sau Frederik cel Mare (1712-1786), rege al Prusiei, dinastia de Hohenzollern, n.a.
[7] Frederik cel Mare, conform https://devcentral.f5.com/s/articles/he-who-defends-everything-defends-nothinghellip-right, accesat la 22.02.2020.
[8] Carl von Clausewitz (1780-1831), *Despre război*, traducere de Corneliu Soare, Editura ANTET XX PRESS, p. 72.
[9] Arhiducele Carol, duce de Teschen, traducere din germană de Antoine Henri Jomini, în 1818, *Principes de la stratégie*, Paris, 1818, *Chapitre premier, Section première*, p. 1.
[10] Carl von Clausewitz, *op. cit*., p. 72.
[11] David M. Glantz, Harold S. Orenstein, *The Evolution of Soviet Operational Art*, 1927-1991: The Documentary Basis, vol. I, Franc Cass London, 1995, p. 6.

nu vede acea armonie, caută adesea genialitatea unde nu este și nici nu poate fi”[12].

Din punctul de vedere al relațiilor internaționale și securității naționale, lect.univ. Edward Mead Earle preciza: *„Strategia este arta de a utiliza şi a controla resursele unei naţiuni”*[13], aspect ce prezintă o nouă abordare științifică a termenului din perspectivă militară, cu efecte asupra securității economice.

Dintr-o altă perspectivă, profesorul Colin Gray menționa că strategia este produsul dialogului dintre politică şi instrumentele puterii și reprezintă o punte între scopurile politice și mijloacele militare: *„Adesea, politicile decid asupra politicii, apoi decid o acțiune, dar neglijează să unească două domenii. Scopul strategului este de a reduce acest decalaj, fiind bine înarmat cu teoria generală a strategiei”*[14].

Strategul trebuie să aibă o viziune integrată, cuprinzătoare asupra câmpului de luptă, unde își va manifesta calitățile de conducător în funcție de o serie de factori, interni și externi, politici și economici, care vor influența demersul său[15]. În acest sens, *„Strategia oferă puntea dintre mijloacele militare și obiectivele politice”*[16], aspect care își găsește fundamentul în unele legi generale ale războiului: *„Legea dependenţei cursului, deznodământului, urmărilor războiului de calitatea actelor de decizie publică; Legea dependenţei confruntării armate de potenţialul economic, tehnic, ştiinţific al statelor implicate; Legea rolului naţiunii în susţinerea efortului de război”*;[17]*„Legea concordanţei dintre scopul politic, forţe, mijloace, resurse şi obiective”*[18].

Strategul trebuie să aibă o viziune integrată, cuprinzătoare asupra câmpului de luptă, unde își va manifesta calitățile de conducător în funcție de o serie de factori, interni și externi, politici și economici, care vor influența demersul său. În acest sens, „Strategia oferă puntea dintre mijloacele militare și obiectivele politice”, aspect care își găsește fundamentul în unele legi generale ale războiului.

Ca o concluzie parțială, menționez că *strategia* este arta conducerii (arta de a conduce, în general), însă nu trebuie să minimizăm latura teoretică, în care strategia reprezintă o știință. Deci, strategia

[12] Carl von Clausewitz, *op. cit.*, p. 72.
[13] Edward Mead Earle (1894-1954) profesor de studii securitate la Princeton, *Strategy: Create and Implement the Best Strategy for Your Business*, Harvard Business Review, p. XII.
[14] Colin Gray (1943) – profesor la Oxford şi Manchester – studii strategice, Colin Gray, John Baylis, James Wirtz, *Strategy in the Contemporary World*, Oxford University Press, 2019, p. 391.
[15] David M. Glantz, Harold S. Orenstein, *op. cit.*, p. 6.
[16] Colin Gray, *op. cit.*, p. 5.
[17] Mircea Mureşan, Costică Ţenu, Lucian Stăncilă, *Corelaţia artei militare cu fenomenul militar contemporan, Curs de artă militară*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2005, pp. 95-100.
[18] Gheorghe Văduva, *Principii ale războiului și luptei armate-realități și tendințe*, Universitatea Națională de Apărare, Centrul de Studii Strategice de Apărare și Securitate, București, 2003, p. 4.

reprezintă, dincolo de controversa asupra naturii, o știință și o artă, în egală măsură.

Având prezentate aceste elemente caracteristice ale termenului, consider că strategia națională de securitate este arta şi ştiinţa de angajare a instrumentelor politice, economice, psihologice, militare şi de securitate ale unei naţiuni, în vederea îndeplinirii obiectivelor politice în competiţie cu alţi actori care îşi urmăresc interesele. În opinia mea, strategia face obiectul unui acord unanim, este artă şi ştiinţă, astfel aceasta reprezintă o punte între teorie şi practică; deci, strategia este un proces, cu un conținut mult mai complex decât sensul pe care îl îmbracă.

Dacă facem referire la strategia unei organizații, aceasta este modul prin care se pregătește organizaţia pentru un viitor incert, prin care să facă față provocărilor de orice natură, printr-un răspuns identificat ca soluție.

Strategia reprezintă modul în care trebuie făcute lucrurile și prezintă calea generală prin care se realizează obiectivele stabilite. Subliniez faptul că strategia este un proces în sine și nu este un scop. Dacă facem referire la strategia unei organizații, aceasta este modul prin care se pregăteşte organizaţia pentru un viitor incert, prin care să facă față provocărilor de orice natură, printr-un răspuns identificat ca soluție.

În opinia mea, strategia se manifestă prin două componente: *hard* și *soft*. Componentele *hard* sunt reprezentate de elementele puterii militare; componentele *soft* sunt reprezentate de politica, economia, tehnologia, cultura, tradiția statului etc.

În continuare, voi aborda termenul din perspectiva securității și apărării și influența acestuia asupra componentei *hard* (puterea militară).

Pentru a identifica la ce nivel al conducerii putem dezvolta o strategie, voi face apel la nivelurile artei militare: strategic, operativ și tactic.

NIVELURILE STRATEGIEI

Nivelurile strategiei sunt identificate, în primul rând, la nivel politic și militar. Strategia politică (denumită *Marea strategie*[19]) este ansamblul instrumentelor de putere ale statului[20]. Strategia militară

[19] *„Grand strategy”* (Liddell Hart, Clausewitz, Corbett) se referă la nivelul diplomatic și politico-militar al strategiei, n.a.

[20] *Strategy: Ends and Means*, p. 39, conform https://www.globalsecurity.org/military/library/policy/usmc/mcdp/1-1/mcdp1-1_chap2.pdf, accesat la 22.02.2020, „grand strategy”, „grand national strategy” or, currently in the United States, „national security strategy”.

descrie modul de angajare a instrumentului militar pe timp de pace, criză, război: *„Politica reprezintă modalitățile (metodele sau modelele) prin care strategia își atinge obiectivele”*[21].

În domeniul militar, strategia are influențe la nivel operativ și tactic. La nivel operativ, strategia din teatrul de operaţii descrie modul de angajare a instrumentului militar la nivel regional. La nivel tactic, strategia categoriilor de forțe descrie un concept strategic specific (strategie).

Să vedem, în continuare, în cadrul căror domenii putem identifica oportunitatea dezvoltării unor strategii. Personal, am identificat patru niveluri de manifestare a strategiei: *Marea strategie*[22]*; nivelul strategic; nivelul operativ* și *nivelul tactic.*

Marea strategie reprezintă nivelul la care se iau deciziile politico-militare, se stabilește concret dacă o ţară intră sau nu în război, cine vor fi inamicii, care vor fi aliaţii şi ce-şi doreşte ţara respectivă în urma păcii. La acest nivel, este esenţial să poți conduce războiul, să realizezi alianțe, coaliții, înțelegeri, pentru a ști de la bun început ce poziție dorești să ocupi în negocieri (care este pacea pe care o dorești). Deci, *Marea strategie* reprezintă politica de război a statului. Scopul acesteia este de a coordona şi dirija toate resursele naţiunii sau ale unei coaliţii, alianțe, uniuni, parteneriat, pentru a atinge obiectivul politic al războiului. SUA nu utilizează termenul *mare strategie*, ci, mai degrabă, termenul *strategie națională*, iar Marea Britanie îl definește astfel: *„aplicarea resurselor naționale pentru atingerea obiectivelor politicii naționale și implică componente economice, industriale, politice și militare”*[23].

Marea strategie reprezintă politica de război a statului. Scopul acesteia este de a coordona şi dirija toate resursele naţiunii sau ale unei coaliţii, alianțe, uniuni, parteneriat, pentru a atinge obiectivul politic al războiului.

Nivelul strategic vizează conducerea generală a războiului, estimează forţele care vor fi disponibile şi distribuie efortul de război între diferitele teatre de război. Nivelul operativ reprezintă nivelul care vizează modalitatea de atingere a finalităţii războiului cu forţele repartizate. Acesta este nivelul la care sunt întocmite planurile pentru angajarea forţelor terestre, aeriene şi maritime şi este stipulat nivelul de angajare al acestor forţe pe parcursul campaniei. Nivelul tactic este

[21] *Ibidem*.

[22] Colin Gray, *op. cit*., pp. 319-321.

[23] G. Sheffield, G. Till, *The Challenges of High Command: The British Experience,* Palgrave Macmillan, New York, 2003, p. 191.

nivelul la care forţele oponente se confruntă fizic şi unde obiectivele stabilite de eşalonul superior sunt clare: *„Orice plan strategic trebuie să poată fi realizat de către primarii tacticii”*[24]. Acesta este nivelul de execuție, de punere în practică a sarcinilor specifice obiectivelor precizate în misiune. Îndeplinirea ordinelor la nivel tactic nu solicită un efort mental deosebit, însă necesită cunoștințe, intuiție, experiență, voință, determinare, care sunt atribute ale unui bun tactician.

GÂNDIREA STRATEGICĂ ȘI GÂNDIREA OPERATIVĂ

În conformitate cu cele prezentate, am identificat două paliere de gândire, respectiv *gândirea strategică* și *gândirea operativă*, printr-o delimitare substanțială între nivelul superior al aplicării (nivelul strategic) și nivelul inferior (nivelul operativ și tactic). Practic, am diferențiat palierul teoretic, aferent nivelului politico-militar, de palierul practic, aferent nivelului operativ-tactic.

Gândirea strategică este realizată pe termen lung. Este o gândire conceptuală, reflectiv-cognitivă, pentru că se bazează pe fundamente teoretice, legi, principii, decizia fiind argumentată științific: „Armele strategului sunt gândirea strategică, consecvența și coerența”.

Gândirea strategică este realizată pe termen lung. Este o gândire conceptuală, reflectiv-cognitivă, pentru că se bazează pe fundamente teoretice, legi, principii, decizia fiind argumentată științific: *„Armele strategului sunt gândirea strategică, consecvența și coerența”*[25]. Gândirea strategică este conjuncturală, identifică oportunităţile, variantele de răspuns cele mai adecvate situației ipotetice. Dinamica mediului de acțiune implică o adaptare a strategiei strategice la noutățile existente prin soluții inedite. Gândirea strategică urmărește realizarea unui raport de eficacitate optim. Astfel, la acest nivel, strategia are rolul de a identifica acele variante de răspuns care sunt cele mai adecvate (cele care trebuie), imaginea planificatorilor fiind una de ansamblu.

Gândirea operativă este realizată într-un termen mai scurt, aplicabilă imediat, într-un mod concret de acțiune. Acest tip de gândire este caracterizat de rutină, de experiență acțională, de euristica liderului de nivel operativ: o acțiune în dinamică, adaptativă; pe parcurs ce apar problemele, acestea sunt rezolvate. Gândirea strategică urmărește atingerea obiectivelor prin soluții eficiente, care să rezolve problemele

[24] Arhiducele Carol, duce de Teschen, *op. cit*., p. 3.
[25] Kenichi Ohmae (1943, decan UCLA), *The Mind of the Strategist: The Art of Japanese Business*, Paperback, Editura McGraw-Hill Education, 1991, p. 57.

cu toate mijloacele. Astfel, la nivel operativ, strategia are rolul de a identifica soluții adecvate (cum trebuie), imaginea planificatorilor fiind una locală, limitată.

STRATEGIA: PROCES VERSUS CONCEPT

Din cele prezentate până în acest punct, se poate concluziona că strategia este un concept în sine, pentru că înglobează o serie de sensuri și termeni descriptivi, care se coagulează în jurul științei și artei. Deci, strategia nu este o sumă de elemente componente ale unui sistem, strategia este un concept. De asemenea, am mai subliniat faptul că strategia este un proces.

În continuare, vom analiza caracteristicile dominante ale strategiei ca proces, în comparație cu strategia la nivel de concept. Astfel, strategia ca proces înglobează o serie de acțiuni interdependente, care se desfășoară pe toate palierele de manifestare a securității: determinarea obiectivelor securităţii naţionale; formularea strategiei politice; dezvoltarea strategiei militare; realizarea strategiei operative (doctrine); formularea strategiei pe câmpul de luptă (tactici).

Din punct de vedere conceptual, strategia delimitează interdependențe politico-militare, adică realizează legătura dintre politică şi operaţiile militare, definește criterii de analiză politice şi militare, astfel că o strategie eficientă trebuie să integreze criteriile politice și militare în loc să le separe, evitând tendința de separare a opiniilor liderilor civili şi militari.

Din punct de vedere conceptual, strategia delimitează interdependențe politico-militare, adică realizează legătura dintre politică şi operaţiile militare, definește criterii de analiză politice şi militare, astfel că o strategie eficientă trebuie să integreze criteriile politice şi militare în loc să le separe, evitând tendința de separare a opiniilor liderilor civili şi militari.

Având în vedere noua conjunctură de securitate regională, consider că este oportună dezvoltarea unor strategii care să răspundă fenomenului de globalizare în condițiile noilor competitori, provocărilor și pericolelor, riscurilor și amenințărilor etc. Competiția pentru resurse a generat noi actori regionali, astfel că vechile principii necesită adaptare la noul climat de securitate. Vremuri noi, principii noi, se spune. Totuși, sunt de părere că adaptarea e cheia succesului, deci și vechile principii rămân în atenție. De ce am avea nevoie de o nouă strategie? Dacă ne uităm la mediul de securitate, acesta este definit ca fiind multipolar, astfel că argumentele prezentate vin în sprijinul ideii unei noi strategii.

O posibilă soluție de realizare a unei strategii.

„Strategia Națională de Apărare a Țării pentru perioada 2015-2019. O Românie puternică în Europa și în lume” a avut ca perioadă de aplicare anii 2015-2019. *„Documentul facilitează înțelegerea modului în care statul, respectând drepturile și libertățile fundamentale ale cetățeanului, își exercită, prin instituțiile sale, atribuțiile privind securitatea țării și siguranța cetățenilor săi”*[26].

Chiar dacă mediul de securitate este într-o continuă dinamică, elemente de conținut ale strategiei încă își mai păstrează, în mare parte, actualitatea. Sunt sigur că noile amenințări la adresa securității vor fi analizate și vor fi luate în calcul pentru definirea viitoarelor direcții strategice ale unei strategii naționale.

O strategie are la bază opţiunile şi deciziile politice şi strategice ale Parlamentului României, ale instituţiilor publice care au atribuţii în domeniul securităţii şi apărării naţionale, care trebuie să estimeze resursele alocate și mijloacele necesare pe termen lung, pentru a oferi posibilitatea realizării obiectivelor de securitate şi apărare naţionale.

În acest sens, doresc să identific o posibilă soluție de realizare a unei strategii, să vedem, de fapt, care este procesul în sine, de la demersul instituțional la conținutul acesteia. Procesul instituțional de elaborare a unei strategii naționale de apărare începe printr-o dezbatere la nivel național privind realizarea unui proiect de strategie, apoi urmează o rafinare și optimizare a conținutului. În această formă se prezintă Parlamentului, de către Preşedintele României, în termen de cel mult șase luni de la învestitură[27].

Strategia de apărare înglobează măsuri şi activităţi care trebuie adoptate şi desfăşurate de statul român în scopul de a garanta suveranitatea naţională, independenţa şi unitatea statului, integritatea teritorială a ţării şi valorile democraţiei constituţionale, cu un orizont de evaluare de cinci ani. Strategia de apărare este un produs al autorităţilor publice naţionale stabilite prin Constituţia României. O strategie are la bază opţiunile şi deciziile politice şi strategice ale Parlamentului României, ale instituţiilor publice care au atribuţii în domeniul securităţii şi apărării naţionale, care trebuie să estimeze resursele alocate și mijloacele necesare pe termen lung, pentru a oferi posibilitatea realizării obiectivelor de securitate şi apărare naţionale.

[26] Conform https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019, accesat la 25.02.2020.

[27] *Ordonanța nr. 52 (art. 4) din 12 august 1998 privind planificarea apărării naționale a României*, republicată în *Monitorul Oficial al României*, Partea I, nr. 185 din 28 aprilie 2000; *Legea 203/2015 privind planificarea apărării*.

PROCESUL DE REALIZARE A UNEI STRATEGII

În urma analizei a mai multor strategii la nivel internațional, am identificat faptul că, în prima etapă, se definește scopul național, care este bazat pe valori, credință și etică, interese naționale, la care se adaugă viziune, educație strategică și politici.

În următoarea etapă se realizează o analiză de nivel strategic (analiză strategică), la nivelul mediului de securitate, care se finalizează în patru pași, pe care i-am identificat și îi voi prezenta în continuare.

Modelul de analiză se bazează pe un proces de identificare a unor direcții de acțiune. Acesta începe cu definirea mediului strategic (pasul I), la nivelul mediului de securitate global și intern. În pasul următor (pasul II), este necesară o analiză atentă a efectelor mediului strategic definit asupra securității naționale din toate punctele de vedere, în raport și cu strategiile existente ale vecinilor. Este necesară o evaluare a strategiilor țărilor emergente (pasul III), pentru a identifica interesele comune și pe cele care contravin intereselor naționale. După acești primi trei pași, la pasul IV se determină variante ale direcțiilor de acțiune privind securitatea națională.

Analiza mediului global constă în identificarea actorilor regionali, puterea armată pe care o dețin, interesele regionale, tendințe ale mediului de securitate global și regional. Acesta este un proces de analiză în care sunt identificați competitorii, condițiile economice, efectele globalizării la nivelul regiunii, dezvoltarea tehnologică a vecinilor și legile internaționale care influențează securitatea regională.

Etapa a treia reprezintă etapa identificării unor posibile direcții de acțiune, riscuri și amenințări.

Analiza mediului global constă în identificarea actorilor regionali, puterea armată pe care o dețin, interesele regionale, tendințe ale mediului de securitate global și regional. Acesta este un proces de analiză bazat pe un model similar celui prezentat anterior. Sunt identificați competitorii, condițiile economice, efectele globalizării la nivelul regiunii, dezvoltarea tehnologică a vecinilor, legile internaționale care influențează securitatea regională. De asemenea, se identifică organizațiile internaționale care acționează în zonă, actorii regionali cu influență, statali sau non-statali. În cele din urmă, având toate elementele prezentate, în raport cu toate variabilele care influențează securitatea, se vor identifica riscurile și amenințările care pot influența securitatea națională din exterior.

În general, mediul intern de securitate este în relație directă cu sistemul de guvernământ, care oferă posibilitatea manifestării în condiții optime a tuturor funcțiilor statului privind asigurarea securității. Analiza mediului intern constă în identificarea autorităţilor naţionale care au răspunderi privind consolidarea securității naționale.

Sunt identificate condițiile economice, nevoile societății, caracteristica socială dominantă (nivelul dezvoltării sociale), moralul societății, independența mass-mediei etc.

Cel mai cunoscut model de proces privind realizarea unei strategii este modelul anglo-saxon, definit în termeni clari chiar de școala americană: *Ends, Ways&Means*[28]:

- *ENDs (obiective)*: de nivel politic și de nivel politico-militar (marea strategie, strategia națională);
- *WAYs (căi)*: care pot fi identificate la nivelul gândirii strategе și la nivelul gândirii operative dintr-o perspectivă comprehensivă *(comprehensive approach)*;
- *MEANs (mijloace)*: dezvoltarea capabilităților și mijloacelor; implementarea direcțiilor strategice cu ajutorul mijloacelor dezvoltate și a celor la dispoziție (la nivelul gândirii operativ-tactice).

Procesul de elaborare a unei strategii naționale poate să se bazeze pe modelul obiective-căi-mijloace, în care identificăm: obiectivele naționale; conceptul strategic și instrumentele de putere națională.

Consider că procesul de elaborare a unei strategii naționale poate să se bazeze pe *modelul obiective-căi-mijloace*, în care identificăm:

- obiectivele naționale *(Ends)*; de identificat finalitățile;
- conceptul strategic *(Ways)*; de identificat calea;
- instrumentele de putere națională *(Means)* de identificat acele mijloace care trebuie dezvoltate ca să se atingă finalitățile; identificat acele resurse cu ajutorul cărora pot fi dezvoltate capabilitățile cu care să oferim răspuns optim, adecvat nevoilor de securitate din următorii ani.

Plecând de la acest model de elaborare a unei strategii, bazat pe rezultatul analizei globale și interne, în urma căruia am identificat posibile direcții de acțiune strategică, în continuare vom realiza o analiză strategică dintr-o abordare comprehensivă. Această abordare constă în identificarea intereselor naționale pe baza prioritizării acestora, definirea valorilor și principiilor naționale, evaluarea problemelor identificate, a tendinţelor şi provocărilor, riscurilor și ameninţărilor, oportunităţile de manifestare a intereselor naționale privind securitatea. Urmează aplicarea modelului propus anterior, care constă în: determinarea obiectivelor *(Ends*), elaborarea alternativelor, a căilor *(Ways)*, în funcție de resursele disponibile sau necesare *(Means)* pentru îndeplinirea obiectivelor. Având realizată această analiză,

[28] Gregory D. Miller, Chris Rogers, Francis J.H. Park, William F. Owen, Jeffrey W. Meiser, *On Strategy as Ends, Ways, and Means*, Journal of the US Army War College 47(1):125-126, ianuarie 2017.

se poate trece la următorul pas, evaluarea riscului, în sensul identificării celui mai vulnerabil pilon al modelului *obiective-căi-mijloace*. Rezultatul este o recomandare de politică strategică bine fundamentată. Acest model se poate verifica printr-o analiză care ia în calcul următoarele criterii: adecvarea, acceptabilitatea, fezabilitatea, evaluarea riscului. Dacă direcțiile strategice obținute răspund pozitiv analizei pe criteriile menționate, atunci putem spune că avem o strategie.

STUDIU DE CAZ

Vom verifica aplicabilitatea modelului printr-o analiză a conținutului strategiei naționale de apărare: *Strategia Naţională de Apărare a Ţării pentru perioada 2015-2019. O Românie puternică în Europa şi în lume*.

Etapa I:

Scopul definit: *„O Românie puternică în Europa şi în lume, un stat care asigură securitatea cetăţenilor săi oriunde s-ar afla ei”*[29].

Identificăm valorile naționale: *„demnitatea; coeziunea civică şi afirmarea identităţii naţionale; democraţia constituţională şi statul de drept; integritatea statală şi teritorială a României”*[30].

Identificăm principiile naționale: *„continuitatea; predictibilitatea; legalitatea; proporţionalitatea”*[31]. De asemenea, sunt definite interesele naționale de securitate. Acestea le putem identifica în capitolul *1.2. Interese naţionale de securitate*[32].

Etapa a II-a

Pasul I: definirea și evaluarea mediului strategic global și intern.

În *Capitolul II* al strategiei identificăm *„evaluarea mediului internaţional de securitate”*[33], în care găsim o prezentare a mediului global de securitate, a dimensiunii de securitate la nivel euroatlantic și a mediului de securitate regional. În acest capitol sunt prezentate starea mediului de securitate, evoluția și tendințele acestuia.

În Capitolul II al Strategiei Naţionale de Apărare a Ţării identificăm „evaluarea mediului internaţional de securitate”, în care găsim o prezentare a mediului global de securitate, a dimensiunii de securitate la nivel euroatlantic și a mediului

Pasul II: se realizează o analiză atentă a efectelor mediului strategic asupra securității naționale.

[29] *Strategia Națională de Apărare a Țării pentru perioada 2015-2019. O Românie puternică în Europa și în lume*, Administrația Prezidențială, București, 2015.
[30] *Ibidem*.
[31] *Ibidem*, p. 7.
[32] *Ibidem*, p. 8.
[33] *Ibidem*, p. 11.

Pasul III: evaluarea strategiilor actorilor regionali, pentru a identifica interesele comune și pe cele care contravin intereselor naționale.

În urma acestei analize, putem să identificăm care sunt ameninţările, riscurile şi vulnerabilităţile la adresa securității naționale, prezentate în *Capitolul III*: *„ameninţări, riscuri şi vulnerabilităţi”*[34].

După această etapă se obțin, obiectivele *(Ends)*, care reprezintă primul pilon din tripticul *Ends, Ways&Means*. Identificăm, așadar, care sunt obiectivele *(Ends)* naţionale de securitate:

- *„consolidarea profilului României în NATO şi UE prin contribuţii atât conceptuale, cât şi operaţionale;*
- *respectarea principiilor şi valorilor fundamentale ale UE;*
- *consolidarea parteneriatului strategic cu SUA, inclusiv în domeniul economic şi comercial;*
- *asigurarea securităţii în Marea Neagră;*
- *aprofundarea cooperării cu statele vecine şi cu cele din flancul estic;*
- *intensificarea cooperării regionale inclusiv în domeniul apărării;*
- *susţinerea parcursului european al Republicii Moldova;*
- *promovarea intereselor politice, economice şi de securitate în regiuni de relevanţă strategică pentru ţara noastră”*[35].

Evaluarea strategiilor actorilor regionali se realizează pentru a identifica interesele comune și pe cele care contravin intereselor naționale. În urma acestei analize, putem să identificăm care sunt ameninţările, riscurile şi vulnerabilităţile la adresa securității naționale.

Pasul IV. Definirea direcțiilor de acțiune, în urma identificării ameninţărilor, riscurilor şi vulnerabilităţilor, care reprezintă, de fapt, căile *(Ways)*, al doilea pilon din tripticul *Ends, Ways&Means*. Să vedem care sunt căile *(Ways)* prezentate în strategie, prin care aceste obiective pot fi aplicate. Acestea sunt prezentate în *Capitolul IV: Direcţii de acţiune şi principalele modalităţi pentru asigurarea securităţii naţionale a României*[36]. Dacă analizăm conținutul, putem concluziona că aici sunt prezentate și mijloacele *(Means*), care, în opinia mea, nu sunt suficient de detaliate.

Direcţiile de acţiune şi principalele modalităţi de asigurare a securităţii naţionale *(Ways)* sunt prezentate astfel: *„Dimensiunea de apărare; Dimensiunea de ordine publică; Dimensiunea de informaţii, contrainformaţii şi de securitate; Dimensiunea economică şi energetică;*

[34] *Ibidem*, pp. 14-16.
[35] *Ibidem*, p. 10.
[36] *Ibidem*, pp. 18-22.

Dimensiunea diplomatică; Dimensiunea de management al situaţiilor de criză; Dimensiunea educaţională, de sănătate, socială şi demografică”[37].

Acestea reprezintă principalele repere privind definirea unor posibile direcții de acțiune și identificarea riscurilor și amenințărilor la adresa securității naționale.

În concluzie, modelul *obiective-căi-mijloace* se aplică bine Strategiei Naționale de Apărare, cu mențiunea că mijloacele *(Means)* pot fi detaliate, adică ar trebui identificat modul concret de dezvoltare a acelor direcții prezentate, astfel oferind premisele materializării lor. În urma analizei, am identificat obiectivele naționale *(Ends)*, am identificat căile *(Ways)*, însă nu am identificat suficient de bine reprezentate mijloacele *(Means)*. Dacă mijloacele nu sunt definite, acest aspect se transmite și documentelor strategice care își extrag direcțiile din acest document de referință națională.

Având validate metoda de realizare a unei strategii, consider că aceste aspecte reprezintă un rezultat al teoriei și artei școlii românești care valorifică teoria și aplică arta gândirii strategice moderne.

Locul unei strategii maritime

În continuare, mi-am propus să identific locul unei strategii maritime, care își extrage scopul și obiectivele din direcțiile precizate în strategia națională. Tot de aici își extrage fundamentul și o strategie militară. Având elaborată o strategie națională de apărare a țării, există premisele dezvoltării unei strategii militare care să răspundă liniilor directoare privind securitatea țării.

Componenta maritimă a securității reprezintă un alt obiectiv național care nu trebuie neglijat, precizat în cadrul strategiei naționale în *Capitolul I*[38]. Astfel, o strategie maritimă a Mării Negre trebuie să reprezinte, de asemenea, un demers instituțional național prioritar. Avantajele unei strategii maritime se reflectă prin existența securității, a mediului propice de dezvoltare a economiei, ceea ce duce la multiplicarea bunăstării țării. Din acest punct de vedere, securitatea maritimă este foarte importantă.

O strategie maritimă trebuie să ocupe un spațiu mai larg, bine delimitat, în Strategia națională, în Strategia militară, cât și în planurile

O strategie maritimă a Mării Negre trebuie să reprezinte un demers instituțional național prioritar. Avantajele unei strategii maritime se reflectă prin existența securității, a mediului propice de dezvoltare a economiei, ceea ce duce la multiplicarea bunăstării țării. Din acest punct de vedere, securitatea maritimă este foarte importantă.

[37] *Ibidem.*
[38] *Ibidem*, p. 10.

strategice militare. În opinia mea, există toate premisele dezvoltării unei strategii maritime care să definească în mod clar interesele naționale în mediul maritim. Reamintesc faptul că strategia reprezintă un mijloc de îndeplinire a scopurilor definite de politică. Astfel, strategia maritimă reprezintă mijlocul prin care se îndeplinesc interesele naționale în mediul maritim.

Prin urmare, acest aspect al demersului meu consider că reprezintă noutatea prezentului articol, care constă în identificarea locului strategiei maritime în cadrul Strategiei Naționale de Apărare și a Strategiei militare.

Manifestarea intereselor naționale în mediul maritim are o directă legătură cu puterea maritimă a statului. Elementele componente ale puterii maritime trebuie să reprezinte subiecte de analiză a unei strategii maritime. Cea mai vizibilă componentă a puterii maritime este puterea navală, reprezentată de Forțele Navale Române.

Manifestarea intereselor naționale în mediul maritim are o directă legătură cu puterea maritimă a statului. Elementele componente ale puterii maritime trebuie să reprezinte subiecte de analiză a unei strategii maritime. Cea mai vizibilă componentă a puterii maritime este puterea navală, reprezentată de Forțele Navale Române. Capabilitățile acestei componente *(Means)* reprezintă cel mai important vector de îndeplinire a obiectivelor strategiei maritime. Consider că, alături de forțele navale, resursa umană și învățământul reprezintă cele mai la îndemână mijloace de îndeplinire a acestor obiective, componente care trebuie să fie pe deplin exploatate și valorificate.

În opinia mea, după ce am analizat conținutul strategiilor anterioare, consider că acestea nu au reprezentat în mod eficient strategiile maritime. De asemenea, aduc în atenție componeta fluvială. Să nu uităm de fluviul Dunărea! În această direcție, apreciez că o strategie maritimă trebuie să cuprindă și interesele fluviale ale României. Nu cred că putem vorbi încă de oportunitatea dezvoltării unei strategii pentru fluviul Dunărea, pentru că fluviul Dunărea nu este pe deplin exploatat, însă putem aborda domeniul în cadrul strategiei maritime a României.

De aceea, consider oportune două variante de prezentare a intereselor maritime ale României. În prima variantă, o strategie maritimă de sine stătătoare. În a doua variantă, consider că aceasta poate fi regăsită în strategia națională de apărare. Întrebarea provocatoare este cât și cum trebuie reprezentată o strategie maritimă în strategia națională de apărare și cât în cea militară, subiect pe care îl voi relua într-o altă abordare științifică.

În ipoteza în care nu suntem încă pregătiți să avem o strategie maritimă separată, în această variantă, propun un capitol separat

în strategia națională de apărare, care să definească securitatea maritimă și fluvială.

O scurtă analiză comparativă

Pentru a realiza o imagine comparativă, voi analiza cum este abordat aspectul securității naționale și maritime în țările vecine. Am ales, în acest sens, doi parteneri și aliați, respectiv Bulgaria și Polonia, identificând modelul și direcțiile strategice ale principalelor documente strategice.

Am ales Bulgaria, deoarece avem foarte multe puncte comune privind manifestarea intereselor regionale și pentru a vedea care este viziunea vecinilor bulgari privind securitatea și cum își dezvoltă capabilitățile pentru a o asigura. De asemenea, am ales Polonia pentru că am observat o implicare considerabilă în consolidarea securității regionale, o creștere a capabilităților de acțiune și un consens politic care sprijină măsurile prevăzute în strategia națională de securitate.

În urma analizei strategiei naționale a Bulgariei, am constatat că aceasta este construită tot pe modelul anglo-saxon, adoptat după accederea în NATO, și definește foarte detaliat obiectivele, căile și mijloacele necesare consolidării securității naționale. Armata este principalul vector de garantare a îndeplinirii intențiilor politice, mijloacele necesare fiind de natură umană, materială, informațională și financiară[39]. De remarcat că vecinii noștri dețin o strategie maritimă de sine stătătoare, prin intermediul căreia își promovează propriile interese maritime, dar și pe cele comune comunitare, promovând inclusiv măsuri de cooperare cu vecinii săi[40].

În urma analizei strategiei naționale a Bulgariei, se constată că aceasta este construită pe model anglo-saxon, adoptat după accederea în NATO, și definește foarte detaliat obiectivele, căile și mijloacele necesare consolidării securității naționale. Armata este principalul vector de garantare a îndeplinirii intențiilor politice, mijloacele necesare fiind de natură umană, materială, informațională și financiară.

Analizând Strategia Națională de Securitate a Poloniei[41], am constatat faptul că aceasta este foarte dinamică și adaptativă la mediul de securitate internațional. Strategia de securitate a Poloniei pleacă de la obiectivele stabilite la nivel politic, stabilește finalitățile *(Ends)*, pentru mărirea capacității de descurajare, stabilește calea *(Way)*, adică modelarea formei dorite a armatei poloneze, astfel fiind numite și mijloacele prin care se realizează aceste obiective.

[39] *National defense strategy,* Sofia, 2011, conform www.strategy.bg, accesat la 27.02.2020.
[40] Conform https://www.moew.government.bg/en/water/marine-environment/marine-strategy-of-republic-of-bulgaria/ accesat la 27.02.2020.
[41] *National security strategy of the Republic of Poland*, Varsaw, 2014.

Am remarcat că Polonia a lansat, în 2016, un nou concept strategic, foarte realist, care să răspundă nevoilor de securitate în condițiile unor amenințări de tip A2AD[42], definind foarte clar obiectivele, căile și mijloacele prin care să le îndeplinească. Documentul însă accentuează și detaliază modalitățile prin care se pot atinge obiectivele strategice cu un termen stabilit în 2032, în centrul atenției fiind capabilitățile de apărare, sistemul de comandă și control, capacitatea de reacție. Un rol important îl are mediul politic[43]. Interesant este că se observă deja efectele aplicării acestei strategii, forțele armate poloneze fiind foarte vizibile la nivel regional, în Alianță și în UE, aspect care îi conferă o poziție de generator credibil de securitate.

Polonia a lansat, în 2016, un nou concept strategic, foarte realist, care să răspundă nevoilor de securitate în condițiile unor amenințări de tip A2AD, definind foarte clar obiectivele, căile și mijloacele prin care să le îndeplinească.

Referitor la strategia maritimă a Poloniei[44], am identificat că documentul strategic conține evaluarea mediului de securitate maritim, amenințările, riscurile, oportunitățile și provocările, evaluarea forțelor maritime ale țării, definește interesele naționale și obiectivele strategice. Sunt prezentate elementele de tradiție, contextul istoric și social-cultural. Practic, reprezintă un forum de dialog coerent, care necesită o abordare sinergică și integrată[45]. În opinia mea, reprezintă un document strategic foarte bine echilibrat, modelul obiective *(Ends)* - căi *(Ways)* - mijloace *(Means)* fiind bine aplicat[46].

În urma analizei, am remarcat două abordări diferite ale securității, una declarativă și una acțională. Exemplul Poloniei este referențial pentru țările membre din flancul estic al blocului euroatlantic, care ar trebui urmat. Au identificat potențialul și oportunitățile care au generat conștientizarea adaptării proactive la amenințările mediului de securitate și au identificat căile de exprimare a intențiilor și intereselor naționale. De remarcat este faptul că Polonia chiar a găsit cheia succesului, pe care l-am identificat la nivelul voinței politice.

[42] Conform https://www.defence24.com/polish-national-defence-concept-new-division-and-5th-generation-fighter-aircraft, accesat la 29.02.2020.
[43] Conform https://www.gov.pl/web/national-defence/polish-defence-in-the-perspective-of-2032, accesat la 29.02.2020.
[44] Conform https://en.bbn.gov.pl/ftp/dok/SKBMRPENG.pdf accesat la 27.02.2020.
[45] *Ibidem*, p. 6.
[46] Tomasz Szatkowski, Undersecretary of State at the Polish Ministry of Defence, conform https://www.defence24.com/polish-national-defence-concept-new-division-and-5th-generation-fighter-aircraft, accesat la 29.02.2020.

CONCLUZII

În urma prezentării unei posibile soluții de realizare a unei strategii și a analizei conținutului Strategiei Naționale de Apărare, consider că o strategie trebuie să fie definită de următoarele caracteristici: să fie proactivă şi anticipativă; să fie ierarhică, adică să definească clar obiectivele, să definească și să identifice căile de realizare, să identifice și să ofere posibilitatea dezvoltării mijloacelor pentru îndeplinirea obiectivelor. Practic, aceasta trebuie să realizeze un echilibru adecvat între obiective, căi şi mijloace *(Ends, Ways, Means)*. Obiectivele politice trebuie să domine într-o strategie națională de apărare.

Consider că Strategia Națională de Apărare a României este bine structurată, însă, chiar dacă am identificat clar obiectivele *(Ends)* și căile *(Ways*), nu am găsit bine reprezentate mijloacele concrete de realizare a obiectivelor politice *(Means)*.

Ca specialist în domeniul artei operative maritime, am simțit nevoia promovării unui astfel de demers, pentru că o strategie articulată a Mării Negre nu există, iar realizarea acesteia este un efort care necesită timp și resurse.

Succesul în promovarea strategiei maritime depinde de conștientizarea de către clasa politică a importanței manifestării puterii maritime, a valorificării resurselor mediului maritim și fluvial.

Succesul în promovarea strategiei maritime depinde de conștientizarea de către clasa politică a importanței manifestării puterii maritime, a valorificării resurselor mediului maritim și fluvial. Consider că îndeplinirea intereselor maritime naţionale se realizează prin crearea şi dezvoltarea unei puteri maritime susţinute de existenţa unei strategii navale, care să sublinieze apărarea intereselor statului pe mare.

Veriga lipsă în cadrul strategiei naționale de apărare o reprezintă definirea politicii maritime și fluviale naționale. În opinia mea, deocamdată, România nu este pregătită pentru o strategie maritimă de sine stătătoare, însă, pe termen lung, acest obiectiv trebuie atins. De aceea, consider că este oportun a se demara un astfel de demers, privind promovarea strategiei maritime a României, care să fie rezultatul unei viziuni integrate privind motivația protejării intereselor maritime și fluviale ale țării noastre.

BIBLIOGRAFIE:

1. ***, *National defense strategy, Sofia, 2011*, www.strategy.bg.
2. ***, *National security strategy of the Republic of Poland*, Varsaw, 2014.
3. ***, *Ordonanța nr. 52, (art. 4) din 12 august 1998 privind planificarea apărării naționale a României*, republicată.
4. ***, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019. O Românie puternică în Europa și în lume*, Administrația Prezidențială, București, 2015.
5. Antoine Henri Jomini, *Principes de la stratégie*, Paris, 1818; traducere din limba germană în limba franceză.
6. David M. Glantz, Harold S. Orenstein, *The Evolution of Soviet Operational Art, 1927-1991: The Documentary Basis,* vol I., Franc Cass London, 1995.
7. Colin Gray, John Baylis, James Wirtz, *Strategy in the Contemporary World*, Oxford University Press, 2019.
8. Gregory D. Miller, Chris Rogers, Francis J.H. Park, William F. Owen, Jeffrey W.Meiser, *On Strategy as Ends, Ways, and Means*, Journal of the US Army War College 47(1):125-126, ianuarie 2017.
9. Mircea Mureşan, Costică Ţenu, Lucian Stăncilă, *Corelaţia artei militare cu fenomenul militar contemporan, Curs de artă militară*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2005.
10. Gheorghe Văduva, *Principii ale războiului şi luptei armate – realităţi şi tendinţe*, Universitatea Naţională de Apărare, Centrul de Studii Strategice de Apărare şi Securitate, Bucureşti, 2003.
11. Wilhelm Rustow, *The war for the Rhine frontier 1870, its political and military*, Vol. 2, p. 281.

WEBOGRAFIE:

1. dexonline.ro
2. https://www8.gsb.columbia.edu/articles/ideas-work/von-clausewitz-war-six-lessons-modern-strategist
3. https://devcentral.f5.com/s/articles/he-who-defends-everything-defends-nothinghellip-right
4. https://www.globalsecurity.org/military/library/policy/usmc/mcdp/1-1/mcdp1-1_chap2.pdf
5. https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019
6. https://www.moew.government.bg/en/water/marine-environment/marine-strategy-of-republic-of-bulgaria/
7. https://www.defence24.com/polish-national-defence-concept-new-division-and-5th-generation-fighter-aircraft
8. https://www.gov.pl/web/national-defence/polish-defence-in-the-perspective-of-2032
9. https://en.bbn.gov.pl/ftp/dok/SKBMRPENG.pdf.

DESIGNUL OPERAȚIEI LA NIVEL TACTIC

Locotenent-colonel Cătălin CHIRIAC
Universitatea Națională de Apărare „Carol I”, București

Apariția „Manualului de planificare a operațiilor” la nivel național a determinat regândirea modului de realizare a planificării operațiilor, la toate nivelurile artei militare: strategic, operativ și tactic.

Implicit, noile concepte și abordări propuse prin intermediul manualului au fost însușite, explicate și adaptate specificului național într-o anumită măsură și aplicate de către toate nivelurile, chiar dacă unele dintre acestea necesitau clarificări și abordări diferite, cum ar fi, de exemplu, designul operației.

Cuvinte-cheie: operație, nivel tactic, designul operației, documente de planificare, cadru operațional.

INTRODUCERE

Scopul acestui articol este de a deschide acel dialog care poate conduce către clarificarea sensului conceptului de *design al operațiilor* și a modului în care acesta poate fi dezvoltat la nivelurile operativ și, mai ales, tactic.

Apărut în limbajul planificatorilor militari odată cu bine-cunoscutul, de acum, *COPD – Directiva Comandamentului Aliat pentru Operaţii pentru planificarea cuprinzătoare a operaţiilor*[1], *designul operației* s-a dorit a fi procesul care să fundamenteze *„dezvoltarea concepţiei campaniei/operaţiei şi a documentelor de planificare”*[2]. Însușirea și dezvoltarea acestui concept a generat și încă generează numeroase probleme planificatorilor militari de la nivelul operativ și, mai ales, celor de la nivelul tactic, atât prin insuficienta explicare a acestuia în cadrul manualelor sau al doctrinelor specifice planificării operațiilor, cât și prin lipsa exemplificărilor. Deși *Manualul de planificare a operațiilor* asigură definirea conceptului și stabilește locul acestuia în cadrul procesului desfășurat de către nivelul operativ, nu oferă totuși lămuriri sau detalii privind abordarea acestui concept la nivel tactic. În aceste condiții, consider că principalele elemente care necesită aprofundare și o atentă clarificare se referă la nivelul și modul în care *designul operației* poate fi dezvoltat.

Designul operației s-a dorit a fi procesul care să fundamenteze „dezvoltarea concepţiei campaniei/ operaţiei şi a documentelor de planificare”.

Una dintre cele mai dificile probleme la care grupurile de planificare sau statele majore de la nivelul tactic trebuie să găsească răspuns o constituie *existența și dezvoltarea designului operației* la acest nivel. Problema este anevoioasă, deoarece acest concept este detaliat doar pentru nivelul strategic și operativ și există o oarecare nesiguranță atunci când este luat în discuție la nivelul tactic.

[1] ***, *Allied Command Operations Comprehensive Operations Planning Directive.* La nivel național, prevederile COPD se regăsesc în cadrul *Manualului de planificare a operațiilor*, Statul Major General, București, 2016.
[2] ***, *Doctrina Armatei României*, Statul Major General, București, 2012, p. 150.

Cu toate că *Manualul de planificare a operațiilor* precizează faptul că, *„la nivel naţional, designul îmbracă două aspecte – designul strategic şi designul la nivel operativ”*[3], el nu aduce totuși lămuriri suplimentare privind abordarea nivelului tactic, în condițiile în care același manual reprezintă fundamentul elaborării manualelor specifice de planificare ale categoriilor de forțe.

Chiar dacă apariția conceptului a pus, la un moment dat, sub semnul întrebării existența și desfășurarea procesului de planificare, designul nu trebuie văzut ca un înlocuitor al acestuia. Actualele procese de planificare pentru nivelurile strategic și operativ stabilesc clar momentul în care designul este desfășurat, produsele specifice acestui proces și modul în care acestea asigură fluiditate desfășurării ulterioare a procesului. În anul 2009, fostul comandant al US Joint Forces Command, generalul James Mattis, a propus următorul enunţ pentru relația dintre design și planificare: *„Designul nu înlocuiește planificarea, iar planificarea este incompletă fără design. Echilibrul dintre cele două variază de la o operație la alta, precum și în cadrul fiecărei operații. [...] Executate corect, cele două procese sunt întotdeauna complementare, suprapuse, sinergice și continue”*[4]. În aceste condiții, designul și planificarea ar face posibilă transformarea direcționărilor și ordinelor ample ale comandanților eșaloanelor strategic și operativ în misiuni și sarcini concrete pentru nivelul tactic.

În anul 2009, fostul comandant al US Joint Forces Command, generalul James Mattis, a propus următorul enunţ pentru relația dintre design și planificare: „Designul nu înlocuiește planificarea, iar planificarea este incompletă fără design. Echilibrul dintre cele două variază de la o operație la alta, precum și în cadrul fiecărei operații. Executate corect, cele două procese sunt întotdeauna complementare, suprapuse, sinergice și continue”.

DESIGNUL OPERAȚIEI LA NIVEL OPERATIV

La nivel operativ, *designul operației* reprezintă atât un proces, cât și un produs. Un proces – datorită pașilor concreți care trebuie urmați pentru realizarea acestuia și un produs – deoarece aplicarea procesului are ca finalitate un cumul de informații și elemente specifice necesare continuării procesului. Produs ca urmare a aplicării artei operative[5],

[3] ***, *Manualul de planificare a operațiilor, op. cit.*, p. 18.

[4] Generalul James Mattis, *Vision for a Joint Approach to Operational Design*, 6 octombrie 2009, disponibil la www.smallwarsjournal.com/blog/usjfcom-releases-approach-to-operational-design-vision, accesat la 23.01.2020.

[5] *Manualul de planificare a operațiilor* definește *arta operativă ca reprezentând angajarea cu abilitate a instrumentului militar în scopul realizării obiectivelor strategice și/sau la nivel operativ, prin designul, organizarea, integrarea și conducerea campaniilor, operațiilor, bătăliilor și luptelor, realizând legătura între strategia și tactica militară.*

designul operației reprezintă expresia viziunii comandantului privind transformarea situației inacceptabile de la începutul campaniei, într-o serie de condiții acceptabile la sfârșitul acesteia[6].

Realizarea *designului operației* prin contribuția unitară a grupului de planificare și a comandantului permite nivelului operativ să vizualizeze imaginea de ansamblu a întregii campanii întrunite și să identifice elementele care asigură fluiditate acțiunilor de nivel tactic. În timp ce în responsabilitatea grupului de planificare se află elaborarea *cadrului operațional* (o serie de concepte specifice, identificate sau determinate în conformitate cu precizările în vigoare), comandantul structurii are obligația de a stabili și a emite *intenția inițială*. Împreună, aceste două elemente formează **designul inițial al operației**[7].

La nivel național[8], cadrul operațional este dezvoltat pe baza conceptelor specifice *designului operației*, concepte aliniate, de altfel, celor identificate la nivelul Alianței. Utilizate într-o succesiune progresivă, conceptele designului sunt necesare pentru înțelegerea cerințelor operaționale și facilitarea activităților planificatorilor. Documente naționale prevăd un număr de 12 concepte, astfel: starea finală dorită, tranziţia şi terminarea, obiectivele, efectele, indicatorii de performanţă şi eficacitate, criteriile de măsurare a succesului, centrele de greutate şi capabilităţile, cerinţele şi vulnerabilităţile asociate acestora, punctele decisive şi condiţiile decisive, liniile de angajare strategică sau liniile de operaţii, geometria operaţiei, succesiunea acţiunilor şi fazele operaţiei (stabilite prin aplicarea următoarelor concepte operaţionale: sincronizarea, sinergia şi efectul de multiplicare, simultaneitatea şi adâncimea, manevra, tempo-ul operaţional şi efortul principal), contingenţele – variantele şi alternativele, punctul culminant/culminaţia, pauzele operaţionale, abordarea directă şi cea indirectă[9].

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Realizarea designului operației prin contribuția unitară a grupului de planificare și a comandantului permite nivelului operativ să vizualizeze imaginea de ansamblu a întregii campanii întrunite și să identifice elementele care asigură fluiditate acțiunilor de nivel tactic.

În timp ce în responsabilitatea grupului de planificare se află elaborarea cadrului operațional, comandantul structurii are obligația de a stabili și a emite intenția inițială. Împreună, aceste două elemente formează designul inițial al operației.

[6] ***, COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, 4 octombrie 2013, pp. 4-52.

[7] ***, *Manualul de planificare a operațiilor, op. cit.*, p. 114.

[8] ***, *Doctrina planificării operațiilor în Armata României*, Statul Major General, București, 2013, p. 40.

[9] Conceptele sunt prezentate și detaliate în *Doctrina planificării operațiilor în Armata României, op. cit.*, pp. 40-57.

Practic însă, la nivel operativ, cadrul operațional este realizat pe parcursul Fazei 3 a procesului de planificare – *estimarea la nivel operativ*, prin stabilirea: *condițiilor decisive, efectelor, acțiunilor operaționale și a celor non-militare, liniilor de operații, secvențelor și fazelor operației, variantelor și alternativelor liniilor de operații*[10]. Această abordare trebuie văzută ca o cale *logică a secvenţelor elaborării cadrului operațional, dar care poate varia în funcţie de direcționările comandantului şi de experienţa grupului de planificare*[11].

Intenția comandantului este enunțată pe timpul *Briefingului de analiză a misiunii*, moment în care este validat și cadrul operațional, în timp ce designul operației, în ansamblu, va fi aprobat pe timpul *Briefingului de luare a deciziei*.

DESIGNUL OPERAȚIEI LA NIVEL TACTIC

În conformitate cu prevederile Doctrinei Armatei României, nivelul tactic reprezintă nivelul „la care ciocnirile şi luptele sunt planificate şi executate cu scopul de a realiza obiectivele militare ale unităţilor şi marilor unităţi tactice”.

În conformitate cu prevederile *Doctrinei Armatei României*, nivelul tactic reprezintă nivelul *„la care ciocnirile şi luptele sunt planificate şi executate cu scopul de a realiza obiectivele militare ale unităţilor şi marilor unităţi tactice”*[12]. Documentele elaborate în sprijinul planificării și evaluării operațiilor sau procesului de management al țintelor aduc precizări suplimentare, în sensul în care nivelul tactic începe cu categoriile de forțe și componentele operaționale. Această realitate, indiferent de categoria de forțe (terestră, aeriană, navală sau de operații speciale), impune ca planificarea operațiilor pentru acest nivel să răspundă cerințelor și particularităților tuturor structurilor componente și specificului genurilor de arme. Luând în considerare aceste elemente, realizarea designului operației la nivelul tactic ridică mai multe semne de întrebare legate de oportunitatea acestuia și de modul în care se poate realiza, precum și de nivelul până la care se poate aplica.

Consider că principala problemă a *designului operației* la nivel național o constituie chiar definirea acestuia. La nivelul NATO, există, în cadrul literaturii de specialitate, noțiunea de *„operational design”*, care, la nivel național, a fost tradusă și implementată sub denumirea

[10] ***, *Manualul de planificare a operațiilor*, *op. cit.*, pp. 116-117.
[11] *Ibidem*, p. 116.
[12] *** *Doctrina Armatei României*, *op. cit.*, p. 159.

de *„designul operației”* și nu sub forma de *„designul operațional”*, așa cum ar fi fost mai potrivit. Pentru o corectă informare, în cadrul Alianței Nord-Atlantice există *„operational design”* și *„operations planning”,* pentru a se putea face distincția între nivelul de planificare și operație[13].

Preluarea și traducerea cuvântului *„operational”* din limba engleză prin cuvântul *„operațional”*, dar, în același timp, și prin *„operativ”* a generat o serie de dificultăți sau anomalii în cadrul manualelor sau doctrinelor naționale. În aceste condiții, nivelul dintre strategic și tactic este *nivelul operativ*, care face o evaluare a *mediului operațional*, elaborează deopotrivă planuri *operaționale și operative* și răspunde unor cerințe *operaționale*. *Designul operației* la acest nivel are la bază *cadrul operațional* (preluat corect din *„operational framework”*) și nu *cadrul operativ* (în logica preluării termenului *„operational”)* și intenția comandantului.

În cadrul Alianței Nord-Atlantice există „operational design” și „operations planning”, pentru a se putea face distincția între nivelul de planificare și operație.

Dacă, la nivelul NATO, *„operational design”* este relaționat nivelului operațional și operației specifice acestuia, la nivel național, prin *„designul operației”* se poate înțelege că acest concept se adresează tuturor structurilor ce desfășoară operații. Lucru care, de altfel, a și introdus această stare de incertitudine în utilizarea conceptului.

Un alt aspect care îngreunează elaborarea *designului operației* la nivelul tactic îl constituie caracteristicile nivelului în sine. Analiza nivelului tactic impune luarea în considerare a unui palier destul de mare de structuri, plecând de la categoriile de forțe și componentele operaționale și terminând cu subunități de nivel batalion sau chiar companie. În aceste condiții, realizarea *designului operației* devine imposibilă, deoarece respectarea formatului standard al conceptului este imposibilă pentru toate aceste structuri. Totuși, în aceste condiții, opțiunea nivelului tactic s-ar rezuma la stabilirea acelor structuri care pot îndeplini cerințele realizării designului operației.

Un ultim aspect care trebuie luat în considerare atunci când se discută depre *designul operației* la nivel tactic îl constituie conceptele acestuia care, pur și simplu, nu sunt caracteristice acestui nivel, indiferent de eforturile depuse de către planificatori în acest sens.

[13] Termenul utilizat la nivelul Alianței pentru planificarea operațiilor militare la toate nivelurile este *operations planning*. Vezi COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, *op. cit.*, pp. 1-3.

Consider că principalele concepte care nu pot fi identificate la nivelul tactic, în sensul în care acestea își pot aduce contribuția la realizarea *designului operației*, sunt *condițiile decisive*, *efectele* și *liniile de operații*.

Elementul principal de la care trebuie pornit atunci când se discută despre *designul operației* îl constituie prevederile documentelor de planificare. Pentru a putea realiza *designul operației*, trebuie să existe un *cadru operațional* și o *intenție a comandantului*. *Chiar dacă există o intenție a comandantului, dar un cadru operațional incomplet, lipsit de elementele importante, nu putem discuta despre designul operației, așa cum a fost prezentat anterior.* Atât pe plan național, cât și în cadrul Alianței, este prevăzut destul de clar că, la nivelul întrunit, cadrul operațional și, implicit, designul sunt dezvoltate prin stabilirea *„condiţiilor decisive pe liniile de operaţii în scopul îndeplinirii obiectivelor de nivel operativ şi contribuind, astfel, la îndeplinirea obiectivelor strategice şi realizarea stării finale”*[14]. Consider că este necesar ca utilizarea sintagmei *„design al operației”* să se facă respectând definiția, termenii și, mai ales, semnificația acestora, trasate prin documentele specifice.

Elementul principal de la care trebuie pornit atunci când se discută despre designul operației îl constituie prevederile documentelor de planificare. Pentru a putea realiza designul operației, trebuie să existe un cadru operațional și o intenție a comandantului. Chiar dacă există o intenție a comandantului, dar un cadru operațional incomplet, lipsit de elementele importante, nu putem discuta despre designul operației.

În aceste condiții, analizarea definițiilor și a caracteristicilor principalelor concepte amintite anterior, așa cum sunt acestea prezentate în documentele naționale specifice, determină următoarele elemente importante:

❖ *Condiţiile decisive* sunt critice pentru obținerea unui obiectiv operațional, sfera acestui concept fiind mult mai cuprinzătoare decât *punctele decisive*. În timp ce punctele decisive se *pot* utiliza pentru realizarea *designului operațional* al unei operații de tipul forță contra forță[15,16], folosirea condițiilor decisive este mult mai aproape de realitatea mediului de operare și specifică pentru *„operaţiile actuale, deoarece reflectă mai adecvat contribuţia militară la abordarea cuprinzătoare”*[17]. Aceeași concluzie se poate desprinde și din analiza definirii conceptelor menționate în *tabelul nr. 1*. Astfel, pentru

[14] ***, *Manualul de planificare a operațiilor*, *op. cit.*, p. 20 și COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive*, *op. cit.*, pp. 1-13.
[15] Force-on-force operations.
[16] ***, COPD INTERIM V2.0, Allied Command Operations Comprehensive Operations Planning Directive, op. cit., pp. 4-52.
[17] ***, *Doctrina planificării operațiilor în Armata României, op. cit.*, p. 49.

nivelul tactic este oportună utilizarea, atunci când situația impune, a *„punctelor decisive”* și nu a condițiilor decisive, mult prea generoase și complexe pentru acest nivel. Dar, în aceste condiții, nu mai este realizată concordanța cu definirea și conceptele cadrului operațional prezentate anterior.

Punct decisiv	Condiție decisivă
Un punct din care un centru de greutate, al propriilor forțe sau ostil, poate fi amenințat. Acest punct poate exista în timp, în spațiu sau în mediul informațional.	O combinație de circumstanțe și/sau efecte, un eveniment important, un factor-cheie sau o funcție de luptă, a căror apariție/exercitare îi permite comandantului să obțină un avantaj tangibil asupra unui adversar sau care contribuie substanțial la obținerea unui obiectiv operațional.

Tabelul nr. 1: Definirea termenilor punct decisiv și condiție decisivă[18,19]

❖ La modul general, un efect poate fi definit ca reprezentând *„o modificare a stării fizice sau comportamentale a unui sistem sau a unui element al unui sistem, care este creat prin rezultatul uneia sau a mai multor acţiuni”*[20]. Caracteristic acestui concept este faptul că efectele sunt utilizate în planificarea și desfășurarea operațiilor doar la nivelurile strategic și operativ[21], nivelul tactic concentrându-se pe *„sarcinile necesare îndeplinirii misiunii care, în final, conduc la realizarea efectelor dorite la nivel strategic şi operativ”*[22]. Chiar dacă acțiunile specifice nivelului tactic sunt urmate în mod logic de efectele normale desfășurării acestora (conform definirii efectului), consider că *efectele* nu pot fi cuantificate la adevărata valoare la acest nivel sau, în anumite condiții, pot fi confundate cu obiectivele stabilite atât la nivelul eșalonului superior, cât și la nivelul propriei structuri. Este, astfel, logic ca nivelul tactic să depună eforturi pentru identificarea sarcinilor necesare *îndeplinirii misiunilor primite* de la nivelul operativ

La modul general, un efect poate fi definit ca reprezentând „o modificare a stării fizice sau comportamentale a unui sistem sau a unui element al unui sistem, care este creat prin rezultatul uneia sau a mai multor acţiuni”.

Caracteristic acestui concept este faptul că efectele sunt utilizate în planificarea și desfășurarea operațiilor doar la nivelurile strategic și operativ, nivelul tactic concentrându-se pe „sarcinile necesare îndeplinirii misiunii care, în final, conduc la realizarea efectelor dorite la nivel strategic și operativ”.

[18] ***, *Doctrina Armatei României*, *op. cit.*, pp. 148, 167.
[19] ***, *NATO Glossary of Terms and Definitions (English and French)*, North Atlantic Treaty Organization, NSO, 2016, p. 40.
[20] ***, *Manualul de planificare a operațiilor, op. cit.*, p. 187.
[21] *Ibidem*, p. 17, și COPD INTERIM V2.0, *Allied Command Operations Comprehensive Operations Planning Directive, op. cit.*, pp. 1-11.
[22] ***, *Manualul de planificare a operațiilor*, *op. cit.*, p. 81.

și nu pe *identificarea efectelor*. Totuși, la nivelul tactic, comandanții de structuri pot face recomandări privind acțiunile care pot fi executate de către forțele proprii pentru obținerea efectelor stabilite la nivelul operativ.

❖ Linia de operații reprezintă *„o secvenţă logică ce leagă în timp şi în spaţiu efectele şi punctele decisive, pe drumul către centrul de greutate, pentru îndeplinirea unui obiectiv operaţional, în cadrul unei campanii sau operaţii”*[23] și, de obicei, există o linie de operații pentru fiecare obiectiv[24]. În condițiile în care linia de operații realizează legătura dintre efecte, puncte decisive și obiective, în mod logic, lipsa unuia sau a mai multor elemente constitutive atrage după sine anularea ei. Considerăm, astfel, că, în absența efectelor sau a condițiilor decisive, nu se pot identifica linii de operații la nivel tactic.

Conceptele designului operației sunt elaborate logic și se află într-o relație de determinare, în sensul în care identificarea unui concept conduce către stabilirea și identificarea următorului. În același timp însă, absența unui concept poate crea probleme în identificarea unui alt concept sau poate conduce chiar la imposibilitatea stabilirii cadrului operațional așa cum a fost el definit.

CONCLUZII

Conceptele *designului operației* sunt elaborate logic, așa cum am amintit, și se află într-o relație de determinare, în sensul în care identificarea unui concept conduce către stabilirea și identificarea următorului. În același timp însă, absența unui concept poate crea probleme în identificarea unui alt concept sau poate conduce chiar la imposibilitatea stabilirii cadrului operațional așa cum a fost el definit, situație în care se află astăzi nivelul tactic.

Designul operației sub forma adoptată în cadrul documentelor elaborate la nivel național nu se poate dezvolta la nivelul tactic, având în vedere argumentele prezentate anterior. Există totuși posibilitatea ca acest lucru să se întâmple fie datorită prevederilor manualelor de la acest nivel, fie unui exces de zel al comandanților sau al grupului de planificare, prin adoptarea forțată a efectelor, a condițiilor decisive sau a liniilor de operații. *Efectele* unei astfel de abordări conduc către o suprasolicitare a personalului implicat și o aglomerare nejustificată a procesului, în condițiile în care timpul avut la dispoziție este din ce în ce mai limitat.

[23] *Ibidem*, p. 190.
[24] *Ibidem*, p. 117.

REFERINȚE BIBLIOGRAFICE:

1. ***, *Allied Command Operations Comprehensive Operations Planning Directive* – COPD Interim V2.0, SHAPE, 2013.
2. ***, *Doctrina Armatei României*, Statul Major General, Bucureşti, 2012.
3. ***, *Doctrina planificării operaţiilor în Armata României*, Statul Major General, Bucureşti, 2013.
4. ***, *Manualul de planificare a operaţiilor*, Statul Major General, Bucureşti, 2016.
5. General James Mattis, *Vision for a Joint Approach to Operational Design*, 6 octombrie 2009.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

RĂZBOIUL CIBERNETIC ȘI TERORISMUL CIBERNETIC – TRĂSĂTURI ȘI RĂSPUNSURI LA ACESTE AMENINȚĂRI –

Colonel (r.) dr. Romică CERNAT

În ultimii ani, spațiul cibernetic a obținut o importanță strategică ascendentă, astfel că statele au început să-l trateze ca pe un domeniu similar celui terestru, maritim și aerian, care trebuie să fie securizat pentru a-și proteja interesele lor naționale. Atacurile cibernetice sunt, acum, un element comun al conflictelor internaționale, atât separat, cât și în contextul unor operații militare mai ample. Atacurile în spațiul virtual s-au amplificat și diversificat în ceea ce privește actorii și metodele. Deoarece statele au devenit mult mai dependente de tehnologia informației și componentele rețelei critice de infrastructură, apar multe întrebări cu privire la faptul dacă un stat este organizat în mod corespunzător pentru a-și apăra mijloacele sale digitale strategice. Spațiul cibernetic integrează funcționarea infrastructurilor critice, precum instituțiile guvernamentale, de securitate națională și comerțul. Întrucât spațiul virtual transcende granițele geografice, o mare parte a acestuia este în afara controlului și influenței unui stat.

Cuvinte-cheie: război cibernetic, sistem informatic, program nuclear, terorism cibernetic, virus informatic.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

CONSIDERAȚII PRELIMINARE

Conceptul de *„atac cibernetic”* este relativ recent și se referă la o gamă largă de activități desfășurate prin utilizarea tehnologiei informației și a comunicațiilor (TIC). Utilizarea atacurilor de Interdicție a Serviciului de Distribuție a Datelor (ISDD) a devenit o metodă larg răspândită pentru a îndeplini obiective politice, prin întreruperea serviciilor on-line. În acest tip de atacuri, un server este copleșit de traficul de internet, astfel încât accesul la anumite site-uri este degradat sau interzis. Apariția virusului informatic Stuxnet, în iunie 2010, pe care unii îl consideră primul atac cibernetic, a arătat că atacurile cibernetice ar putea avea un efect distructiv și de durată. Creat pentru a sabota programul nuclear al Iranului, sistemul distructiv de programe pentru calculatoare Stuxnet a atacat sistemele de control industriale computerizate, cu care operează centrifugele nucleare ce produc uraniu îmbogățit, și avea ca finalitate autodistrugerea fizică a instalațiilor. Evenimente internaționale recente au ridicat semne de întrebare cu privire la situația în care un atac cibernetic ar putea fi considerat un act de război și ce fel de opțiuni de răspuns au la dispoziție statele victimă.

Apariția virusului informatic Stuxnet, în iunie 2010, pe care unii îl consideră primul atac cibernetic, a arătat că atacurile cibernetice ar putea avea un efect distructiv și de durată. Creat pentru a sabota programul nuclear al Iranului, Stuxnet a atacat sistemele de control industriale computerizate, cu care operează centrifugele nucleare ce produc uraniu îmbogățit, și avea ca finalitate autodistrugerea fizică a instalațiilor.

Având în vedere cele prezentate, consider că este imperios ca fiecare stat să dispună măsurile și mecanismele necesare la nivel național și de participare la nivel european și internațional, în domeniul asigurării securității rețelelor și sistemelor informatice, în vederea asigurării unui nivel comun ridicat de securitate și a stimulării cooperării în domeniu[1].

Atacurile cibernetice asupra Sony Entertainment ilustrează dificultățile în clasificarea atacurilor și elaborarea unei politici de răspuns. Pe 24 noiembrie 2014, corporația Sony a fost obiectul unui atac cibernetic care a dezactivat sistemele sale TIC, a distrus datele și stațiile de lucru și a accesat e-mailuri interne și alte date. Biroul Federal de Investigații (FBI) al Statelor Unite ale Americii și directorul Serviciului de Informații Naționale (SIN) au atribuit atacurile informatice guvernului

[1] *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, în *Monitorul Oficial*, Partea I nr. 21 din 9 ianuarie 2019, p. 1.

nord-coreean. Coreea de Nord a negat implicarea sa în atac, dar a lăudat un grup de hacktiviști, numit *„Gardienii Păcii”*, pentru că au făcut o *„faptă justă”*. În timpul unei conferințe de presă, pe 19 decembrie 2014, președintele Obama a promis să *„răspundă proporțional”* la presupusa agresiune cibernetică a Coreii de Nord, *„într-un loc, timp și mod ales de noi”*[2]. Președintele Obama a categorisit incidentul ca un act de *„cyber-vandalism”*, în timp ce alți analiști l-au catalogat ca un act de război cibernetic.

Odată cu natura globalizată a internetului, autorii pot lansa atacuri cibernetice de oriunde în lume și pot direcționa atacurile prin servere ce aparțin unor terțe țări. O analiză profundă a principalelor atacuri cibernetice asupra agențiilor guvernamentale, companiilor din sectorul de apărare și de înaltă tehnologie sau a infracțiunilor economice cu pierderi de mai mult de un milion de dolari evidențiază amploarea acestui fenomen.

Acest incident ilustrează dificultățile în ceea ce privește clasificarea atacurilor cibernetice, actorii implicați, motivațiile lor, precum și problemele de suveranitate referitoare la site-ul pe care actorii au fost localizați fizic. Odată cu natura globalizată a internetului, autorii pot lansa atacuri cibernetice de oriunde în lume și pot direcționa atacurile prin servere ce aparțin unor terțe țări. O analiză profundă a principalelor atacuri cibernetice asupra agențiilor guvernamentale, companiilor din sectorul de apărare și de înaltă tehnologie sau a infracțiunilor economice cu pierderi de mai mult de un milion de dolari evidențiază amploarea acestui fenomen[3]. A fost atacul cibernetic asupra Sony, o corporație privată cu sediul în Japonia, un atac asupra SUA? Mai mult, ar putea fi considerat un act de terorism, o utilizare a forței sau o infracțiune informatică? În categorisirea atacurilor asupra Sony ca un act de *„vandalism cibernetic”*, care, de obicei, include compromiterea site-urilor web și este, în genere, domeniul actorilor motivați politic cunoscuți sub numele de *„hacktiviști”*, președintele Obama a avut rezerve despre ce tip de răspuns ar putea fi considerat *„proporțional”* și împotriva cui. O altă întrebare potențială asociată ar putea fi circumstanțele în care SUA ar angaja trupe pentru a răspunde la un atac cibernetic. În relație logică este și întrebarea dacă SUA și alte state puternice au o strategie eficientă de descurajare în vigoare? Directorul Serviciului Național de Informații al SUA, James Clapper, a afirmat despre actorii războiului cibernetic că, *„dacă ei obțin*

[2] Barack Obama, *„Remarks by the President in Year-End Press Conference”*, 12 decembrie 2014, în *The White House Office of the Press Secretary*, disponibil la https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference, accesat la 20.12.2019.

[3] *„Significant Cyber Incidents Since 2006”*, în *Center for Strategic & International Studies*, disponibil la https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa, accesat la 7 ianuarie 2020.

recunoaștere la nivel mondial, la un cost redus și nu vor suferi nicio consecință, ei vor acționa în același mod, din nou, și vor continua să o facă iarăși, până când vom acționa împotriva lor”[4].

POZIȚIA STATELOR ȘI ORGANISMELOR INTERNAȚIONALE PRIVIND RĂZBOIUL CIBERNETIC

Infrastructura critică a statelor a fost, pentru mult timp, supusă amenințărilor fizice, iar acum este din ce în ce mai expusă riscului de atacuri în spațiul virtual[5]. Războiul cibernetic este, de obicei, conceptualizat ca acțiune stat-contra-stat, echivalent cu un atac armat sau folosirea forței în spațiul virtual, care poate declanșa un răspuns militar, cu o utilizare proporțională a forței. Infractorii, teroriștii și spionii, în activitatea lor, se bazează foarte mult pe tehnologiile cu suport cibernetic pentru a îndeplini obiectivele organizaționale. Teroriștii cibernetici sunt indivizi sponsorizați de actori statali și nestatali, care se angajează în atacuri informatice pentru a-și îndeplini obiectivele. Organizațiile teroriste transnaționale, insurgenții și jihadiștii au folosit internetul ca instrument pentru planificarea atacurilor, radicalizare și recrutare, ca o metodă de popularizare a propagandei, ca mijloc de comunicare, precum și pentru scopuri perturbatorii.

Teroriștii cibernetici sunt indivizi sponsorizați de actori statali și nestatali, care se angajează în atacuri informatice pentru a-și îndeplini obiectivele. Organizațiile teroriste transnaționale, insurgenții și jihadiștii au folosit internetul ca instrument pentru planificarea atacurilor, radicalizare și recrutare, ca o metodă de popularizare a propagandei, ca mijloc de comunicare, precum și pentru scopuri perturbatorii.

Nu există încă niște criterii clare pentru a stabili dacă un atac cibernetic este o infracțiune, un act de hacktivism, terorism sau utilizarea forței de către un stat, echivalentă cu un atac armat. De asemenea, nu au fost încă elaborate instrumente legale internaționale, cu caracter obligatoriu, care să reglementeze în mod explicit relațiile inter-statale în spațiul virtual.

În septembrie 2012, Departamentul de Stat al SUA a luat o poziție publică cu privire la faptul dacă atacurile cibernetice ar putea fi interpretate ca utilizare a forței în conformitate cu prevederile articolului 2, alineatul 4, din Carta ONU și ale Dreptului Internațional cutumiar. Potrivit consilierului de stat pe probleme juridice în funcție, Harold Koh, *„activitățile cibernetice care au ca rezultat nemijlocit*

[4] Chris Strohm, *„FBI Provides More Proof of North Korea Link to Sony Hack”*, 7 ianuarie 2015, în *Bloomberg*, disponibil la https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony, accesat la 20 decembrie 2019.

[5] The White House, *National Strategy for Counterterrorism of the United States of America*, octombrie 2018, p. 19, disponibil la https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf, accesat la 20 decembrie 2019.

moartea, vătămarea persoanelor sau distrugeri semnificative vor fi tratate, cel mai probabil, ca utilizare a forței”[6]. Exemplele oferite în comentariile lui Koh au inclus declanșarea distrugerii unei uzine nucleare, deschiderea unui baraj și provocarea de pagube prin inundații sau de accidente aviatice prin interferarea în controlul traficului aerian. Concentrându-se mai degrabă pe efectele obținute decât pe mijloacele cu care acestea sunt realizate, această definiție a războiului cibernetic se integrează cu ușurință în cadrul juridic internațional existent. În cazul în care un actor folosește un mijloc cibernetic pentru a produce efecte cinetice, care ar putea justifica utilizarea forței militare în alte circumstanțe, atunci întrebuințarea acestei arme cibernetice poate fi asimilată utilizării forței.

Unul dintre obiectivele de apărare ale SISC este de a lucra la nivel internațional „pentru a încuraja un comportament responsabil și să se opună celor care ar încerca să perturbe rețelele și sistemele, făcându-i să renunțe și să descurajeze actorii rău intenționați, rezervându-și dreptul de a-și apăra bunurile naționale”.

Koh a explicat că atacurile cibernetice asupra rețelelor informatice pe timpul unui conflict armat în curs de desfășurare vor fi guvernate de aceleași principii de proporționalitate care se aplică altor acțiuni în temeiul legii conflictelor armate. Aceste principii includ represalii ca răspuns la un atac cibernetic, cu o utilizare proporțională a forței militare. În plus, *„activitățile specifice rețelei de calculatoare, care se ridică la nivelul unui atac armat sau al unei amenințări iminente”*, pot declanșa dreptul unui stat la autoapărare, în conformitate cu prevederile articolului 51 din Carta ONU. Koh citează, în remarcile sale, Strategia Internațională pentru Spațiul Cibernetic 2011 (SISC), care prevede că, *„atunci când se justifică, Statele Unite vor răspunde la actele ostile din spațiul cibernetic așa cum ar răspunde la orice altă amenințare la adresa țării noastre”*[7]. Unul dintre obiectivele de apărare ale SISC este de a lucra la nivel internațional *„pentru a încuraja un comportament responsabil și să se opună celor care ar încerca să perturbe rețelele și sistemele, făcându-i să renunțe și să descurajeze actorii rău intenționați, rezervându-și dreptul de a-și apăra bunurile naționale”*[8]. Creșterea gradului de conștientizare a amenințării mediului

6 Harold Hongju Koh, *„International Law in Cyberspace”*, în *U.S. Department of State*, *Archived content*, 18 septembrie 2012, disponibil la https://2009-2017.state.gov/s/l/releases/remarks/197924.htm, accesat la 20 decembrie 2019.

7 *„International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”*, mai 2011, în *U.S Departament of State*, p. 14, disponibil la https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accesat la 20 decembrie 2019.

8 *Ibidem*, p. 12.

în spațiul virtual a condus la două procese internaționale majore, orientate spre dezvoltarea unui consens expertizat internațional în rândul autorităților cibernetice internaționale.

Reglementări NATO pentru spațiul cibernetic. La un an după atacul privind ISDD în 2007, din Estonia, NATO a înființat Centrul de Excelență și Cooperare în Domeniul Apărării Cibernetice (CECDAC) în Tallinn, Estonia. CECDAC găzduiește grupuri de lucru și cursuri de drept și etică în spațiul virtual, precum și exerciții de apărare împotriva atacurilor cibernetice. În 2009, Centrul a convocat un grup internațional de experți independenți pentru a elabora un manual care să fie aprobat printr-un act normativ și să reglementeze modul de acțiune în cazul unui război cibernetic. Manualul Tallinn, după cum este cunoscut, a fost publicat în 2013[9]. Acesta stabilește 95 de *„norme severe scrise”*, care reglementează consecințele conflictului cibernetic în raport cu suveranitatea și responsabilitatea statului, legea conflictelor armate, dreptul umanitar și legea neutralității. Manualul Tallinn este un text academic și, deși oferă justificări rezonabile pentru aplicarea dreptului internațional, nu este obligatoriu, iar autorii evidențiază faptul că nu vorbesc în numele NATO sau al CECDAC.

Manualul Tallinn stabilește 95 de „norme severe scrise”, care reglementează consecințele conflictului cibernetic în raport cu suveranitatea și responsabilitatea statului, legea conflictelor armate, dreptul umanitar și legea neutralității.

Se poate spune că NATO, în prezent, nu are o poziție clară privind modul de aplicare a prevederilor articolelor 4 și 5 din Tratatul NATO în spațiul cibernetic și nu definește atacurile informatice ca o acțiune militară explicită. Manualul Tallinn echivalează utilizarea forței cu acele operații cibernetice ale căror *„efecte ... sunt asimilate cu cele care ar rezulta dintr-o acțiune care se califică drept un atac armat cinetic”*[10]. În cazul în care un atac este considerat a fi orchestrat de o organizație cibernetică infracțională, fie motivată politic sau financiar, atunci poate fi responsabilitatea statului atacat pentru a selecta un răspuns adecvat jurisdicției sale. Cu toate acestea, caracterul transnațional al majorității organizațiilor infracționale în spațiul cibernetic poate complica deciziile privind competența.

Manualul Tallinn este un text academic și, deși oferă justificări rezonabile pentru aplicarea dreptului internațional, nu este obligatoriu, iar autorii evidențiază faptul că nu vorbesc în numele NATO sau al CECDAC.

Dreptul conflictelor armate privind războiul cibernetic. Represalii ca răspuns la atacuri armate sunt permise în dreptul internațional

9 *„Tallinn Manual on the International Law Applicable to Cyber Warfare”*, în *The NATO Cooperative Cyber Defence Centre of Excellence*, p. 5, disponibil la http://csef.ru/media/articles/3990/3990.pdf, accesat la 6 ianuarie 2020.

10 *Ibidem*, p. 54.

atunci când un stat beligerant încalcă, în timp de pace, dreptul internațional sau legea conflictelor armate în timp de război. Cu toate acestea, termenul de *„atac armat”* nu are o definiție prevăzută de un act normativ și este încă deschis la interpretare, completare și modificare în ceea ce privește atacurile cibernetice. Așa-numita *„Lege a Războiului”*, de asemenea, cunoscută ca *Legea Conflictului Armat*, concretizată în Convențiile de la Geneva, Haga și Carta ONU, poate, în anumite circumstanțe, să se aplice și atacurilor cibernetice, dar nu s-au consemnat încercări din partea statelor de a o aplica sau existența unor acorduri specifice cu privire la aplicabilitatea sa, relevanța sa, în aceste condiții, rămânând neclară. Aplicarea devine complicată, de asemenea, și din cauza dificultăților în atribuire, de utilizarea potențială a computerelor de la distanță, precum și de posibilele daune produse unor terțe părți rezultate din contraatacurile cibernetice, care ar putea fi dificil de controlat sau restricționate. În plus, rămân problemele legate de granițele teritoriale și ceea ce reprezintă un atac armat în spațiul cibernetic. Aplicarea legii ar părea mai clară în situațiile în care un atac cibernetic provoacă daune fizice, cum ar fi întreruperea unei rețele electrice. După cum am menționat, Manualul Tallinn abordează mai multe dintre aceste întrebări[11]. În lipsa unei definiții juridice pentru ceea ce constituie un *„atac armat”* în spațiul cibernetic, profesorul Michael Schmitt a propus următoarele criterii de analiză în conformitate cu dreptul internațional: severitatea, urgența, cauzalitatea, invazivitatea, cuantificarea, legitimitatea prezumtivă și responsabilitatea[12].

În lipsa unei definiții juridice pentru ceea ce constituie un „atac armat” în spațiul cibernetic, profesorul Michael Schmitt a propus următoarele criterii de analiză în conformitate cu dreptul internațional: severitatea, urgența, cauzalitatea, invazivitatea, cuantificarea, legitimitatea prezumtivă și responsabilitatea.

Principiile de bază cuprinse în Convenția de la Haga privind întrebuințarea forțelor armate sunt cele referitoare la necesitate militară, proporționalitate, umanitarism și echitate. Dacă armata unui stat desfășoară operații cibernetice în conformitate cu aceste principii, se poate spune că este angajată într-un război cibernetic.

Poziția Consiliului Europei privind infracționalitatea informatică. În acest context, Convenția Consiliului Europei privind infracționalitatea informatică este primul tratat internațional care încearcă să armonizeze

[11] Oona A. Hathaway, *„The Law of Cyber-Attack”,* în *California Law Review*, vol. 100, nr. 4, 2012, pp. 6-23, disponibil la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932, accesat la 6 ianuarie 2020.

[12] Katharina Ziolkowski, *„Ius ad bellum in Cyberspace – Some Thoughts on the ‹Schmitt-Criteria› for Use of Force”*, în *Legal&Policy Branch NATO CCD COE*, pp. 1-7, disponibil la https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf, accesat la 6 ianuarie 2020.

legile din fiecare țară, cu privire la ceea ce constituie activitatea infracțională în domeniul cibernetic. Acest tratat de aplicare a legii, de asemenea, cunoscut sub numele de *„Convenția de la Budapesta”*, impune semnatarilor să adopte legi penale împotriva diferitelor tipuri de activități specifice în spațiul virtual, pentru a permite instituțiilor de aplicare a legii să investigheze astfel de activități și să coopereze cu agenții similare ale altor state semnatare[13]. Deși este larg recunoscut ca cel mai de substanță acord internațional privind securitatea cibernetică, unii observatori îl consideră totuși un eșec[14]. Unii criticii avertizează că prevederile Convenției sunt limitate pe partea de implementare și nu există legislație corespondentă în toate țările, astfel că infractorii, în acest domeniu, pot opera nestingheriți. În plus, până în septembrie 2019, doar 64 de state au ratificat-o.

Rezoluțiile Adunării Generale a ONU referitoare la spațiul cibernetic. O serie de rezoluții ale Adunării Generale a ONU referitoare la securitatea informatică au fost adoptate în ultimii 19 ani. O rezoluție a solicitat redactarea unui raport elaborat de un grup internațional de experți guvernamentali din 15 state, inclusiv SUA. Scopul declarat al acestui proces a fost de a construi o *„cooperare pentru un mediu al TIC, pașnic, sigur, eficient și deschis”*, prin realizarea unui acord asupra *„normelor, regulilor și principiilor de comportament responsabil al statelor”* și identificarea măsurilor de consolidare a încrederii și a capacităților, inclusiv pentru schimbul de informații. Spre deosebire de activitatea desfășurată la Tallinn sub auspiciile NATO, acest proces, condus de SUA, a inclus atât China, cât și Rusia. Raportul rezultat în 2010, denumit uneori ca Raportul Grupului de Experți Guvernamentali, a recomandat o serie de măsuri pentru a *„reduce riscul de interpretări eronate care rezultă din întreruperile TIC”*, dar nu a inclus niciun acord cu caracter obligatoriu[15].

O serie de rezoluții ale Adunării Generale a ONU referitoare la securitatea informatică au fost adoptate în ultimii 19 ani. Una dintre rezoluții a solicitat redactarea unui raport elaborat de un grup internațional de experți guvernamentali din 15 state, inclusiv SUA, cu scopul de a construi o „cooperare pentru un mediu al TIC, pașnic, sigur, eficient și deschis”, prin realizarea unui acord asupra „normelor, regulilor și principiilor de comportament responsabil al statelor” și identificarea măsurilor de consolidare a încrederii și a capacităților, inclusiv pentru schimbul de informații.

[13] *„Convention on Cybercrime”*, Budapesta, 23.XI.2001, în *Council of Europe, European Treaty Series No. 185*, pp. 7-13, disponibil la https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680081561, accesat la 6 ianuarie 2020.

[14] Jack Goldsmith, *„Cybersecurity Treaties: A Skeptical View”*, 2 iunie 2011, în *Future Challenges in National Security and Law, edited by Peter Berko witz*, pp. 1-11, disponibil la http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf., accesat la 6 ianuarie 2020.

[15] United Nations Secretary General, *„Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”*, 30 iulie 2010, *United Nations General Assembly*, pp. 7-8, disponibil la https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201, accesat la 6 ianuarie 2020.

Cu toate acestea, unii analiști consideră că raportul reprezintă un progres în depășirea diferențelor dintre SUA și Rusia cu privire la diferite aspecte ale securității cibernetice. În decembrie 2001, Adunarea Generală a adoptat Rezoluția 56/183, care a aprobat Summitul Mondial privind Societatea Informațională, pentru a discuta oportunitățile și provocările societății informaționale. Acest Summit a fost convocat pentru prima dată la Geneva, în 2003, apoi în Tunis, în 2005, și, ulterior, la Geneva, în mai 2013. Delegați din 175 de țări au participat la primul Summit, unde au adoptat o Declarație de Principii – o foaie de parcurs pentru realizarea unei societăți informaționale deschise. Summitul de la Geneva a lăsat alte probleme, mai controversate, nerezolvate, inclusiv problema administrării și a finanțării internetului. La ambele reuniuni la nivel înalt, propunerile ca SUA să renunțe la controlul Corporației Internet pentru Alocarea Numelor și Numerelor au fost respinse. Un tratat internațional care să interzică războiul cibernetic și utilizarea informațiilor ca armă a fost propus în cadrul ONU de către delegațiile Rusei și Germaniei.

În decembrie 2001, Adunarea Generală a adoptat Rezoluția 56/183, care a aprobat Summitul Mondial privind Societatea Informațională, pentru a discuta oportunitățile și provocările societății informaționale. Acest Summit a fost convocat pentru prima dată la Geneva, în 2003, apoi în Tunis, în 2005, și, ulterior, la Geneva, în mai 2013. Delegați din 175 de țări au participat la primul Summit, unde au adoptat o Declarație de Principii – o foaie de parcurs pentru realizarea unei societăți informaționale deschise.

Alte acorduri internaționale privind războiul cibernetic. Unele organisme de drept internațional, în special cele asociate cu aviația și marina, pot aplica normele de securitate cibernetică, de exemplu, prin interzicerea perturbării controlului traficului aerian sau a altui comportament care ar putea pune în pericol siguranța aeronautică[16]. Planuri bilaterale, tratate reciproce de asistență juridică între țări pot fi aplicabile pentru investigații infracționale în domeniul securității cibernetice și al urmăririi penale.

TERORISMUL CIBERNETIC – CARACTERISTICI DEFINITORII

Ca și în cazul războiului cibernetic, în majoritatea legislațiilor naționale sau în legislația internațională nu există un consens privind o definiție a ceea ce constituie *terorismul cibernetic*. Unele definiții, abordând actele de terorism ce transcend frontierele, fac trimitere la activități și prejudicii definite în legislația privind fraudele și abuzurile în rețelele și sistemele informatice. Un aspect important al acestor documente juridice face referire la *„pedeapsa pentru o infracțiune”*, care atrage după sine amenzi sau închisoare și sugerează că partea agresoare săvârșește un act infracțional mai degrabă decât un act de terorism, în timp ce alții susțin că este un act de război, dacă sunt săvârșite de către un actor statal

De exemplu, Statele Unite ale Americii consideră că este ilegal pentru o entitate să *„acceseze cu bună știință un calculator fără autorizare sau să depășească nivelul de acces autorizat și, prin intermediul unor astfel de comportamente, să se obțină informații, pentru care s-a considerat de către Guvern, printr-un act normativ, că necesită protecție împotriva divulgării neautorizate, din motive de securitate națională sau relații externe, sau sunt restricționate din alte rațiuni, cu motive să se creadă că astfel de informații, obținute în modul acesta, pot fi utilizate pentru a prejudicia SUA sau pot fi folosite în avantajul oricărui stat străin”*[17]. Potrivit FBI, internetul și utilizarea mediei sociale, în special, sunt printre principalii *„factorii care au contribuit la evoluția peisajului amenințării terorismului”*, de la atacurile teroriste din 11 septembrie 2001[18].

Statele Unite ale Americii consideră că este ilegal pentru o entitate să „acceseze cu bună știință un calculator fără autorizare sau să depășească nivelul de acces autorizat și, prin intermediul unor astfel de comportamente, să se obțină informații, pentru care s-a considerat de către Guvern, printr-un act normativ, că necesită protecție împotriva divulgării neautorizate, din motive de securitate națională sau relații externe, sau sunt restricționate din alte rațiuni”.

Unele analize juridice definesc terorismul cibernetic ca *„utilizarea premeditată de activități perturbatoare sau amenințarea cu acestea, împotriva calculatoarelor sau rețelelor, cu intenția de a cauza un prejudiciu sau a realiza alte obiective sociale, ideologice, religioase, politice sau similare sau pentru a intimida orice persoană în scopul promovării unor astfel de obiective”*[19]. Cu toate acestea, astfel de acțiuni au, de asemenea, statut infracțional și, în general, se referă la persoane sau organizații mai degrabă decât la actorii statali. Unele definiții ale terorismului cibernetic se concentrează pe distincția dintre acțiunea distructivă și cea perturbatoare, terorismul generând o teamă comparabilă cu cea a atacului fizic și nu este doar un dezastru costisitor. Deși blocarea distribuită a unui serviciu în sine nu produce acest tip de frică sau de distrugere, problema este potențialul pentru efectele de ordinul al doilea sau al treilea[20]. De exemplu, dacă serviciile de telecomunicații și de urgență au fost complet inoperabile

[16] Oona A. Hathaway, *op. cit.*, pp. 11, 28, 31-32.

[17] H. Marshall Jarrett, *„Prosecuting Computer Crimes”*, în *Office of Legal Education Executive Office for United States Attorneys*, pp. 12-13, disponibil la https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ccmanual.pdf, accesat la 6 ianuarie 2020.

[18] FBI, *„Terrorism”*, în *What We Investigate*, disponibil la https://www.fbi.gov/investigate/terrorism, accesat la 6 ianuarie 2020.

[19] Barry C. Collin, *„Cyberterrorism”*, în *Institute for Security and Intelligence, 11th Annual International Symposium on Criminal Justice Issues*, p. 1, disponibil la https://www.nato.int/structur/library/bibref/cyberterrorism.pdf , accesat la 6 ianuarie 2020.

[20] DDoS – Distributed Denial of Service.

În literatura de specialitate, în scop analitic și statistic, există diferite definiții pentru sintagma „terorism cibernetic", la fel cum există mai multe definiții pentru termenul „terorism".

Terorismul a fost definit ca fiind violența premeditată, motivată politic, comisă împotriva țintelor necombatante, de subgrupuri naționale sau agenți clandestini, de obicei în scopul de a influența o anumită colectivitate.

într-o perioadă de criză, efectele unui astfel de atac asupra infrastructurii ar putea fi catastrofale. Cu toate acestea, într-o astfel de situație, sistemul de servicii de urgență în sine nu este cel mai probabil o țintă, ci, mai degrabă, rezultatul unor daune colaterale la o rețea de telecomunicații vulnerabilă**.** De la atacul din 2007 în Estonia, NATO a stabilit autoritățile cu responsabilități în domeniul apărării cibernetice, cu obiective de dezvoltare a strategiei în acest domeniu și de centralizare a capacităților de apărare în rândul membrilor. O politică privind apărarea cibernetică și un plan de acțiune asociat au fost adoptate în 2011, iar pentru a facilita efortul de centralizare, a fost înființată, în 2012, Agenția Comunicațiilor și Societății Informaționale NATO[21].

Caracteristicile terorismului cibernetic. În literatura de specialitate, în scop analitic și statistic, există diferite definiții pentru sintagma *„terorism cibernetic"*, la fel cum există mai multe definiții pentru termenul *„terorism"*. Terorismul a fost definit ca fiind violența premeditată, motivată politic, comisă împotriva țintelor necombatante, de subgrupuri naționale sau agenți clandestini, de obicei în scopul de a influența o anumită colectivitate. Dorothy Denning, expert în securitate, definește terorismul cibernetic ca fiind *„... operațiile motivate politic, de pătrundere neautorizată în rețele de date și informații secrete, menite să provoace prejudicii grave, cum ar fi pierderea de vieți omenești sau pagube economice cu consecințe grave"*[22]. Agenția Federală de Managementul Urgențelor a SUA definește terorismul cibernetic ca *„atacurile ilegale și amenințările de atac împotriva computerelor, rețelelor, precum și informațiilor stocate pe acestea, atunci când sunt săvârșite pentru a intimida sau a constrânge un guvern sau populația unui stat, în scopul promovării unor obiective politice sau sociale"*[23].

Alți analiști evidențiază faptul că un atac fizic care distruge centrele computerizate pentru infrastructurile critice, cum ar fi internetul, telecomunicațiile sau rețelele de energie electrică, chiar fără a atinge vreodată o tastatură, de asemenea, poate contribui la sau să fie etichetat ca terorism cibernetic[24]. Proporția din infracționalitatea informatică ce poate fi atribuită în mod direct sau indirect teroriștilor este dificil de determinat. Cu toate acestea, există legături între grupurile teroriste și infractori, care permit rețelelor teroriste să se extindă la nivel internațional, prin valorificarea resurselor informatice, activități de spălare a banilor sau prin rutele de tranzit operate de infractori[25].

Unii experți estimează că atacuri cibernetice avansate sau structurate, împotriva mai multor sisteme și rețele, inclusiv supravegherea țintelor și testarea unor noi instrumente sofisticate de *pătrunderi neautorizate*, ar putea necesita o perioadă de pregătire de la doi la patru ani, în timp ce un atac cibernetic complex coordonat, care să provoace perturbări în masă împotriva sistemelor integrate, eterogene poate necesita șase la zece ani de pregătire[26].

***Circumstanțe de analiză privind terorismul cibernetic*.** Distincțiile dintre infracțiune, terorism și război tind să se estompeze atunci când se încearcă să se descrie un atac asupra unei rețele de calculatoare (ARC), în moduri comparative din alte domenii ale vieții sociale. De exemplu, în cazul în care un stat ar sponsoriza în secret actori nestatali care inițiază un ARC pentru a sprijini activitățile teroriste sau pentru a crea perturbări economice, distincția dintre infracționalitatea informatică și războiul cibernetic devine mai puțin clară, deoarece este dificil de spus de unde provine un atac cibernetic, având în vedere că un atacator poate direcționa suspiciune către o terță parte, inocentă.

Proporția din infracționalitatea informatică ce poate fi atribuită în mod direct sau indirect teroriștilor este dificil de determinat. Cu toate acestea, există legături între grupurile teroriste și infractori, care permit rețelelor teroriste să se extindă la nivel internațional, prin valorificarea resurselor informatice, activități de spălare a banilor sau prin rutele de tranzit operate de infractori.

[21] Olivier Kempf, *„NATO and Cyberdefense"*, în *NDC Research Paper*, article nr. III.6, mai 2013, p. 3, disponibil la https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf, accesat la 7 ianuarie 2020.

[22] Dorothy Denning, *„Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy",* în *Nautilus Institute,* conference on *„The Internet and International Systems"*, p. 3, disponibil la https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf , accesat la 6 ianuarie 2020.

[23] Sarah Gordon, *„Cyberterrorism?"*, în *Symantec white paper*, iulie 2002, p. 4, disponibil la https://www.symantec. com/avcenter/reference/cyberterrorism.pdf , accesat la 7 ianuarie 2020.

[24] Edward V. Linden, *„Focus on terrorism"*, în *Nova Science Publishers, Inc*, vol. 9, p. 6, disponibil la https://books.google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+200,+p.6&source=bl&ots=dRkvffLk4i&sig=ACfU3U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4 sKHSzXB8wQ6AEw AH oECAoQAQ#v =onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism%E2%80%9D%2C%20Computerworld%2C%20August%2011%2C%202003%2C%20p.6&f=false, accesat la 7 ianuarie 2020.

[25] Rollie Lal, *„Terrorists and organized crime join forces"*, în *The New York Times*, 24 mai 2005, p. 1, disponibil la https://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html, accesat la 7 ianuarie 2020.

[26] Clay Wilson, *„Computer Attack and Cyberterrorism"*, în *Naval History and Heritage Command*, p. 17, disponibil la https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html, accesat la 7 ianuarie 2020.

De asemenea, interacțiunile dintre teroriști și infractorii care folosesc TIC pot estompa, uneori, distincția dintre infracționalitatea informatică și terorismul cibernetic.

Totodată, pot fi cazuri în care persoane fizice furnizează expertiză în calculatoare unui infractor sau terorist și pot să nu conștientizeze intențiile persoanei care a solicitat sprijinul. În acest context, rămâne, în continuare, dificilă identificarea surselor responsabile pentru cele mai multe atacuri perturbatoare, dar din ce în ce mai sofisticate, care compromit internetul. Având în vedere dificultatea de a determina autorul intruziunii sau al atacurilor cibernetice, unii autori susțin că, spre deosebire de răspunderea specifică actelor infracționale tradiționale, accentul ar trebui să fie pus mai degrabă pe faptă decât pe făptuitor, iar pragul pentru declanșarea de acțiuni defensive sau ofensive ar trebui să fie coborât. Internetul a fost folosit ca principal instrument de recrutare pentru insurgenți în Irak[27]. Insurgenții au creat multe site-uri în limba arabă, care au avut responsabilitatea de a conține planuri codificate pentru noi atacuri. Unele dintre acestea oferă sfaturi cu privire la modul de a construi și a întrebuința arme și cum să se treacă prin punctele de control la frontieră[28]. Alte articole de știri relatează despre o generație mai tânără de teroriști și extremiști, cum au fost cei din spatele atentatelor cu bombă din iulie 2005, din Londra, care au învățat noi abilități tehnice pentru a-i ajuta să evite detectarea, potrivit prevederilor legii aplicate TIC[29].

Pot fi cazuri în care persoane fizice furnizează expertiză în calculatoare unui infractor sau terorist și pot să nu conștientizeze intențiile persoanei care a solicitat sprijinul. În acest context, rămâne, în continuare, dificilă identificarea surselor responsabile pentru cele mai multe atacuri perturbatoare, dar din ce în ce mai sofisticate, care compromit internetul.

Când este considerat atacul cibernetic terorism cibernetic? Unii analiști sunt de părere că sintagma de *„terorism cibernetic”* este inadecvată, deoarece un atac cibernetic la scară largă poate produce, pur și simplu, dezordine, suferință, nu teroare, așa cum ar produce o bombă sau o altă armă chimică, biologică, radiologică sau nucleară. Cu toate acestea, alți analiști cred că efectele unui atac la scară largă asupra rețelelor de calculatoare ar fi imprevizibile și ar putea produce suficientă perturbare economică, frică și decese în rândul civililor, pentru a se califica drept un act de terorism[30]. Așadar, se pot evidenția cel puțin două puncte de vedere pentru a defini termenul de terorism cibernetic, și anume:

1. *bazat pe efecte*: terorismul cibernetic există atunci când atacurile informatice duc la efecte care sunt suficient de perturbatoare pentru a genera o teamă comparabilă cu cea a unui act tradițional de terorism, chiar dacă sunt săvârșite de către infractori;
2. *bazat pe intenție*: terorismul cibernetic există atunci când atacurile informatice ilegale sau motivate politic sunt săvârșite pentru a intimida sau a constrânge un guvern sau anumite personalități pentru a promova un obiectiv politic sau pentru a provoca prejudicii sau pagube economice grave.

Eficiența legislației curente. Au instituțiile cu rol în domeniul securității autoritatea de care au nevoie pentru a lupta în mod eficient și a câștiga războiul în spațiul virtual? Anumiți analiști au susținut că, pentru a-și îndeplini misiunea de apărare, instituțiilor cu atribuții în domeniul apărării ar trebui să li se acorde o autoritate sporită asupra protecției infrastructurilor critice din sectorul privat. Cu toate acestea, proprietarii de afaceri, în special în sectorul IT, susțin că acest lucru ar reprezenta o *„militarizare a spațiului cibernetic”*, care ar crea neîncredere în rândul consumatorilor și al acționarilor și ar putea limita potențialul de inovare, ceea ce ar duce la scăderea profitului.

Se pot evidenția cel puțin două puncte de vedere pentru a defini termenul de terorism cibernetic, și anume: unul bazat pe efecte și unul bazat pe intenție.

Așa cum s-a evidențiat, comunitatea internațională trebuie să elimine doza de ambiguitate cu privire la ceea ce constituie un *„atac armat”* în spațiul cibernetic și care sunt pragurile pentru ca un atac cibernetic să fie considerat un act de război, un incident de importanță națională sau ambele. Fără o linie de delimitare clară și consecințe specifice conturate cu claritate, strategiile de descurajare pot fi incomplete. Pe de altă parte, o lipsă de limitări explicite și consecințe ar putea constitui o formă de ambiguitate strategică, ceea ce ar genera instituțiilor cu atribuții în domeniul apărării manevrabilitate operațională.

---

[27] Jonathan Curiel, *„Iraq's tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet”*, în *San Francisco Chronicle*, 10 iulie 2005, pp. 1-3, disponibil la https://www.sfgate.com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php, accesat la 7 ianuarie 2020.

[28] *Ibidem*, p. 1.

[29] Michael Evans și Daniel McGrory, *„Terrorists Trained in Western Methods Will Leave Few Clues”*, în *London Times*, 12 iulie 2005, pp. 1-3, disponibil la https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q, accesat la 7 ianuarie 2020.

[30] Serge Krasavin, *„What is Cyber-terrorism?”*, în *Computer Crime Research Center,* p. 1, disponibil la http://www. crime-research.org/analytics/Krasavin/, accesat la 7 ianuarie 2020.

CONCLUZII

Astăzi, în mod evident, spațiul cibernetic a devenit o altă dimensiune cu potențial atât de cooperare, cât și de conflict. Îngrijorarea în ceea ce privește potențialul de daune generat de terorismul cibernetic a crescut, deoarece un volum tot mai mare al activității economice se desfășoară on-line.

Majoritatea instituțiilor din domeniul apărării, ordinii publice și securității naționale sunt susținute parțial de servicii și produse de înaltă tehnologie civile, cel mai adesea sub formă de sisteme de comunicații și software de calculator. Un procent ridicat de mesaje militare *„curge”* prin canale de comunicare comerciale, iar această situație creează o vulnerabilitate pe timpul unui conflict sau al unei situații de criză. În conflictele viitoare, care implică războiul cibernetic între state, distincția dintre țintele militare și civile ale unui stat s-ar putea estompa și sistemele informatice civile pot fi văzute tot mai mult ca ținte viabile, vulnerabile la atac de către adversari. Tehnologia rețelelor și sistemelor informatice, de asemenea, a estompat granițele dintre războiul cibernetic, infracționalitatea informatică și terorismul cibernetic. Reprezentanți ai guvernelor și companiilor civile afirmă că, acum, infracționalitatea informatică și disponibilitatea pentru închirierea serviciilor aferente în vederea unui atac cibernetic, de către organizațiile infracționale, sunt o amenințare în creștere la adresa securității naționale a statelor, precum și pentru economia acestora.

Majoritatea instituțiilor din domeniul apărării, ordinii publice și securității naționale sunt susținute parțial de servicii și produse de înaltă tehnologie civile, cel mai adesea sub formă de sisteme de comunicații și software de calculator.

Instrumente noi și sofisticate de infracționalitate informatică ar putea opera pentru a permite unui actor statal sau grup terorist să rămână neidentificat în timp ce conduce atacuri informatice prin intermediul internetului. Putem concluziona că incidente de terorism convențional din trecut au fost deja asociate cu infracționalitatea informatică și că vulnerabilitățile calculatoarelor pot face sistemele de infrastructură critice guvernamentale și civile să pară atractive ca ținte pentru un atac cibernetic. Sunt indici care sugerează posibile legături între infractori cibernetici și grupurile teroriste care doresc să prejudicieze economia unui stat sau interesele de securitate națională ale acestuia.

Este clar faptul că grupările teroriste folosesc calculatoare și internetul pentru obiective suplimentare, asociate cu propagarea terorismului. Acest lucru poate fi văzut în modul în care extremiștii

creează și utilizează numeroase site-uri pe internet pentru activități de recrutare și de strângere de fonduri, precum și în scopuri de instruire a Jihadului. Mai mulți infractori care au fost recent condamnați pentru infracțiuni cibernetice au folosit abilitățile lor tehnice pentru a obține informații de pe cardurile de credit furate, în scopul de a finanța alte activități teroriste convenționale.

Statele întâmpină dificultăți legate de stabilirea strategiei pentru selectarea și aplicarea unui răspuns adecvat militar sau juridic, după un astfel de atac cibernetic.

Etichetarea unui *„atac cibernetic”* ca *„infracționalitate informatică”* sau *„terorism cibernetic”* este problematică din cauza dificultății în stabilirea cu certitudine a identității, intenției sau motivațiilor politice ale atacatorului.

Sugestiile pentru creșterea motivației privind securitatea spațiului cibernetic pot include solicitarea ca toate programele achiziționate pentru agențiile naționale să fie certificate în cadrul unui program de testare, cu anumite criterii comune, și să reprezinte o cerință obligatorie pentru achiziționarea de software, cu toate că analiștii din domeniu subliniază faptul că procesul de certificare software este de lungă durată și poate interfera cu inovația și competitivitatea pe piața de software la nivel mondial.

Statele întâmpină dificultăți legate de stabilirea strategiei pentru selectarea și aplicarea unui răspuns adecvat militar sau juridic, după un astfel de atac cibernetic.

În final, am putea sugera ca agențiile care operează sistemele naționale de securitate să achiziționeze produse software dintr-o listă de produse evaluate și testate în laborator, într-un program derulat de instituțiile cu atribuții în domeniul securității.

BIBLIOGRAFIE:

1. ***, *„Convention on Cybercrime”*, în *Council of Europe, European Treaty,* disponibil la https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680 081561.
2. ***, FBI, *„Terrorism”*, în *What We Investigate*, disponibil la https://www.fbi.gov/investigate/terrorism
3. ***, *„International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”*, în *U.S Departament of State*, disponibil la https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ international_ strategy_for_cyberspace.pdf.
4. ***, *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice*, în *Monitorul Oficial*, partea I nr. 21 din 09 ianuarie 2019.

5. *** *„National Strategy for Counterterrorism of The United States of America”*, în *The White House*, disponibil la https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.
6. ***, *„Significant Cyber Incidents Since 2006”*, în *Center for Strategic & International Studies*, disponibil la https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa.
7. ***, *„Tallinn Manual on the International Law Applicable to Cyber Warfare”*, în *The NATO Cooperative Cyber Defence Centre of Excellence*, disponibil la http://csef.ru/media/articles/3990/ 3990.pdf.
8. ***, United Nations Secretary General, *„Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”*, *United Nations General Assembly*, disponibil la https://www.un.org/ga/search/ view_ doc.asp?symbol=A/65/201.
9. Barry C. Collin, *„Cyberterrorism”*, în *Institute for Security and Intelligence*, *11th Annual International Symposium on Criminal Justice Issues*, disponibil la https://www.nato.int/structur/library/bibref/cyberterrorism.pdf.
10. Jonathan Curiel, *„Iraq’s tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet”*, în *San Francisco Chronicle*, disponibil la https://www.sfgate.com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php.
11. Dorothy Denning, *„Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy”*, în *Nautilus Institute,* conference on *„The Internet and International Systems”,* disponibil la https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf .
12. Michael Evans și Daniel Mcgrory, *„Terrorists Trained in Western Methods Will Leave Few Clues”*, în *London Times*, disponibil la https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q.
13. Jack Goldsmith, *„Cybersecurity Treaties: A Skeptical View”*, în *Future Challenges in National Security and Law”,* disponibil la http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.
14. Sarah Gordon, *„Cyberterrorism?”*, în *Symantec white paper*, disponibil la https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.
15. Oona A. Hathaway, *„The Law of Cyber-Attack”,* în *California Law Review,* disponibil la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.
16. Jarrett H. Marshall, *„Prosecuting Computer Crimes”*, în *Office of Legal Education Executive Office for United States Attorneys,* disponibil la

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ccmanual. pdf .
17. Olivier Kempf, *„NATO and Cyberdefense”*, în *NDC Research Paper*, disponibil la https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf.
18. Harold Hongju Koh, *„International Law in Cyberspace”*, în *U.S. Department of State*, *Archived content*, disponibil la https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
19. Serge Krasavin, *„What is Cyber-terrorism?”*, în *Computer Crime Research Center,* disponibil la http://www.crime-research.org/analytics/Krasavin/.
20. Rollie Lal, *„Terrorists and organized crime join forces”*, în *The New York Times*, disponibil la https://www.nytimes. com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html.
21. Edward V. Linden, *„Focus on terrorism”*, în *Nova Science Publishers, Inc*, disponibil la https://books.google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+2003, +p.6&source=bl&ots=dRkvffLk4i&sig=ACfU3U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4sKHSzXB8wQ6AEwAHoECAoQAQ#v=onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism%E2%80%9D%2C%20Computerworld%2C%20August%2011%2C%20 2003%2C%20p.6&f=false.
22. Barak Obama, *„Remarks by the President in Year-End Press Conference”*, în *The White House Office of the Press Secretary*, disponibil la https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.
23. Chris Strohm, *„FBI Provides More Proof of North Korea Link to Sony Hack”*, în *Bloomberg*, disponibil la https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony.
24. Clay Wilson, *„Computer Attack and Cyberterrorism”*, în *Naval History and Heritage Command*, disponibil la https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html.
25. Katharina Ziolkowski, *„Ius ad bellum in Cyberspace – Some Thoughts on the ‹Schmitt-Criteria› for Use of Force”*, în *Legal & Policy Branch NATO CCD COE*, disponibil la https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

SECURITATEA INFORMAȚIILOR ȘI A SISTEMELOR INFORMAȚIONALE MILITARE

Colonel (rtr.) prof. univ. dr. Gheorghe BOARU
Membru titular al Academiei de Ştiinţe ale Securităţii Naţionale, Membru titular al Academiei Oamenilor de Știință din România

Colonel dr. Iulian Marius IORGA
Ministerul Apărării Naționale

În abordarea domeniului securității informațiilor și a sistemelor informaționale militare s-a plecat de la realitatea faptului că România este membră a NATO și că, în acțiunile militare comune, utilizează sisteme informaționale care trebuie să fie compatibile și interoperabile, dar și protejate.

Din punct de vedere informaţional, în acţiunile militare se duce o luptă pentru informaţie, prin intermediul informaţiei și împotriva informaţiei și, de aceea, securitatea acesteia este o activitate specială, îndeosebi privind informaţiile clasificate.

Țările membre ale Alianţei, implicit România, trebuie să asigure, individual sau prin acorduri de cooperare bilaterale, resursele informaţionale protejate, atât ca proces, cât și ca sistem, necesare pentru îndeplinirea obiectivelor operaţiilor întrunite sub comandă NATO.

Foarte multe dintre ameninţările informaţionale vin prin intermediul spaţiului virtual. În acest sens, se consideră că securizarea spaţiului virtual a devenit una dintre provocările de securitate cele mai presante ale secolului al XXI-lea.

Cuvinte-cheie: informaţie, sistem informaţional, vulnerabilităţi, ameninţări, securitate cibernetică.

INTRODUCERE

Pentru îndeplinirea misiunilor de răspuns la noile provocări ale mediului de securitate, Armata României a fost angajată într-un amplu proces de transformare, care a fost stabilit în *Strategia de transformare a Armatei României*[1].

În acest sens, până în 2025, procesul de transformare a fost planificat a se desfașura parcurgând urmatoarele trei faze[2]:

- cea a **restructurării de bază** (2005-2007);
- cea a **integrării operaționale în NATO și în UE** (2008-2015);
- cea a **integrării tehnice depline în NATO și în UE** (2016-2025).

Cea de-a treia fază va asigura îndeplinirea obiectivelor de transformare pe termen lung: eforturile și resursele financiare și umane vor fi concentrate pentru asigurarea capabilităților asumate și incluse în țintele de capabilități și participarea la NATO și UE – conducerea misiunilor și operațiilor; continuarea activității de îmbunatățire și înzestrare cu echipamente noi și atingerea nivelului de interoperabilitate cu forțele armate ale altor națiuni ale UE și ale NATO etc.

În acest context, obiectivul de bază al procesului de transformare îl constituie ajustarea structurii Forțelor Armate Române la mediul de securitate prezent și viitor, pentru a putea îndeplini angajamentele naționale față de Alianță, în concordanță cu procesele și fenomenele din planul de transformare al NATO. Scopul este de a face Forțele Armate Române capabile să participe la întregul spectru de misiuni desfășurate de Alianță și UE.

Obiectivul de bază al procesului de transformare îl constituie ajustarea structurii Forțelor Armate Române la mediul de securitate prezent și viitor, pentru a putea îndeplini angajamentele naționale față de Alianță, în concordanță cu procesele și fenomenele din planul de transformare al NATO.

Considerăm că acesta este contextul legal în care Armata României poate desfăşura acţiuni militare, acțiuni în care procesele de comandă și control au la bază procesele informaționale specifice.

[1] *Strategia de transformare a Armatei României*, București, 2007.
[2] Vezi https://fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/, accesat la 20 februarie 2020.

INFORMAȚIA MILITARA ȘI SECURITATEA ACESTEIA

Este cunoscut faptul că o asigurare informaţională temeinică poate determina un proces de comandă și de control eficient.

În armata noastră, *sprijinul cu informaţii al operaţiilor* este bine reglementat, constituind o *„formă de bază a asigurării acţiunilor și a protecţiei forţelor și reprezintă ansamblul de măsuri și de acțiuni, desfășurate continuu și într-o concepție unitară, de către toate forțele participante și la toate eșaloanele pentru planificarea, obținerea, verificarea, procesarea și valorificarea datelor și a informațiilor referitoare la factorii de situație”*[3].

În armata noastră, sprijinul cu informaţii al operaţiilor este bine reglementat, constituind o „formă de bază a asigurării acţiunilor și a protecţiei forţelor și reprezintă ansamblul de măsuri și de acţiuni, desfăşurate continuu şi într-o concepţie unitară, de către toate forţele participante şi la toate eşaloanele pentru planificarea, obţinerea, verificarea, procesarea şi valorificarea datelor şi a informaţiilor referitoare la factorii de situaţie”.

În literatura de specialitate, informația este abordată atât ca *„o armă puternică, precum și ca o țintă preferată”*[4] sau se afirmă că *„informația poate fi cea mai de temut armă în cadrul evoluțiilor tehnologice din spațiul de luptă”*[5].

Dacă aceste informații sunt corelate cu alte informații deja cunoscute și dacă sunt analizate în corelație cu experiențe trecute (colaționare și procesare), ele vor da naștere la un nou set de semnificații cu o altă valoare informativă, un proces denumit *„intelligence”.*

Studiind relația dintre date, informații și intelligence, putem concluziona că informațiile procesate sunt transformate în produse de intelligence, care se obțin în urma unui proces structurat, denumit, în doctrinele NATO sau în cele ale unor state aliate, *ciclu de intelligence.*

Apreciem că, în cazul operațiilor întrunite multinaționale desfășurate de NATO, *„intelligence”* nu înseamnă *„informații”,* ci reprezintă un proces complex, prin care se determină intențiile și cursul cel mai probabil de acțiune al inamicului.

În cadrul sistemelor și proceselor de bază implicate în planificarea operației întrunite multinaționale – *intelligence* poate avea atributul de[6]: funcțiune de luptă; capabilitate de luptă; ciclu; proces și sistem.

[3] I.P.S.- 3.1, *Manualul privind procedurile de informaţii militare pentru sprijinul operaţiilor*, Statul Major General, București, 2006, p. 14.
[4] *Corner stones of Information Warfare,* Department of the Air Force, Washington D.C., 1995, p. 2.
[5] Peter Grier, *„Information Warfare”*, în *Air Force Magazine*, nr. 3, martie 1995, p. 23.
[6] Colonel (r.) prof. univ. dr. Gheorghe Boaru, colonel drd. Iulian-Marius Iorga, *Ciclul informațional ca proces, procesul și ciclul „intelligence” – în cadrul acțiunilor militare moderne,* în *Revista de Științe Militare*, editată de Academia Oamenilor de Știință din România, nr. 1, 2017, pp. 84-85.

În analiza procesului de intelligence, am luat ca sistem de referință *Doctrina NATO pentru intelligence*[7], pentru că la aceasta au fost raportate aspectele de intelligence analizate din activitatea unor forțe NATO, a unor forțe armate ale unor state aliate, precum și a doctrinelor de intelligence ale acestora[8].

Pentru realizarea cerințelor de intelligence, sunt necesare structuri de intelligence adaptate noilor realități ale mediului operațional, bazate pe o pregătire care să le permită abordarea cu succes a provocărilor legate de aplicarea noilor concepte aliate: *„hybrid operations”, ,,comprehensive approach”, „information sharing”, „need to know vs. need to share”.*

Pentru realizarea cerinţelor de intelligence, sunt necesare structuri de intelligence adaptate noilor realităţi ale mediului operaţional, bazate pe o pregătire care să le permită abordarea cu succes a provocărilor legate de aplicarea noilor concepte aliate: „hybrid operations”, ,,comprehensive approach”, „information sharing”, „need to know vs. need to share”.

Conform opiniei unor specialiști militari români[9], în armatele statelor membre ale NATO, pentru integrarea activităților de informații/ intelligence sub o denumire unică, este standardizat conceptul ISTAR (**I**ntelligence, **S**upraveghere, **A**chiziția **Ț**intelor și **R**ecunoaștere). Aceiași autori precizează, totodată, că se mai folosesc diferite variante ale acronimului ISTAR, cum ar fi: STAR, RSTA, STA, ISR, numai pentru evidențierea unor activități informaționale parțiale.

În Armata României, conform *Doctrinei pentru Informații, Contrainformații și Securitate a Armatei*, conceptul ISTAR[10] a fost acceptat și integrat, în normele specifice naționale, ca o *„soluție de natură organizatorică, menită să integreze funcțional totalitatea capabilităților de colectare disponibile, definite normativ, în condițiile utilizării unui ansamblu de acțiuni, de procedee, de măsuri și de resurse (tehnice, umane, financiare etc.)”*[11]. Acest concept a fost proiectat normativ pentru a asigura *legătura dintre culegerea, procesarea și diseminarea datelor și informațiilor în vederea sprijinirii comandantului pentru atingerea obiectivelor operaționale din spectrul de conflict*[12].

[7] AJP-2*, Doctrina Aliată pentru informații, contrainformații și securitate,* 2003.
[8] Doctrina pentru sprijinul cu informații al operațiilor întrunite (a Forțelor Armate ale României, n.a.), 2003; Doctrina pentru intelligence în operațiile întrunite (a Forțelor Armate ale Canadei, n.a.), 2003; JDP 2-00, Înțelegerea și sprijinul de intelligence în operațiile întrunite (a Forțelor Armate ale Marii Britanii, n.a.), 2011; JP-2, Intelligence în operațiile întrunite (a Forțelor Armate ale Statelor Unite ale Americii, n.a.), 2007.
[9] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale militare – servicii și tehnologie*, Editura Universității Naționale de Apărare *„Carol I”*, București, 2010, pp. 24-25.
[10] *Ibidem.*
[11] *Doctrina pentru Informaţii, Contrainformaţii şi Securitate a Armatei*, Bucureşti, 2005, p. 34.
[12] *Ibidem*, p. 35.

Faptul că există o astfel de capabilitate normativă și de execuție în domeniul informațiilor militare, la nivelul Armatei României, demonstrează faptul că esența concepției de integrare a eforturilor de sprijin informativ este aceea de utilizare, într-un mediu integrat, a tuturor posibilităților oferite pentru acest domeniu, permițând, astfel, integrarea mediului procedural românesc cu cel al altor state membre ale NATO.

În acest context normativ informațional, securitatea informațiilor și a sistemelor informaționale militare este obligatorie, deci necesită cunoaștere și preocupare pentru acest domeniu, precum și stabilirea celor mai eficiente măsuri.

Armatele moderne acordă problematicii securității informației o atenție deosebită, considerând-o ca pe un obiectiv primordial pentru câștigarea bătăliei informaționale, al cărei fundament este reprezentat de introducerea, pe scară extinsă, a tehnologiei informației și a mijloacelor moderne de comunicații și informatică, pe întregul spațiu de luptă.

Din aceste motive, considerăm că este justificată preocuparea ofițerilor de stat major de a cunoaște și de a aborda problematica securității informației, în contextul apartenenței României la NATO și în perspectiva adaptării și transformării unor abordări doctrinare și acționale românești, conform cerințelor Alianței.

Armatele moderne acordă acestei problematici o atenție deosebită, considerând-o ca pe un obiectiv primordial pentru câștigarea bătăliei informaționale, al cărei fundament este reprezentat de introducerea, pe scară extinsă, a tehnologiei informației și a mijloacelor moderne de comunicații și informatică, pe întregul spațiu de luptă.

Apreciem că deosebit de importante sunt și aspectele legate de informațiile clasificate, cele care necesită protecția împotriva dezvăluirii neautorizate și care poartă identificatori specifici în acest sens, precum și informațiile neclasificate care nu sunt destinate publicului și care sunt protejate prin măsuri interne specifice fiecărei organizații, dar și informațiile de interes public, respectiv acele informații care privesc sau rezultă din activitățile unei autorități publice sau instituții publice.

De asemenea, în regulamentele și în manualele militare ale NATO şi ale armatelor aliate sunt prezentate măsurile pentru protecţia informaţiilor împotriva pericolelor și ameninţărilor specifice erei informaţionale.

În concordanţă cu *Legea nr. 182/2002*, a fost elaborată și *Hotărârea de Guvern nr. 585/2002* privind Standardele naţionale de protecţie a informaţiilor clasificate. Totodată, au fost stabilite nivelurile de echivalență a informaţiilor clasificate din România cu cele din NATO și/sau UE, aşa după cu se prezintă în *tabelul nr. 1*.

Tabelul nr. 1

Echivalența nivelurilor de clasificare ROMÂNIA – NATO – UE[13]

Informații clasificate – România		**Informații clasificate – NATO**	**Informații clasificate – UE**
Secret de stat	Strict secret de importanță deosebită/ SSID	NATO TOP SECRET/ NTS	TRÈS SECRET UE/TSUE
	Strict secret/SS	NATO SECRET/NS	SECRET UE/SUE
	Secret/S	NATO CONFIDENTIAL/ NC	CONFIDENTIEL UE/ CUE
Secret de serviciu/SSv		NATO RESTRICTED/NR	RESTREINT UE/RUE

Asigurarea securității informaţiilor NATO[14] se realizează conform *Legii nr. 423/2004*, iar prin *Hotărârea de Guvern nr. 353/2002* sunt stabilite Normele privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România.

În acest context, am considerat că securitatea informaţiei este un domeniu de activitate a cărui importanţă este în continuă creştere şi care trebuie abordat din toate unghiurile posibile, începând de la concepte, vulnerabilităţi, riscuri și management.

SECURITATEA SISTEMELOR INFORMAȚIONALE MILITARE

Organizaţiile militare utilizează sisteme informaţionale care, cu cât sunt mai complexe, cu atât au nevoie de o cantitate mai mare de informaţie pentru funcţionarea lor. De aceea, componenta informaţională a oricărui sistem este în continuă creştere şi diversificare, iar lipsa de informaţii determină însăşi dispariţia acestuia.

Rezultă așadar că sistemele informaţionale trebuie să fie proiectate și realizate, astfel încât să fie eficiente, iar securitatea acestora să fie asigurată în orice situație. Doar în acest fel se pot asigura siguranța, veridicitatea și oportunitatea informațiilor necesare procesului de comandă și de control, ca element fundamental al acţiunilor militare.

Organizaţiile militare utilizează sisteme informaţionale care, cu cât sunt mai complexe, cu atât au nevoie de o cantitate mai mare de informaţie pentru funcţionarea lor. De aceea, componenta informaţională a oricărui sistem este în continuă creştere şi diversificare, iar lipsa de informaţii determină însăşi dispariţia acestuia.

[13] Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne*, Editura Universității Naționale de Apărare *„Carol I”*, București, 2018, p. 93.

[14] *Legea nr. 423/2004 privind Aderarea României la Acordul dintre părțile la Tratatul Atlanticului de Nord pentru securitatea informațiilor*, adoptată la Bruxelles, la 6 martie 1997.

Ca element specific domeniului militar, importanţa sistemelor informaţionale creşte continuu, ele realizând simbioza cu procesele de comandă și de control, funcţionând integrat şi dând o calitate superioară conducerii acţiunilor organizate şi/sau desfăşurate.

Activităţile de comandă și de control, specifice domeniului militar, dar, în mod special, desfăşurarea efectivă a acţiunilor militare, capacitatea entităţii militare de a efectua cu succes o misiune sunt influenţate de nevoile de date şi de informaţii, precum şi de capabilităţile de obţinere a avantajului informaţional, determinat de capacităţile informaţionale la dispoziţie și de securitatea sistemului informaţional-decizional.

Ca element specific domeniului militar, importanţa sistemelor informaţionale creşte continuu, ele realizând simbioza cu procesele de comandă și de control, funcţionând integrat şi dând o calitate superioară conducerii acţiunilor organizate şi/sau desfăşurate.

Conceptul de sistem informațional a fost studiat de specialiști din diferite domenii de activitate, atât din punctul de vedere al structurii, cât și al funcționării acestuia, însă nu s-a ajuns la o definiție unică.

Structura sistemului informațional este dependentă de destinația acestuia, de complexitatea și de distribuirea spațială a elementelor structurii de comandă și de control deservite, precum și de obiectivele și de procesele acesteia.

Au fost studiate diferite categorii de sisteme informaționale, cum ar fi cele de securitate și de apărare națională, tehnice, sociale, economice etc., între care există deosebiri importante și care au elemente de structură comune, dar și elemente specifice, care constituie diferența.

Putem considera că structura constituie componenta organizatorică ce definește concepția sistemică și permite configurarea unui sistem informațional din module (subsisteme). Acest lucru se poate face prin identificarea, gruparea, dispunerea și interconectarea optimă a elementelor de infrastructură și de management, ținând cont și de resursele tehnice, de bazele de date, de componentele software și, neapărat, de elementele de securitate.

O temeinică asigurare informațională a structurilor organizatorice, la care comanda și controlul și activitățile operaționale (de execuție) sunt bine conturate, poate constitui o premisă favorabilă pentru succesul misiunii.

În organizația militară, structura sistemului informațional este determinată și depinde esențial de structura sistemului de comandă și de control. Între cele două structuri, există o interdependență reciprocă, biunivocă.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Studiind și analizând mai multe **definiții ale sistemului informațional**[15], prezentate în lucrări de specialitate militare și/sau civile, românești și/sau străine, am constatat că toate au la bază elemente de structură, tehnice, funcționale și de management specific domeniului abordat.

Prezentăm cinci dintre cele mai semnificative definiții menționate în literatura de specialitate, la care am făcut referire mai înainte, în care sistemul informațional:

1. *„este un sistem de persoane, de înregistrări de date și activități privind prelucrarea datelor și a informațiilor în cadrul unei organizații, incluzând procese de prelucrare manuală sau automată a acestora. Tehnologia informației constituie o componentă principală a sistemului informațional”*[16];

2. *„reprezintă ansamblul integrat de componente pentru colectarea, memorarea, prelucrarea și comunicarea informației. Elementele sale principale sunt: calculatoarele (hardware), produsele software, bazele de date, sistemele de comunicații, resursele umane și procedurile”*[17];

3. *„reprezintă un ansamblu de echipamente, de metode și de proceduri și, dacă este necesar, personal, organizat pentru îndeplinirea funcțiilor de prelucrare a informațiilor”*[18];

4. *„cuprinde întreaga infrastructură, circuite și fluxuri informaționale, organizate într-o concepție unitară, personalul, toate componentele care culeg, transmit, stochează, prelucrează, elaborează/procesează informații și asigură afișarea și diseminarea acestora, în vederea valorificării în procesul de conducere (comandă și control) și în desfășurarea acțiunilor militare”*[19];

5. *„cuprinde întreaga infrastructură, organizare, personal și componente destinate culegerii, prelucrării, memorării, transmiterii, afișării, diseminării și acționării asupra informațiilor”*[20].

Sistemul informațional „cuprinde întreaga infrastructură, organizare, personal şi componente destinate culegerii, prelucrării, memorării, transmiterii, afişării, diseminării şi acţionării asupra informaţiilor”.

[15] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare *„Carol I”*, București, 2018.

[16] *Information Systems*, Wikipedia, the free encyclopedia, http:/en.wikipedia.org/wiki/Information Systems, accesat la 12 ianuarie 2020.

[17] *Britannica Encyclopaedia*, http://www.britannica.com/EBchecked/topic/287895/Information Systems, accesat la 12 ianuarie 2020.

[18] AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008, p. 2-I-4.

[19] FM 101-5-1, *Termeni și simboluri operaționale*, Statul Major al Trupelor de Uscat, SUA.

[20] U.S. Army Field Manual 100-6, *Information Operations*, 1996; JP-02, DoD Dictionary Military Terms, 2008, p. 261.

Raportându-se la **sistemul informațional managerial** *(MIS – Management Information System)*, centrat pe obiective manageriale, o abordare interesantă o au și următoarele două definiții:

1. *„sistemul informațional managerial (MIS) este constituit din ansamblul datelor, informațiilor, fluxurilor și circuitelor informaționale, procedurilor și mijloacelor de tratare a informațiilor, menite să contribuie la stabilirea și realizarea obiectivelor organizației”*[21].

2. MIS este definit ca o *„combinație de resurse umane și informatice care urmăresc colectarea, stocarea, organizarea, apelarea, comunicarea, distribuirea și utilizarea datelor și a informațiilor pe care le folosesc managerii în exercitarea funcțiilor de conducere, în scopul realizării unui management eficient. Aceste sisteme oferă acces direct, online la informațiile relevante memorate, interfață prietenoasă, într-un dialog ușor de exploatat”*[22].

Sistemul informațional managerial este definit ca o „combinație de resurse umane și informatice care urmăresc colectarea, stocarea, organizarea, apelarea, comunicarea, distribuirea şi utilizarea datelor și a informațiilor pe care le folosesc managerii în exercitarea funcţiilor de conducere, în scopul realizării unui management eficient”.

Din analiza acestor definiții, rezultă că sunt evidențiate atât componente esențiale, cât și anumite caracteristici ale sistemului informațional, fiecare dintre acestea necesitând însă, în opinia noastră, anumite adăugări, precizări și actualizări.

Trei specialiști în domeniu, din Universitatea Națională de Apărare *„Carol I”*, ținând seamă de realizările actuale în domeniu și sintetizând opiniile diferiților specialiști, au formulat următoarea definiție generală: *„sistemul informațional reprezintă ansamblul integrat al datelor, al informațiilor și al cunoștințelor necesare organizației, gestionate cu precădere în format electronic, împreună cu infrastructura informațională...”*[23].

În accepțiunea acelorași autori, spre deosebire de alte opinii, în infrastructura informațională sunt incluși, pe lângă *tehnologia informației și a comunicațiilor*, *specialiștii în domeniu*, precum și *structura de management a informațiilor.*

[21] Ovidiu Nicolescu şi alţii, *Sistemul informaţional managerial al organizaţiei*, Editura Economică, București, 2001, p. 25.

[22] Club IT&C, *Cum să exploatezi informaţia în mod intelligent. Management Information Systems*, Club IT&C, Cum să exploatezi informaţia în mod inteligent-Management Information Systems, [https://www.google.ro/Club+IT%26C, +Cum+s%C4%83+exploatezi+informa%C5%A3ia +%C3%AEn+mod+inteligent-Management+Information+ Systems&tbm...], accesat la 1 februarie 2020.

[23] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale – fundamente teoretice*, Editura Universităţii Naţionale de Apărare *„Carol I”*, Bucureşti, 2009, pp. 194-195.

În aceeași abordare, se are în vedere ca sistemul informațional să asigure datele și informațiile necesare procesului de comandă și de control, în scopul realizării optime a obiectivului sau a misiunii stabilite și obținerii de *avantaje competitive*[24]. *Avantajul competitiv* constituie o sinteză a masei critice a avantajelor relative din domeniile: informațional, cunoștințelor, înțelegerii și luării deciziilor (comandă și control), incluzând, de asemenea, calitățile morale și de conducere.

Concret, *sistemul informaţional militar*[25] este un sistem mare, dinamic, complex, compus din mai multe sisteme (care, ierarhic, sunt subsisteme) interdependente, care trebuie singularizate, cu grad ridicat de automatizare şi autoreglare, conduse centralizat. Este, de fapt, un supersistem (federaţie de sisteme), care cuprinde un ansamblu omogen de reţele interconectate, împreună cu elementele lor integrate pentru management, având intrările, structura internă și ieşirile necesare, fiind caracterizat printr-un grad mare de autonomie şi eterogenitate.

Sistemul informaţional militar este un sistem mare, dinamic, complex, compus din mai multe sisteme interdependente, care trebuie singularizate, cu grad ridicat de automatizare şi autoreglare, conduse centralizat.

Sistemele C4ISR/C5ISR-D presupun furnizarea de informaţii şi cunoştinţe factorilor de decizie politico-militari pentru a asigura o conştientizare situaţională superioară. Având în vedere că operaţiile militare se vor desfăşura cu o mai mare precizie decât oricând, eficacitatea unei misiuni va depinde tot mai mult de sistemele C4ISR/C5ISR-D, care sunt reţele complexe de subsisteme.

Sistemul informaţional militar reprezintă latura dinamică a sistemului de comandă și de control (management) din care face parte, care asigură luarea optimă a deciziei, funcţionarea și coeziunea acestuia, din care cauză, în unele lucrări de specialitate, este denumit sistem informaţional-decizional sau, în literatura occidentală, *sistem informaţional managerial*[26].

„Sistemul informaţional-decizional reprezintă un sistem cibernetic, organizat piramidal, în fluxuri reciproce, verticale şi orizontale, pe baza unui mecanism unitar de culegere și prelucrare a informaţiilor, de la cel mai mic nivel ierarhic până la cel mai mare, care permite fundamentarea,

[24] D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington DC, CCRP-Data publication, august 2001, p. 41.

[25] W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, EdituraTehnică, Bucureşti, 1970, p. 227.

[26] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *op. cit.,* p. 195.

adoptarea şi urmărirea îndeplinirii deciziilor. Prin acest sistem se asigură implementarea pachetului de decizii şi urmărirea efectelor aplicării acestuia pentru îndeplinirea obiectivelor organizaţiei”[27].

Sistemul informaţional nu conţine numai elemente tehnice, ci este constituit ca un ansamblu complex de oameni specializaţi, precum şi activităţi practice, echipamente tehnice de culegere a informaţiilor (inclusiv prin senzori), comunicaţii, memorare, prelucrare și afișare a informaţiilor, software, baze de date şi proceduri, orientate către identificarea necesităţilor de informaţii şi a modalităţilor de satisfacere a lor, pentru asigurarea informaţională a proceselor de conducere (comandă şi control), inclusiv transmiterea deciziilor către nivelurile operaţionale (eşaloanele) subordonate.

În sistemul informațional intră informațiile de stare provenind de la organele de execuție, surse diferite de informații, sisteme de senzori, elemente cu care se cooperează sau colaborează și ies informațiile de comandă produse de organele de comandă.

Într-o altă abordare, *„Sistemul informaţional este liantul dintre sistemul de comandă și de control şi sistemul operaţional (de execuţie), care contribuie la simbioza (apropierea) acestora, întărirea disciplinei și creşterea răspunderii asupra activităţilor desfăşurate. El nu trebuie considerat doar o interfaţă între aceste sisteme, ci și un element de legătură între mediul informaţional intern al organizaţiei (structurii militare) și cel extern acesteia prin care se obţine cvasitotalitatea datelor şi a informaţiilor necesare”*[28].

În sistemul informațional intră informațiile de stare (rapoarte, informări, propuneri, sinteze, înștiințări...) provenind de la organele de execuție, surse diferite de informații, sisteme de senzori, elemente cu care se cooperează sau colaborează și ies informațiile de comandă (ordine, dispoziții, comenzi, precizări, indicații, orientări...) produse de organele de comandă.

Privind rolul sistemului informaţional, analizat în strânsă corelaţie cu locul acestuia în cadrul organizaţiei (structurii militare), putem aprecia că acesta constă în:

- determinarea volumelor de date, de informaţii şi de cunoştinţe necesare, astfel încât procesele decizionale și de execuţie ale structurii militare să aibă o desfăşurare optimă;
- să permită stabilirea surselor care pot procura informaţiile;

[27] Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informaţională şi protecţia informaţiilor*, Editura Detectiv, Bucureşti, 2006, p. 71.

[28] Vasile Dumitru şi alţii, *Sisteme informaţionale militare*, Editura CERES, Bucureşti, 2000, p. 38.

- să se stabilească mijloacele tehnice, care să asigure circulația fluxurilor informaționale și a mijloacelor informatice pentru prelucrarea informațiilor;
- stabilirea resurselor informaţionale (date, informaţii), a circuitelor şi a fluxurilor informaţionale care trebuie asigurate. *Resursele informaţionale* sunt constituite din informaţii împreună cu personalul, echipamentele tehnice și tehnologia informaţiei;
- asigurarea funcţiilor informaţionale specifice (activităţile de culegere, de transmitere, de memorare, de prelucrare și de diseminare a informaţiilor în mod operativ), necesare pentru comanda, controlul (managementul) și execuţia activităţilor;
- asigurarea parametrilor calitativi necesari informaţiei (obiectivitate, oportunitate, precizie, integritate, relevanţă, autenticitate) pentru sistemele de comandă şi de control ale organizaţiei (structurii militare);
- aplicarea eficientă a politicilor de securitate, care vizează atât informațiile, cât și procesele informaţionale.

Funcţionarea sigură şi neîntreruptă a sistemelor informaţionale, care depinde, în totalitate, de măsurile organizatorice, tehnice și funcţionale adoptate, constituie o necesitate pentru oricare organizaţie (structură militară). Afectarea, chiar şi parţială, a lucrului elementelor de structură şi a echipamentelor acestora (hardware, software) aduce prejudicii informaţionale grave, prin întreruperea sau prin întârzierea proceselor de comandă și de control (management) şi a celor operaţionale (de execuţie).

Funcționarea sigură și neîntreruptă a sistemelor informaționale, care depinde, în totalitate, de măsurile organizatorice, tehnice și funcționale adoptate, constituie o necesitate pentru oricare organizație (structură militară).

Afectarea, chiar și parțială, a lucrului elementelor de structură și a echipamentelor acestora (hardware, software) aduce prejudicii informaționale grave, prin întreruperea sau prin întârzierea proceselor de comandă și de control (management) și a celor operaționale (de execuție).

Utilizarea tehnologiei informaţiei și a comunicaţiilor a creat posibilitatea realizării unor sisteme informaţionale moderne, în care reţelele informatice și comunicaţiile au un rol hotărâtor, dar care prezintă şi vulnerabilităţi semnificative. Totodată, acestea sunt supuse și ameninţărilor informaţionale, din cauza acţiunii unor factori interni, dar, mai ales, externi, care urmăresc limitarea sau întreruperea activităţilor de culegere, de transmitere, de prelucrare și de diseminare a informaţiilor, pentru funcţionarea anormală sau chiar blocarea funcţiilor sistemului.

Foarte multe dintre aceste ameninţări vin prin intermediul spaţiului virtual. În acest sens, se consideră că *„Securizarea spaţiului virtual a devenit una dintre provocările de securitate cele mai presante*

ale secolului al XXI-lea, prin importanța sa pentru viața de zi cu zi, pentru guvern, securitate națională, afaceri și deopotrivă pentru cetățeni. Lumea cibernetică și tehnologiile asociate au creat, pe de o parte, mai multe oportunități sociale, culturale, economice și politice pentru toți, iar pe de altă parte, natura sa fără frontiere a adus cu ea amenințări sub formă de atacuri cibernetice și criminalitate informatică"[29].

Conexiunea la internet reprezintă o facilitate, dar creează, de cele mai multe ori, mari probleme de securitate pentru aceste rețele, prin formarea unor breşe, care pot fi accesate în mod neautorizat.

Întrebările esențiale referitoare la securitatea rețelelor informaționale: *„Cine? Când? De unde? Ce? De ce?"* determină împreună o nouă sintagmă, *„a celor cinci W" (5W – Who, When, Where, What, Why?)*. Cine accesează rețeaua? Când și unde se produce accesul? Ce informații sunt accesate și de ce? Aceste aspecte trebuie monitorizate și securizate, în funcție de importanța informațiilor, de caracterul public sau privat al rețelelor de comunicații și informatice, indiferent de terminalul folosit.

Conexiunea la internet reprezintă o facilitate, dar creează, de cele mai multe ori, mari probleme de securitate pentru aceste reţele, prin formarea unor breşe, care pot fi accesate în mod neautorizat. Scopul serviciilor de securitate în domeniul reţelelor de comunicaţii şi informatice vizează, pe de o parte, menţinerea acestora în funcţiune, iar pe de altă parte, asigurarea securităţii aplicaţiilor, precum și a informaţiilor stocate pe suport sau transmise prin reţea.

Scopul serviciilor de securitate în domeniul reţelelor de comunicaţii şi informatice vizează, pe de o parte, menţinerea acestora în funcţiune, iar pe de altă parte, asigurarea securităţii aplicaţiilor, precum și a informaţiilor stocate pe suport sau transmise prin reţea.

Securitatea acestor rețele este asigurată, în primul rând, prin reglementări de nivelul strategiilor și doctrinelor, precum și prin dezvoltarea unei culturi de securitate la nivel național și european.

Considerăm că aceste strategii trebuie să fie aplicate atât la nivel european, cât și la nivel național. Astfel, se apreciază că *„Îmbunătățirea modului în care UE asigură securitate cibernetică este esențială pentru a putea continua asigurarea beneficiilor sociale, economice, financiare și culturale pe care cetățenii și afacerile care provin din internet le obțin și, în sens mai larg, evoluția tehnologiilor pentru comunicaţii şi informaţii. Mai mult decât atât, este esențial pentru UE de a atinge o biectivele pe care le-a stabilit în Agenda digitală pentru Europa (2010) și, la fel de semnificativă, forța motrice a unei astfel de agende – Strategia Europa 2020"*[30].

[29] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Război și apărare în spațiul virtual,* în *Revista de Științe Militare*, Academia Oamenilor de Știință din România, nr. 2, 2018, p. 51.

[30] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* în *Revista Academiei de Științe ale Securității Naționale*, nr. 2, 2017, p. 71.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

În deplin acord cu acțiunile europene, la nivel naţional a fost aprobată, în februarie 2015, *Strategia Națională privind Agenda Digitală pentru România 2020*[31].

Această strategie *„definește patru domenii de acțiune, dintre care amintesc doar primul domeniu, care este: e-Guvernare, Interoperabilitate, Securitate Cibernetică, Cloud Computing și Social Media. Acest document a preluat și adaptat la specificul țării noastre elementele Agendei Digitale pentru Europa. Agenda Digitală definește, astfel, rolul major pe care utilizarea TIC trebuie să-l joace în realizarea obiectivelor Europa 2020"*[32].

Sistemele informaționale militare, de tipul C4I (C4I^2,C4ISR, C5ISR,...), un concept de actualitate în teoria și în practica militară europeană și euroatlantică, integrează subsistemele de comandă, pe cele informatice, de comunicații și de informații și se bazează pe doctrine și pe proceduri specifice, pe structuri flexibile, pe echipamente de ultimă generație și, în principal, pe un personal înalt profesionalizat.

Sistemele informaționale militare, de tipul C4I (C4I^2,C4ISR, C5ISR), un concept de actualitate în teoria și în practica militară europeană și euroatlantică, integrează subsistemele de comandă, pe cele informatice, de comunicaţii şi de informaţii şi se bazează pe doctrine şi pe proceduri specifice, pe structuri flexibile, pe echipamente de ultimă generaţie şi, în principal, pe un personal înalt profesionalizat.

În principiu, orice stat sau organizaţie neguvernamentală cu intenţii ostile poate dispune de resursele financiare şi de capacitatea tehnologică de a ameninţa un sistem C4I. Din cauza costului redus al echipamentelor necesare diverselor forme ale atacului informaţional, comparativ cu fondurile necesare realizării unui sistem de tipul C4I, precum și ca urmare a faptului că majoritatea cunoştinţelor solicitate sunt liber răspândite în lume, ameninţările pot surveni inclusiv din partea grupurilor teroriste sau a hackerilor.

Astfel de atacuri se pot desfășura în scopul dezinformării, spionajului electronic pentru obținerea avantajului competitiv global, modificării clandestine a datelor sensibile din cadrul teatrelor de operații sau pentru alterarea sau întreruperea funcționării unor infrastructuri critice naționale, cum ar fi cele de energie, apă, combustibil, comunicații, bancare sau transport, care sunt esențiale pentru funcționarea societății și economiei: *„În plan militar, acestea pot urmări sabotajul, subversiunea, spionajul sau terorismul și sunt concretizate în exploatarea/provocarea de scurgeri de informații,*

[31] *Strategia Națională privind Agenda Digitală pentru România 2020* a fost aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.

[32] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană*, *op. cit.*, p. 72.

Specificul amenințărilor la adresa securităţii cibernetice este dat și de faptul că ele nu sunt limitate de frontiere și înregistrează o creștere permanentă a frecvenţei și a gradului de sofisticare, dar și de apartenenţa universală a spaţiului cibernetic.

Riscurile de securitate pe care le implică atacurile cibernetice și caracterul global al efectelor lor impun eforturi comune de cooperare internaţională pentru asigurarea securităţii sistemelor informaţionale ale statelor membre ale Alianţei.

împiedicarea desfășurării misiunilor, provocarea unor anomalii în cursul de desfășurare al operațiilor”[33].

În România, cadrul general de cooperare care reunește acele autorități și instituții publice cu responsabilități și competențe în domeniul securității cibernetice este reprezentat de Sistemul Național de Securitate Cibernetică (SNSC). Activitatea SNSC este coordonată la nivel strategic de Consiliul Suprem de Apărare a Țării.

„Caracteristica comună a confruntărilor din spațiul cibernetic este raportul antagonic continuu stabilit între amenințările care se manifestă în spațiul cibernetic – terorism, spionaj, sabotaj, subversiune și crimă organizată, pe de o parte, și securitatea informațională, pe de altă parte. Aceste amenințări se manifestă într-un mediu foarte larg, oferit de războiul informațional, într-o accentuată interferență conceptuală și acțională între războiul electronic, cel al hackerilor, cel psihologic, economic și într-o tipologie complexă a atacurilor informatice”[34].

În concluzie, în actuala eră a informaţiei, securitatea tehnologică are o importanţă deosebită și priveşte, în egală măsură, reţelele de calculatoare *(COMPUSEC)* și reţelele de comunicaţii *(COMSEC)*.

Considerăm că specificul ameninţărilor la adresa securităţii cibernetice, care au devenit din ce în ce mai serioase în ultimii ani, este dat şi de faptul că ele nu sunt limitate de frontiere şi înregistrează o creştere permanentă a frecvenţei şi a gradului de sofisticare, dar şi de apartenenţa universală a spaţiului cibernetic. Riscurile de securitate pe care le implică atacurile cibernetice şi caracterul global al efectelor lor impun eforturi comune de cooperare internaţională pentru asigurarea securităţii sistemelor informaţionale ale statelor membre ale Alianţei.

❖ Vulnerabilităţi

Ca în orice domeniu de activitate, și în cel privind informațiile și sistemele informaționale există anumite *vulnerabilități*, adică *„părți slabe și slăbiciuni ale sistemului, infrastructurii, mediului de control sau proiectării rețelelor, care nu sunt generate de acțiunile adversarilor, ci de soluțiile proprii adoptate, ce pot fi atacate relativ ușor și exploatate, pentru a deteriora integritatea acelui sistem”*[35].

[33] *Idem, Război și apărare în spațiul virtual, op. cit.*, p. 54.
[34] *Ibidem,* pp. 54-55.
[35] *Noul dicționar universal al limbii române*, Editura Litera Internațional, București-Chișinău, 2006, p. 1645.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Din punct de vedere tehnic, vulnerabilitatea este prezentată ca o caracteristică a unui sistem, care îi poate provoca acestuia o degradare precisă (incapacitatea de a-și îndeplini funcțiile proiectate), ca rezultat al faptului de a fi fost obiect al unui nivel precis al efectelor, într-un mediu ostil nenatural.

În cadrul operațiilor informaționale, *vulnerabilitatea* este definită ca o slăbiciune în proiectarea sistemului de securitate a informațiilor, a procedurilor, a implementării sau a controlului intern, care poate fi exploatată pentru a obține accesul neautorizat la informații sau la sistemul informațional. În cadrul sistemelor de comunicații și informatice, vulnerabilitatea este reprezentată de un punct în care un sistem este susceptibil de a fi atacat. Orice sistem informatic sau cu un grad semnificativ de informatizare este vulnerabil la atac.

În cadrul sistemelor informaționale militare, se remarcă ponderea mult crescută a celor specifice computerelor și rețelelor de calculatoare. Această pondere se explică atât prin faptul că, în sistemele informaționale actuale, subsistemul de calculatoare are un rol sistemic integrator, cât și prin faptul că subsistemul de comunicații este, la rândul său, în punctele cele mai importante, informatizat.

În acelaşi timp, trebuie subliniat faptul că atât componentele hardware (staţii de lucru, cablaje de reţea etc.), cât şi cele software principale (sisteme de operare) utilizate sunt de origine civilă, fapt care atrage următoarele inconveniente, din punctul de vedere al securităţii:

- multe dintre acestea sunt la dispoziţia publicului larg, deci caracteristicile lor tehnice sunt cunoscute în detaliu de potenţialul adversar;
- componentele produse special pentru sistemul militar, care, deşi sunt proiectate și realizate în condiţiile de securitate stabilite și monitorizate de acesta, pot fi supuse totuşi acţiunilor spionajului industrial, fenomen caracteristic agresivităţii pieţei libere de înaltă tehnologie şi pieţei IT, în particular;
- componentele respective permit o personalizare redusă, deci rezultatele unui studiu de vulnerabilitate asupra sistemelor civile pot fi aplicate, în mare măsură, şi celor militare;
- există, în proporţie covârşitoare, componente de import sau, în cea mai bună situaţie, produse şi verificate în afara sferei militare, intenţionat şi foarte bine camuflat;

Din punct de vedere tehnic, vulnerabilitatea este prezentată ca o caracteristică a unui sistem, care îi poate provoca acestuia o degradare precisă (incapacitatea de a-şi îndeplini funcţiile proiectate), ca rezultat al faptului de a fi fost obiect al unui nivel precis al efectelor, într-un mediu ostil nenatural.

- sistemele militare se bazează pe o componentă logică – cea software –, care poate fi atacată tot cu mijloace logice, deci mijloace care nu necesită tehnologii scumpe, gama acestora diversificându-se continuu şi prin contribuţia infractorilor informaţionali.

Aşadar, se urmăreşte ca tehnologia modernă din sistemele informaţionale să fie combătută tot prin tehnologie avansată, confirmându-se concluzia specialiştilor că, şi în conflictele militare viitoare, cu cât mai mare va fi avantajul obţinut din tehnologia informaţiei și a comunicaţiilor, cu atât va creşte și vulnerabilitatea sa potenţială.

În ceea ce priveşte domeniul sistemelor de comunicaţii şi informatice, vulnerabilitatea este reprezentată de un punct în care un sistem este susceptibil de a fi atacat. Orice sistem informaţional, care are un grad semnificativ de informatizare, este vulnerabil la o diversitate de forme de atac.

Se poate trage concluzia că obiectivul principal al conflictelor militare contemporane nu trebuie să se concretizeze, cu precădere, în distrugerea totală a tehnicii, a armamentului sau a forţei vii a adversarului, ci, mai ales, în neutralizarea şi în dezintegrarea sistemelor complexe ale acestuia, în principal a sistemelor informaţionale.

În ceea ce priveşte domeniul sistemelor de comunicaţii şi informatice, vulnerabilitatea este reprezentată de un punct în care un sistem este susceptibil de a fi atacat. Orice sistem informaţional, care are un grad semnificativ de informatizare, este vulnerabil la o diversitate de forme de atac.

Pe lângă vulnerabilităţile specifice, externe, interne, nu sunt de neglijat nici cele de tip *„erori umane”.*

Politicile şi produsele de securitate pot reduce posibilităţile şi probabilitatea ca un atac să penetreze sistemul informatic sau, prin arhitectura de securitate adoptată, pot impune agresorului să investească atât de mult timp şi alte resurse, încât atacul să nu mai fie profitabil.

Specialiştii din întreaga lume sunt în unanimitate de acord că nu există sisteme complet securizate, deci vulnerabilităţile sunt prezente chiar și în cazul celor mai perfecţionate sisteme.

❖ Ameninţări

O *amenințare* este un posibil pericol pentru sistem. Pericolul poate fi reprezentat de o persoană (un cracker de sistem), un element material (o componentă de echipament tehnic imperfectă, de exemplu) sau de un eveniment (calamități naturale, incendii etc.), care pot exploata o vulnerabilitate a sistemului.

Ameninţările sunt analizate în relaţie cu evenimentele care pot surveni, ca urmare a activităţii acestora, evenimente denumite atacuri, precum și cu vulnerabilităţile care pot fi exploatate de acestea.

Literatura de specialitate clasifică sursele ameninţărilor după mai multe criterii, prezentate în rândurile care urmează.

După modul de manifestare, sursele ameninţărilor pot fi:

- manifeste sau deschise, la vedere, acestea fiind observabile;
- acoperite, mascate sau conspirate;
- accidentale și naturale.

Ameninţările acoperite sunt: spionajul, sabotajul, actele subversive, terorismul, actele care compun criminalitatea specifică.

Ameninţările acoperite sunt: spionajul, sabotajul, actele subversive, terorismul, actele care compun criminalitatea specifică.

Ameninţările la vedere sunt: bruiajul radio, radioreleu, de radiolocaţie sau de radionavigaţie; impulsul electromagnetic (EMP); activităţile SIGINT; operaţiile speciale.

Ameninţările accidentale și naturale sunt clasificate astfel:

- cele naturale: fulgere, inundaţii, cutremure, temperaturi extreme, vânt puternic;
- cele accidentale: erori umane, de software, precum și defecţiuni hardware;
- incendii, scurgeri de apă, tensiuni periculoase din reţeaua de alimentare.

După originea lor, sursele ameninţărilor pot fi: din interior, din exterior sau din mediu.

Ameninţările la vedere sunt: bruiajul radio, radioreleu, de radiolocaţie sau de radionavigaţie; impulsul electromagnetic (EMP); activităţile SIGINT; operaţiile speciale.

În cadrul agresiunilor informaţionale planificate, ameninţările posibile la adresa sistemelor informaţionale militare provin din toate cele trei tipuri de surse.

Atunci când un mesaj este transmis printr-un canal de comunicaţii, există o multitudine de ameninţări voluntare sau accidentale generale.

❖ Riscuri

Ca abordare generală în interiorul domeniului militar[36], *riscul* este definit ca probabilitatea și severitatea unei pierderi, legată de existența unor pericole. În mod distinct, riscul este privit ca o limită, un prag maxim pentru care o contramăsură, stabilită prin norme, a fost demonstrată ca fiind eficientă în eliminarea unei vulnerabilități, în corelație cu un nivel de susceptibilitate și de amenințare dat.

[36] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare, op. cit.*, pp. 39-40.

Riscul definește un indicator care reprezintă probabilitatea și ritmul de apariție a unui eveniment sau acțiune care, dacă se produce, cauzează deteriorarea informației în sine sau a suportului material ce susține informația.

Există o relație direct proporțională între vulnerabilitate și risc, în raport cu amenințările[37].

Având în vedere că nu putem influența în niciun fel amenințările, implicit nici probabilitatea de apariție, singura modalitate de reducere a riscurilor este pârghia de acțiune asupra vulnerabilității, respectiv a gradului de vulnerabilitate.

ATACURI ASUPRA REȚELELOR DE COMUNICAȚII ȘI INFORMATICE

Riscul definește un indicator care reprezintă probabilitatea și ritmul de apariție a unui eveniment sau acțiune care, dacă se produce, cauzează deteriorarea informației în sine sau a suportului material ce susține informația.

Atacurile asupra rețelelor de comunicații se pot grupa, în funcție de anumite criterii. După locul de unde se execută, atacurile pot fi:

- locale (local);
- de la distanță (remote).

Atacurile locale se materializează prin compromiterea securității unei rețele de către un utilizator local.

Riscul de a compromite securitatea unei rețele poate fi tratat (eliminat, diminuat, repartizat) în diferite moduri:

- acordarea de privilegii strict necesare utilizatorilor locali, pentru îndeplinirea atribuțiilor zilnice, conform sarcinilor înscrise în fișele posturilor;
- supravegherea rețelei, pentru a preîntâmpina posibile tentative de încălcare a normelor impuse a se respecta, inclusiv după terminarea orelor de program;
- restricționarea accesului la echipamentele de rețea importante;
- repartizarea echilibrată a sarcinilor complexe personalului din cadrul organizației militare.

Există însă și posibilitatea nefericită ca aceste măsuri de protecție să fie ineficiente, dacă sunt trădători din interiorul rețelei care contribuie la compromiterea măsurilor de securitate ale sistemului.

De aceea, în vederea acordării unor privilegii de utilizare a resurselor rețelei, utilizatorii trebuie ierarhizați pe mai multe niveluri

[37] Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acțiunile militare,* Editura AÎSM, București, 2003, pp. 17-25.

de încredere, în funcție de vechimea în rețea, de comportamentul acestora și de gravitatea unor evenimente de securitate în care au fost implicați.

Atacul la distanță (remote attack) reprezintă o acțiune inițiată asupra unei rețele de comunicații sau asupra unui echipament din rețea, atunci când agresorul nu dispune, inițial, de niciun control.

Atacul la distanță se poate realiza în trei etape:

Prima etapă este una de informare, în care atacatorul trebuie să descopere informații despre:

- administratorul rețelei;
- echipamentele din rețea și funcțiile acestora;
- sisteme de operare folosite;
- puncte de vulnerabilitate;
- topologia rețelei;
- politici de securitate etc.

Această **primă etapă** este asimilată unui atac, denumit **atac de recunoaștere**, și constă în maparea neautorizată a unui sistem informatic, a serviciilor și a vulnerabilităților lui.

A doua etapă este una de tatonare și constă în clonarea unei ținte și atacarea acesteia, pentru a se simula modalitatea de răspuns.

Etapa a treia constă în lansarea atacului asupra rețelei. Un atac de succes se execută rapid, atunci când rețeaua prezintă vulnerabilități.

Potrivit unei alte clasificări a atacurilor adresate rețelelor de comunicații/informatice, după modul în care se desfășoară acestea, ca destinație și sursă, atacurile pot fi **focalizate** pe o singură țintă (este atacat un anumit server de pe un singur echipament) sau pot fi **distribuite** (inițiate din mai multe locuri sau de către mai multe echipamente concomitent).

După modul de interacțiune a atacatorului cu informația accesată neautorizat, ca rezultat al acțiunii reușite, se disting două categorii de atacuri: **pasive** și **active**.

Atacurile pasive sunt acele atacuri în urma cărora atacatorul se limitează la supravegherea modului în care informația circulă prin sistem fără a interveni în acest flux. Tot în categoria atacurilor pasive intră și interceptarea (radio, radioreleu, fir/fibră optică) propriu-zisă și goniometrarea (radio, radioreleu).

Atacurile pasive sunt acele atacuri în urma cărora atacatorul se limitează la supravegherea modului în care informația circulă prin sistem fără a interveni în acest flux. Tot în categoria atacurilor pasive intră și interceptarea (radio, radioreleu, fir/fibră optică) propriu-zisă și goniometrarea (radio, radioreleu).

Atacurile pasive pot avea unele caracteristici comune, precum:

- nu creează prejudicii imediate şi care pot fi detectate, deoarece nu şterg şi nu modifică date, nu blochează reţeaua, nu perturbă traficul;
- încalcă regulile de confidenţialitate;
- obiectivul constă în a asculta datele schimbate pe canalele de comunicaţii;
- datele ascultate sunt supuse altor etape de prelucrare, în scopul extragerii informaţiilor utile pentru alte operaţiuni, inclusiv alte atacuri pasive;
- sunt greu, chiar imposibil, de sesizat.

Aceste atacuri se pot realiza prin diverse metode, cum ar fi: supravegherea convorbirilor telefonice, radio sau radioreleu, exploatarea radiațiilor electromagnetice emise, în scopul transmiterii informațiilor sau a radiațiilor parazite compromițătoare, routarea datelor, prin noduri secundare mai slab protejate.

Atacurile active reprezintă acele atacuri prin care atacatorul își materializează acțiunea în distrugerea, în furtul, în modificarea sau în reluarea mesajelor ori în inserarea de mesaje false.

Atacurile active au ca scop furtul sau falsificarea informațiilor transmise ori stocate în rețea, reducerea disponibilității rețelei, prin supraîncărcarea acesteia cu pachete (flooding), perturbarea sau blocarea comunicațiilor, prin atac fizic sau logic asupra echipamentelor din rețea și a căilor de comunicații. Aceste atacuri sunt mai periculoase, deoarece modifică starea sistemelor de calcul, de management și a celor de comutare, precum și a datelor. Există o serie de atacuri active, în cazul acestora impunându-se o nouă analiză, conform criteriului efectului produs de acestea, astfel:

a. Atacuri care afectează preponderent starea de organizare

- bruiajul electronic – constă în modificarea semnalelor de recepție;
- dezinformarea – se realizează prin interceptarea și prin modificarea conținutului mesajului, urmate de retransmiterea oportună a comunicării;
- mascarada – este un atac în care o țintă din rețea (utilizator, client, serviciu sau server) indică o altă identitate, pentru a prelua informații confidențiale (parole de acces, date

Atacurile active au ca scop furtul sau falsificarea informaţiilor transmise ori stocate în reţea, reducerea disponibilităţii reţelei, prin supraîncărcarea acesteia cu pachete (flooding), perturbarea sau blocarea comunicaţiilor, prin atac fizic sau logic asupra echipamentelor din reţea şi a căilor de comunicaţii. Aceste atacuri sunt mai periculoase, deoarece modifică starea sistemelor de calcul, de management şi a celor de comutare, precum şi a datelor.

de identificare, chei de criptare, informații despre cărți de credit și altele);

- reluarea – se produce atunci când un mesaj sau o componentă a acestuia este reluat (repetat), cu intenția de a produce un efect neautorizat;
- modificarea mesajelor – datele mesajului sunt supuse, în mod neautorizat, modificării, inserării sau ștergerii;
- refuzul serviciului *(DoS/Denial of service attack)* – se produce atunci când o entitate autorizată nu izbutește să îndeplinească propria funcție sau când o entitate intrusă desfășoară prin acțiuni, care împiedică o altă entitate în îndeplinirea altor funcții;
- repudierea serviciului – apare atunci când o entitate nu vrea să recunoască un serviciu executat.

b. Atacuri active cu efect preponderent distructiv – în sistemele dependente de componentele informatizate, astfel de atacuri se realizează prin intermediul unor programe create în acest scop, care afectează, uneori esențial, securitatea calculatoarelor, inclusiv a serverelor. Aceste atacuri urmăresc citirea neautorizată a informațiilor, dar, cel mai frecvent, distrugerea parțială sau totală a datelor sau chiar a echipamentelor de procesare. Dintre aceste programe distructive, le amintim pe următoarele:

- viruşii sunt reprezentaţi de programe informatice, care se multiplică singure în programele proprii sistemului atacat, utilizând spaţiul rezident din memorie/hard-disk şi blochează computerul sau, după un număr programat de multiplicări, poate produce chiar distrugeri;
- bomba software este o parte de cod sau procedură, inserată într-o aplicaţie necesară, care poate fi lansată de un eveniment programat. Creatorul bombei informează despre acest eveniment, lăsând-o să desfăşoare acţiunile distructive, programate prin efectul *„exploziei”*;
- viermii produc, de cele mai multe ori, efecte distructive, similare cu cele ale bombelor şi ale viruşilor. Diferenţa constă în faptul că viermii nu rezidă la o adresă fixă sau nu se multiplică singuri. În schimb, se mută permanent, ceea ce îi face foarte dificil de detectat;

Bomba software este o parte de cod sau procedură, inserată într-o aplicaţie necesară, care poate fi lansată de un eveniment programat. Creatorul bombei informează despre acest eveniment, lăsând-o să desfăşoare acţiunile distructive, programate prin efectul „exploziei”.

- Calul Troian este o aplicaţie care se prezintă sub forma unei funcţii de utilizare cunoscută şi care, în mod disimulat, îndeplineşte şi o altă funcţie.

Există o multitudine de posibilități de atacuri la adresa sistemelor informaționale, care pot exploata vulnerabilitățile acestora.

❖ **Vulnerabilităţi specifice sistemelor informaţionale**

Vulnerabilităţile informaţionale constituie o componentă a vulnerabilităţii de securitate a sistemelor, generată de stări de fapt sau de procese interne ale organizației, care pot duce la reducerea capabilităților de reacție la amenințările posibile, de orice natură, inclusiv informaţionale.

În general, vulnerabilităţile informaţionale sunt cu atât mai mari, cu cât reţelele informaţionale și structura informaţiilor sunt mai complexe, deci mai greu de administrat, fiind mai greu de organizat şi de protejat.

„Vulnerabilităţile sporesc direct proporţional cu nivelul tehnologic implementat în construcţia și în funcţionarea echipamentelor sistemelor informaţionale”.

De asemenea, se consideră că *„vulnerabilităţile sporesc direct proporţional cu nivelul tehnologic implementat în construcţia și în funcţionarea echipamentelor (mai ales digitale) sistemelor informaţionale”*[38].

Cele mai cunoscute vulnerabilităţi, în cazul sistemelor informaţionale militare, sunt:

- erori de proiectare și de funcționare a sistemului;
- posibilitatea defectării unor componente tehnice;
- dificultăți în testarea integrală și integrată a sistemului;
- cantitatea excesivă a informațiilor de analizat;
- dispersarea utilizatorilor și a punctelor de acces, pe o rază geografică întinsă;
- insuficienta pregătire a personalului în domeniul siguranței naționale;
- neexecutarea unei noi acreditări de securitate, după o modificare a sistemului;
- conectarea calculatoarelor din rețele locale neclasificate la alte rețele clasificate;
- adrese routere și firewall greșit configurate/introduse;

[38] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *op. cit.,* p. 294.

- nerespectarea normelor TEMPEST;
- depășirea termenelor de schimbare a parolelor și a cheilor de secretizare;
- nerestricționarea conexiunilor Dal-in în LAN și nerestricționarea serviciului de poștă electronică;
- folosirea unor canale nesecretizate, pentru transmiterea unor informații clasificate.

Referitor la analiza infrastructurii informaționale, se consideră că principalele vulnerabilități ar putea fi următoarele[39]:

- existenţa posibilităţilor de interceptare a informaţiilor din reţelele de comunicaţii şi de calculatoare atât din interior (de către utilizatori), cât şi din exterior (de către adversari);
- existenţa unui volum foarte mare de informaţii produse, vehiculate și prelucrate în sistemele informaţionale, care pot fi supuse cercetării şi atacului, distruse, falsificate sau sustrase de către adversarii potenţiali;
- îngreunarea managementului infrastructurii informaţionale, din cauza complexităţii acesteia, ceea ce determină imposibilitatea detectării accesului fraudulos la informaţii şi favorizarea atacurilor cibernetice;
- folosirea aceloraşi benzi de frecvenţe atât ale mijloacelor proprii, cât și ale potenţialilor adversari;
- standardizarea echipamentelor tehnice, a componentelor software și a bazelor de date utilizate;
- utilizarea unor elemente comune ale infrastructurii informaţionale naţionale, ceea ce creează condiţii pentru acces fraudulos şi dezinformare;
- posibilitatea ca firmele furnizoare de aparatură să încorporeze din timp, în echipamentele de calcul și de comunicaţii, unele module software maliţioase, care pot fi activate de către adversari, în anumite momente stabilite de aceştia, creând dezordine și haos în reţelele informaţionale și în cele decizionale;

Una dintre vulnerabilitățile infrastructurii informaționale o reprezintă existenţa unui volum foarte mare de informaţii produse, vehiculate și prelucrate în sistemele informaţionale, care pot fi supuse cercetării şi atacului, distruse, falsificate sau sustrase de către adversarii potenţiali.

[39] Constantin Alexandrescu, *Amenințări și riscuri electronice privind sistemele informaționale militare moderne în spațiul de luptă*, în volumul Sesiunea de comunicări științifice a U.N.Ap. *„Carol I” – „Sisteme Informaționale SI-2007”*, pp. 107-115.

- vulnerabilităţile la pătrunderi neautorizate (cu rea intenţie sau din neatenţie) din cauza faptului că organizaţiile sunt conectate la internet, intranet sau extranet;
- nerespectarea integrală a cerinţelor şi a standardelor UE și NATO privind compatibilitatea şi interoperabilitatea sistemelor informaţionale, mai ales în ceea ce priveşte schimbul de informaţii (formatul mesajelor), accesul la bazele de date, criptarea automată a comunicărilor și caracteristicile canalelor pentru legătură;
- posibilitatea folosirii de către adversarii potenţiali a războiului electronic împotriva mijloacelor radioelectronice din principalele sisteme informatice și de comunicaţii, cu precădere asupra canalelor care asigură legătura surselor de informaţii cu organele centrale de fuziune și de prelucrare a datelor;
- interceptarea de către adversar (forţele ostile) a comunicărilor transmise prin radio, decriptarea acestora în timp oportun, în cazul folosirii unor sisteme criptografice neperformante şi utilizarea, în scopuri proprii, a acestor informaţii, pentru obţinerea superiorităţii informaţionale;
- mijloacele tehnice actuale ale sistemelor informaţionale nu au asigurată protecţia temeinică împotriva atacului fizic, electromagnetic şi cibernetic, acestea putând fi distruse, deteriorate sau extrasă informaţia stocată;
- dispunerea în locuri necorespunzătoare, din punct de vedere funcţional şi al securităţii fizice și electromagnetice, a echipamentelor tehnice ale sistemelor informaţionale, în principal a mijloacelor de comunicaţii şi de calcul, ceea ce sporeşte vulnerabilitatea de interceptare a informaţiilor şi de atac fizic;
- utilizarea, pentru exploatarea sistemelor informaţionale, a unor persoane insuficient verificate şi neloiale, predispuse a fi racolate de către adversarii potenţiali și determinate să efectueze acţiuni de sabotaj sau să furnizeze acestora informaţii obţinute fraudulos;
- neutralizarea legăturii radio pe unde scurte, mai ales la distanţe mari, bazată pe propagarea undelor electromagnetice, prin ionosferă, prin schimbarea caracteristicilor electrice ale acesteia;

Dispunerea în locuri necorespunzătoare, din punct de vedere funcţional şi al securităţii fizice și electromagnetice, a echipamentelor tehnice ale sistemelor informaţionale, în principal a mijloacelor de comunicaţii şi de calcul, sporeşte vulnerabilitatea de interceptare a informaţiilor şi de atac fizic.

- existenţa, la adversarii potenţiali, a armelor electronice cu radiaţii infraacustice, bazate pe propagarea în spaţiu a undelor subsonice, care acţionează asupra personalului, cauzând greţuri grave, vomismente, buimăceală, teamă, depresii etc., determinând inactivarea acestuia, pe anumite perioade de timp şi, implicit, întreruperea funcţionării sistemelor informaţionale;
- instalarea antenelor mijloacelor de comunicaţii, în câmp deschis sau în spaţii fără proprietăţi naturale de protecţie, ceea ce permite scoaterea lor uşoară din funcţiune şi întreruperea legăturilor, mai ales a celor realizate cu staţii radio și/sau radioreleu de putere mare;
- suprimarea accesului la internet al sistemelor informaţionale, pentru izolarea acestora şi împiedicarea folosirii surselor de informaţii deschise ;
- utilizarea internetului pentru acţiuni teroriste, de dezinformare și pentru atac cibernetic asupra infrastructurii informaţionale;
- proiectarea necorespunzătoare a infrastructurii, cu redundanţă informaţională redusă, centralizată excesiv și cu posibilităţi scăzute de replicare a informaţiilor existente în bazele de date;
- preocuparea insuficientă pentru ascunderea şi pentru mascarea elementelor infrastructurii informaţionale, măsuri neadecvate de pază și de apărare a acestora;
- măsurile insuficient studiate de asigurare a securităţii comunicaţiilor (COMSEC – **Com**munications **sec**urity), a calculatoarelor (COMPUSEC – **Comput**er **sec**urity) şi a echipamentelor electronice în ansamblu prin interzicerea (restricţionarea) interceptării radiaţiilor parazite (protecţia TEMPEST – **T**ransient **E**lectro **M**agnetic **P**ulse **E**manation **St**andard).

Din analiza efectuată, rezultă că există numeroase vulnerabilităţi, dar, dintre acestea, esenţiale sunt cele care privesc: neorganizarea optimă a sistemelor informaţionale, alegerea necorespunzătoare a echipamentelor tehnice utilizate şi a produselor software comerciale, realizarea programelor (software) de aplicaţii şi a bazelor de date, precum și a softwarelor pentru criptarea automată a informaţiilor în sistemele informaţionale, dar și personalul neloial sau insuficient verificat.

Există numeroase vulnerabilităţi, dar esenţiale sunt cele care privesc: neorganizarea optimă a sistemelor informaţionale, alegerea necorespunzătoare a echipamentelor tehnice utilizate şi a produselor software comerciale, realizarea programelor de aplicaţii şi a bazelor de date, precum și a softwarelor, pentru criptarea automată a informaţiilor în sistemele informaţionale, dar și personalul neloial sau insuficient verificat.

CONCLUZII

În noul mediu informaţional global, dezvoltarea tehnologică a adus, odată cu avantajele și facilităţile pe care le oferă, și o serie de ameninţări, de riscuri şi de vulnerabilităţi la adresa securităţii informațiilor și a sistemelor informaţionale.

Preocupările de abordare a ameninţărilor, a vulnerabilităţilor şi a riscurilor, în dinamica specifică ultimelor decenii, cuprind o arie extinsă, eforturi importante fiind concentrate pe domeniul informaţional.

Având în vedere că atacurile informaţionale reprezintă o ameninţare la adresa securităţii sistemelor informaţionale, specialiştii încearcă să implementeze noi metode de luptă împotriva atacurilor informatice și informaţionale, care să vizeze, în principal, protejarea propriilor informaţii şi a sistemelor de informaţii.

Pentru ca o vulnerabilitate să fie exploatată, trebuie să fie cunoscută sau să poată fi descoperită de o ameninţare. Aceasta face importantă urmărirea aplicării principiului „need to know”, cu respectarea măsurilor legate de securitate şi a aplicării lor atât de către personal, cât şi în domeniul tehnologiei.

Plecând de la faptul că nu se poate face un control absolut, ci doar o limitare a acestora, experţii au declanşat o nouă ofensivă, pentru perfecţionarea legislaţiei, întărirea rolului agenţiilor de profil şi pentru perfecţionarea produselor necesare depistării delictelor informaţionale și a celor informatice.

Pentru ca o vulnerabilitate să fie exploatată, trebuie să fie cunoscută sau să poată fi descoperită de o ameninţare. Aceasta face importantă urmărirea aplicării principiului *„need to know”,* cu respectarea măsurilor legate de securitate şi a aplicării lor atât de către personal, cât şi în domeniul tehnologiei. De asemenea, pune accentul pe reacţia corespunzătoare a instituţiei la identificarea oricărei vulnerabilităţi care o poate afecta.

Apreciem că se pot face estimări, cu un anumit nivel de încredere, însă este dificil, din punct de vedere ştiinţific, să se realizeze analize cu exactitate privind ameninţările la adresa sistemelor informaţionale. Aceste estimări sunt dependente, în primul rând, de factorul uman, de gândirea sa, de subiectivismul și de incertitudinea pe care acestea le implică.

Asigurarea securităţii sistemelor informaţionale militare este o activitate complexă şi dificil de realizat, întrucât aceasta se face prin punerea în practică, pe teritoriul naţional, dar şi în afara acestuia, pe baza legislaţiei şi a reglementărilor internaţionale, de alianţă/coaliţie și naţionale, a unor măsuri specifice care, de regulă, sunt: generale, organizatorice, de protecţie fizică, de protecţie a personalului, de protecţie a documentelor, de protecţie juridică și procedurală,

de securitate industrială, precum și a unor măsuri particulare, de securitate a sistemelor informatice și de comunicaţii.

Securitatea sistemului de comunicaţii şi informatic, componentă a sistemului informaţional (C4I), vizează protecţia informaţiilor, componentelor hardware și software, prin măsuri eficiente, de natură să împiedice accesul la informaţii şi intervenţia în procesele informaţionale (colectare, transmitere, stocare, prelucrare, distribuţie, conversie, afişare).

În reţelele locale de calculatoare și în sistemul de comunicaţii, măsurile de securitate trebuie să asigure: autentificarea (verificarea identităţii unei entităţi de comunicare la distanţă); controlul accesului la resurse; confidenţialitatea datelor; integritatea datelor; protecţia fizică a echipamentelor tehnice.

În general, securitatea sistemelor informaţionale reprezintă un domeniu foarte complex, în care este implicat întregul personal şi care, prin restricţiile și algoritmii pe care le adoptă și le impune, generează de multe ori contradicţii şi birocraţii în exces. Cu toate neajunsurile şi inconvenientele pe care le poate genera, este de preferat să se respecte regulile decât să se pună în pericol îndeplinirea misiunii.

Dependenţa din ce în ce mai mare a activităţilor de comandă și control de securitatea sistemele informaţionale conduce la creşterea tipologiei vulnerabilităţilor cărora organizaţiile trebuie să le facă faţă.

Mai mult, problema protecţiei trebuie să aibă în vedere, de multe ori, interconectarea reţelelor private cu serviciile publice. Dacă, la acest aspect, mai adăugăm și problema partajării informaţiilor, se conturează un tablou destul de complicat, în care implementarea unor controale eficiente devine o sarcină dificilă pentru specialistul IT&C.

Considerăm că securitatea informaţiilor nu este doar o problemă tehnică, este, în primul rând, o problemă managerială.

Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizaţiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securităţii informaţiilor. Standardul poate fi folosit, în funcţie de gradul de expunere a fiecărei organizaţii în parte, pentru a conştientiza, la nivelul conducerii, aspectele legate de securitatea informaţiei sau pentru a crea o cultură organizaţională, în ceea ce priveşte securitatea informaţiilor, sau pentru a obţine certificarea sistemului de securitate.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizaţiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securităţii informaţiilor. Standardul poate fi folosit, în funcţie de gradul de expunere a fiecărei organizaţii în parte, pentru a conştientiza, la nivelul conducerii, aspectele legate de securitatea informaţiei sau pentru a crea o cultură organizaţională, în ceea ce priveşte securitatea informaţiilor, sau pentru a obţine certificarea sistemului de securitate.

Stabilirea cerinţelor de securitate, a măsurilor necesare pentru asigurarea nivelului de control dorit are o componentă deseori subiectivă, fiind dificil de cuantificat, în termeni monetari, pierderea suferită, în cazul unui incident de securitate.

Din studiul acestui domeniu foarte complex al securităţii informaţiilor și a sistemelor informaţionale militare, opinăm pentru câteva măsuri concrete:

- organizarea optimă a sistemelor informaţionale, astfel încât să se asigure condiţia fundamentală pentru funcţionarea eficientă a acestora – reconfigurarea, mobilitatea şi adaptabilitatea lor la mediul de informaţii în continuă dezvoltare;
- să se aibă permanent în vedere condiţiile, restricţiile și standardele care sunt stabilite, ca ţară membră a UE și a NATO. Acestea se impun a fi respectate în totalitate şi aplicate cu fermitate, pentru a se îndeplini criteriile de compatibilitate şi interoperabilitate cu alte organizaţii din ţară şi din exterior;
- informaţiile clasificate vor fi diseminate numai persoanelor care deţin un certificat de securitate corespunzător;
- respectarea reglementărilor NATO[40], prin care aplicarea standardelor minime de asigurare a securităţii informaţiilor este obligatorie pentru tot personalul care accesează sistemul informaţional;
- creşterea responsabilităţii şi a controlului pentru protecţi informaţiilor clasificate de către fiecare persoană care deţine, procesează sau are cunoştinţă de asemenea informaţii;
- executarea periodică a unor analize de risc asupra sistemelor informaţionale și prelucrarea acestora în faţa personalului militar, sub formă de lecţii învăţate;
- achiziţiile de noi tehnologii informaţionale să ţină cont de scopul micşorării vulnerabilităţilor specifice;
- pregătirea profesională a personalului să cuprindă și teme pe domeniul securităţii informaţiei și a sistemelor informaţionale.

Trebuie respectate reglementările NATO, prin care aplicarea standardelor minime de asigurare a securităţii informaţiilor este obligatorie pentru tot personalul care accesează sistemul informaţional.

În concluzie, în actuala eră a informaţiei, securitatea tehnologică are o importanţă deosebită și priveşte, în egală măsură, reţelele de calculatoare (*COMPUSEC*) și reţelele de comunicaţii (*COMSEC*).

[40] *AD 70-1, ACO Security Directive*, NATO HQ, Brussels, 2006, p. I-2-4.

Din păcate, nu există un sistem de securitate sigur 100%, dar, prin definirea unei politici de securitate realiste, trebuie găsite permanent cele mai eficiente căi de evitare a riscurilor la care este supusă reţeaua informaţională militară.

BIBLIOGRAFIE:

1. ***, AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008.
2. ***, AD 70-1, *ACO Security Directive*, NATO HQ, Brussels, 2006.
3. ***, AJP-3(C), *Allied Joint Doctrine for the conduct of Operations,* NATO, 2019.
4. ***, AJP-2*, Doctrina Aliată pentru informaţii, contrainformaţii şi securitate,* 2003.
5. ***, *Doctrina Armatei României*, București, 2012.
6. ***, *Doctrina pentru intelligence în operațiile întrunite (a Forțelor Armate ale Canadei)*, 2003.
7. ***, *Doctrina pentru Informații, Contrainformații și Securitate a Armatei*, București, 2005.
8. ***, *Doctrina pentru sprijinul cu informații al operațiilor întrunite*, 2003.
9. ***, FM 3-13, *Information Operations*, Washington D.C., December 2016.
10. ***, FM 101-6, *Information Operations*, 1996.
11. ***, *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*, Administrația Prezidențială, București, 2015.
12. ***, IPS-3, *Doctrina pentru informații, contrainformații și securitate a Armatei*, București, 2005.
13. ***, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 2016.
14. ***, JP-2, *Intelligence în operațiile întrunite* (a Forțelor Armate ale Statelor Unite ale Americii), 2007.
15. ***, *Legea nr. 182/2002 privind protecţia informaţiilor clasificate.*
16. ***, *Normele privind protecția informațiilor clasificate în Ministerul Apărării Naționale*, aprobate de *Ordinul Ministrului Apărării Naționale nr. M.9/2013,* publicat în *Monitorul Oficial al României*, Partea I, nr. 115, din 28 februarie 2013.
17. ***, *Strategia Națională privind Agenda Digitală pentru România 2020,* aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.
18. ***, *Strategia națională de apărare a României*: *„Pentru o Românie care garantează securitatea și prosperitatea generațiilor viitoare”*, București, 2010.
19. ***, *Strategia de securitate națională a României*: *„România Europeană, România Euroatlantică: pentru o viață mai bună într-o țară democratică, mai sigură și prosperă”*, București, 2007.

20. ***, *Strategia de Transformare a Armatei României*, București, 2007.
21. D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington D.C., CCRP-Data publication, august 2001.
22. Constantin Alexandrescu, *Amenințări și riscuri electronice privind sistemele informaționale militare moderne în spațiul de luptă*, în volumul Sesiunea de comunicări științifice a U.N.Ap. *„Carol I” – „Sisteme Informaționale SI-2007”.*
23. Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale – fundamente teoretice*, Editura Universității Naționale de Apărare *„Carol I”*, București, 2009.
24. Gelu Alexandrescu, Gheorghe Boaru, Constantin Alexandrescu, *Sisteme informaționale pentru management,* Editura Universității Naționale de Apărare *„Carol I”*, București, 2012.
25. Francisco Martínez Álvarez, Alicia Troncoso Lora, José António Sáez Muñoz, Héctor Quintián, Emilio Corchado, *Sinteza Informational Security International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on European Transnational Education (ICEUTE 2019): Seville, Spain, May 13th-15th, 2019 Proceedings,* Series: Advances in Intelligent Systems and Computing 951,Publisher: Springer International Publishing, Year: 2020.
26. Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, Editată de Academia Oamenilor de Știință din România, nr. 2, 2018.
27. Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, nr. 2, 2017.
28. Colonel (r.) prof. univ. dr. Gheorghe Boaru, colonel drd. Iulian-Marius Iorga, *Ciclul informațional ca proces, procesul și ciclul „intelligence” – în cadrul acțiunilor militare moderne,* Revista de Științe Militare, editată de Academia Oamenilor de Știință din România, nr. 1, 2017.
29. Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acțiunile militare*, Editura AÎSM, București, 2003.
30. Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informațională și protecția informațiilor*, Editura Detectiv, București, 2006.
31. Abhishek Chopra, Mukund Chaudhary, *Implementing An Information Security Management System: Security Management Based On ISO 27001 Guidelines,* Publisher: Apress, Year: 2020.
32. Vasile Dumitru și alții*, Sisteme informaționale militare*, Editura CERES, București, 2000.
33. James Dunningan, *O nouă amenințare mondială. Cyber-Terorismul*, Editura Curtea Veche, 2010.
34. Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne,* Editura Universității Naționale de Apărare *„Carol I”*, București, 2018.

35. W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, Editura Tehnică, București, 1970.
36. Ovidiu Nicolescu şi alţii, *Sistemul informaţional managerial al organizaţiei*, Editura Economică, București, 2001.
37. Ramjee Prasad, Vandana Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology,* Series: Springer Series In Wireless Technology, Publisher: Springer, Year: 2020.
38. *ENISA-Country Reports, 2008*, http://www.enisa.europa.eu.
39. *Information Systems*, Wikipedia, the free encyclopedia, http:/en.wikipedia.org/ wiki/Information Systems.
40. *Information Security*, http:/en.Wikipedia.org/wiki/informationsecurity, 2009.
41. https://*fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/*.
42. www.dodccrp.org.

UTILIZAREA MASS-MEDIEI CA INSTRUMENT AL RĂZBOIULUI HIBRID

Căpitan Marian-Valentin BÎNĂ
Doctorand, Universitatea Națională de Apărare „Carol I”, București

Maior Cristian DRAGOMIR
Doctorand, Universitatea Națională de Apărare „Carol I”, București

Obiectivul acestei lucrări este analizarea sistemului pe care mass-media l-a oferit campaniilor de dezinformare rusești într-un presupus context de război hibrid. Expunerea știrilor oferite de principalele canale mass-media permite concentrarea analizei pe conceptul de război hibrid și compararea acestuia cu concepția strategică tradițională, pentru a determina dacă activitățile în cauză pot fi clasificate în acest tip de conflicte.

Războiul informațional și componentele conexe, precum războiul cibernetic sau războiul electronic, devin din ce în ce mai complexe și pot fi folosite atât în mod defensiv, cât și în mod ofensiv în actualul context de securitate oferit de către mass-media.

Cuvinte-cheie: război hibrid, mass-media, propagandă, capacitate strategică, Federația Rusă.

INTRODUCERE

Încorporarea tehnologiilor informaționale și de comunicare a adus o schimbare totală a modului în care interacționăm și comunicăm, dar și în modul în care ne informăm. Extinderea a ceea ce numim astăzi *„internet”* a permis milioanelor de oameni din întreaga lume să aibă acces la cea mai mare sursă de informații din istoria omenirii, în principal prin intermediul smartphone-urilor, al computerelor personale și al tabletelor de ultimă generație.

Extinderea a ceea ce numim astăzi „internet” a permis milioanelor de oameni din întreaga lume să aibă acces la cea mai mare sursă de informații din istoria omenirii, în principal prin intermediul smartphone-urilor, al computerelor personale și al tabletelor de ultimă generație.

Unul dintre domeniile în care răspândirea internetului a avut cel mai mare impact a fost *comunicarea*, atât în structura mass-media, cât și în sfera audienței sale și în conținutul propriu-zis. Mass-media tradițională a fost nevoită să își adapteze organizația la noi formate și la o cerere continuă de informații din partea cititorilor, pe lângă faptul că trebuie să facă față apariției de noi suporturi, exclusiv digitale. Dar, această cerere informativă a generat, de asemenea, anumite îndoieli cu privire la credibilitatea și calitatea informațiilor, lucru cu adevărat îngrijorător dacă luăm în considerare importanța mass-mediei în societățile democratice. Viteza cu care acum se propagă *actualitatea* – fie prin intermediul site-urilor web, al mass-mediei sau al rețelelor sociale – are un impact aproape imediat asupra opiniei publice și, în multe cazuri, și efemer. Nevoia de a genera în mod continuu știri a însemnat că acestea au o volatilitate enormă, condiționând, în același timp, calitatea informațiilor.

În acest context, reclamațiile publice ale guvernelor occidentale cu privire la presupuse campanii de dezinformare dirijate de guvernul Federației Ruse au concentrat o mare parte din atenția mass-mediei internaționale. Concepte precum *atacuri cibernetice, știri false* și *amenințări hibride* au fost răspândite pentru a denunța explozia de știri false cu scopul destabilizării unor procese interne de genul Brexit (ianuarie 2020), cazul alegerilor prezidențiale din SUA (2016) sau criza politico-socială catalană din Spania, ce a avut apogeul

în octombrie 2017. Potrivit unor declarații pe aceste subiecte, încercările de a interveni s-ar baza pe utilizarea informațiilor înțelese ca un element militar, de natură asimetrică, într-un presupus context de război hibrid, îndreptat de Federația Rusă împotriva democrațiilor occidentale, prin așa-numita *„Doctrină Gerasimov”.*

METODOLOGIE

Scopul acestei analize este de a compara expunerea jurnalistică pe care mass-media a oferit-o campaniilor de dezinformare și problemelor hibride rusești. Conceptul de *hibrid*, dezvoltat în mod tradițional dintr-un domeniu strategic-militar, a influențat evenimentele menționate, în actualul context al războiului hibrid, după cum subliniază majoritatea mass-mediei și analiștii din acest domeniu.

Articolul pornește de la prezentarea unei serii de știri legate de campaniile de dezinformare de origine rusă și de la influența pe care a avut-o în acest context conceptul de *război hibrid*. Datorită cantității mari de știri publicate pe aceste teme, prin procedură sintetică, o selecție generală de știri din diferite mass-medii naționale și internaționale de prestigiu au oferit o varietate de perspective, precum *The Guardian, The Washington Post, BBC.* Urmând metoda descriptivă, sintagma de *război hibrid* este introdusă de la concepția sa tradițională, pornind de la originea conceptului, trecând prin unele definiții și caracteristici generale ale acestuia și contextualizându-l în ceea ce a devenit popular ca *doctrina Gerasimov*. În cele din urmă, prin metoda comparativă, expunerea jurnalistică a acestui tip de conflict este comparată cu concepția strategică tradițională.

În ultimii ani, luând ca referință temporară referendumul care a avut loc în Marea Britanie pentru a părăsi Uniunea Europeană și, mai ales, după alegerile prezidențiale din SUA, ce au avut loc în luna noiembrie 2016, mass-media a concentrat o mare parte din informațiile sale internaționale avertizând asupra pericolului pe care îl reprezintă știrile false – popularizate prin numele de fake news – pentru democrațiile occidentale.

CONTEXTUALIZAREA RĂZBOIULUI HIBRID

În ultimii ani, luând ca referință temporară referendumul care a avut loc în Marea Britanie pentru a părăsi Uniunea Europeană și, mai ales, după alegerile prezidențiale din SUA, ce au avut loc în luna noiembrie 2016, mass-media a concentrat o mare parte din informațiile sale internaționale avertizând asupra pericolului pe care îl reprezintă știrile false – popularizate prin numele de *fake news* – pentru democrațiile occidentale.

În obiectivul său de informare, mass-media a folosit tot felul de concepte, noi pentru o mare parte a publicului, cum ar fi *cyberspațiul, atacul cibernetic, războiul cibernetic* sau *războiul hibrid*, pentru a explica evenimentele petrecute prin ceea ce numim, în mod obișnuit, internetul, în care un stat, în cazul de față Federația Rusă, ar folosi sfera digitală pentru a interfera cu procesele interne ale altuia, în scopul destabilizării sistemelor sale democratice. În acest context inedit și complex, să vedem cum s-a raportat media la aceste evenimente.

Deși Brexitul este considerat, în prezent, un exemplu de imixtiune rusească în campania electorală[1], am găsit puține referințe în mass-media care, atât în timpul campaniei, cât și în perioada de după referendum, au acuzat guvernul lui Vladimir Putin că a dorit să influențeze votul referendumului și au definit aceste activități drept război hibrid. În cea mai mare parte, analizele post-electorale s-au concentrat pe incertitudinea generată de ieșirea Regatului Unit din Uniunea Europeană, pe consecințele economice, politice și sociale care ar putea urma, precum noul rol propriu al Uniunii Europene din acel moment.

În mare măsură, abia în alegerile prezidențiale ale SUA, din 2016, mass-media a menționat că Moscova ar fi efectuat atacuri informatice împotriva Partidului Democrat și campanii de dezinformare orchestrate pentru a influența votul opiniei publice. În acest moment, accentul a fost pus pe cyberspațiu și pe vulnerabilitățile pe care le reprezintă acesta pentru democrațiile occidentale. În ciuda acestui fapt, abia după câteva luni au început să apară informații despre posibila interferență a Kremlinului în referendumul britanic, prin răspândirea de știri false, precum și prin utilizarea rețelelor de socializare.

Aceste evenimente au marcat rolul pe care o putere străină l-ar fi jucat în încercarea de a influența un proces electoral intern. Acestea erau un semnal de avertizare pentru țările europene asupra faptului că, luni mai târziu, urmau să organizeze diferite procese electorale. În acest context, ziarul *The Guardian* a menționat, într-un titlu,

În obiectivul său de informare, mass-media a folosit tot felul de concepte, noi pentru o mare parte a publicului, cum ar fi cyberspațiul, atacul cibernetic, războiul cibernetic sau războiul hibrid, pentru a explica evenimentele petrecute prin ceea ce numim, în mod obișnuit, internetul, în care un stat, în cazul de față Federația Rusă, ar folosi sfera digitală pentru a interfera cu procesele interne ale altuia, în scopul destabilizării sistemelor sale democratice.

[1] The Cipher Brief, *The Use of Disinformation in the British Election*, https://www.thecipherbrief.com/column/soufan-center/the-use-of-disinformation-in-the-british-election, accesat la data de 20.02.2020.

că *„UE își sporește campania împotriva propagandei rusești”*[2] din cauza fricii care ar fi generat posibila influență rusă la alegerile din SUA, deoarece aceasta s-ar putea extinde spre Europa. Este accentuat aici faptul că Uniunea Europeană *„își va spori eforturile pentru a contracara campania de război hibrid a Rusiei după alegerea lui Donald Trump”*[3]. Știrile se referă la grupul de lucru East Stratcom, o organizație creată în 2015 de Serviciul European de Acțiune Externă al UE, și, prin urmare, înaintea proceselor prezentate aici, pentru a contracara campaniile de dezinformare rusești în timpul crizei din Ucraina.

Richard A. Clarke, fost coordonator național în domeniul securității, protecției infrastructurii și combaterii terorismului Statelor Unite și consilier special al președintelui în securitatea cibernetică, definește cyberwar-ul ca fiind acele „acțiuni întreprinse de un stat-națiune pentru a pătrunde în computere sau în alte rețele ale statelor cu scopul de a provoca pagube sau modificări”.

În acest context internațional de dezinformare, știri false, de influențe rusești în procesele electorale, de atacuri informatice și presupusul război hibrid, Spania a fost cufundată într-o criză politică și socială importantă din cauza convocării unui referendum de către guvernul regional al Cataluniei, la începutul lunii octombrie 2017. Intenția guvernului era de a decide, prin consultare, asupra posibilității independenței de statul spaniol, fără acordul guvernului Spaniei. Aceste activități au fost repede încorporate în limbajul informațional. Astfel, în titluri precum *„Cyberwar între guvernele catalane și spaniole pentru închiderea site-ului referendumului”*[4], publicat în ziarul *El País* cu câteva zile înainte de referendum, sau *„Marele cyberwar catalan din 2017”*[5], publicat de *The Washington Post*, la doar două săptămâni după ce a avut loc referendumul, a fost folosit conceptul de *cyberwar* într-un mod generic, indiferent de semnificația și implicațiile sale posibile, pentru simplul fapt că anumite activități au fost desfășurate prin intermediul rețelelor.

Conceptul de *cyberwar* a fost unul dintre cele mai utilizate din domeniul jurnalistic pentru a face referire la activitățile care se desfășoară pe internet, dar, la rândul său, a generat confuzii. Richard A. Clarke, fost coordonator național în domeniul securității, protecției

[2] Daniel Boffey, Jennifer Rankin, *EU escalates its campaign against Russian propaganda*, în *The Guardian*, 23 noiembrie 2017.

[3] Daniel Boffey, *UE strânge fonduri pentru combaterea războiului de dezinformare cu Rusia*, în *The Guardian*, 5 decembrie 2018.

[4] Jordi Pueyo, *Ciberguerra entre los gobiernos catalán y español por el cierre de la web del referéndum*, în *El País*, 14 septembrie 2017, https://elpais.com/ccaa/2017/09/14/catalunya/1505390726_024743.html, accesat la 14 iunie 2019.

[5] Christian Caryl, *The great Catalonian cyberwar of 2017*, în *The Washington Post*, 18 octombrie 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/10/18/the-great-catalonian-cyberwar-of-2017/, accesat la 4 august 2019.

infrastructurii și combaterii terorismului Statelor Unite și consilier special al președintelui în securitatea cibernetică, definește cyberwar-ul ca fiind acele *„acțiuni întreprinse de un stat-națiune pentru a pătrunde în computere sau în alte rețele ale statelor cu scopul de a provoca pagube sau modificări”*[6]. Cu excepția atacurilor cibernetice împotriva Partidului Democrat, pentru care au avut acces, în campanie, la datele și informațiile membrilor Partidului, activitățile de propagandă care au avut loc în Brexit și în conflictul catalan nu pot fi descrise drept cyberwar, potrivit definiției lui Clarke, întrucât nu ar fi dus la accesul nelegitim la sistemele sau rețelele altor state, cu scopul de a provoca pagube sau modificări, ci, mai degrabă, ar fi catalogate drept activități influente și manipulatoare prin intermediul rețelelor.

Această nouă doctrină, elaborată în Rusia, încearcă să slăbească democrațiile, amestecându-se în procesele lor electorale și alimentând conflictele lor interne, fie ideologice sau teritoriale, folosind instrumente precum știrile false sau manipularea rețelelor sociale. În schimb, se afirmă doar că ne aflăm într-un conflict (război hibrid) promovat de un actor de stat (Rusia), prin răspândirea de știri false prin intermediul internetului și al rețelelor sociale, cu scopul final de a slăbi guvernele democratice occidentale. De asemenea, știrile referitoare la aceste activități prezintă războiul hibrid ca pe ceva nou, care face parte din doctrina militară de origine rusă – *doctrina Gerasimov*.

ORIGINEA ȘI CARACTERISTICILE RĂZBOAIELOR HIBRIDE

Există autori care atribuie originea sintagmei de *război hibrid* generalului în rezervă Robert Walker (Marina americană), care, în 1998, a analizat într-o lucrare a sa modelul hibrid al războaielor[7]. Pe de altă parte, există autori care subliniază că originea ar trebui să fie plasată câțiva ani mai târziu, în 2002, atunci când sintagma a fost folosită pentru a explica acțiunile tactice ale primului război cecen, care a avut loc între anii 1994 și 1996. Cu toate acestea, conceptul

Există autori care atribuie originea sintagmei de „război hibrid” generalului în rezervă Robert Walker (Marina americană), care, în 1998, a analizat într-o lucrare a sa modelul hibrid al războaielor. Pe de altă parte, există autori care subliniază că originea ar trebui să fie plasată câțiva ani mai târziu, în 2002, atunci când sintagma a fost folosită pentru a explica acțiunile tactice ale primului război cecen, care a avut loc între anii 1994 și 1996.

[6] Richard A. Clarke, Robert K. Knake, *Cyber War: the next threat to national security and what to do about it,* EEUU: Harper Collins Publishers, 2010.

[7] Robert G. Walker, *Spec Fi: The United States Marine Corps and Special Operations Teză de master*, Naval Postgraduate School, 1998, https://apps.dtic.mil/dtic/tr/full-text/u2/a359694.pdf, accesat la 9 februarie 2020.

nu a fost folosit într-un mod oficial până la Strategia de Apărare Națională a SUA din 2005[8]. Abia odată cu publicarea, în 2005, a articolului *Future Warfare: The Rise of Hybrid Warfare*, de generalul James N. Mattis și colonelul Frank G. Hoffman, și a lucrării *Conflict in the 21st Century. Rise of Hybrid Wars*, scrisă de Frank G. Hoffman, conceptul a dobândit conținut teoretic și a devenit popular.

Conceptul a fost, apoi, extins într-o mare măsură pentru a se încerca înțelegerea războaielor contemporane între actorii statali și nonstatali, în care un actor, teoretic superior în domeniul tehnologiei, al capacității militare sau doctrinare, a fost surprins de către un actor nonstatal.

Războiul hibrid este „unul în care cel puțin unul dintre adversari recurge la o combinație de operații convenționale și război neregulat, amestecat cu acesta din urmă, cu acțiuni teroriste și conexiuni cu crima organizată”.

Definiții ale războiului hibrid

Una dintre definițiile războiului hibrid îl prezintă ca *„aflându-se în interstițiile dintre războiul special și războiul convențional”*[9]. La rândul său, F.G. Hoffman lărgește și specifică natura acestuia, considerând că *„amestecă letalitatea conflictului de stat cu fervoarea fanatică și răspândită a războiului neregulat”*[10]. Poate fi promovat atât de actori statali, cât și de cei nonstatali. Astfel de conflicte *„încorporează o varietate de moduri diferite de purtare a războiului, inclusiv capacități convenționale, tactici și formațiuni neregulate, activități teroriste, inclusiv violență și constrângere fără discriminare și tulburare criminală”*[11]. În practică, aceasta implică o combinație de activități convenționale și neregulate. Într-o linie similară, colonelul de infanterie al armatei spaniole, José Luis Calvo Albero, definește războiul hibrid drept *„unul în care cel puțin unul dintre adversari recurge la o combinație de operații convenționale și război neregulat, amestecat cu acesta din urmă, cu acțiuni teroriste și conexiuni cu crima organizată”*[12].

[8] Guillem Colom, *La amenaza híbrida: mitos, leyendas y realidades*, Instituto Español de Estudios Estratégicos, Documento de Trabajo, 2019, http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf, accesat la 19 ianuarie 2020.

[9] Robert G. Walker, *op. cit.*

[10] Frank G. Hoffman, *Conflict in the 21st Century. The Rise of Hybrid Wars*, Virginia: Potomac Institute for Policy Studies, 2007, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, accesat la 9 februarie 2020.

[11] *Ibidem.*

[12] José Miguel Palacios, *Rusia: guerra híbrida y conflictos asimétricos*, în *Revista Ejército*, nr. 904, iulie-august 2016, pp. 22-27.

În ciuda acestor abordări, nu există, în prezent, o definiție precisă a conceptului, care să fie acceptată pe scară largă, dincolo de cel mai mic numitor comun al combinației de mijloace, proceduri și tactici convenționale și asimetrice. În conflictele de după Războiul Rece, cei care s-au confruntat cu statele occidentale ar fi folosit, în anumite momente, forțe convenționale, trupe neregulate, acte teroriste și chiar crimă organizată.

Caracteristicile războaielor hibride

Știrile au prezentat războiul hibrid ca un conflict inedit, concentrându-se, în principal, pe elementul informativ, pe dezinformare și știri false, pe difuzarea acestuia pe internet. Dar, astfel de conflicte ar implica, de asemenea, combinarea altor elemente de luat în considerare, precum actorii participanți, tipul de arme pe care le dețin și scenariile care se dezvoltă încontinuu. Unele dintre caracteristicile războaielor hibride sunt prezentate în cele ce urmează:

❖ *Fizionomia actorilor implicați*: printre acești actori se numără state, grupări de gherilă și teroriști, precum și grupuri de criminalitate organizată sau contractori militari privați. Aceste tipuri de conflicte pot fi asumate de actori statali sau actori nonstatali. După cum am menționat, analizele războiului hibrid s-au axat pe confruntările dintre actorii nonstatali, în mod regulat atașați de un stat eșuat, și statele occidentale, cum a fost în cazul războaielor din Afganistan, Irak și în confruntarea dintre Hezbollah și Israel. Grupurile insurgente ar dezvolta războiul hibrid, deoarece acestea ar avea capacități inferioare actorilor statali, deficiențe de personal, de doctrină, armament și tehnologie. Format, în principal, din voluntari, obiectivul ar fi contracararea superiorității actorului statal și exploatarea vulnerabilităților acestuia. Pe de altă parte, acest tip de conflict poate apărea și din partea actorilor statali, într-o posibilă confruntare convențională cu alți actori statali, superiori din punct de vedere militar. Un caz inedit ar fi conflictul dintre Ucraina și Rusia, din 2014, în care Rusia – statul cel mai puternic, teoretic – a fost cel care a folosit războiul hibrid împotriva celor mai puțin dezvoltați. Această decizie ar urma să se bazeze pe evitarea unei confruntări convenționale și, la rândul său, pe o posibilă confruntare cu Statele Unite și NATO, în care Rusia ar fi tocmai partea afectată.

Analizele războiului hibrid s-au axat pe confruntările dintre actorii nonstatali, în mod regulat atașați de un stat eșuat, și statele occidentale, cum a fost în cazul războaielor din Afganistan, Irak și în confruntarea dintre Hezbollah și Israel.

❖ *Tipul de armament utilizat:* forțele neregulate au armament mai mult decât armatele obișnuite, cum ar fi tehnologiile de ultimă generație și armele grele, ceea ce face mai dificilă distincția între formele de război convenționale și cele neregulate.

❖ *Tactica folosită:* se are în vedere utilizarea acțiunilor convenționale, recurgerea la acte teroriste, la acțiuni insurgente, operații informative sau computerizate.

❖ *Utilizarea tehnologiilor informaționale și de comunicare*: această caracteristică a războiului hibrid include controlul mass-mediei tradiționale până la internet și rețelele sociale. Acest lucru ar face posibilă consolidarea propriei imagini sau contracararea celei a adversarului, cu scopul de a ajunge la *„inimile și mințile oamenilor”*[13], care ar fi, în mare parte, un război psihologic. În acest fel, se remarcă o importanță din ce în ce mai mare acordată așa-numitului război informațional și utilizării cyberspațiului.

Forțele neregulate au armament mai mult decât armatele obișnuite, cum ar fi tehnologiile de ultimă generație și armele grele, ceea ce face mai dificilă distincția între formele de război convenționale și cele neregulate.

❖ *Scenariile privind spațiul de luptă*: aceste tipuri de conflicte sunt considerate esențial urbane, spre deosebire de războaiele de gherilă, care ar avea loc în junglă sau în munți. Acest lucru creează dificultăți mai mari în realizarea obiectivelor militare, din cauza prezenței populației civile și a posibilelor consecințe asupra infrastructurii critice, cum ar fi transportul și energia.

❖ *Legătura cu grupurile teroriste și criminalitatea organizată*: este obișnuit faptul ca grupurile implicate în războaiele hibride să aibă legături cu grupări teroriste sau cu criminalitatea organizată. Acest lucru nu implică neapărat și faptul că au obiective comune.

❖ *Importanța crescândă a elementului psihologic:* există o nesocotire intenționată a legalității și a dreptului umanitar internațional de către promotorii războaielor hibride și ai grupurilor criminale și teroriste aferente. Dimpotrivă, forțele armate occidentale sunt supuse unor reguli, tradiții militare sau reguli de confruntare. Prin urmare, războaiele hibride pot fi considerate formal diferite de conflictele tradiționale, în măsura în care *„s-au luptat în mod convențional și simetric pe fronturi clar definite, cu mijloace tehnologice avansate în timp și supuse utilizărilor și obiceiurilor de război frecvent acceptate pentru concurenți”*[14].

[13] James K. Wither, *Making Sense of Hybrid Warfare,* Connections, The Quarterly Journal, nr. 2, 2016.

❖ *Planificarea*: promotorii acestui tip de conflict ar detecta anterior punctele slabe ale adversarului, în domeniul politic, ideologic, economic sau demografic, cu scopul de a prelungi conflictul, a crește costurile sau a influența percepția societăților din statele occidentale.

Trebuie remarcat faptul că războaiele hibride includ un ansamblu de elemente regulate și neregulate. Prin urmare, utilizarea unuia dintre aceste elemente nu implică faptul că un conflict poate fi considerat neapărat și *„hibrid”*. Activitățile rusești în cazul Brexit, al alegerilor americane și în conflictul catalan au primit calificarea de *hibrid* în mare parte datorită utilizării cyberspațiului și combinării atacurilor informatice, propagandei și dezinformării, a folosirii tehnologiilor informaționale și de comunicare, precum și a operațiunilor informaționale. Cu toate acestea, nu a fost în niciun caz o confruntare armată care să implice actori statali sau nonstatali.

Războaiele hibride includ un ansamblu de elemente regulate și neregulate. Prin urmare, utilizarea unuia dintre aceste elemente nu implică faptul că un conflict poate fi considerat neapărat și „hibrid”.

RĂZBOIUL HIBRID ȘI LEGĂTURA ACESTUIA CU MASS-MEDIA

Potrivit presei, Rusia conduce un război hibrid împotriva statelor occidentale. Cu toate acestea, clasificarea amintită prezintă un scenariu diferit de cele descrise. Noutatea, potrivit știrilor, este că un singur stat, Rusia, ar conduce acest tip de războaie simultan împotriva mai multor state, printre care sunt incluse și principalele puteri militare, ca Statele Unite și Marea Britanie. Acesta este un proces continuu, care se extinde în timp, dar în care putem identifica momente de înaltă presiune, de exemplu, cu puțin timp înaintea proceselor electorale din Marea Britanie. În ciuda dezvoltării pe care Rusia a făcut-o în sfera digitală, împreună cu campaniile de dezinformare, totuși, ea nu are monopol

[14] Guillem Colom, *La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo*, în *Revista Ejército*, nr. 933, decembrie 2018, https://www.ugr.es/~gesi/Doctri-na-Gerasimov.pdf, accesat la 1 februarie 2020.

asupra acestor activități[15]. Mass-media a raportat că este o activitate aproape exclusivă a Rusiei. Totuși, trebuie avut în vedere faptul că una dintre caracteristicile fundamentale ale războiului hibrid ar consta nu numai în utilizarea tehnologiilor informaționale și de comunicare, ci și în folosirea simultană a altor componente menționate în acest material. Adică o combinație de elemente obișnuite și neregulate, la care face referire F.G. Hoffman. În presupusul război hibrid dintre Rusia și statele occidentale, nu există un conflict armat în care să participe forțe regulate și neregulate, să fie utilizate arme avansate sau să fie efectuate acte teroriste.

Unul dintre elementele caracteristice ale războaielor hibride este spațiul în care se dezvoltă, în principal centrele urbane. În cazul în care analizăm conflictul din estul Europei, Rusia ar fi folosit cyberspațiul ca etapă principală a activităților sale.

Una dintre caracteristicile subliniate de mass-media a fost presupusa noutate a acestui tip de conflict și exclusivitatea pe care Rusia a avut-o în abordarea războaielor hibride. Unii experți consideră că *„aceste forme de acțiune cu greu pot fi descrise drept noi sau considerate ca un răspuns specific la stilul de luptă occidentalizat”*[16].

Pe de altă parte, unul dintre elementele caracteristice ale războaielor hibride este spațiul în care se dezvoltă, în principal centrele urbane. În cazul în care analizăm conflictul din estul Europei, Rusia ar fi folosit cyberspațiul ca etapă principală a activităților sale. Deși au fost efectuate operațiuni informatice prin intermediul internetului, nu numai diseminare de știri, ci și atacuri informatice precum cele desfășurate împotriva Partidului Democrat al Statelor Unite, care au permis accesul la conturile de e-mail, aceste activități au fost definite, în cadrul evenimentelor prezentate la știri, drept război hibrid.

DOCTRINA GERASIMOV ȘI RĂZBOIUL HIBRID

Dacă sintagma de *război hibrid* s-a concentrat pe o parte a analizei, alte concepte au fost folosite pentru contextualizarea acestor conflicte. Mass-media a subliniat faptul că războiul hibrid face parte din *doctrina Gerasimov*, care a prezentat linia de separare a războiului de pace,

[15] The Cipher Brief, *The Use of Disinformation in the British Election*, https://www.thecipherbrief.com/column/soufan-center/the-use-of-disinformation-in-the-british-election, accesat la data de 20.02.2020.

[16] Guillem Colom, *Vigencia y limitaciones de la guerra híbrida*, în *Revista Científica General José María Córdova*, nr. 1, 2012.

ca atare trebuie dezvoltate tactici care să permită lucrul *„din umbră”*, să condiționeze procesele electorale, să agite populația civilă sau să pirateze țintele din alte țări.

Originea conceptului datează din februarie 2013, odată cu publicarea articolului *„Valoarea științei în anticipație”* al șefului Statului Major al Apărării al Armatei Ruse, generalul Valeri Gerasimov, în revista *Voyenno-Promyshlennyy Kuryer*. Pentru o mare parte din mass-media și analiști occidentali, articolul reprezintă documentul de temelie a ceea ce, în Occident, este cunoscută sub numele de *doctrina Gerasimov*. *„Este interpretată ca o propunere pentru un nou mod rusesc de război care combină războiul convențional și neconvențional cu aspectele puterii naționale”*[17], în care se face referire la metode indirecte și asimetrice. Odată cu evenimentele din Crimeea și Ucraina, au fost identificate unele dintre elementele expuse în documentul din 2013 al lui Gerasimov și s-a propagat ideea că acesta expune un nou mod de acționa. Atunci, *hibridul* a trecut granița dezbaterii strategice pentru a deveni un cuvânt cu o utilizare comună și a fost folosit pentru a defini gama întreagă de activități informative, de destabilizare și subversiune pe care Kremlinul le-ar putea desfășura într-un mod ascuns, semiacoperit sau clandestin, sub pragul conflictului.

Originea conceptului de „război hibrid” datează din februarie 2013, odată cu publicarea articolului „Valoarea științei în anticipație” al șefului Statului Major al Apărării al Armatei Ruse, generalul Valeri Gerasimov. Pentru o mare parte din mass-media și analiști occidentali, articolul reprezintă documentul de temelie a ceea ce, în Occident, este cunoscută sub numele de „doctrina Gerasimov”.

În ciuda acceptării pe scară largă a conceptului și a faptului că reprezintă o nouă doctrină, unii analiști au pus la îndoială dacă este o doctrină militară sau o propunere a unei noi modalități rusești de a duce un război. Trebuie subliniat faptul că Gerasimov a declarat, în articolul său, *„perspectiva sa despre trecutul recent, prezentul și viitorul așteptat al războiului”*[18], bazat, în mare parte, pe ceea ce s-a întâmplat în *„Primăvara arabă”* și în *„Revoluția culorilor”*[19]. Gerasimov pune accent pe creșterea mijloacelor non-militare, cum ar fi operațiuni

[17] Charles K. Bartles, *Cómo comprender el artículo de Gerasimov*, în *Military Review*, 2016.

[18] Valeri Gerasimov, *Ценностьнаукивпредвидении*, în VPK, nr. 476, 8 martie 2013, https://vpk-news.ru/articles/14632, accesat la 2 februarie 2020.

[19] *Primăvara arabă* reprezintă o serie de mișcări de protest care au avut loc în mai multe țări din Orientul Mijlociu și Africa de Nord începând cu sfârșitul anului 2010. În principal, acestea au avut loc mai ales în țări arabe, unde domnea un regim autoritar sau totalitar, https://ro.wikipedia.org/wiki/Prim%C4%83vara_arab%C4%83, accesat la 24 februarie 2020. *Revoluția culorilor* este răsturnarea non-violentă a puterii prin proteste stradale, https://ro.odkurzacze.info/2746-the-most-famous-color-revolutions.html, accesat la 23 februarie 2020.

politice, economice, umanitare, sub acoperire, precum și pe importanța informațiilor. La rândul său, Rusia consideră că războiul hibrid este un termen occidental și, prin urmare, diferit de sistemul său doctrinar. De fapt, Federația Rusă se referă la diferiți termeni legați de războiul hibrid, cum ar fi *„război neliniar”, „război ambiguu”* și *„războiul rețelelor”*[20].

Trei ani mai târziu, Gerasimov a publicat un nou articol, în care a prezentat câteva idei despre războaiele contemporane, aparent similar cu expunerea anterioară, dar în care a adăugat experiențele conflictelor din Ucraina și Siria. Gerasimov a identificat metodele hibride în *Revoluția culorilor* și afirmă că aceste mișcări sunt, de fapt, materii promovate de Occident. Spre deosebire de articolul din 2013, acest document se referă în mod deschis la războaiele și metodele hibride, dar într-un mod diferit față de Occident.

Gerasimov consideră că, în conflictele contemporane, este din ce în ce mai frecvent să acordăm prioritate unei utilizări comune a măsurilor non-militare, politice, economice, informaționale și de altă natură care sunt puse în practică cu sprijinul forței militare.

După cum am menționat, războiul hibrid ar combina metode convenționale și neregulate, printre care găsim legături cu crima organizată sau grupurile teroriste, în timp ce Gerasimov consideră că, în conflictele contemporane, este din ce în ce mai frecvent să acordăm prioritate unei utilizări comune a măsurilor non-militare, politice, economice, informaționale și de altă natură care sunt puse în practică cu sprijinul forței militare[21]. Totalitatea acestor elemente integrate sub aceeași umbrelă se numesc *metode hibride*.

În practică, aceasta ar presupune o percepție mai limitată a acțiunilor hibride decât o face Occidentul. În ciuda acestei diferențe, autorul susține că integrarea activităților tradiționale cu cele hibride este o caracteristică a conflictelor armate contemporane, în care el indică elementul informativ ca principal instrument în cazul metodelor hibride. Aceasta pentru că falsificarea evenimentelor, limitarea activității mass-mediei devin unele dintre cele mai eficiente metode asimetrice în desfășurarea războaielor. Efectul său poate fi comparabil cu rezultatele unei utilizări masive de trupe.

[20] Mira Milosevich, *El poder de la influencia rusa: la desinformación*, Real Instituto Elcano, ARI 7/2017.

[21] Valeri Gerasimov, *По опыту Сирии*, în *VPK*, nr. 624, 9 martie 2016, https://www.vpk-news.ru/articles/48913 accesat la 23 februarie 2020.

Pe scurt, Gerasimov se referă la metode de război hibride, deoarece consideră că Rusia ar trebui să facă față acestor tipuri de războaie și, prin urmare, trebuie să le cunoască și să se adapteze la ele. În plus, trebuie să se țină seamă de faptul că Gerasimov îl prezintă într-un scenariu de război armat, în timp ce campaniile de dezinformare și știrile false din Occident s-ar desfășura într-un context de tensiune și confruntare politică și socială, dar în absența unui conflict armat. Nu în ultimul rând, Mark Galeotti, analistul care a inventat sintagma *doctrina Gerasimov*[22], nu numai că a negat existența acelei presupuse doctrine, dar, de asemenea, observă că articolul lui Gerasimov avea scopul de a rezolva modul de luptă împotriva acțiunilor neconvenționale.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

CONCLUZII

Este obișnuit să găsim știri legate de campaniile de dezinformare de origine rusă care susțin că sunt înregistrate într-un context de război hibrid împotriva Occidentului. Problema principală a informațiilor jurnalistice prezentate aici este că, în cea mai mare parte, autorii nu expun nici măcar o scurtă aproximare față de conceptele utilizate, sensul și implicațiile acestora, cum ar fi dezinformare, fake news, cyberwar sau război hibrid. Uneori, acest lucru duce la utilizarea unora dintre aceste concepte ca fiind sinonime. Posibil, unul dintre motivele confuziei este amestecul dintre utilizarea conceptelor recente, în acest caz, cele legate de spațiul cibernetic , cu altele, care sunt localizate în mod tradițional într-un domeniu militar și academic, în încercarea de a dori să se informeze despre schimbări care apar pe scena internațională. De asemenea, acest lucru se datorează și spiralei în care a intrat mass-media, împinsă de o cerere constantă de informații din partea cetățenilor, dorind să informeze, aproape minut de minut, despre cele mai recente știri, ceea ce presupune mai degrabă o cantitate informativă decât calitatea mesajelor transmise.

Utilizarea cibernetică și a informațiilor de către Rusia a fost în centrul atenției vizavi de știrile legate de războiul hibrid. Dar, deși este adevărat că această țară a încurajat utilizarea operațiunilor de informare și a profitat de potențialul mediului digital în favoarea intereselor sale, dezvoltarea campaniilor de dezinformare și utilizarea tehnologiilor informaționale și de comunicare nu se pot identifica totuși exclusiv cu războiul hibrid.

Fără îndoială, utilizarea cibernetică și a informațiilor de către Rusia a fost în centrul atenției vizavi de știrile legate de războiul hibrid. Dar, deși este adevărat că această țară a încurajat utilizarea operațiunilor

[22] Mark Galeotti, *I’m sorry for creating the ‘Gerasimov Doctrine’*, în *Foreign Policy*, martie 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doc-trine/, accesat la 23 februarie 2020.

de informare și a profitat de potențialul mediului digital în favoarea intereselor sale, dezvoltarea campaniilor de dezinformare și utilizarea tehnologiilor informaționale și de comunicare nu se pot identifica totuși exclusiv cu războiul hibrid. Una dintre caracteristicile conflictelor hibride constă în combinarea diferitelor elemente convenționale și asimetrice, dar știrile s-au concentrat aproape exclusiv pe elementul digital, prin care au fost dezvoltate campaniile de dezinformare, știrile false și utilizarea masivă a rețelelor sociale. Deși pot face parte din conflicte hibride, având în vedere că, în ultimii ani, elementul cibernetic câștigă o importanță enormă în cadrul conflictelor, totuși, nu putem afirma că aceste activități sunt mișcări ale războiului hibrid.

Conceptul de „zonă gri" definește acele activități aflate sub pragul conflictului, care se desfășoară pe timp de pace, spre deosebire de războiul hibrid, și care includ atacuri informatice sau campanii de dezinformare și propagandă care ar avea drept trăsătură comună dificultatea de a determina atribuirea acestora.

Prin urmare, dacă am conchide că evenimentele care au avut loc cu ocazia Brexitului, la alegerile din SUA și în conflictul catalan nu pot fi descrise ca un război hibrid, un cadru de analiză semnificativ pentru a înțelege noutățile cyberspațiului și impactul său asupra relațiilor internaționale în aceste scenarii ar putea fi totuși dezvoltat din conceptul de *zonă gri*. Conceptul definește acele activități aflate sub pragul conflictului, care se desfășoară pe timp de pace, spre deosebire de războiul hibrid, și care includ atacuri informatice sau campanii de dezinformare și propagandă care ar avea drept trăsătură comună dificultatea de a determina atribuirea acestora. Prin urmare, acest concept ar permite o analiză a activităților care nu sunt descrise în mod specific drept acțiuni de război, dar ar putea deveni la fel de decisive precum un conflict militar.

Analiza prezentată în cadrul acestui articol s-a concentrat pe importanța conceptualizării și contextualizării faptelor raportate. Este clar că exercitarea jurnalismului diferă de domeniul academic, dar este la fel de adevărat că știrile ar trebui să transmită informația cu cea mai mare rigoare posibilă și să-i expună cititorului ceea ce se întâmplă în contextul lor specific, încercând să utilizeze concepte adecvate în fiecare caz. Ne aflăm încă într-o etapă timpurie în analiza capacităților cyberspațiului, iar reducerea acesteia la utilizarea pe care un singur stat o poate face pentru diseminarea campaniilor de propagandă ar însemna să nu înțelegem potențialul său în relațiile internaționale.

BIBLIOGRAFIE:

1. ***, BBC, *Brexit: Ce se întâmplă acum?,* 29 iunie 2016, https://www.bbc.com/news/uk-politics-eu-referendum-36420148
2. Karla Adam, William Booth, *Creșterea alarmei în Marea Britanie față de răzbunarea rusă în votul Brexit*, în *The Washington Post*, 17 noiembrie 2017.
3. Josep Baqués, *Rolul Rusiei în conflictul din Ucraina: Războiul hibrid al marilor puteri*, în *Journal of International Security Studies*, 41-60, 2015.
4. Charles K. Bartles, *Cum să înțelegem articolul lui Gerasimov*, în *Revista militară*, martie-aprilie, 2016.
5. Daniel Boffey, *UE strânge fonduri pentru combaterea războiului de dezinformare cu Rusia*, în *The Guardian*, 5 decembrie 2018.
6. Richard A. Clarke, Robert K. Knake, *Războiul cibernetic: următoarea amenințare la adresa securității naționale și ce trebuie făcut în acest sens*, SUA, Harper Collins Publishers, 2010.
7. Valeri Gerasimov, *Ценность науки в предвидении*, în *VPK*, nr. 476, 8 martie 2013, https://vpk-news.ru/articles/14632
8. Valeri Gerasimov, *По опыту Сирии*, în *VPK*, nr. 624, 9 martie 2016, https://vpk-news.ru/articles/29579
9. Robert G. Walker, *Corpul marin al Statelor Unite în operațiuni speciale.* Teză de master, Școala postuniversitară navală, https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf.

CAMPANIILE DE DEZINFORMARE – COMPONENTE IMPORTANTE ALE RĂZBOIULUI HIBRID –

Căpitan ing. drd. Viorica Ionela TRINCU
Universitatea Națională de Apărare „Carol I”, București

Evoluția mediului internațional de securitate și a tehnologiei informației a oferit un imbold deosebit dezvoltării comunicării interumane și intercomunitare, în special prin new media. Războiul hibrid reprezintă exemplul cel mai elocvent de adaptare a fenomenului război la evoluția societății umane și a tehnologiei informației. Dezinformarea are un rol foarte important în desfășurarea și stabilirea rezultatului confruntării hibride, aceasta fiind utilizată în toate genurile de confruntare intercomunitară. Mass-media, în special platformele de socializare online, constituie vehiculele cele mai utilizate și cele mai eficiente pentru desfășurarea și propagarea acțiunilor de dezinformare.

Cuvinte-cheie: război hibrid, stratagemă militară, dezinformare, surprindere militară, mass-media.

INTRODUCERE

Societăţile democratice s-au fundamentat pe o exprimare liberă a voinţei cetăţenilor – drept care este asigurat de puterile şi instituţiile statului, sub monitorizarea permanentă a unei mass-medii libere şi independente.

Mass-media contribuie în mod substanţial la realizarea comunicării între puterile şi instituţiile statului, pe de o parte, şi populaţie, pe de altă parte. Practic, mass-media colectează informaţiile relevante pentru populaţie şi le pune la dispoziţia cetăţenilor cu scopul de a-i ajuta să îşi formeze opinii proprii despre funcţionarea instituţiilor statului (calitatea guvernării, transparenţă şi responsabilitate[1]) şi situaţia comunităţii umane din care fac parte. Prin modul în care funcţionează mass-media – monitorizarea şi analizarea activităţii instituţiilor statului –, aceasta contribuie la promovarea democraţiei, iar prin informarea corectă a populaţiei, contribuie la asigurarea dreptului acesteia la informare şi la exprimarea liberă.

Deși mass-media ar trebui să fie obiectivă, imparţială şi independentă[2], aceasta are un rol dual[3]. În majoritatea cazurilor, mass-media din statele democratice îşi respectă statutul autoasumat prin codurile deontologice ale jurnaliştilor şi ale celorlalţi profesionişti angajaţi ai mijloacelor de comunicare în masă, contribuind la buna funcţionare a democraţiei şi la informarea corectă şi oportună a populaţiei.

Mass-media contribuie în mod substanţial la realizarea comunicării între puterile şi instituţiile statului, pe de o parte, şi populaţie, pe de altă parte. Practic, mass-media colectează informaţiile relevante pentru populaţie şi le pune la dispoziţia cetăţenilor cu scopul de a-i ajuta să îşi formeze opinii proprii despre funcţionarea instituţiilor statului şi situaţia comunităţii umane din care fac parte.

[1] Irina Moroianu Zlătescu, *Drepturile omului – un sistem în evoluție*, Institutul Român pentru Drepturile Omului, București, 2017, p. 3, disponibil pe http://irdo.ro/irdo/pdf/175_ro.pdf, accesat în octombrie 2019.

[2] Silvia Șpac, *Impactul mass-media asupra formării personalității elevului de vârstă școlară mică*, Studia Universitatis Moldaviae, 2015, disponibil pe http://ojs.studiamsu.eu/index.php/education/article/view/279/237, accesat în octombrie 2019.

[3] Din cauza efectelor duale ale mass-mediei, Paul Dobrescu asemăna comunicarea cu un despot, pentru că aceasta este *„o armă, poate cea mai puternică, de condiționare și mistificare a ființei umane” (Un despot modern – opinia publică,* în *Revista română de comunicare și relații publice*, nr. 2-3/2000, p. 15).

În statele democratice există şi mass-media partizane, dar şi mass-media care aparţin unor patroni, acestea fiind obligate să reprezinte interesele acestora prin articolele şi reportajele audio şi video pe care le produc şi le difuzează.

Mass-media au un rol negativ atunci când apără intenţia şi interesul unei persoane (grup de persoane) care nu concordă cu interesul general al comunităţii. În aceste cazuri, se folosesc mijloace de influenţare, în principal dezinformarea şi manipularea, pentru a determina cetăţenii să susţină acest interes sau să nu se opună îndeplinirii obiectivelor iniţiatorului dezinformării.

Dezinformarea a fost folosită cu succes în toate confruntările desfăşurate de-a lungul timpului. În prezent, această metodă de influenţare a populaţiei are o contribuţie extrem de importantă la desfăşurarea şi stabilirea rezultatului războiului hibrid.

Pierderile umane cauzate de confruntările armate i-au determinat pe mulţi gânditori să iniţieze proiecte de reducere până la eliminare a războaielor dintre state, respectiv dintre comunităţi din cadrul statelor.

RĂZBOIUL HIBRID – ETAPĂ NOUĂ DE EVOLUŢIE A CONFRUNTĂRILOR INTERCOMUNITARE

Războiul a fost considerat multă vreme o formă de confruntare armată căreia i-au fost asociate acţiuni în domeniile politic, diplomatic, economic, financiar, cultural şi informaţional.

Despre război, ca formă de rezolvare a diferendelor între comunităţile umane, s-au scris multe studii istorice, opere literare şi articole în mass-media. Secvenţe memorabile din diferite războaie au fost subiectele principale ale multor producţii artistice – filme, picturi, sculpturi etc., prin care au fost glorificate fapte de eroism sau au fost făcute cunoscute opiniei publice acţiuni şi atitudini abominabile (crime în masă, atacuri teroriste, distrugeri deliberate ale unor vestigii istorice şi ale unor lăcaşe de cult etc.) ale unor persoane care nu au avut nimic comun cu umanitatea.

Pe măsura trecerii timpului, a dezvoltării tehnologiei informaţiei şi a inteligenţei artificiale, omenirea a cunoscut, inclusiv în timp real în ultimele decenii, atrocităţile generate de unii dintre participanţii la confruntările intercomunitare violente.

Pierderile umane cauzate de confruntările armate i-au determinat pe mulţi gânditori să iniţieze proiecte de reducere până la eliminare a războaielor dintre state, respectiv dintre comunităţi din cadrul statelor.

Unele dintre cele mai cunoscute proiecte de acest gen aparţin Abatelui de Saint Pierre şi lui Immanuel Kant. Idei despre eliminarea războaielor din relaţiile internaţionale au emis Jean Jacques Rousseau şi alţi gânditori renascentişti. Ideile respective s-au dovedit, în mare parte, utopice, pentru că se pare că noi, oamenii, avem o tendinţă naturală spre confruntare[4].

Cele două războaie mondiale au îndoliat zeci, poate chiar sute de milioane de familii din toată lumea şi încheierea acestora a relansat unele dintre ideile emise de Kant, Abatele de Saint Pierre şi alţi gânditori care s-au pronunţat împotriva confruntărilor armate, ca modalitate de soluţionare a disensiunilor dintre state. Pe cale de consecinţă, s-au înfiinţat unele organizaţii internaţionale guvernamentale, care au responsabilităţi în domeniul asigurării securităţii la nivel global (ONU)[5] şi regionale (Organizaţia pentru Securitate şi Cooperare în Europa – OSCE, Organizaţia Statelor Americane – OSA, Organizaţia Unităţii Africane – OUA, Liga Arabă – LA)[6] etc. De asemenea, au fost elaborate şi ratificate de majoritatea statelor lumii tratate, convenţii şi acorduri pentru interzicerea armelor chimice şi a minelor antipersonal, neproliferarea armelor de distrugere în masă, limitarea şi reducerea armelor nucleare, reducerea armelor convenţionale în Europa, dezarmarea şi dezangajarea militară etc.

Cele două războaie mondiale au îndoliat zeci, poate chiar sute de milioane de familii din toată lumea şi încheierea acestora a relansat unele dintre ideile emise de Kant, Abatele de Saint Pierre şi alţi gânditori care s-au pronunţat împotriva confruntărilor armate, ca modalitate de soluţionare a disensiunilor dintre state.

În pofida acestor măsuri organizatorice şi a actelor normative internaţionale ce reglementează raporturile dintre state, respectiv dintre cetăţeni şi statele lor, confruntările violente au continuat, dar cu un număr mai redus de victime umane. Această tendinţă, pe fondul încheierii Războiului Rece, i-a determinat pe unii analişti politico-militari şi experţi în securitatea internaţională să estimeze că asistăm la declinul războiului. Alţi autori reputaţi se lansau în predicţii de genul

[4] Majid Khadduri, *War and Peace in the Law of Islam*, John Hopkins University Press, Baltimore, 1955, p. 57, apud Dr. Lewis B. Ware, *An Islamic Concept of Conflict in Its Historical Context*, Stephen J. Blank, Lawrence E. Grinter, Karl P. Magyar, Bynum E. Wheaters, *Conflict, Culture and History*, Air University Press, Maxwell Air Force Base, Alabama, SUA, 1993, p. 67 *(„natura umană face războiul o normă, nu o excepţie”)*.

[5] Madeleine Albright, *Who Broke the U.N.*?, în *Foreign Policy*, 13.08.2012, http://foreignpolicy.com/2012/08/13/who-broke-the-u-n/, consultat în decembrie 2019.

[6] Roberta Cohen, *The Role of Regional Organizations*, ECOWAS, Brookings, Monday, 30 septembrie 2002, https://www.brookings.edu/on-the-record/the-role-of-regional-organizations-ecowas/, consultat în decembrie 2019.

„sfârşitul geografiei” (Paul Virilio – 1997)[7], *„sfârşitul naturii”* (Charles McKibben – 1990), *„sfârşitul istoriei”* (Francis Fukuyama – 1992), *„sfârşitul ştiinţei”* (John Horgan – 2012)[8] etc.

Fenomenul război, în ultimul secol, s-a manifestat în principal prin confruntarea brută, în care mijloacele folosite erau preponderent distructive şi letale. În prezent, mijloacele nonmilitare au rolul cel mai important, iar forţa militară este menţinută în rezervă, cu rol de avertizare-ameninţare, care ar putea fi folosită la nevoie, după principiul *„când diplomaţia tace, armele vorbesc”*.

Fenomenul război, în ultimul secol, s-a manifestat în principal prin confruntarea brută, în care mijloacele folosite erau preponderent distructive şi letale. În prezent, mijloacele nonmilitare au rolul cel mai important, iar forţa militară este menţinută în rezervă, cu rol de avertizare-ameninţare, care ar putea fi folosită la nevoie, după principiul „când diplomaţia tace, armele vorbesc”.

În prezent, confruntările au luat preponderent forma războiului hibrid – o combinaţie de concepte de folosire a mijloacelor de luptă şi a sistemelor de armă convenţionale şi neconvenţionale, menite să surprindă adversarul şi să aducă victoria iniţiatorului.

Unii autori consideră că războiul hibrid ar fi apărut în secolul XXI, dar un scurt recurs la istoria confruntărilor armate, numai din secolul XX, ne relevă existenţa multor similitudini cu conceptul de război hibrid. Există, desigur, destul de multe diferenţe, pentru că tehnologia a evoluat foarte mult, atât cea destinată producerii mijloacelor letale şi distructive, cât şi a celor din categoria *„soft power”*. Mai trebuie menţionat rolul comunităţii internaţionale şi al organizaţiilor guvernamentale internaţionale care, prin decizii şi reglementări, au cerut rezolvarea divergenţelor dintre state pe cale paşnică, iar în cazul izbucnirii unor conflicte violente, de reducere a numărului victimelor şi a distrugerilor. Aceste cerinţe s-au materializat în adaptări conceptuale şi tehnologice care au diminuat pierderile colaterale şi inutile. Aşa au fost realizate mijloacele de lovire cu precizie chirurgicală, sistemele de armă inteligente, mijloacele aeriene fără pilot, dronele, roboţii de cercetare, sateliţii cu destinaţie militară etc.

Războiul hibrid este un exemplu de adaptare a fenomenului război la evoluţia situaţiei internaţionale de securitate, la evoluţia tehnologiei informatice şi informaţionale şi de aplicare a principiile luptei armate la această situaţie, în special a principiului realizării surprinderii şi evitării

[7] Paul Virilio, *Un monde surexposé: fin de l'histoire ou fin de la géographie?*, în *Le monde diplomatique*, august 1997, p. 17, apud Zygmunt Bauman, *Globalizarea şi efectele ei sociale*, Editura Antet, Oradea, an neprecizat, pp. 16-17.

[8] Cristopher Goker, *Future War*, Polity Press, Marea Britanie, 2014, p. 137.

surprinderii. Fiecare comandant militar ştie că va avea şanse mai mari de a învinge într-o confruntare dacă reuşeşte să îşi surprindă inamicul. Aşadar, producerea unor mijloace de luptă şi a unor sisteme de armă noi vor impune şi o adaptare a concepţiilor de întrebuinţare în lupte şi operaţii a acestora. În condiţiile în care aceste elemente de noutate nu sunt cunoscute de adversari, ele constituie premize pentru realizarea surprinderii în confruntările armate. Prin conceptul de război hibrid se îndeplinesc multe dintre condiţiile prezentate anterior, fapt care i-a determinat pe unii autori să afirme că războiul este cameleonic[9], adică îşi schimbă mereu forma de desfăşurare, şi este continuu[10].

SCURT ISTORIC AL UTILIZĂRII DEZINFORMĂRII ÎN CONFRUNTĂRILE ARMATE

Comunicarea este o modalitate de relaţionare între persoane, dar şi între comunităţi, iar dezinformarea este o metodă de comunicare prin care persoanele şi comunităţile umane îşi propun să îşi îndeplinească obiectivele fără să ţină seamă de normele legale şi morale care guvernează societăţile umane.

Atunci când abordează subiectul dezinformării, specialişti reputaţi din toată lumea au opinii destul de diferite, dar aceste opinii au cel puţin două elemente comune: interesul şi intenţia iniţiatorilor dezinformării de a ascunde (deforma, trunchia, modifica) realitatea prin: inventarea unor ştiri-bombă, minimizarea unor evenimente importante, exacerbarea importanţei unor evenimente nesemnificative pentru interesul public etc., evenimente şi acţiuni menite să abată atenţia opiniei publice de la aspectele compromiţătoare pentru iniţiatorii dezinformării sau de a impune opiniei publice idei, proiecte, obiective care să satisfacă interesele iniţiatorilor. Căile de atingere a acestor obiective sunt diferite atât prin mijloacele, cât şi prin metodele folosite. De la Sun Tzu,

Atunci când abordează subiectul dezinformării, specialişti reputaţi din toată lumea au opinii destul de diferite, dar aceste opinii au cel puţin două elemente comune: interesul şi intenţia iniţiatorilor dezinformării de a ascunde realitatea.

[9] Mihail Orzeaţă, *Suntem pregătiţi pentru războiul viitorului?*, în revista *Gândirea Militară Românească*, nr. 4 (octombrie-decembrie), 2016, pp. 20-29, http://www.smg.gmr.ro/gmr/Arhiva_pdf/2016/revista_4_final.pdf, consultat în decembrie 2019.

[10] Mihail Orzeaţă, *Războiul continuu,* Editura Militară, Bucureşti, 2011, vezi şi Tom Toles, Rant Friday, *Perpetual War edition*, *The Washington Post*, 26 septembrie 2014, http://www.washingtonpost.com/news/opinions/wp/2014/09/26/friday-rant-perpetual-war-edition/, consultat în octombrie 2019.

considerat de unii *„profet al dezinformării”*[11], şi până în prezent, mulţi experţi civili şi militari au studiat dezinformarea şi şi-au expus ideile în studii şi lucrări considerate a fi puncte de referinţă în domeniu, deşi unele dintre ele par să conţină *„un amalgam de termeni”*[12]. Pentru a susţine această afirmaţie, prezentăm câteva opinii ale unor specialişti cunoscuţi:

- *„dezinformarea este ansamblul proceselor dialectice puse în joc în mod intenţionat pentru a reuşi manipularea perfidă a persoanelor, grupurilor sau a unei întregi societăţi în scopul devierii conduitelor politice, de a le domina gândirea sau chiar de a le subjuga”*[13]*;*
- *„dezinformarea este manipularea opiniei publice (nu a indivizilor) în scopuri politice (altfel ar putea fi propagandă) a unei informaţii veridice sau nu (nu veridicitatea informaţiei contează, ci felul în care este ea prezentată)”* [14];
- *„manipularea este instrument al dezinformării, alături de intoxicare, propagandă, influenţă, minciună, şiretlicul tactic, subversiune şi diversiune”*[15].

Dezinformarea a existat în orice confruntare armată, pentru că orice comandant militar era interesat să ascundă de adversarul său datele referitoare la trupele proprii pe care le considera a fi vulnerabilităţi (puncte slabe), dar şi să îi anihilieze vigilenţa în legătură cu punctele sale tari (centrele de greutate) şi cu intenţiile sale.

Poate părea paradoxal, dar dezinformarea este dezavuată, respinsă chiar de normele morale ale societăţii, pentru că, în marea majoritate a cazurilor, este asociată cu minciuna, dar, în confruntările armate, este acceptată atât de Dreptul Internaţional, care o consideră *„stratagemă de război”*[16], cât şi de reglementările militare, care o definesc prin sintagma *„înşelare militară...[menită, n.a.] să contribuie la îndeplinirea misiunii”*[17].

Dezinformarea a existat în orice confruntare armată, pentru că orice comandant militar era interesat să ascundă de adversarul său datele referitoare la trupele proprii pe care le considera a fi vulnerabilităţi (puncte slabe), dar şi să îi anihilieze vigilenţa în legătură cu punctele sale tari (centrele de greutate) şi cu intenţiile sale.

[11] Călin Hentea, *Noile haine ale propagandei*, Editura Paralela 45, București, 2008, p. 59.
[12] *Ibidem.*
[13] Henri Pierre Cathala, *Epoca dezinformării*, Editura Militară, București, 1991, p. 24.
[14] Vladimir Volhov, *Dezinformarea văzută din Est*, Editura ProEditură și Tipografie, București, 2007, p. 24.
[15] Ștefan Stanciugelu, *Logica manipulării*, Editura C.H. Beck, București, 2010, p. 64.
[16] Ion Dragoman, *Drept internațional umanitar*, Fundația Andrei Șaguna, Constanța, 1999, p. 69.
[17] *Doctrine for Information Operations*, Joint Pub 3-13, februarie 1998, SUA.

Istoricii au consemnat acţiuni celebre de dezinformare (înşelare), cum ar fi:

- Incidentul Gleiwitz, care a constituit pretextul declanşării celui de-al Doilea Război Mondial – 1 septembrie 1939[18];
- momentul declanșării agresiunii asupra URSS – Operaţia Barbarossa, în al Doilea Război Mondial – 22 iunie 1941;
- atacul japonez de la Pearl Harbor asupra Flotei SUA a Pacificului – 7 decembrie 1941 – şi declanşarea războiului din Pacific dintre Japonia şi SUA;
- locul şi momentul debarcării aliate, în al Doilea Război Mondial – 6 iunie 1944, Normandia;
- dislocarea şi instalarea rachetelor sovietice cu rază medie de acţiune în Cuba (1962)[19] – în perioada Războiului Rece;
- răsturnarea de imagine a liderului sârb Slobodan Miloşevici şi a poporului sârb, înainte de declanşarea războiului din Kosovo[20];
- influenţarea opiniei publice americane şi a unei părţi a comunităţii internaţionale pentru a susţine declanşarea celui de-al doilea război din Golf şi a stopa programele irakiene de dezvoltare a armelor de distrugere în masă [21].

UTILIZAREA DEZINFORMĂRII ÎN RĂZBOIUL HIBRID DIN UCRAINA

Cauzele crizei din Ucraina sunt multiple, unele interne (performanţele slabe ale economiei, divizarea politică şi etno-lingvistică), iar altele externe (influenţarea populaţiei de către Rusia pentru a nu accepta integrarea ţării în organizaţiile euroatlantice, influenţarea populaţiei de către Occident pentru a elimina corupţia şi a dezvolta democraţia,

Cauzele crizei din Ucraina sunt multiple, unele interne – performanţele slabe ale economiei, divizarea politică şi etno-lingvistică –, iar altele externe – influenţarea populaţiei de către Rusia pentru a nu accepta integrarea ţării în organizaţiile euroatlantice, influenţarea populaţiei de către Occident pentru a elimina corupţia şi a dezvolta democraţia, în vederea integrării în organizaţiile euroatlantice.

[18] Dennis Whitehead, *The Gleiwitz incident, „After Batle Magazine”*, nr. 142, martie 2009, http://en.wikipedia.org/Gleiwitz_incident/, consultat în noiembrie 2019.
[19] Prof. dr. Igor A. Amosov, *Caribbean Missile Crisis, 1962 – The World on the Brink of Nuclear Catastrophe*, în colonel dr. Petre Otu, colonel Georghe Vartic, locotenent-colonel dr. Mihai Macuc, coordonatori, *On Both Sides of the Iron Curtin*, Military Publishing House, Bucharest, 2001, pp. 237-246.
[20] Simona Ştefănescu, *Media şi conflictele*, Editura Tritonic, Bucureşti, 2004, pp. 194-218.
[21] Ioan Alexandru, *Între putere și democrație. Presa în politica internă și internațională*, Editura Centrului Tehnic-Editorial al Armatei, București, 2017, pp. 145-158, vezi și Tim Weiner, *CIA. O istorie secretă*, Editura Litera Internațional, București, 2009, pp. 355-356 și 364-366.

în vederea integrării în organizaţiile euroatlantice). Pe acest fond al contradicţiilor interne şi al influenţelor externe, Ucraina a devenit un spaţiu de confruntare între Rusia şi Occident.[22]

Pentru a-şi susţine interesele declarate (sprijinirea populaţiei ruse din partea de est a Ucrainei şi stoparea extinderii NATO spre Est) şi nedeclarate (redobândirea statutului de superputere mondială şi posibila refacere a URSS), conducerea Federaţiei Ruse a declanşat ample acţiuni de influenţare a populaţiei ucrainene, dar şi a comunităţii internaţionale prin manipulare şi dezinformare. Dezinformarea iniţiată de Moscova a fost susţinută prin decizii în planurile politic, diplomatic, economic, financiar, cultural, informaţional şi militar, decizii difuzate în toată lumea printr-un aparat mediatic foarte dezvoltat şi performant. Acţiunile Kremlinului sunt considerate acţiuni specifice războiului hibrid de majoritatea specialiştilor occidentali şi de organizaţiile euroatlantice.

Dezinformarea iniţiată de Moscova a fost susţinută prin decizii în planurile politic, diplomatic, economic, financiar, cultural, informaţional şi militar, decizii difuzate în toată lumea printr-un aparat mediatic foarte dezvoltat şi performant.

Campania de dezinformare a populaţiei ucrainene, practicată de conducerea Rusiei, a evoluat preponderent ascendent, în planurile amplorii şi al intensităţii, după anul 2000, când la conducerea Federaţiei a venit preşedintele Vladimir Putin. Printre cele mai importante şi ample campanii de dezinformare, desfăşurate până la declanşarea actualei crize din Ucraina, trebuie menţionate cele care au avut ca scop influenţarea alegerilor prezidenţiale din anii 2004 şi 2010.

Dacă, în anul 2004, campania rusă de influenţare a dat câştig de cauză prorusului Viktor Ianukovici, protestele populare, generate de militanţii prooccidentali, au determinat reluarea procesului electoral şi victoria candidatului Iuşcenko[23], omul care a vrut să orienteze ţara spre NATO şi UE şi să determine retragerea forţelor militare ruse din Peninsula Crimeea.

În anul 2010, Viktor Ianukovici a candidat din nou, susţinut de Moscova, şi a câştigat fotoliul de preşedinte al Ucrainei. Din această

[22] Mihail Orzeață, *Ucraina – spațiu de confruntare între Rusia și Occident*, în Eugen Lungu, coordonator, *Federația Rusă și echilibrul de putere în secolul al XXI-lea*, Editura Militară, București, 2019, pp. 95-127.

[23] Malin Ostevik, *Communicating conflict: Russian mediated public diplomacy in relation to the annexation of Crimea*, Universitatea din Oslo, mai 2016, p. 21.

postură, Viktor Ianukovici a semnat prelungirea acordului ruso-ucrainean privind staţionarea forţelor Federaţiei în Crimeea până în anul 2017 şi acordul de împrumut a 15 miliarde de USD din Rusia, la pachet cu acordul de reducere a gazelor naturale ruseşti, livrate Ucrainei. Deşi nu s-au comunicat oficial detaliile negocierilor pentru aceste acorduri, surse neoficiale, dar bine informate au devoalat condiţia Kremlinului ca Ianukovici să nu semneze Acordul de asociere cu UE.

Preşedintele Ianukovici a respectat condiţia impusă de conducerea de la Moscova şi nu a semnat acordul cu UE, dar gestul său a declanşat proteste masive la Kiev şi, apoi, în toată ţara. Protestele au degenerat, în numeroase rânduri, în confruntări violente cu forţele de ordine, fapt ce l-a determinat pe preşedintele Ianukovici să se refugieze în Rusia, în februarie 2014, şi să ceară omologului său rus să intervină militar pentru a salva ţara de forţele nedemocratice.

Pe acest fond de instabilitate politică, violenţe de stradă şi tendinţe spre autoritarism, promovate de forţele de dreapta, conducerea de la Moscova a intensificat campania de dezinformare a populaţiei ucrainene, a comunităţii internaţionale şi a propriei populaţiei şi a obţinut câteva succese notabile, dintre care mai importante sunt:

- anexarea Peninsulei Crimeea (18 martie 2014[24]), fără să tragă niciun foc, dar beneficiind de sprijinul populaţiei de etnie rusă din peninsulă, de acţiunile unor militari fără însemne de apartenenţă, infiltraţi anterior în zonele strategice, şi de mai multe zeci de mii de militari echipaţi pentru luptă, care staţionau la frontiera cu Ucraina pentru a *„preveni infiltrarea unor elemente extremiste în Rusia”*;
- sprijinirea secesiunii regiunilor Lugansk şi Donețk, populate majoritar cu etnici ruşi, autoproclamate republici, sub pretextul existenţei unei intenţii de exterminare (alungare) a ruşilor

În anul 2010, Viktor Ianukovici a candidat din nou, susţinut de Moscova, şi a câştigat fotoliul de preşedinte al Ucrainei. Din această postură, Viktor Ianukovici a semnat prelungirea acordului ruso-ucrainean privind staţionarea forţelor Federaţiei în Crimeea până în anul 2017 şi acordul de împrumut a 15 miliarde de USD din Rusia, la pachet cu acordul de reducere a gazelor naturale ruseşti, livrate Ucrainei.

[24] Ilya Somin, *Russian government agency reveals fraudulent nature of the Crimean referendum results*, în *The Washington Post*, 06.05.2014, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/06/russian-government-agency-reveals-fraudulent-nature-of-the-crimean-referendum-results/, consultat în ianuarie 2020.

din Ucraina, intenţie atribuită fostului prim-ministru ucrainean Iulia Timoşenko[25];

- câştigarea încrederii majorităţii populaţiei de etnie rusă din Ucraina, care s-a pronunţat pentru integrarea republicilor autoproclamate în Federaţia Rusă;
- ascensiunea statutului său în relaţiile internaţionale, statut susţinut şi de celelalte membre ale grupului BRICS (Brazilia, Rusia, India, China, Africa de Sud), dar şi de statele aflate în conflict cu SUA şi cu unele state occidentale;
- încercarea de destabilizare a NATO prin apropierea de Turcia, căreia îi vinde rachete sol-aer de tip S-400, determinând excluderea Ankarei de la programul F-35[26];
- eforturile Federaţiei Ruse de spargere a blocadei economico-financiare, instituită de Uniunea Europeană la adresa sa, s-au concretizat în relaţii economico-financiare bilaterale cu Ungaria, Slovacia, Cehia, Germania şi Bulgaria[27].

Eforturile Federaţiei Ruse de spargere a blocadei economico-financiare, instituită de Uniunea Europeană la adresa sa, s-au concretizat în relaţii economico-financiare bilaterale cu Ungaria, Slovacia, Cehia, Germania şi Bulgaria.

CONCLUZII

Dezinformarea este o metodă de influențare a maselor mari de oameni, în plan declarativ, de personalități politice şi de state, dar folosită destul de des în cadrul unor campanii subversive, menite să conducă, prin orice mijloace, la îndeplinirea unor obiective de mare importanță pentru acestea.

Internetul, prin rețelele de socializare şi mass-media clasice[28], a contribuit foarte mult la creșterea amplorii şi eficienței manipulării

[25] Mark Thompson, *Russian Forces Double Along Ukraine Border*, *Time*, 28.03.2014, http://time.com/41490/russia-ukraine-crimea-putin/, consultat în noiembrie 2019; vezi şi Maria Dejovsky, *News of a Russian arms buildup next to Ukraine is part of propaganda war*, în *The Guardian*, 11.04.2013, http://www.theguardian.com/commentsisfree/2014/apr/11/russian-arms-buildup-ukraine-propaganda-war-nato/, consultat în noiembrie 2019.

[26] Ted Galen Carpenter, *Is It Time to Expel Turkey from NATO?*, The National Interest, https://nationalinterest.org/blog/the-skeptics/it-time-expel-turkey-nato-14518, consultat în septembrie 2019; vezi şi Burak Bekdil, *Turkey: Putin's Ally in NATO?*, Gatestone Institute, 19 martie 2019, https://www.gatestoneinstitute.org/13882/turkey-putin-ally-nato, consultat în septembrie 2019.

[27] Tatia Dolidze, *EU Sanctions Policy towards Russia: The Sanctioner-Sanctionee's game of Throne*, CEPS Working Document, Center for European Policy, nr. 402, pp. 8-9, ianuarie 2015, http://www.ceps.be/system/files/WD%20402%20TD%20Sanctions.pdf, consultat la 10.04.2015.

[28] Sonia Cristina Stan, *Manipularea prin presă*, Editura Humanitas, București, 2004, pp. 35-36.

şi a campaniilor de dezinformare[29]. În ultima perioadă, mass-media, în general, și formatorii de opinie, în special, au jucat un rol important în diseminarea informațiilor false. Astfel, s-a înregistrat o creștere semnificativă a numărului de programe de știri care amplifică narațiunile prefabricate şi pe cele exagerate.

Odată cu dezvoltarea tehnologiilor de inteligență artificială, campaniile de dezinformare au devenit mult mai sofisticate și mai bine organizate, pentru a îndrepta atenția cetățenilor către narațiunile preconcepute, pentru a discredita oponenți politici, precum și pentru a contracara opiniile diferite.

Într-un mediu informațional suprasaturat de informații false, narațiunile preconcepute ce fac apel la prejudecățile personale sunt tot mai accesate. Unii cercetători în domeniu au asociat narațiunile preconcepute cu epidemiile, respectiv răspândirea narațiunilor preconcepute este asemănătoare cu răspândirea virusurilor. Acestea transcend spațiul informațional, trecând de la un sistem cognitiv la altul. Prin urmare, problema nu este încrederea irațională, ci se referă la un aspect mult mai profund, și anume la sistemele de credințe personale care determină deciziile și formează prejudecățile. Astfel, experții susțin că sistemul cognitiv uman percepe lumea înconjurătoare ca fiind divizată în obiecte situate în spațiu și în timp, dar nu este întotdeauna capabil să-i reproducă fidel forma.

Odată cu dezvoltarea tehnologiilor de inteligență artificială, campaniile de dezinformare au devenit mult mai sofisticate și mai bine organizate, pentru a îndrepta atenția cetățenilor către narațiunile preconcepute, pentru a discredita oponenți politici, precum și pentru a contracara opiniile diferite.

Campaniile de dezinformare, desfășurate de Federația Rusă la adresa populației ucrainene şi a comunității internaționale, i-au adus numeroase critici şi sancțiuni internaționale, în principal din partea statelor occidentale, dar acestea au generat şi un curs ascendent al statutului său în arena internațională, statut recunoscut, indirect, de acuzele de influențare a alegerilor prezidențiale din Statele Unite ale Americii. Ascensiunea Federației Ruse în arena internațională este facilitată de creșterea curentelor şi a sentimentelor antiglobalizare, antioccidentale şi antiamericane.

[29] Vladimir Volhov definește televiziunea ca *„paradis al dezinformării"*, într-o lume în care cibernetica este un adevărat Olimp, iar internetul – *„câmpiile alizee"* ale dezinformării, Vladimir Volhov, *Tratat de dezinformare. De la calul troian la internet*, Editura Antet, an și localitate neprecizate, p. 213.

BIBLIOGRAFIE:

1. ***, *Doctrine for Information Operations*, Joint Pub 3-13, February 1998, United States of America.
2. ***, *Time to grab and kill damn Russians – Timoshenko in leaked tape*, Russia Today, 24.03.2014, http://rt.com/news/tymoshenko-calls-destroy-russia-917/.
3. Madeleine Albright, *Who Broke the U.N.*?, *Foreign Policy*, 13.08.2012, http://foreignpolicy.com/2012/08/13/who-broke-the-u-n/.
4. Zygmunt Bauman, *Globalizarea și efectele ei sociale*, Editura Antet, Oradea.
5. Henri Pierre Cathala, *Epoca dezinformării*, Editura Militară, București, 1991.
6. Roberta Cohen, *The Role of Regional Organizations*, ECOWAS, Brookings, Monday, 30 septembrie 2002, https://www.brookings.edu/on-the-record/the-role-of-regional-organizations-ecowas/
7. Ion Dragoman, *Drept internațional umanitar*, Fundația Andrei Șaguna, Constanța, 1999.
8. Călin Hentea, *Noile haine ale propagandei*, Editura Paralela 45, București, 2008.
9. Alexandru Ioan, *Între putere și democrație. Presa în politica internă și internațională*, Editura Centrului Tehnic-Editorial al Armatei, București, 2017.
10. Majid Khadduri, *War and Peace in the Law of Islam*, John Hopkins University Press, Baltimore, 1955, *apud* Dr. Lewis B. Ware, *An Islamic Concept of Conflict in Its Historical Context*, Blank, Stephen J, Grinter, Lawrence E., Magyar, Karl P., and Wheaters, Bynum E., *Conflict, Culture and History*, Air University Press, Maxwell Air Force Base, Alabama, SUA, 1993.
11. Irina Moroianu Zlătescu, *Drepturile omului – un sistem în evoluție*, Institutul Român pentru Drepturile Omului, București, 2017.
12. Mihail Orzeaţă, *Războiul continuu*, Editura Militară, Bucureşti, 2011.
13. Mihail Orzeaţă, *Suntem pregătiţi pentru războiul viitorului?,* în revista *Gândirea Militară Românească*, nr. 4 (octombrie-decembrie), 2016.
14. Mihail Orzeaţă, *Ucraina – spaţiu de confruntare între Rusia şi Occident*, în Eugen Lungu, coordonator, *Federaţia Rusă şi echilibrul de putere în secolul al XXI-lea*, Editura Militară, Bucureşti, 2019.
15. Malin Ostevik, *Communicating conflict: Russian mediated public diplomacy in relation to the annexation of Crimea*, University of Oslo, mai, 2016.
16. Sonia Cristina Stan, *Manipularea prin presă*, Editura Humanitas, Bucureşti, 2004.
17. Ștefan Stanciugelu, *Logica manipulării*, Editura C.H. Beck, București, 2010.
18. Silvia Șpac, *Impactul mass-media asupra formării personalității elevului de vârstă școlară mica*, Studia Universitatis Moldaviae, 2015.
19. Simona Ştefănescu, *Media şi conflictele*, Editura Tritonic, Bucureşti, 2004.
20. Paul Virilio, *Un monde surexposé: fin de l'histoire ou fin de la geographie?, Le monde diplomatique*, august 1997.
21. Vladimir Volhov, *Dezinformarea văzută din Est*, Editura ProEditură și Tipografie, București, 2007.
22. Dennis Whitehead, *The Gleiwitz incident*, *„After Batle Magazine"*, nr. 142, martie 2009, http://en.wikipedia.org/Gleiwitz_incident/.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

PROTECȚIA MEDIULUI ÎN CAZUL CONFLICTELOR ARMATE

Mădălina Virginia ANTONESCU

Doctor în drept european, cercetător științific – Universitatea București

Articolul de față explorează un domeniu de actualitate privind relația dintre mediul înconjurător, dreptul generațiilor viitoare de a beneficia de un mediu curat, sănătos și de o planetă sigură, neafectată de războaie, precum și dreptul omului și al generațiilor viitoare de a trăi într-o lume eliberată de teroare, sărăcie și insecuritate. Pe plan internațional, există unele reglementări privind relația dintre mediu și tehnologiile militare sau cele folosite în scopuri ostile, însă acestea trebuie să fie îmbunătățite și corelate cu recentele dezvoltări privind obligațiile statelor în materia dezvoltării durabile și a protecției mediului. Mediul trebuie protejat nu doar în raport cu dreptul la dezvoltare al popoarelor și statelor, ci și în raport cu existența conflictelor militare și a crizelor de orice tip care implică tehnologii distructive la adresa sa. Apreciem că este un domeniu de interes major în care, pornind de la definiția „mediului manipulat militar", se poate ajunge la elaborarea unor studii de drept comparativ și de securitate privind această relație juridică.

Cuvinte-cheie: dreptul internațional al mediului, Pactul global pentru mediu, Pactul verde european, amenințări de securitate, tehnologii militare.

MEDIUL ÎNCONJURĂTOR, CA ATARE, NU ESTE OBIECTIV MILITAR ȘI NU POATE FI CONSIDERAT ASTFEL

Securitatea mediului este, în secolul XXI, parte a securității naționale, europene-regionale și internaționale. Mediul înconjurător capătă o importanță din ce în ce mai mare în cultura juridică și politică a societăților secolului XXI, datorită provocărilor schimbărilor climatice, intensificării gradului de industrializare, poluării aerului, apelor, deteriorării crescânde a calității solului și subsolului, gradului crescut de schimbare și modificare a ecosistemelor naturale și legăturii globale între toate ecosistemele terestre, aflate într-un echilibru fragil.

Responsabilitatea societăților umane asupra calității vieții pe Terra, asupra prezervării ecosistemelor naturale începe să fie privită ca făcând parte dintr-un concept specific, „securitatea mediului", care devine parte a conceptului de securitate națională, regional-europeană și internațională.

Responsabilitatea societăților umane asupra calității vieții pe Terra, asupra prezervării ecosistemelor naturale începe să fie privită ca făcând parte dintr-un concept specific, *„securitatea mediului"*, care devine parte a conceptului de securitate națională, regional-europeană și internațională.

Oricum am privi conceptul de *„securitate a mediului"*, acesta nu mai este unul izolat, ci unul aflat în strânsă legătură cu termeni până acum clasici în accepțiunea lor (securitatea națională, regională, internațională).

Afectarea calității mediului într-un stat poate crea efecte în alt stat, securitatea mediului trebuind a fi gândită în termeni de *securitate transfrontalieră*, pentru care trebuie concepute mecanisme, strategii, instituții de prevenție și de management al crizelor, al dezastrelor, care afectează mediul.

În contemporaneitate, dezvoltarea tehnologiilor militare nu trebuie să afecteze mediul înconjurător, pe măsură ce le este crescut gradul de *„inteligență"* (lovitura de mare precizie). Atât în strategiile, cât și în tacticile militare, protecția mediului înconjurător ar trebui să fie avută în vedere ca o formă de responsabilizare pentru a transmite patrimoniul natural al planetei către generațiile viitoare.

Gradul crescut de tehnologizare și de inteligență artificială în natura armamentelor militare și în modul de a concepe și de a purta războaie în secolul XXI trebuie să plece de la premisa obligatorie a protecției mediului înconjurător, de la definirea lui ca nefiind obiectiv militar, de la obligația generațiilor prezente, oricare ar fi diferendele dintre ele, de a transmite o planetă sănătoasă și bogată în ecosisteme naturale funcționabile și sănătoase, o calitate a vieții crescută, generațiilor viitoare.

Cu alte cuvinte, gradul crescut de tehnologizare și de *inteligență artificială (Artificial Intelligence/AI)* în natura armamentelor militare și în modul de a concepe și de a purta războaie în secolul XXI trebuie să plece de la premisa obligatorie a *protecției mediului înconjurător*, de la *definirea lui ca nefiind obiectiv militar, de la obligația generațiilor prezente*, oricare ar fi diferendele dintre ele, *de a transmite o planetă sănătoasă și bogată în ecosisteme naturale funcționabile și sănătoase, o calitate a vieții crescută, generațiilor viitoare.*

Dreptul generațiilor viitoare la un mediu sănătos[1], la o înaltă calitate a vieții începe deja să devină un drept *fundamental* al omului, dar și al *umanității* (alt concept juridic aflat în atenția juriștilor secolului XXI).

Astăzi, putem spune că asistăm, din nou, *la o cursă a înarmărilor*, datorită unui mod specific de a privi lumea internațională, la un salt tehnologic în materia tipurilor de armamente, dublat atât de *ineficacitatea reglementărilor de dezarmare* a statelor, cât și de *practica recentă a retragerii statelor importante din acorduri internaționale.*

Prin însăși existența lor, tipurile și cantitățile de armament deținute azi de state constituie *amenințări directe și grave la adresa planetei, a ecosistemelor naturale, a mediului înconjurător din orice stat*, consideră doctrina[2]. Existența acestor stocuri de armamente cu potențial de distrugere pe scară întinsă a mediului inconjurător, laolaltă cu așezările urbane vizate sau cu obiectivele vizate, constituie factori de dezechilibre ecologice, după cum a remarcat doctrina, deja[3].

Dreptul internațional al mediului a fost influențat de relația mediu-conflicte armate, trebuind să reglementeze conceptul juridic de *„mediu manipulat militar”*. Astfel, definiția *„mediului manipulat militar”* privește acel tip de mediu *„a cărui compoziție, structură și dinamică este perturbată de utilizarea mijloacelor și metodelor de război, inclusiv a tehnicilor de manipulare a mediului”*[4]. Prin urmare, doctrina folosește o definiție actualizată asupra acestui concept, introducând în cadrul tehnologiilor militare de intervenție violentă

[1] Vezi https://www.un.org/en/universal-declaration-human-rights/, consultat la 18 februarie 2020.
[2] Daniela Marinescu, *Tratat de dreptul mediului*, ediția a IV-a, Editura Universul Juridic, București, 2010, pp. 600-601.
[3] *Ibidem*.
[4] *Ibidem.*

asupra mediului (conflicte armate, războaie) *și tehnicile militare (sau folosite în scop militar) de perturbare a mediului.* În această concepție a doctrinei juridice din materie se includ și *sistemele de influențare sau perturbare a climei sau a vremii* (așa-numitele tehnologii militare din cadrul războiului climatologic)[5].

„Mediul manipulat militar” este un concept care promite să se dezvolte în secolul XXI, pe măsura avansului tehnologiilor militare și civile și a capacității acestora de a fi folosite de actori statali sau non-statali (rețele teroriste, organizații etc.) în războaie, conflicte armate, crize ori pentru provocarea, extinderea unor astfel de crize.

„Mediul manipulat militar” poate suporta intervenția tehnicilor militare sau civile în caz de conflicte armate, dar și de crize locale, regionale de tot felul, *cu implicarea unor actori non-statali sau supra-statali* (miliții, forțe de securitate, trupe paramilitare, trupe ale unor generali rivali în statele colapsate sau cu autoritate în disoluție etc.).

„Mediul manipulat militar” poate suporta nu doar intervenția unor categorii recunoscute de dreptul internațional public (popoarele care luptă pentru independență, beligeranții, forțele militare reprezentând state sau alianțe de state), ci și intervenția (non-autorizată, non-legitimată din punctul de vedere al dreptului internațional public) *a actorilor non-statali* (rețele teroriste, grupări religioase înarmate etc.).

Nu ar trebui însă, în opinia noastră, să considerăm că, devreme ce un actor are calitatea de subiect de drept internațional public, acesta ar avea și *„legitimitatea”* de a distruge mediul înconjurător prin tehnicile sale și tehnologiile militare sau pe cele folosite în scopuri militare.

Mediul înconjurător nu trebuie să devină și nici să fie tratat ca obiectiv militar, deoarece el reprezintă elementul esențial pentru supraviețuirea speciei umane, fiind compus din ansamblul de ecosisteme unice, dependente unele de altele și dispuse la nivel global într-un mod interconectat. Cu alte cuvinte, *responsabilitatea statelor* în secolul XXI, care se dorește un secol al avansului tehnicii și tehnologiilor și al științei (inclusiv în domeniul militar și asupra conceptului de război sau conflict militar), trebuie să conțină, din punct de vedere juridic și politic, la nivel *național, regional și global*, o răspundere *directă* privind mediul.

„Mediul manipulat militar” poate suporta nu doar intervenția unor categorii recunoscute de dreptul internațional public (popoarele care luptă pentru independență, beligeranții, forțele militare reprezentând state sau alianțe de state), ci și intervenția (non-autorizată, non-legitimată din punctul de vedere al dreptului internațional public) a actorilor non-statali (rețele teroriste, grupări religioase înarmate etc.).

[5] *Ibidem*, p. 601.

Statul, într-o ordine westphaliană, continuă să rămână principalul actor și subiect de drept internațional al mediului care își va asuma răspunderea pentru intervenția violentă asupra mediului (în caz de conflicte armate, de război sau de orice acțiune teroristă sau a altor grupări non-statale sau cvasi-statale) și care răspunde pentru că a permis sau nu a împiedicat intervenția sau nu a restaurat mediul afectat de o astfel de intervenție.

Statele ar trebui să își asume în mod expres, prin legislație internă, prin cea regională (europeană, de exemplu), dar și internațională, obligația *de a descuraja* orice acțiune a vreunui alt actor statal sau non-statal în a deteriora sau a afecta, prin tehnici și tehnologii militare sau civile folosite în scop militar, *calitatea și însăși existența* ecosistemelor *de pe teritoriul lor* și asupra cărora ele își angajează responsabilitatea potrivit principiilor și normelor de drept internațional și național al mediului.

Suveranitatea statului implică și suveranitatea sa asupra teritoriului său, asupra tuturor ecosistemelor naturale și artificiale din limitele jurisdicției sale.

Statul, prin urmare, într-o ordine westphaliană, continuă să rămână *principalul actor și subiect de drept internațional al mediului care își va asuma răspunderea pentru intervenția violentă asupra mediului* (în caz de conflicte armate, de război sau de orice acțiune teroristă sau a altor grupări non-statale sau cvasi-statale) și care răspunde pentru că a permis sau nu a împiedicat intervenția sau nu a restaurat mediul afectat de o astfel de intervenție.

De asemenea, o legislație regională sau internațională adaptată secolului XXI ca secol al interpendențelor globale (în care, dacă un ecosistem dintr-o regiune este afectat prin intervenție armată de orice fel, se creează efecte dăunătoare asupra calității vieții și mediului în alte state sau regiuni) ar trebui să prevadă *obligații întărite de solidaritate a statelor* pe plan regional și internațional și *mecanisme, proceduri colective clare de activat în asemenea cazuri*, în care intervențiile militare de orice fel produc dezastre sau efecte grave asupra mediului dintr-o țară sau o anumită regiune.

În secolul XXI, datorită creșterii gradului distructiv al tehnologiilor și tehnicilor militare, trebuie *să crească în mod corespunzător și gradul de răspundere juridică al statelor* pentru distrugerea sau nerepararea mediului manipulat militar.

Am spune chiar că, în secolul schimbărilor climatice, când deja se vorbește de războaie climatice, pe măsura avansului tehnologic militar al statelor, conceptul de *„mediu manipulat militar”* devine unul extrem de important pentru a asigura garanții juridice și politice pentru pacea planetei și dreptul generațiilor prezente și viitoare la pace, la o înaltă calitate a vieții.

Până în prezent, în dreptul internațional al mediului se consideră că există consacrate *două principii generale* (însă, acesta este un domeniu care se cere *în permanență adaptat și îmbunătățit*). Primul principiu are în vedere obligațiile fiecărui stat (fiind deci limitat la sfera actorilor statali, deși intervenții de tip militar, indiferent de denumire, pot fi realizate și de actorii non-statali) *de a nu cauza pagube mediului dincolo de competența sa teritorială*. Beligeranții nu sunt exonerați de această obligație, aceștia fiind supuși răspunderii pentru pagube transfrontaliere cauzate mediului natural[6]. Dar, poate exista o obligație juridică în viitor, pentru beligeranți, să își angajeze răspunderea și în caz de prejudicii la nivel transfrontalier sau infra-local cauzate *mediului artificial* (așezări urbane, sate) sau *mediului mixt* (părți de mediu natural integrate în mediul urban sau rural), precum cele de la periferiile marilor orașe sau din orice spațiu care înconjoară un grup sau o așezare urbană sau rurală. Aceasta ar fi o *extindere a obligațiilor de răspundere juridică în cazul beligeranților*, care s-ar aplica îndeosebi statelor (deci, nu doar în cazul *mediului natural* afectat de tehnologii militare).

În dreptul internațional al mediului se consideră că există consacrate două principii generale. Primul principiu are în vedere obligațiile fiecărui stat de a nu cauza pagube mediului dincolo de competența sa teritorială. Al doilea principiu privește obligația statelor de a respecta mediul, în general.

Al doilea principiu privește *obligația statelor de a respecta mediul, în general*. După cum vedem, este vorba tot de un principiu privind *statele,* deci de unul limitat, în vreme ce, în mod real, se pot cauza mediului afectări sau distrugeri ireparabile chiar, prin manipulare militară nu doar din partea statelor, *ci și a actorilor non-statali sau cvasi-statali*.

Acest al doilea principiu privește obligațiile statelor de a respecta mediul și de a nu-l deteriora în afara jurisdicțiilor lor, de pildă în zonele mării libere, pe fundul mărilor și oceanelor, în spațiile de interes comun al umanității, precum Luna, Cosmosul, marea liberă, Antarctica sau corpurile cerești[7].

În alte documente internaționale adoptate sub egida ONU, de pildă în Carta Mondială a Naturii[8], sunt prevăzute principii obligatoriu de respectat *pentru state*, conectate la principiul dezvoltării durabile. Aceste principii, așa cum sunt înscrise în această Cartă, document important pentru definirea ordinii juridice a secolului XXI ca o ordine

[6] Daniela Marinescu, *op. cit.*, p. 601.
[7] *Ibidem*, p. 601.
[8] Vezi https://www.refworld.org/docid/3b00f22a10.html, consultat la 12 februarie 2020.

juridică întemeiată pe responsabilitatea statelor față de mediu și pe obligatoria raportare a politicilor lor de dezvoltare la cerința protejării mediului, sunt:

- principiul respectului față de natură și față de procesele sale naturale, statele fiind obligate în mod expres să nu le afecteze ori să le împiedice (deci, inclusiv o obligație juridică aplicabilă în cazul conflictelor armate sau al crizelor ce implică, indiferent de denumirea și tipul lor, tehnologii militare sau civile folosite în scop militar sau cu impact violent asupra mediului);
- principiul conservării biodiversității și al habitatelor necesare păstrării biodiversității, principiul gestionării sau folosirii ecosistemelor și organismelor, a resurselor uscatului, marine și atmosferice din perspectiva respectării sustenabilității, a respectării integrității unor astfel de ecosisteme sau specii;
- principiul conservării tuturor ariilor Pământului, uscat și apă, cu o protecție specială acordată ariilor unicat și speciilor rare sau primejduite[9].

În Carta Mondială a Naturii apare, în mod expres precizat, principiul protejării naturii împotriva degradărilor cauzate de războaie sau de alte activități ostile.

În Carta Mondială a Naturii apare, *în mod expres precizat, referitor la tema de față, principiul protejării naturii împotriva degradărilor cauzate de războaie sau de alte activități ostile.*

Statele au, prin pct. 21 din Cartă, și obligații juridice, și anume pe acelea de:

- a coopera pentru conservarea naturii, prin activități comune, consultări, schimb de informații;
- a stabili standarde pentru produse și procese de manufactură care *pot produce efecte adverse asupra naturii*;
- a implementa prevederile legale internaționale privind protecția și conservarea mediului înconjurător;
- a se asigura că *activitățile din jurisdicția lor sau de sub controlul lor* nu vor produce pagube sistemelor naturale localizate *în alte state sau în arii de dincolo* de jurisdicția națională;
- a proteja, salva și conserva natura *în ariile de dincolo de* jurisdicția lor națională. Acest punct din Cartă *extinde sfera de responsabilitate juridică nu doar la state, ci și la organizații*

[9] *Ibidem.*

internaționale, care apar precizate în mod expres pentru îndeplinirea obligațiilor de mai sus.

Art. 5 din Carta Mondială a Naturii, în mod expres, se referă la principiul potrivit căruia natura va fi apărată de degradările cauzate de războaie sau de alte acte ostile, iar art. 20 impune statelor ca *activitățile militare care pot produce prejudicii naturii să fie evitate*[10]. Aceste două prevederi sunt *formulate în mod imperativ la adresa statelor* care sunt subiecte de drept internațional. În consecință, *statele trebuie să garanteze* o protecție a mediului în caz de acte ostile sau război, *înlăturând aceste pericole și degradări* care pot fi provocate sau despre care au indicii clare că vor fi provocate indirect sau direct prin acțiunea unor actori non-statali. Această *extensie juridică la cele două principii*, cu privire la răspunderea statelor pentru degradările provocate sau care pot fi provocate de actorii non-statali, cvasi-statali (din regiunile unde autoritatea statelor este slăbită sau în disoluție sau nu mai există), *este una necesară*, considerăm noi, și *ea ar trebui consacrată rapid* în documente regionale și internaționale de protecție adecvată a mediului, de la nivel regional și internațional.

Art. 5 din Carta Mondială a Naturii, în mod expres, se referă la principiul potrivit căruia natura va fi apărată de degradările cauzate de războaie sau de alte acte ostile, iar art. 20 impune statelor ca activitățile militare care pot produce prejudicii naturii să fie evitate.

De asemenea, noi considerăm că s-ar impune *și o aplicare a principiului bunei-vecinătăți și a solidarității regionale a statelor,* în cazul în care un stat este în disoluție sau are o autoritate slabă sau contestată de actorii non-statali care acționează pe teritoriul său (cazul Siriei, Libiei, Irakului, Yemenului), în care se impune fie o răspundere colectivă a statelor participante la conflictul militar de pe acel teritoriu, fie a statelor vecine, fie al comunității internaționale în ansamblu, pentru refacerea, protejarea mediului afectat pe acel teritoriu, de activitățile militare.

Cazul teritoriilor aflate în stare de disoluție sau cu autoritate slabă sau un stat care nu poate controla părți din teritoriul său, fiind într-un conflict armat în care sunt implicate și state, dar și actori non-statali (grupări paramilitare, teroriste, rebeli, miliții etc.), trebuie să impună *urgent o reglementare juridică de protecție a mediului manipulat militar în asemenea cazuri*, atât la nivel regional, cât și internațional, impunând răspunderea directă pentru calitatea mediului a statelor

[10] Daniela Marinescu, *op. cit.*, p. 601.

participante la acel conflict armat, precum și răspunderea statelor participante pentru intervențiile militare ale grupărilor non-statale.

O asemenea răspundere ar trebui să intervină și în cazul protejării și restaurării obiectelor sau așezărilor reprezentând *patrimoniu cultural* de pe teritoriul statelor afectate de conflicte armate.

„Mediul manipulat militar”, în accepțiunea largă, așa cum ar trebui să fie consacrat într-o viitoare convenție internațională, *ar trebui să cuprindă nu doar mediul natural propriu-zis, ci și mediul artificial (urban), mixt (împrejurimile unei așezări, periferia, zonele limitrofe), dar și mediul cultural (obiective turistice, istorice, culturale de tot felul).* Aceste tipuri de medii trebuie să fie protejate de intervenții militare, ferite de distrugere, iar o legislație sancționatorie la nivel național, regional și internațional ar trebui să fie adoptată pentru protejarea sa, indiferent de tipul de mediu.

„Mediul manipulat militar”, în accepțiunea largă, așa cum ar trebui să fie consacrat într-o viitoare convenție internațională, ar trebui să cuprindă nu doar mediul natural propriu-zis, ci și mediul artificial (urban), mixt (împrejurimile unei așezări, periferia, zonele limitrofe), dar și mediul cultural (obiective turistice, istorice, culturale).

De asemenea, mai trebuie menționată și *Convenția privind interzicerea utilizării în scopuri militare sau oricare alte scopuri ostile a tehnicilor de modificare a mediului înconjurător (ENMOD*), adoptată de Adunarea Generală a ONU în 10 decembrie 1976 și intrată în vigoare în 5 octombrie 1978[11]. România a semnat această convenție la 18 mai 1977 și a ratificat-o prin decretul nr. 100 din 28 martie 1983. Acest instrument juridic internațional are valabilitate nelimitată și se convertește, în opinia noastră, într-un cadru legal preliminar și obligatoriu nu doar pentru state, ci care trebuie extins și la actorii non-statali, pentru a asigura o protecție adecvată mediului în secolul XXI. Amintim aici și faptul că textul Convenției stabilește un Comitet Consultativ de experți, ce poate fi convocat ad-hoc la solicitarea statelor părți. Competența acestui Comitet este de a oferi consultări oficiale privind diferende posibile și a determina exact natura activităților cu privire la care sunt suspiciuni că ar fi încălcat Convenția[12]. Alte dispoziții din Convenție se referă la modalitatea de întrunire a delegaților statelor părți în conferințe periodice de re-examinare a funcționării Comisiei. În acest context, trebuie remarcat că și SUA sunt parte a Convenției,

[11] Vezi file:///C:/1976-enmod-icrc-factsheet.pdf, https://www.unog.ch/enmod, consultat la 12 februarie 2020.

[12] Adrian Năstase, *Documenta universales I, Documente fundamentale ale dreptului internațional contemporan și ale relațiilor internaționale,* ediție îngrijită de Roxana Frailich, Asociația Română pentru Educație Democratică, Regia Autonomă Monitorul Oficial, București, 1997, p. 408.

președintele ratificând Convenția la 13 decembrie 1997 și aceasta intrând în vigoare pentru SUA la 17 ianuarie 1980, când s-a depus, la New York, instrumentul de ratificare[13].

Această Convenție are o importanță esențială pentru relația dintre mediu și activitățile militare, fiind *interzise folosirea de metode noi sau de mijloace de luptă destinate să producă sau despre care se poate prevedea că pot produce efecte dăunătoare larg răspândite, de lungă durată* în privința mediului.

Prin Convenție *mai sunt interzise și tehnicile cu efecte larg răspândite, de lungă durată sau grave asupra mediului.* Este apreciată că *însăși existența* unor tehnici noi, de natură să aducă atingere sau modificări în scop militar mediului, poate fi începutul unor dezastre serioase, dacă procesul va lua amploare[14], după cum se arată în Convenție.

Convenția *definește tehnicile de modificare a mediului* ca *„alterând – laolaltă cu modificările deliberate ale proceselor naturale – dinamica, compoziția, structura aerului, incluzând biosfera, atmosfera, litosfera, hidrosfera sau spațiul cosmic, prin producerea de cutremure, avalanșe, alunecări de terenuri etc.”*[15].

Convenția are o importanță esențială pentru relația dintre mediu și activitățile militare, fiind interzise folosirea de metode noi sau de mijloace de luptă destinate să producă sau despre care se poate prevedea că pot produce efecte dăunătoare larg răspândite, de lungă durată în privința mediului.

Convenția consideră ca exemple ale efectelor negative ce ar putea rezulta în urma folosirii tehnicilor de modificare a mediului următoarele: schimbările climatice sau ale agenților climatici, răsturnările echilibrului ecologic, schimbările curenților oceanici, schimbările aduse stratului de ozon sau ale ionosferei.

Pentru vremea la care a fost semnată și ratificată (anii ‘70-’80), Convenția prezintă o neașteptată valoare inovatoare într-un domeniu care avea, decenii mai târziu, până în prezent, să fie considerat ca unul vital pentru supraviețuirea speciei umane și a planetei înseși.

Astăzi, schimbările climatice generează ample și profunde dezbateri între diferite viziuni ale statelor, pro și contra abandonării tehnologiilor și economiilor cu potențial disturbator pe scară largă sau deosebit de intens (ca urmare a gradului de industrializare, agriculturii chimice, defrișărilor masive etc.) la adresa mediului. Între schimbările

[13] *Ibidem*, p. 409.

[14] Vezi file:///C:/1976-enmod-icrc-factsheet.pdf, https://www.unog.ch/enmod, consultat la 12 februarie 2020.

[15] *Ibidem.*

climatice și intervenția umană (aici, a statului, a companiilor, în special) și capacitatea mediului de a se regenera există o legătură strânsă. Convenția se referă expres, în preambulul său, la *Declarația Conferinței Națiunilor Unite privind mediul înconjurător*, de la Stockholm, din 16 iunie 1972, și recomandă utilizarea în *scopuri pașnice* a tehnicilor de modificare a mediului, amintind, în mod expres, *de dreptul generațiilor prezente și viitoare de a beneficia de un mediu conservat și îmbunătățit.*

Convenția (63 de state fiind state părți la ea) recunoaște efectele extrem de dăunătoare pe care le are asupra mediului utilizarea unor astfel de tehnici în scopuri militare sau în oricare alte scopuri ostile (deci, definiție largă, care include *orice acțiune cu caracter ostil mediului, nu doar a celor militare* de manipulare a mediului).

Art. 1 din Convenție introduce în sarcina statelor părți obligația de a nu angaja în utilizarea în scopuri militare sau în oricare alte scopuri ostile tehnici de modificare a mediului, cu efecte larg răspândite, de lungă durată sau grave, ca mijloace provocând distrugeri, daune sau prejudicii altor state părți.

Art. 1 din Convenție introduce în sarcina statelor părți *obligația de a nu angaja* în utilizarea în scopuri militare sau în oricare alte scopuri ostile tehnici de modificare a mediului, cu efecte larg răspândite, de lungă durată sau grave, ca mijloace provocând distrugeri, daune sau prejudicii *altor state părți*. În alineatul 2, o asemenea prevedere prohibitivă a statelor părți se extinde *și la relațiile acestora cu terții* (alte state, un grup de state sau organizații internaționale), statele părți angajându-se *să nu acorde asistență, să nu încurajeze, să nu incite* alte state, grupuri de state sau organizații internaționale la angajarea unor activități contrare alin. 1. Aceasta este o prevedere cu *aplicabilitate largă și extrem de importantă*, care pleacă de la interdicția fixată în sarcina statelor părți de *a prezerva mediul și a nu-l folosi în scopuri militare sau în oricare alte scopuri ostile, nu doar în raporturile dintre ele, dar și cu terții, indiferent că sunt state, grupuri de state (alianțe, coaliții, federații) sau organizații internaționale.* Alte categorii (actori non-statali) care au proliferat în ultimele două decenii în plan infra-local, regional și chiar global nu sunt cuprinse în această Convenție, dar *textul poate fi extins și îmbunătățit*.

Art. IV obligă statele părți să ia orice măsură considerată necesară de a interzice sau a preveni orice activitate *ce contravine acestei Convenții*, în orice loc aflat sub jurisdicția sau sub controlul său.

De asemenea, potrivit art. 5 din Convenție, statele părți sunt obligate *să coopereze și să se consulte reciproc între ele,* pentru a rezolva orice problemă ar putea apărea în legătură cu obiectivele

acestei Convenții sau cu aplicarea ei. Sunt încurajate inclusiv activități de cooperare în cadrul ONU și al organizațiilor sale.

Dacă un stat parte consideră că orice alt stat parte își încalcă obligațiile decurgând din această Convenție, el poate depune o plângere la Consiliul de Securitate al ONU ce are în competență a investiga, conform Cartei ONU, faptele rezultând din plângerea primită de Consiliu. În cazul în care Consiliul de Securitate al ONU decide că partea respectivă a fost vătămată sau riscă să suporte o vătămare ca efect al încălcării acestei Convenții, fiecare stat parte este obligat să acorde asistență sau sprijin cu privire la oricare parte a Convenției care solicită aceasta. Articolul VI introduce *o posibilitate juridică de a lărgi conținutul Convenției, prin depunerea de amendamente de către statele părți*.

DOCUMENTE PE PLAN INTERNAȚIONAL ȘI EUROPEAN PRIVIND RELAȚIA DINTRE MEDIU ȘI AMENINȚĂRILE LA ADRESA SECURITĂȚII

Documentele recent adoptate sub egida ONU se referă în mod repetat la dreptul omului la un mediu sănătos și echilibrat, la dreptul popoarelor și al generațiilor viitoare la o înaltă calitate a vieții, care nu poate fi obținută (la fel ca și dreptul la dezvoltare durabilă, un alt drept fundamental al celei mai recente categorii de drepturi ale omului și ale popoarelor, din ultimele decenii) decât cu condiția prezervării, respectării și îmbunătățirii calității mediului. Printre aceste documente (***care au incidență juridică asupra relației dintre mediu și conflictele armate***, introducând *obligații indirecte* în sarcina statelor cu privire la protecția mediului, inclusiv din prisma folosirii asupra mediului a tehnologiilor în scopuri militare sau în scopuri ostile), putem enumera: rezoluția AG ONU privind Armonia cu Natura (A/RES/67/214); raportul Secretarului General privind Armonia cu Natura (A/67/317); Raportul Secretarului General privind Armonia cu Natura (A/66/302); Rezoluția AG ONU privind Armonia cu Natura (A/RES/65/164); Rezoluția AG ONU privind Armonia cu Natura (A/RES/64/196); Studiul privind nevoia de a recunoaște și respecta drepturile Mamei Pământ (E/C/2010/4); Rezoluția AG ONU privind Ziua Internațională a Mamei Pământ (A/RES/63/278); Rezoluția AG ONU privind Anul Internațional al Planetei

Documentele recent adoptate sub egida ONU se referă în mod repetat la dreptul omului la un mediu sănătos și echilibrat, la dreptul popoarelor și al generațiilor viitoare la o înaltă calitate a vieții, care nu poate fi obținută decât cu condiția prezervării, respectării și îmbunătățirii calității mediului.

Pământ, 2008 (A/RES/60/192), completate cu Agenda 21 sau cu documente elaborate sub egida ECOSOC[16].

În ceea ce privește relația dintre utilizarea tehnologiilor în scopuri militare sau în alte scopuri ostile și impactul lor asupra mediului, trebuie amintit și un alt document internațional, anume *Declarația de la Johannesburg privind Dezvoltarea Durabilă*, din 4 septembrie 2002[17]. Aceasta a fost adoptată în urma Summitului Mondial privind Dezvoltarea Durabilă din Africa de Sud (2-4 septembrie 2002), recunoscându-se *responsabilitatea generațiilor prezente pentru gradul de civilizație și de bunăstare al generațiilor viitoare, dar și pentru calitatea vieții pe planeta Pământ* (statele părți asumându-și anumite obligații privind prezervarea ecosistemelor terestre). Pct. 13 (provocări globale referitoare la mediu) enumeră și degradarea continuă a mediului înconjurător global, prin pierderi continue de biodiversitate, prin *efecte adverse ale schimbărilor climatice (care pot fi produse inclusiv prin tehnologii folosite în scopuri militare sau în alte scopuri ostile mediului și societăților umane)*.

Conform rezoluției adoptate de AG ONU în 22 aprilie 2009, care stabilește Ziua Internațională a Planetei Pământ ca fiind în fiecare an în ziua de 22 aprilie, se recomandă statelor membre ale ONU să adopte în politicile lor „o relație de armonie cu natura și cu Pământul, spre a atinge un echilibru just între nevoile economice, sociale și de mediu ale generațiilor prezente și cele ale generațiilor viitoare”.

Conform rezoluției adoptate de AG ONU (A/RES/63/278) în 22 aprilie 2009, care stabilește Ziua Internațională a Planetei Pământ ca fiind în fiecare an în ziua de 22 aprilie[18], se recomandă statelor membre ale ONU să adopte în politicile lor *„o relație de armonie cu natura și cu Pământul, spre a atinge un echilibru just între nevoile economice, sociale și de mediu ale generațiilor prezente și cele ale generațiilor viitoare”*[19].

Dreptul generațiilor viitoare la un mediu înconjurător curat, sănătos este prevăzut și în alt document internațional, precum *„Agenda 2030”*, adoptată de Adunarea Generală a ONU prin rezoluția din 25 septembrie 2015, nr. 70/1, intitulată *„Transforming our world: the 2030 Agenda for Sustainable Development”* (A/RES/70/1), distribuită în 21 octombrie 2015[20]. Statele părți s-au angajat să transmită ***către generațiile viitoare bunuri și drepturi care trebuie asigurate și garantate în raport cu relația dintre tehnologiile militare și folosirea lor în scopul de a manipula mediul sau în scopuri militare sau ostile care afectează sau pot afecta pe scară largă, de o manieră gravă, mediul.*** Asemenea drepturi sunt: dreptul omului, al popoarelor, al societății umane, în ansamblul său, la un *mediu înconjurător global curat și sănătos*; dreptul omului, al popoarelor, *la un climat internațional de pace și securitate*; dreptul omului, al popoarelor de a trăi pe o *planetă curată, sigură, bogată în resurse*; dreptul omului, al popoarelor *de a trăi o viață eliberată de teamă, teroare, mizerie și indecență ocazionată de sărăcie și de încălcarea drepturilor omului*.

[16] Vezi http://www.un.org/en/events/motherearthday/documents.shtml, consultat la 7 septembrie 2016.

[17] *Johannesburg Declaration on Sustainable Development*, 4 septembrie 2002, https://ec.europa.eu/environment/archives/wssd/documents/wssd_pol_declaration.pdf, consultat la 7 septembrie 2016.

[18] *Chronology of Harmony with Nature*, www.harmonywithnatureun.org/chronology.html, consultat la 7 septembrie 2016.

[19] *Ibidem.*

[20] Vezi https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf, consultat la 7 septembrie 2016.

Prin documentul intitulat „Agenda 2030”, dreptul generațiilor viitoare referitoare la mediu este prevăzut în mod expres. Acestea au beneficiul privind: dreptul la dezvoltare; dreptul la un mediu viitor global caracterizat prin pace și siguranță; dreptul la a trăi într-o lume viitoare eliberată de grijă, frică, mizerie și nevoi; dreptul la a trăi într-o lume viitoare fără sărăcie; dreptul de a se bucura de un mediu înconjurător curat, nepoluat și bogat în resurse; dreptul de a trăi pe o planetă sigură și curată.

În mod expres, Preambulul *„Agendei 2030”* prevede obligația statelor părți de a respecta și de a urmări în politicile lor și în cooperarea multilaterală sau bilaterală *anumite obiective care au directă legătură cu relația mediu-conflicte armate.* Dintre acestea, reținem *„dimensiunea pace”* (presupunând crearea unor societăți tolerante, incluzive, pașnice și juste, eliberate de violență și teamă; conexiunea dintre dezvoltarea durabilă și pace). Punctul 14 din Agendă este legat de problematica sub-dezvoltării, de dezastre naturale, de *amenințările la adresa sănătății globale, de conflicte, de extremisme violente, de terorism și crize umanitare ori de deplasări forțate de persoane*. *„Agenda 2030”* obligă statele părți să acționeze în direcția: ***soluționării și prevenirii conflictelor, a susținerii refacerii post-conflict a țărilor***, precum și a asigurării că femeile sunt implicate în mod real ***în procesele de construcție a păcii și de creare a statului.*** Statele părți mai au și obligația de *a-și conforma acțiunea cu dreptul internațional*, în sensul respectării dreptului la dezvoltare al popoarelor și al dreptului la autodeterminare.

Considerăm că, în ceea ce privește conținutul juridic al unor viitoare convenții internaționale ulterioare *„Agendei 2030”*, s-ar recomanda:

- să se prevadă obligații juridice întărite ale statelor *privind păstrarea păcii și a securității internaționale*. Această obligație ar trebui însoțită de *răspunderi clare* (conform principiului din dreptul mediului *„poluatorul plătește”* și unde folosirea tehnologiilor militare sau civile în scopuri militare sau ostile, care au produs sau sunt susceptibile să producă impact negativ, grav, de lungă durată asupra mediului sau să îl distrugă iremediabil, *să fie considerată drept „acțiune distructivă asupra mediului”*, antrenand obligații ale actorului de dezdăunare, precum și alte acțiuni concrete de restabilire a ecosistemelor afectate prin aplicațiile militare, prin agresiunile armate, prin impactul distructiv al războiului asupra mediului înconjurător);
- *statele care pornesc acțiuni armate de distrugere și atacare a altor națiuni* ar trebui supuse unui regim juridic consolidat privind răspunderea față de distrugerea mediului ca urmare a acțiunilor lor agresive armate sau cu componentă militară.

Principiile stabilite prin Declarația de la Rio (Conferința Pământului) sunt: dreptul tuturor popoarelor la o viață sănătoasă, productivă, în armonie cu natura; dreptul suveran al națiunilor de a-și exploata liber resursele proprii, fără a provoca prin aceasta daune transfrontaliere mediului; principiul poluatorul plătește; obligația națiunilor de a adopta legi eficiente cu privire la mediu etc.

Cu privire la relația dintre mediu și obligația statelor de a-l folosi în mod pașnic, non-distructiv, de a nu-l supune degradării sau distrugerii iremediabile ca urmare a unei acțiuni militare, putem menționa și principiile stabilite prin Declarația de la Rio[21], adoptată în urma Conferinței de la Rio din 3-12 iunie 1992, numită și Conferința Pământului (Earth Summit): dreptul tuturor popoarelor la o viață sănătoasă, productivă, în armonie cu natura; dreptul suveran al națiunilor de a-și exploata liber resursele proprii, *fără a provoca prin aceasta daune transfrontaliere mediului;* principiul *poluatorul plătește; obligația națiunilor de a adopta legi eficiente cu privire la mediu etc.*[22]. Conform principiului 24 din Declarația de la Rio, se consideră că *războiul exercită intrinsec o acțiune distructivă asupra dezvoltării durabile*, de unde obligația expresă a statelor de a se conforma normelor de drept internațional privind protecția mediului în timp de conflict armat și de a participa la dezvoltarea acestui drept, dacă este nevoie[23].

[21] Vezi https://www.cbd.int/doc/ref/rio-declaration.shtml, consultat la 7 septembrie 2016.
[22] Daniela Marinescu, *op. cit.*, pp. 18-19.
[23] *Ibidem*, p. 601.

Acest principiu, practic, caracterizează juridic *mediul ca un „bun civil”,* statele trebuind să renunțe la atacarea și afectarea/distrugerea mediului în caz de conflict armat sau pentru atacarea unui obiectiv militar, dacă distrugerile cauzate sau susceptibil a fi cauzate mediului ar fi mai mari decât cele ale obiectivului vizat[24]. Doctrina amintește, în acest context, rezoluția AG ONU 43/37, din 9 februarie 1993, intitulată *Protecția mediului în timp de conflict armat*[25]. În această rezoluție, AG ONU consideră că distrugerea nejustificată a mediului în raport cu necesitățile militare, precum și cea având un caracter gratuit sunt în mod vădit contrare dreptului internațional în vigoare (paragr. 32). Avizul Curții Internaționale de Justiție (solicitat de AG ONU prin rezoluția 49/75 K din 1994), care citează în jurisprudența sa această rezoluție, cu privire la relația dintre mediu și conflictele armate, consideră implicit ca având *caracter ilegal amenințarea sau folosirea armelor nucleare* (care cauzează distrugeri grave, de lungă durată sau ireparabile, mediului).

Un alt document internațional important este și *Declarația Mileniului*, adoptată în urma Summitului Mondial din 2000[26], document în care, la pct. 4 și 6, apare și *obiectivul protecției și prezervării mediului înconjurător* (exprimat prin *valoarea respectului față de natură*). Acesta este însă un obiectiv care trebuie *conectat cu celelalte principii și obiective* ale Declarației, dintre care unele au relevanță directă pentru tema de față: ***prezervarea unui climat de pace și siguranță internațională***; dreptul la dezvoltare; ***protecția categoriilor vulnerabile (inclusiv a celor care au suferit în urma genocidelor, a războaielor civile, a calamităților naturale);*** îmbunătățirea relațiilor de cooperare între țări[27]. Pct. 6 din Declarația Mileniului *(respectul pentru natură)* consacră principiul necesității transmiterii către generațiile viitoare

În Declarația Mileniului, adoptată în urma Summitului Mondial din 2000, apare și obiectivul protecției și prezervării mediului înconjurător (exprimat prin valoarea respectului față de natură).

[24] *Ibidem*, p. 602.
[25] *Ibidem*. A se vedea A RES 43/97 *Protection of the environment in times of armed conflict*, din 9 februarie 1993, https://undocs.org/en/A/RES/47/37, consultat la 12 februarie 2020. A se vedea și A RES 37/137/*Protection against products harmful to health and to environement*, 17 decembrie 1982, https://undocs.org/en/A/RES/37/137, consultat la 12 februarie 2020; A RES 47/195, 1 martie1993, *Protection of global climate for present and future generations of mankind*, https://undocs.org/en/A/RES/47/195, consultat la 12 februarie 2020.
[26] UNGA, Resolution 55/2, *United Nations Millennium Declaration*, New York, 8 septembrie 2000, www.un.org/millennium/declaration/ares552e.htm, consultat la 12 februarie 2020.
[27] Paul Boncuțiu, *Declarația Mileniului*, Partea întâi, anul 2000, 12 decembrie 2010, Ziare.com, http://www.ziare.com/international/onu/declaratia-mileniului-partea-intai-anul-2000-1061123, consultat la 12 februarie 2020.

a resurselor bogate ale planetei, inclusiv prin *introducerea principiului moderației în managementul* tuturor speciilor vii și al resurselor naturale[28].

Secretarul General al ONU, Ban Ki-Moon, considera, în 2015[29], că una dintre provocările globale ale secolului XXI și ale societății umane de azi sunt ***schimbările climatice, la care se adaugă provocări la adresa păcii și securității internaționale*** *și la adresa drepturilor omului*. Statele au obligația de a crea *un climat universal de pace și securitate internațională*, conectat cu *nevoia de protecție a mediului înconjurător* (***războiul fiind o altă cauză a degradării, a poluării uneori ireversibile a naturii),*** consideră acesta. În viziunea sa, problema schimbărilor climatice trebuie privită ca fiind conectată *„cu probleme globale de tip financiar, economic, intern,* ***de securitate****, având influență asupra securității alimentare, sănătății, apei”*[30].

Secretarul General al ONU, Ban Ki-Moon, considera, în 2015, că una dintre provocările globale ale secolului XXI și ale societății umane de azi sunt schimbările climatice, la care se adaugă provocări la adresa păcii și securității internaționale și la adresa drepturilor omului.

Schimbările climatice sunt privite de Ban Ki-Moon, în alt discurs, *ca implicând* ***„obligația juridică, dar și interesul tuturor națiunilor lumii de a păstra un climat universal de pace și securitate”***[31]. **Schimbările climatice** reprezintă, în viziunea sa, *„un multiplicator de amenințări, mai cu seamă la nivel internațional, vremea extremă, dezastrele naturale provocate de aceasta ducând la crize umanitare și la deplasări masive de populații, tot mai intense, spre țările bogate, punând în pericol securitatea internațională”*[32].

Pe plan european, se poate remarca *interesul UE în a contribui atât la eforturile de consolidare a dreptului internațional al mediului, cât și la o protecție juridică îmbunătățită cu privire la mediu*, ca răspuns la inițiativa Franței de a se negocia la nivel internațional un așa-numit *Pact Global pentru Mediu*[33]. Această inițiativă este destinată să ușureze implementarea deja existentului drept internațional al mediului.

[28] UNGA, Resolution 55/2, *loc. cit.*

[29] Secretarul General Ban Ki-Moon, Paris, 29 aprilie 2015, *Address at the Institute d'Etudes Politiques de Paris: The United Nations at 70: New Global Challenges: A Conversation with Ban Ki-Moon*, UN News Centre, www.un.org/apps/news/infocus/sgspeeches, consultat la 12 februarie 2020.

[30] *Ibidem*.

[31] *Declarație – Secretary-General's Message to High-Level Side Event on Climate Change and Security* (susținută de Janos Pasztor), New York, 30 septembrie 2015, www.un.org/sg/statements, consultat la 12 februarie 2020.

[32] *Ibidem.*

[33] *Road map al Comisiei Europene*, Ref. Ares (2018)900428 - 15/02/2018, http://pactenvironment.org, consultat la 12 februarie 2020.

Proiectul a fost introdus de Franța la AG ONU în 19 septembrie 2017, ca urmare a întrunirii ministeriale a celei de-a 72 sesiuni a AG ONU[34]. La propunerea Franței, s-a reținut ideea de a se crea *un Grup al Prietenilor Pactului*, pentru a emite un proiect de rezoluție spre a fi adoptat de AG ONU și a se deschide formal dezbaterile pentru acest Pact (cu subiecte aflate pe masa negocierilor în 2018)[35]. Scopul Grupului de Prieteni ai Pactului este de a forma un grup de lucru deschis, pentru a negocia Pactul sub auspiciile AG ONU, fiind prevăzut a-și termina lucrările în acest an, când este de dorit să își expună rezultatul unei conferințe interguvernamentale. În acest context, se consideră că UE are competența în câmpul oferit de art. 192 (1) TFEU (protecția de mediu). Comisia poate acționa doar în baza autorizației emise de Consiliu pentru negocierea acestui instrument internațional, în numele UE[36].

Este important de remarcat faptul că *Pactul Global pentru Mediu* propus de Franța se dorește, de la bun început, a fi o *codificare a principiilor înscrise în Declarația de la Rio, ca un al treilea pact internațional.* El s-ar înscrie în categoria pactelor internaționale privind drepturile omului, precum Pactul internațional privind drepturile civile și politice/1966, Pactul internațional privind drepturile economice, culturale și sociale/1966 sau chiar Declarația universală a drepturilor omului din 1949. În data de 10 mai 2018, AG ONU a adoptat rezoluția 72/277, intitulată *„Towards a Global Pact for the Environment”*[37].

În *Pactul Global pentru Mediu*, supus dezbaterilor AG ONU, la inițiativa franceză, încă din 2017, apar *inovații și codificări importante*, precum: stabilirea unui drept universal la un mediu sănătos, intact, ca drept al omului, ce poate fi invocat în fața instanțelor judiciare pe plan național, internațional și regional; unificarea principiilor directoare ale dreptului internațional al mediului într-un singur document legal; împuternicirea cetățenilor de a face responsabile guvernele lor și pe cele vecine pentru politicile de mediu[38].

GÂNDIREA MILITARĂ ROMÂNEASCĂ

În Pactul Global pentru Mediu, supus dezbaterilor AG ONU, la inițiativa franceză, încă din 2017, apar inovații și codificări importante, precum: stabilirea unui drept universal la un mediu sănătos, intact, ca drept al omului, ce poate fi invocat în fața instanțelor judiciare pe plan național, internațional și regional; unificarea principiilor directoare ale dreptului internațional al mediului într-un singur document legal; împuternicirea cetățenilor de a face responsabile guvernele lor și pe cele vecine pentru politicile de mediu.

[34] *Ibidem.*

[35] *Ibidem.*

[36] *Ibidem.*

[37] *Global Pact for the Environment*, https://www.iucn.org/commissions/world-commission-environmental-law/wcel-resources/global-pact-environment, consultat la 12 februarie 2020.

[38] *Ibidem.*

Pe plan european, în cadrul UE, trebuie remarcat și recentul document intitulat *Pactul Verde European*[39], care se dorește o prioritate a Comisiei Europene, sub conducerea Ursulei von der Lyen. Prin acest Pact, un adevărat program de guvernare europeană propus și asumat de Comisia Europeană în 2020, se recunoaște de către UE faptul că *„schimbările climatice și climatul global sunt semnificativi multiplicatori de amenințări și o sursă de instabilitate”*. *Interesele de securitate*, menționate în acest context, *„sunt factori ce vor fi preschimbați de tranziția ecologică”*[40], fapt ce, în aprecierea UE, va crea provocări pentru un anumit număr de țări și societăți. UE va lansa *Pactul European privind Clima în martie 2020*, pentru a încuraja înțelegerea extinsă (la nivelul opiniei publice) a amenințărilor de mediu ca *amenințări de securitate* și modul de combatere a acestor amenințări[41]. Este important de menționat angajamentul luat de UE prin Comisia Europeană, care a lansat acest Pact ambițios, de a încuraja *„cooperarea cu toți partenerii” (state, actori non-statali, state terțe, state membre) pentru „a crește capacitatea de a preveni ca amenințările de mediu să devină surse de conflict, de insecuritate globală, de deplasări de populații și de migrări forțate”*[42]. Politica externă și politica de apărare și securitate comună a UE trebuie să includă și dimensiunea politicilor climatice[43], în viziunea Comisiei. Nu sunt însă prevăzute impactul tehnologiilor militare sau al tehnologiilor civile folosite în scopuri militare sau în alte scopuri ostile, asupra mediului, și nici măsurile de prevenire a degradării sau distrugerii mediului ca urmare directă a războaielor, a conflictelor armate de orice tip.

Pactul Verde European se dorește o prioritate a Comisiei Europene, sub conducerea Ursulei von der Lyen. Prin acest Pact, un adevărat program de guvernare europeană propus și asumat de Comisia Europeană în 2020, se recunoaște de către UE faptul că „schimbările climatice și climatul global sunt semnificativi multiplicatori de amenințări și o sursă de instabilitate”.

CONCLUZII

După cum am observat, este vorba de un domeniu al dreptului internațional al mediului explorând o relație juridică (mediu-conflicte armate), pe care o considerăm de mare importanță pentru societatea secolului XXI, dat fiind *necontenitul avans tehnologic și științific privind*

[39] Brussels, 11.12.2019 COM(2019) 640 final. *Communication from the Commission to the European Parliament, European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Green Deal*, https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_en.pdf, consultat la 12 februarie 2020.

[40] *Ibidem.*

[41] *Ibidem.*

[42] *Ibidem.*

[43] *Ibidem.*

tehnologiile militare și cele civile folosite însă în scopuri ostile, precum și cursa înarmărilor, la care asistăm în prezent, ca o reluare a perspectivei neo-realiste în politica internațională. *Mediul și dreptul internațional al mediului devin, atât din perspectiva problemelor globale, precum schimbările climatice, cât și a celor expuse aici, domenii esențiale* pentru a oferi o protecție sporită ecosistemelor terestre și părților lor care pot fi expuse sau sunt expuse în mod concret, în cazul unor crize cu componentă militară sau al unor conflicte militare, inclusiv regionale, pericolului de distrugere sau de degradare de lunga durată, grave sau ireparabile.

Este important că doctrina și jurisprudența internațională în materie *recunosc necesitatea consacrării exprese la nivelul unei convenții internaționale pe acest subiect, a mediului ca bun civil.* Ar trebui introdusă și *interdicția expresă* în sarcina statelor, dar și a actorilor non-statali implicați în conflicte armate, de a utiliza mediul în sens militar, mediul ca fiind o componentă militară a războiului sau a conflictului respectiv. Ar trebui introdusă, de asemenea, *o interdicție expresă privind folosirea armelor de distrugere în masă asupra mediului*, fie cu caracter gratuit, fie cu scop de intimidare a altor state, fie cu scop de agresiune asupra altor state sau grup de state. Ar trebui introdusă și *interdicția de a utiliza drone în conflictele militare cu scopul de a distruge mediul aflat în jurisdicția altor state sau în zonele libere*. Ar trebui introdusă și *interdicția de a folosi tehnologii civile în scopuri ostile mediului, indiferent că vorbim de mediu natural mixt sau urban (artificial, adică așezările umane).* Se pot face corelări și îmbunătățiri juridice între convențiile clasice deja adoptate de state în materia purtării războaielor și obligațiile recente, asumate de state prin *declarațiile de la Rio, Johannesburg* ori prin *„Agenda 2030”*.

Rezultă că ne aflăm în prezența unui *domeniu ce trebuie îmbunătățit juridic*, atât prin efortul statelor (pe calea dezbaterii și adoptării *prin AG ONU a diferitelor rezoluții* în materie sau prin *semnarea unei convenții internaționale* special dedicate acestui subiect), cât și prin *implicarea actorilor non-statali* (ONG-uri, media globale, organizații, corporații transnaționale) pentru a prezerva mediul și a-l transmite generațiilor viitoare ca un mediu sănătos, curat, neafectat de distrugerile cauzate de războaie și de conflicte armate sau de tehnologiile civile folosite în scopuri ostile mediului.

Mediul și dreptul internațional al mediului devin domenii esențiale pentru a oferi o protecție sporită ecosistemelor terestre și părților lor care pot fi expuse sau sunt expuse în mod concret, în cazul unor crize cu componentă militară sau al unor conflicte militare, inclusiv regionale, pericolului de distrugere sau de degradare de lunga durată, grave sau ireparabile.

BIBLIOGRAFIE:

1. ***, A RES 37/137/*Protection against products harmful to health and to environement*, 17 decembrie 1982. https://undocs.org/en/A/RES/37/137
2. ***, A RES 47/195, 1 March 1993, *Protection of global climate for present and future generations of mankind*, https://undocs.org/en/A/RES/47/195
3. ***, A RES 43/97 *Protection of the environment in times of armed conflict*, din 9 februarie 1993. https://undocs.org/en/A/RES/47/37.
4. *Global Pact for the Environment*, https://www.iucn.org/commissions/world-commission-environmental-law/wcel-resources/global-pact-environment
5. ***, *Harmony with Nature*, Report of the Secretary General, UNGA, A/67/317.
6. ***, *The Millennium Development Goals Report*, 2014, *We Can End Poverty*, United Nations, New York, 2014, www.undp.org/content/undp/en
7. ***, Resolution adopted by the General Assembly, 60/192, *International Year of Planet Earth*, 2008, A/RES/60/192.
8. ***, Secretary-General Ban Ki-Moon, Paris, 29 April 2015, *Address at the Institute d'Etudes Politiques de Paris: The United Nations at 70: New Global Challenges: A Conversation with Ban Ki-Moon,* UN News Centre, www.un.org/apps/news/infocus/sgspeeches
9. ***, UNGA, Resolution 55/2, *United Nations Millennium Declaration*, New York, 8 sept. 2000, www.un.org/millennium/declaration/ares552e.htm
10. Paul Boncuțiu, *Declarația Mileniului*, Partea întâi, anul 2000, 12 decembrie 2010, Ziare.com, http://www.ziare.com/international/onu/declaratia-mileniului-partea-intai-anul-2000-1061123.
11. Daniela Marinescu, *Tratat de dreptul mediului*, ediția a IV-a, revăzută și adăugită, Editura Universul Juridic, București, 2010.
12. Adrian Năstase, *Documenta universales I, Documente fundamentale ale dreptului internațional contemporan și ale relațiilor internaționale,* ediție îngrijită de Roxana Frailich, Asociația Română pentru Educație Democratică, Regia Autonomă Monitorul Oficial, București, 1997.

WEBOGRAFIE:

1. http://www.un.org/en/events/motherearthday/documents.shtml, accesat în 7 sept. 2016.
2. https://www.un.org/en/universal-declaration-human-rights/
3. https://www.cbd.int/doc/ref/rio-declaration.shtml

4. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf
5. https://ec.europa.eu/environment/archives/wssd/documents/wssd_pol_declaration.pdf
6. file:///C:/1976-enmod-icrc-factsheet.pdf
7. https://www.unog.ch/enmod
8. https://www.refworld.org/docid/3b00f22a10.html.

DESPRE EUROREGIUNILE DE COOOPERARE TRANSFRONTALIERĂ ALE ROMÂNIEI

Conf. univ. dr. Vasile BOGDAN
Universitatea DANUBIUS, Galați

Drd. Viorel-Cătălin MIHALCEA
Universitatea Națională de Apărare „Carol I”, București

Populații de etnii diferite sunt obligate să trăiască în state diferite, separate prin granițe care mutilează sentimentul național și perspectiva populațiilor. În perioada relativ recentă, Uniunea Europeană a procedat la depășirea consecințelor trecutului, creând punți între statele vecine cu populații care trăiesc de ambele părți ale graniței. Abordarea servește nevoia de echilibru, pace și relaxare în zonele care au fost dificile în conflict în trecut. Inițiativa a venit din Occident, fiind o prioritate datorită preocupărilor germane, spațiul fiind greu încercat în ultimele conflagrații mondiale. În cadrul colaborărilor transfrontaliere stabilite, cel mai important este sprijinul economico-financiar pentru creșterea nivelului de viață și așteptări în comunitățile sărace. În acest context, în ceea ce privește colaborarea transfrontalieră în zona care se învecinează cu teritoriul național, România se prezintă ca extrem de constructivă, făcând parte din cele 12 euroregiuni, care se găsesc în mod diferit la toate granițele țării.

Cuvinte-cheie: cooperare teritorială, macroregiuni, standard de viață, dezvoltare regională, piloni de stabilitate.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

INTRODUCERE

Este în logica istoriei că, dintotdeauna, mai-marii vremurilor duc acțiuni destabilizatoare, producând stoparea dezvoltării unitare a neamurilor pe arie de afirmare și locuire. În mod evident, este și cazul neamului românesc, puternic zguduit în dăinurirea colectivă pe spațiul de constituire și trăire, fiindu-i ciuntite teritorii masive. Astfel, urmașii românilor au fost obligați să-și ducă existența pe zone dispuse în compunerea diferitelor state vecine României sau chiar îndepăratate.

În astfel de condiții, discontinuitatea produsă în dăinuirea neamului românesc, spațială și politică, în același trup, trebuie să constituie imboldul strategic în desfășurarea eforturilor pentru surmontarea frontierelor vremelnice ce despart spațiile izolate, de maximă importanță fiind dorința de colaborare și sprijin a focarelor etnice din afara țării. După cum se cunoaște, rapturi teritoriale din trupul țării au fost materializate din anul 1940 dinspre toate cele patru puncte cardinale, România reducându-și drastic suprafața, resursele și populația.

CONTEXTUL GENERAL

Uniunea Europeană are în compunere 27 de state între care intervin legături strânse, fiind asigurată, astfel, desfășurarea fluxurilor forței de muncă, a capitalului, mărfurilor și serviciilor. Ca măsură de protecție în fața valului globalizării, pot fi activate modalități diferite de contracarare. Structuri ale aceleiași etnii, separate în trecutul istoric, la ora actuală își pot duce existența în compunerea a state diferite, deci separate de frontiere naționale. Este meritul Uniunii Europene de a fi creat cadrul legal necesar cooperării și sprijinului multiplu, realizat între etnii divizate de granițele actuale. Menținând subordonarea față de structurile naționale abilitate, structurilor din teritorii li se oferă posibilitatea să identifice soluții pentru administrarea locală prin eforturi proprii, pentru realizarea nivelului de trai sau a standardului de viață, cu atingerea progresului în viitor, în raport cu posibilitățile de care dispun în teritoriu.

Uniunea Europeană are în compunere 27 de state între care intervin legături strânse, fiind asigurată, astfel, desfășurarea fluxurilor forței de muncă, a capitalului, mărfurilor și serviciilor. Ca măsură de protecție în fața valului globalizării, pot fi activate modalități diferite de contracarare. Structuri ale aceleiași etnii, separate în trecutul istoric, la ora actuală își pot duce existența în compunerea a state diferite, deci separate de frontiere naționale.

Actele juridice fundamentale privitoare la cooperarea transfrontalieră sunt reprezentate de *Tratatul de la Maastricht* (semnat la 7 febuarie 1992 și intrat în vigoare la 1 noiembrie 1993), *Tratatul de la Roma* (semnat la 25 martie 1957, producând efecte după data de 1 ianuarie 1958), *Tratatul de la Lisabona* (semnat la 13 decembrie 2007, intrat în vigoare la 1 decembrie 2009), precum și prin *deciziile* și *tratatele de aderare*[1]. Dezvoltarea regională și cea locală sunt de dorit pentru acordarea de fonduri și facilități comunităților regionale și locale, pentru materializarea unor inițiative în plan autohton, pentru soluționarea unora dintre nevoile sociale sau pentru bunăstarea colectivităților din teritoriu[2]. În acest sens, după anul 2004, a apărut în România o *lege a dezvoltării regionale*[3].

Geneza euroregiunilor s-a produs după anul 1990 în Europa Occidentală, ca urmare a căderii Cortinei de Fier, pe fostul traseu al liniei de separare respective, în preajma frontierelor Germaniei, Franței, Olandei, Belgiei și Elveției. La fel, au apărut euroregiuni (sub impactul exemplului german) la contactul dintre Europa Occidentală și cea Centrală (Germania, Polonia, Cehia) ori cu Europa de Est (Rusia, Lituania, Polonia).

Cooperarea teritorială are în vedere convenirea, declanșarea și realizarea de acțiuni unitare, subsumate politicilor de dezvoltare unitară a unor teritorii care sunt incluse administrativ unor jurisdicții separate[4]. În paradigma dezvoltării regionale, vom admite euroregiunile ca fiind *„... zone sau regiuni de interferență economică și nu numai, în care două sau mai multe state valorifică în comun resursele materiale și umane prin inițierea și derularea unor activități și programe agricole, industriale, de transport și telecomunicații, turistice, comerciale”*[5]. Geneza euroregiunilor s-a produs după anul 1990 în Europa Occidentală, ca urmare a căderii *Cortinei de Fier*, pe fostul traseu al liniei de separare respective, în preajma frontierelor Germaniei, Franței, Olandei, Belgiei și Elveției. La fel, au apărut euroregiuni (sub impactul exemplului german) la contactul dintre Europa Occidentală și cea Centrală (Germania, Polonia, Cehia) ori cu Europa de Est (Rusia, Lituania, Polonia). După 2007, au fost create euroregiuni și în Europa

[1] Academia Română, Institutul de Geografie, coord. Radu Săgeată, *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*. Studiu geografic, Editura Academiei Române, București, 2014. Tabelul 10. Sistemul de euroregiuni de la frontiera de est a României, pp. 29-32.
[2] Tiberiu Brăilean, *Dezvoltare regională și cooperare transfrontalieră*, Editura Junimea, Iași, 2007, p. 21.
[3] *Legea nr. 315 din 28 iunie 2004 (reactualizată) privind dezvoltarea regională în România*, publicată în *Monitorul* Oficial, nr. 577 din 29 iunie 2004.
[4] Adrian Pop (coord.), Dan Manoleli, *Spre o strategie europeană în bazinul Mării Negre. Cooperarea teritorială,* Institutul European din România, București, 2008, p. 53.
[5] *Stadiul actual al reglementărilor naționale și comunitare în domeniul cooperării transfrontalier*e, Editura Primus, Oradea, 2009, p. 43.

de Est (zona carpatică[6], Dunărea de Jos, Dunăre-Mureș-Tisa ori Prutul Superior)[7].

Cooperarea transfrontalieră este robustă în regiunea baltică, aceasta fiind o consecință a implicării statelor cu democrații consolidate și deținătoare ale unui nivel economico-social ridicat; deci, putem spune că există posibilitatea asigurării pentru locuitori a unui standard adecvat de viață. Între actorii internaționali au fost semnate acorduri bilaterale sau de format mai larg, fiind sprijinite și inițiativele partenerilor[8]. Etapele succesive, proprii relațiilor transfrontaliere, pot fi enumerate astfel: depășirea limitelor de frontieră și manifestarea relațiilor între entități sau populații, schimburile de informații, în special în cazul colectivităților locale, acceptarea unanimă, cooperarea, optimizarea și integrarea programelor de dezvoltare regională[9]. Ultimele două etape nu au putut fi atinse în practica edificării euroregiunilor, fiind doar ipotetice în ceea ce privește posibilitățile de conlucrare în viitor[10].

SISTEMUL DE EUROREGIUNI DIN PROXIMITATEA ROMÂNIEI

În vecinătatea României, istoria a fost generoasă dacă ne referim la crearea unor zone de continuitate etnică în ariile de locuire, regăsite sub jurisdicția mai multor state. Este important de știut că zonele de cooperare transfrontalieră au conservat trasăturile definitorii ale elementului etnic și au menținut relațiile de bună vecinătatate și de colaborare mutuală cu patria-mamă. Mai trebuie recunoscut că granițele trasate arbitrar au îngreunat transferul firesc ale influențelor, fară a fi totuși vorba de întreruperi ale fluxurilor de colaborare.

În vecinătatea României, istoria a fost generoasă dacă ne referim la crearea unor zone de continuitate etnică în ariile de locuire, regăsite sub jurisdicția mai multor state. Este important de știut că zonele de cooperare transfrontalieră au conservat trasăturile definitorii ale elementului etnic și au menținut relațiile de bună vecinătatate și de colaborare mutuală cu patria-mamă.

Furtunile istoriei au așezat populații românești în toate punctele cardinale, în raport cu România. Cooperarea transfrontalieră produsă cu intenția soluționării benefice a dorințelor de cunoaștere reciprocă, de efort comun, dezvoltare mai susținută, cu atingerea unor nivelului mai bune ale bunăstării comune, toate acestea au găsit înțelegerea cuvenită, cu acceptarea limitelor implicărilor locale. Este demn

[6] Polonia, Slovacia, Ungaria, Ucraina și România.
[7] Vasile Bogdan, *Euroregiuni de cooperare transfrontalieră ale României*, Editura CTEA, București, 2019, pp. 31-33.
[8] Uniunea Europeană, *Ghidul cooperării transfrontaliere. Euro Dobrogea*, Constanța, 2005, pp. 25-26.
[9] ***, Consiliul Europei, *Manual de cooperare transfrontalieră*, București, 2000, p. 56.
[10] Vasile Bogdan, *op. cit.*, pp. 45-48.

de subliniat că România este parte la constituirea eruroregiunilor spre toate punctele cardinale:

- la frontiera de est, fiinţează euroregiunile *Dunărea de Jos, Siret-Prut-Nistru* şi *Prutul Superior*;
- la graniţa de vest, evidenţiem euroregiunile *Bihor-Hajdú-Bihar, Dunăre-Criş-Mureş-Tisa*, precum şi *Dunărea de Mijloc-Porţile de Fier*;
- la frontiera de nord, este constituită *euroregiunea carpatică*, ce cuprinde teritoriul aparţinând a cinci state (Polonia, Slovacia, Ungaria, Ucraina şi România);
- la graniţa sudică, se regăsesc *Asociaţia de cooperare transfrontalieră „Dunărea 21”* şi euroregiunile *Dunărea de Sud, Giurgiu-Ruse, Danubius* şi *Dunăre-Dobrogea*[11].

Euroregiunile conturate la frontierele de stat ale României mai trebuie analizate şi ca parte a macroregiunii Dunării, fiind amplasate pe axul riveran Rhin-Main-Dunăre sau dispuse în spaţiul Pontului Euxin. Analiza macroregiunii Dunării trebuie parcursă în manieră similară macroregiunilor adriatică şi ioniană, alpină ori a Mării Baltice *(figura nr. 1)*[12].

Figura nr. 1: Macroregiunea Dunării[13]

[11] *Ibidem*, pp. 103-175.
[12] Conform http://www.interreg-danube.eu/, acesat la data de 13.12.2019.
[13] Sursa: http://www.danube-region.eu/, accesat la 13.12.2019.

Pilonii de stabilitate vor fi asiguraţi prin: consolidarea potenţialului macroregiunii Dunării, conectarea regiunii la identităţi similare, în contextul transportului pe apă, existenţa posibilităţilor sistemelor terestru, aerian şi feroviar, protecţia mediului (cu diminuarea riscurilor naturale şi antropice, sporirea calităţii apei, a solului, aerului şi biodiversităţii), edificarea bunăstării şi prosperităţii (prin competitivitate, implicarea populaţiei, specializare şi pregătire multidisciplinară), toate aceste aspecte fiind subsumate cerinţelor proprii societăţii cunoaşterii[14].

Pilonii de stabilitate vor fi asiguraţi prin: consolidarea potenţialului macroregiunii Dunării, conectarea regiunii la identităţi similare, în contextul transportului pe apă, existenţa posibilităţilor sistemelor terestru, aerian şi feroviar, protecţia mediului, edificarea bunăstării şi prosperităţii, toate aceste aspecte fiind subsumate cerinţelor proprii societăţii cunoaşterii.

EUROREGIUNI LA FRONTIERA DE EST

În manieră progresivă, la frontiera de est a României, după 1997, au fost definite trei euroregiuni: *Dunărea de Jos, Prutul Superior* şi *Siret-Prut-Nistru*. Indiscutabil, euroregiunile sunt amplasate în cadrul graniţelor externe aparţinând Uniunii Europene şi NATO, generând aspecte particulare privind integrarea în spaţiul geopolitic[15] *(tabelul nr. 1)*.

Date generice ale euroregiunii	Ţări implicate
Dunărea de Jos Înfiinţată în anii 1997-1998 Suprafaţă de 53.496 km²	România
	Ucraina
	Republica Moldova
Prutul Superior Înfiinţată în anul 2000 Suprafaţă de 42.809 km²	România
	Ucraina
	Republica Moldova
Siret-Prut-Nistru Înfiinţată în anul 2002 Suprafaţă de 31.434 km²	România
	Republica Moldova

Tabelul nr. 1: Euroregiunile situate la frontiera de est a României[16]

Priorităţile din cadrul euroregiunilor situate la frontiera de est a României subscriu îndeplinirii unor obiective majore: edificarea unei economii mai competitive în spaţiul transfrontalier, scăderea presiunii asupra mediului şi pregătirea pentru situaţii de urgenţă şi extinderea manifestărilor gen *„people to people”* (extinderea cooperării între

[14] *Ibidem.*
[15] Vasile Bogdan, Emanuel-Ştefan Marinescu, *Cooperarea transfrontalieră şi studii de arie. Curs*, Editura CTEA, Bucureşti, 2019, pp. 35-36.
[16] Academia Română, Institutul de Geografie, *op. cit.*, p. 61.

colectivitățile din spațiul transfrontalier)[17]. În spațiul adiacent Prutului vor fi relevate cele două zone metropolitane, Iași și Brăila-Galați.

Dunărea de Jos a fost creată ca urmare a demersurilor României de constituire a euroregiunii, intervenită la Summitul de la Ismail, din 3-4 iulie 1997. Semnarea *„Declarației privind cooperarea trasnfrontalieră”* a fost realizată de către președinții României, Ucrainei și Republicii Moldova[18]. La data de 14 august 1998, în municipiul Galați a fost semnat *„Acordul cu privire la constituirea Euroregiunii Dunărea de Jos”*. După evenimentele din anii 2014-2015, dintre Ucraina și Federația Rusă, delimitările teritoriale din zona Peninsulei Crimeea s-au schimbat radical *(figura nr. 2)*.

Dunărea de Jos a fost creată ca urmare a demersurilor României de constituire a euroregiunii, intervenită la Summitul de la Ismail, din 3-4 iulie 1997. Semnarea „Declarației privind cooperarea trasnfrontalieră” a fost realizată de către președinții României, Ucrainei și Republicii Moldova.

Figura nr. 2: Euroregiunea Dunărea de Jos[19]

[17] Cosmin Sabău, *Efectele benefice ale cooperării transfrontaliere în euroregiuni: Euroregiunea Bihor-Hajdú-Bihar*, Editura Mirton, Timișoara, 2012, pp. 148-149.

[18] Centrul Român de Politici Europene, *Contribuții la Parteneriatul pentru dezvoltare dintre România și Republica Moldova*, 29 mai 2013, Chișinău, p. 14.

[19] Radu Săgeată (coord.), *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, Editura Academiei Române, București, 2014, figura nr. 29, p. 66.

Siret-Prut-Nistru a luat ființă prin semnarea *„Protocolului cooperării transfrontaliere a Euroregiunii Siret-Prut-Nistru”* în data de 18 septembrie 2002, la Iași, ca urmare a inițiativelor consiliilor locale din România și Republica Moldova[20]. În data de 4 decembrie 2002, la Ungheni (Republica Moldova), a fost semnat *Statutul de funcționare a Euroregiunii Siret-Prut-Nistru*, cu ocazia Reuniunii Forumului Președinților[21] *(figura nr. 3)*.

Siret-Prut-Nistru a luat ființă prin semnarea „Protocolului cooperării transfrontaliere a Euroregiunii Siret-Prut-Nistru” în data de 18 septembrie 2002, la Iași, ca urmare a inițiativelor consiliilor locale din România și Republica Moldova.

Figura nr. 3: Euroregiunea Siret-Prut-Nistru[22]

Aspecte organizatorice au fost definitivate la *Forumul Președinților*, reuniune desfășurată la Ialoveni (Republica Moldova), în 6 aprilie 2004. Cu acel prilej, a fost aprobat *„Regulamentul de organizare și funcționare a Euroregiunii Siret-Prut-Nistru”*, documentul având un set de modificări semnificative. Cele trei județe românești sunt entități teritoriale cu un potențial economic diferit, fiind indiscutabilă valoarea județului Iași, capitală a fostei provincii istorice Moldova.

Prutul Superior (sau Prutul de Sus) își datorează constituirea inițiativei părții române, începuturile fiind realizate prin *„Tratatul*

[20] Ion Talabă, *România și tematica euroregiunilor*, în *Euroregiunile. Prezent și viitor*, Editura Performantica, Iași, 2005, p. 198.

[21] Felicia Dediu, *Participarea României la realizarea unor inițiative în domeniul cooperării tranfrontaliere regionale*, în Buletinul U.N.Ap. *„Carol I”*, nr. 4/2007, pp. 221-222.

[22] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic* (Radu Săgeată coord.), *loc. cit.*, figura nr. 22, p. 78 (1.- Capitală. 2. - Nucleu de polarizare. 3. - Conexiuni transfrontaliere. 4 - Aeroporturi. 5 - Frontiere. 6 - Limite administrative).

privind relațiile de bună vecinătate și colaborare între România și Ucraina”, semnat la data de 2 iulie 1997[23]. Mai trebuie reamintit *„Acordul de constituire a Euroregiunii Prutul de Sus”*, document semnat la 22 septembrie 2000, la Botoșani *(figura nr. 4)*.

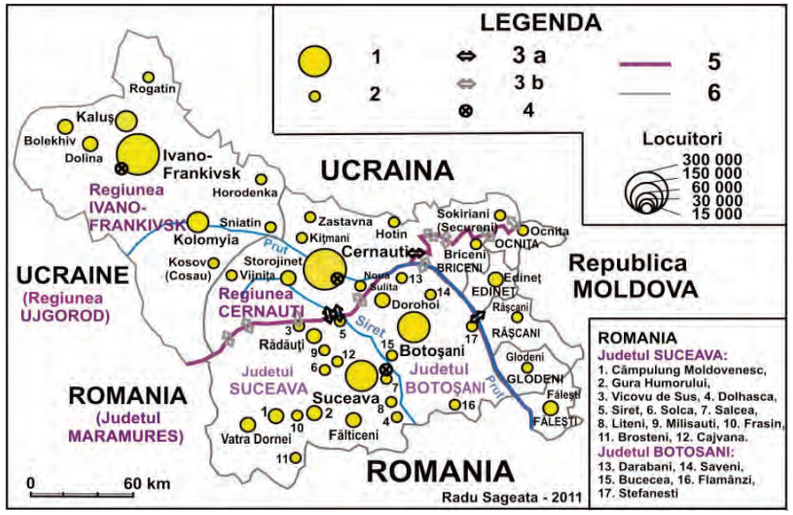

Figura nr. 4: Euroregiunea Prutul Superior[24]

Prutul Superior (sau Prutul de Sus) își datorează constituirea inițiativei părții române, începuturile fiind realizate prin „Tratatul privind relațiile de bună vecinătate și colaborare între România și Ucraina”, semnat la data de 2 iulie 1997.

Conducerea este asigurată de un Consiliu, iar exercitarea funcțiilor se realizează prin președinția Consiliului Euroregiunii și secretariat, ca și prin Centrele de Coordonare (de la Bălți, Suceava și Cernăuți) și prin patru comisii de lucru[25]. Cele patru comisii au priorități complementare: comisia 1 (probleme economice, de infrastructură și turism), comisia 2 (securitatea ecologică, protecția cadrului natural și bioeconomia), comisia 3 (colaborarea în domeniile științei, învățământului, culturii, sănătății, sportului și tineretului) și comisia 4 (creșterea și armonizarea relațiilor de colaborare inter-regionale, interetnice și autoconducerii locale)[26].

Trebuie remarcată dorința comunităților locale de edificare a unui spațiu de colaborare, întrajutorare și progres al spațiilor

[23] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 116-118.
[24] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, *loc. cit.*, figura nr. 28, p. 87 (1.- Nuclee de polarizare regională. 2.- Nuclee de polarizare locală. 3. - Conexiuni transfrontaliere: 3 a. Trafic internațional. b. Mic trafic de frontieră. 4 - Aeroporturi. 5 - Frontiere. 6 - Limite administrative).
[25] Andrei Balînschi, *Problemele și perspectivele dezvoltării Euroregiunii „Prutul de Sus” în condițiile proceselor integrării europene*, în *Euroregiunile. Prezent și viitor*, *op. cit.*, p. 201.
[26] Felicia Dediu, *op. cit.*, p. 220.

transfrontaliere evidențiate, cu luarea în considerare a implicărilor geostrategice proprii Federației Ruse. În acest sens, este imperios să fie conștientizate măsurile de control și de influență provenite din exterior, prezente în zonele aflate la răsăritul frontierei României, care stopează demersurile de colaborare și afectează reziliența populației. Deficitul major al resurselor financiare face necesar sprijinul cu fonduri masive. Reprezintă o certitudine slaba dezvoltare economică a zonelor, îmbătrânirea, pauperizarea și scăderea numărului populației, nivelul modest al comunicațiilor rutiere, promovarea slabă a turismului, parcul industrial și de transport (rutier și feroviar), reduse și învechite, nivelul mediocru al învățământului, migrarea masivă a forței de muncă autohtone spre Est și Vest. În acest sens, se impun măsuri pentru protecția mediului, în vederea stopării degradării nivelului de trai în sectorul rural, aflat la nivelul sărăciei extreme, precum și măsuri energice pentru accesarea de fonduri europene[27].

EUROREGIUNI LA FRONTIERA DE NORD

Frontiera de nord a României, situată în contextul graniței externe a Uniunii Europene și NATO, se regăsește și pe axa baltico-pontică, destul de cunoscută pentru presiunile politice din plan regional.

Euroregiunea Carpatică are în compunere cinci state: Ungaria (5 județe), Polonia (4 voievodate), Slovacia (9 județe), Ucraina (4 regiuni) și România (7 județe)[28]. Din România sunt incluse județele Satu Mare, Maramureș, Sălaj, Bihor, Suceava, Botoșani și Harghita (din anul 2000). Euroregiunea a luat ființă la 14 februarie 1993, la Debrețin (Ungaria), fiind constituită cu ocazia reuniunii miniștrilor de externe ai statelor interesate, unde au luat parte reprezentanții administrațiilor locale[29] *(figura nr. 5)*.

Documentele de constituire sunt *„Acordul privind înființarea unei asocieri interregionale ‹Euroregiunea Carpatică› și Statutul Asociației interregionale ‹Euroregiunea Carpatică›”*. Managementul este asigurat de Consiliul Euroregiunii Carpatice, cu rol decident în strategia euroregiunii și în problemele de interes major. Secretariatul internațional a funcționat, inițial, la Uzgorod (Ucraina), fiind, apoi, mutat la Debrecen (Ungaria). Comisiile de lucru se regăsesc în responsabilitatea

Euroregiunea Carpatică are în compunere cinci state: Ungaria, Polonia, Slovacia, Ucraina și România. Euroregiunea a luat ființă la 14 februarie 1993, la Debrețin (Ungaria), fiind constituită cu ocazia reuniunii miniștrilor de externe ai statelor interesate, unde au luat parte reprezentanții administrațiilor locale

[27] Vasile Bogdan, *op. cit.*, pp. 93-94.
[28] Ion Talabă, *op. cit.*, p. 193.
[29] Vasile Bogdan, Emanuel-Ştefan Marinescu, *op. cit.*, pp. 134-143.

a câte unui stat, astfel: Dezvoltarea regională (Ungaria), Prevenirea dezastrelor naturale (Slovacia), Turism și mediu (Polonia), Dezvoltarea comerțului (România) și Infrastructură socială (Ucraina)[30].

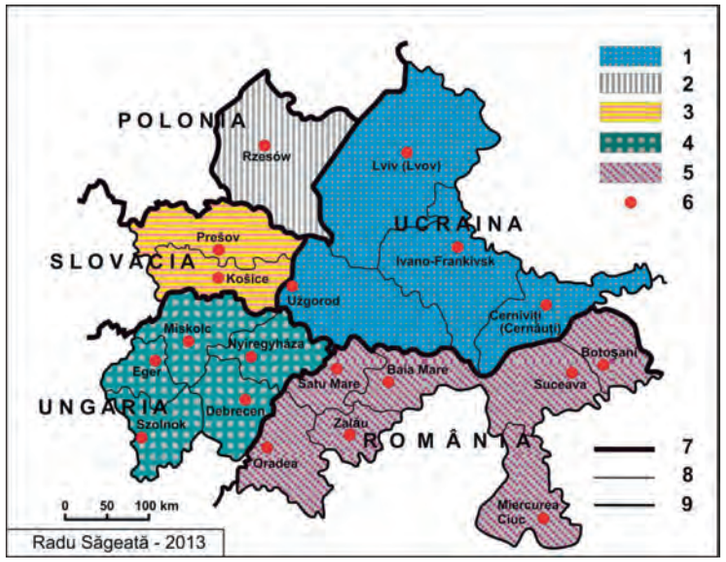

Figura nr. 5: Euroregiunea Carpatică[31]

Euroregiunea Carpatică este structura de gen transfrontalier unicat în care sunt întreprinse contacte bi- și trilaterale. În existența euroregiunii, este important mesajul transmis popoarelor Europei, potrivit căruia genul respectiv de cooperare poate fi fezabil. De asemenea, există un imbold al dezvoltării altor euroregiuni din Europa, cu posibilități de cooperare, dialog și sprijin mutual.

Euroregiunea Carpatică este structura de gen transfrontalier unicat în care sunt întreprinse contacte bi- și trilaterale. În existența euroregiunii, este important mesajul transmis popoarelor Europei, potrivit căruia genul respectiv de cooperare poate fi fezabil. De asemenea, există un imbold al dezvoltării altor euroregiuni din Europa, cu posibilități de cooperare, dialog și sprijin mutual. Este validată simbolistica edificării unei euroregiuni cu participare cvadripartită, ca spațiu de colaborare și progres, spre demonstrarea viabilității politicilor Uniunii Europene în domeniul dezvoltării regionale și cooperarii transfrontaliere cu participări multiple. Se remarcă spiritul antreprenorial și practicile diversificate, preocupările comerciale, economice, culturale și administrative, cultivarea spiritului apartenenței

[30] Cristina Dogot, *Romanian Local Administrations and their activities in Carpathian Euroregion*, în *Cross-Border Cooperation. Models of Good Practice in Carpathian Region* (editor Adrian-Claudiu Popoviciu), Editura CH Beck, Oradea, 2014, pp. 174-175.

[31] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, *loc. cit.*, figura nr. 52, p. 128 (1-5 sectoare: 1. ucrainean, 2. polonez, 3. slovac, 4. maghiar, 5 românesc, 6. centre de polarizare, 7. granițe de stat. 8. limite administrative, 9. limita Euroregiunii Carpatice).

la valorile specifice Occidentului, cu respectarea politicilor UE în domeniul transfrontalier. Calitatea și seriozitatea factorului uman, maturitatea și coerența demersurilor realizate sunt în acord cu obiectivele de atins. Infrastructura educațională este pe un trend optimist, existând un nivel ridicat al calificării forței de muncă.

EUROREGIUNI LA FRONTIERA DE VEST

În continuare, vom analiza situația la frontiera de vest a României, pe cele două tronsoane distincte: segmentul graniței româno-ungare, cu euroregiunea Bihor-Hajdú-Bihar, deci bipartită (România și Ungaria), și sectorul graniței româno-sârbe, cu euroregiunea Dunărea de Mijloc-Porțile de Fier, așadar bipartită (România și Serbia). Ca excepție, va fi evidențiată Euroregiunea Dunăre-Criș-Mureș-Tisa, structură tripartită (România, Ungaria și Serbia)[32]. *Bihor-Hajdú-Bihar* a luat ființă la finele anului 2002, prin demersurile simultane inițiate de Consiliul Județean Bihor și Autoguvernarea Locală Hajdú-Bihar (Ungaria). Aspectele practice au fost statuate prin *„Concepția și programul de dezvoltare a regiunii transfrontaliere româno-ungare”*[33].

Figura nr. 6: Euroregiunea Bihor-Hajdú-Bihar[34]

Bihor-Hajdú-Bihar a luat ființă la finele anului 2002, prin demersurile simultane inițiate de Consiliul Județean Bihor și Autoguvernarea Locală Hajdú-Bihar (Ungaria). Aspectele practice au fost statuate prin „Concepția și programul de dezvoltare a regiunii transfrontaliere româno-ungare”.

[32] Academia Română, Institutul de Geografie, *op. cit.*, pp. 140-141.

[33] Vasile Bogdan, Emanuel-Ștefan Marinescu, *op. cit.*, pp. 151-155.

[34] După *Hungary Population Census*, apud *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării. Studiu geografic*, *loc. cit.*, figura nr. 60, p. 152.

Euroregiunea *Bihor-Hajdú-Bihar* este structură transfrontalieră extrem de dinamică și prosperă. Numeroasele și rodnicile inițiative ale părților aflate în cooperare sprijină populațiile frontaliere să atingă un nivel de bunăstare înalt, realizat prin eforturi comune.

Dunăre-Criș-Mureș-Tisa (DKMT) a fost fondată prin *„Acordul de cooperare bilaterală între Timiș (România) și Csongrad (Ungaria)”* și *„Protocolul de Cooperare Regională Dunăre-Mureș-Tisa”*, semnat în anul 1997 *(figura nr. 7)*.

Dunăre-Criș-Mureș-Tisa (DKMT) a fost fondată prin „Acordul de cooperare bilaterală între Timiș (România) și Csongrad (Ungaria)” și „Protocolul de Cooperare Regională Dunăre-Mureș-Tisa”, semnat în anul 1997.

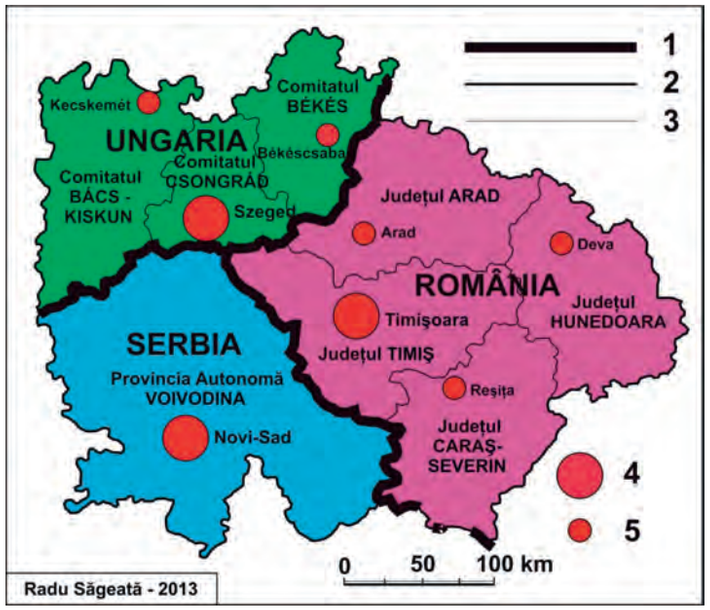

Figura nr. 7: Euroregiunea Dunăre-Criș-Mureș-Tisa[35]

Scopurile se referă la intensificarea democratizării regiunii și accelerarea integrării europene, dezvoltarea social-economică, realizarea de contacte și de relații speciale în mediul transfrontalier. Obiectivele majore sunt axate atât pe amplificarea relațiilor reciproce în domeniile economic, educație și cultură, asistență sanitară, știință, sport, cât și pe colaborarea în domeniul integrării europene[36].

Dunărea de Mijloc-Porțile de Fier a luat ființă la 6 octombrie 2005. La Vidin au fost semnate documentele de constituire, în fapt, *Acordul de Asociere și Statutul Euroregiunii Dunărea de Mijloc-Porțile de Fier*.

[35] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.,* figura nr. 70, p. 181.
[36] Felicia Dediu, *op. cit.*, p. 212.

Sunt implicate județele românești Caraș-Severin și Mehedinți, cu districtele sârbe Bor și Branicevski[37] *(figura nr. 8)*.

Figura nr. 8: Euroregiunea Dunărea de Mijloc-Porțile de Fier[38]

În efortul euroregiunii se detașază implicarea majoră a părților romană și sârbă în sprijinul Parcului Național *„Porțile de Fier”* (România) și, în oglindă, a Parcului Național *„Djerdap”* (Serbia).

Sunt ilustrative eficiența ridicată a politicilor de guvernare locală și colaborarea dintre autorități, comunitățile locale și mediul de afaceri în spirit de cooperare destinsă, prosperitate și progres. Se remarcă spiritul antreprenorial dezvoltat, manifestarea îndelungatelor schimburi comerciale, culturale și administrative, operarea de practici comerciale de succes. Este certă conștientizarea apartenenței la nivelurile civilizației și culturii, specifice Occidentului. De asemenea, este utilizată experiența pozitivă acumulată, ca punte spre rezultate transfrontaliere marcante.

[37] Vasile Bogdan, *op. cit.*, pp. 154-157.
[38] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.*, figura nr. 87, p. 215.

Pregătirea și calitatea resursei umane, maturitatea și responsabilitatea demersurilor întreprinse sunt în acord cu obiectivele tangibile formulate. Sunt conturate un sistem fezabil și o rețea de învățământ extinse, cu nivel ridicat de calificare a forței de muncă. Există resurse naturale și de mediu, valorificate optim prin preocupări turistice[39].

EUROREGIUNI LA FRONTIERA SUDICĂ

Sistemul de euroregiuni de la frontiera de sud cuprinde structurile de cooperare transfrontalieră: *Dunărea de Sud, Dunărea Inferioară, Asociația „Dunărea 21”, Giurgiu-Ruse, Danubius* și *Dunăre-Dobrogea*.

Asociația de cooperare transfrontalieră „Dunărea 21”[40] a fost înființată la 18 ianuarie 2002 la Vidin, prin documentele semnate de primarii orașelor Calafat, Vidin și Zaječar[41]. Asociația este amplasată în spațiul de interferență a trei state (România, Bulgaria și Serbia). Cuprinde o suprafață de 1.144 km² [42] cu așezări din trei state: *România* (orașul Calafat și comunele Desa, Poiana Mare, Ciupercenii Noi și Cetate), *Bulgaria* (orașul Vidin și comunele Macriș, Rujnuti, Lom, Belogradcic, Kula, Novo Selo și Dimovo) și *Serbia* (orașul Zaicear și comunele Kladovo, Sokobania, Bolivat, Bor, Kniajevat și Mandanpec)[43] *(figura nr. 9)*.

Sistemul de euroregiuni de la frontiera de sud cuprinde structurile de cooperare transfrontalieră: Dunărea de Sud, Dunărea Inferioară, Asociația „Dunărea 21”, Giurgiu-Ruse, Danubius și Dunăre-Dobrogea.

Extrem de importantă este semnarea, la 1 august 2006, a *„Acordului dintre România și Bulgaria privind construcția podului Calafat-Vidin”*, costurile fiind estimate la circa 236 de milioane de euro (costurile totale fiind de 226 de milioane de euro), asigurate de Uniunea Europeană și Banca Europeană de Investiții[44]. Podul, în lungime de 1.971 de metri, a fost finalizat la 14 iunie 2013. Asociația *„Dunărea 21”* este structură tripartită cu format atipic, cu pondere redusă a părții române, comparativ cu implicarea sârbă și bulgară.

[39] *Ibidem*, pp. 156-159.
[40] Asociația dispune de toate particularitățile componente și funcționale specifice euroregiunii. Termenul este concordant cu dimensiunile spațiale mai modeste ale structurii transfrontaliere de față (n.a.).
[41] Adrian Pop (coord.), *op. cit.*, p. 71.
[42] Vasile Bogdan, Emanuel-Ștefan Marinescu, *op. cit.*, pp. 165-169.
[43] Felicia Dediu, *op. cit.*, p. 214.
[44] *Ibidem*, pp. 214-215.

Figura nr. 9: Asociația de cooperare transfrontalieră „Dunărea 21”[45]

Dunărea de Sud a fost înființată în martie 2001, având în compunere structuri de cooperare transfrontalieră din România (consiliile locale ale municipiilor Alexandria, Turnu Măgurele, Zimnicea și Roșiorii de Vede[46]) și Bulgaria (trei municipalități urbane: Nikopol, Belene și Veliko-Târnovo[47]).

Dunărea de Sud a fost înființată în martie 2001, având în compunere structuri de cooperare transfrontalieră din România (consiliile locale ale municipiilor Alexandria, Turnu Măgurele, Zimnicea și Roșiorii de Vede) și Bulgaria (trei municipalități urbane: Nikopol, Belene și Veliko-Târnovo).

Activitatea euroregiunii prezintă un dinamism mai redus. Dezvoltarea infrastructurii (cu o posibila trecere permanentă peste Dunăre, realizată în zonă) ar putea revitaliza aspectele economice necesare pentru zona accentuat pauperă.

[45] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*, *loc. cit.*, figura nr. 94, p. 237 (1. Sectorul românesc. 2. Sectorul sârbesc. 3. Sectorul bulgăresc. 4. Centru de polarizare).
[46] Adrian Pop (coord.), *op. cit.*, p. 71.
[47] Vasile Bogdan, Emanuel-Ștefan Marinescu, *op. cit.*, pp. 169-172.

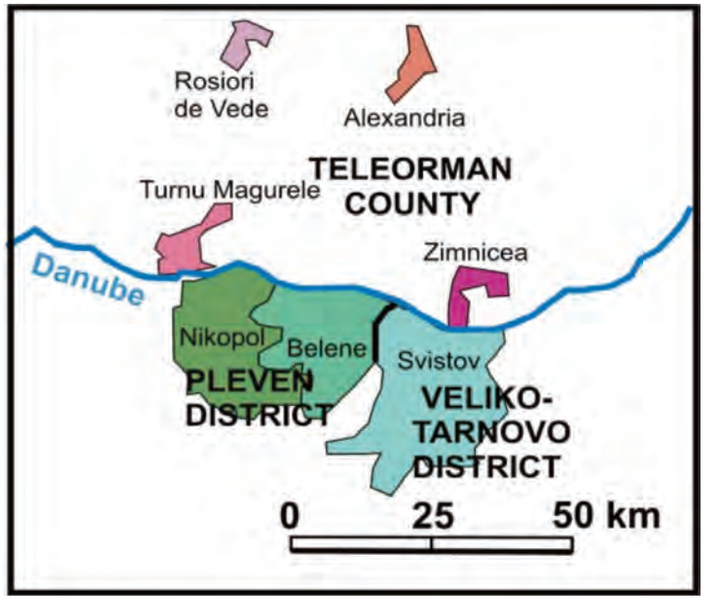

Figura nr. 10: Euroregiunea Dunărea de Jos[48]

Danubius a fost instituită în anul 2002 prin preocupările comune ale Consiliului județean Giurgiu (România) și ale Prefecturii Ruse (Bulgaria).

Giurgiu-Ruse are ca document de început *Convenția de constituire*, semnată de primarii municipiilor Giurgiu și Ruse la 23 aprilie 2001, în orașul Giurgiu[49].

Euroregiunea cuprinde Primăria Giurgiu, Primăria Ruse și Agenția Municipală Energetică din Ruse (ONG). Euroregiunea este plasată pe linia de schimburi comerciale strategice din fostul CAER, Moscova-Kiev-București, cu acces posibil spre Sofia și Burgas, motiv pentru care a fost construit podul Giurgiu-Ruse, în perioada 1952-1954.

La reuniunile trimestriale sunt evaluate probleme de mediu, sănătate publică și de șeptel, cu soluționarea rapidă a cerințelor sau proiectelor în format bilateral *(figura nr. 11)*. Euroregiunea are dimensiuni reduse și posibilități modeste de efort economic și cooperare. Totuși, menține imboldul derulării schimburilor reciproce și lucrului efectiv al administrațiilor locale din zonele riverane Dunării[50].

Danubius a fost instituită în anul 2002 prin preocupările comune ale Consiliului județean Giurgiu (România) și ale Prefecturii Ruse

[48] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării*, *loc. cit.*, figura nr. 99, p. 246 (1. Sectorul românesc. 2. Sectorul bulgaresc. 3. Frontiera de stat).
[49] Ion Talabă, *op. cit.*, p. 195.
[50] Vasile Bogdan, Emanuel-Ștefan Marinescu, *op. cit.*, pp. 172-175.

Figura nr. 11: Euroregiunea Giurgiu-Ruse, structura administrativă[51]

(Bulgaria). Cuprinde partea română, cu teritoriul județului Giurgiu, și *partea bulgară*, cu provincia Ruse[52] *(figura nr. 12)*.

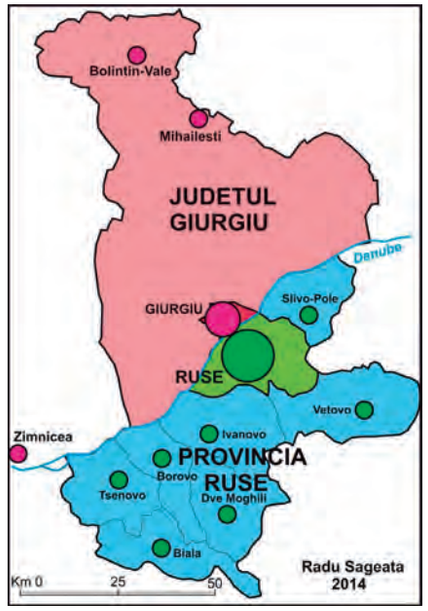

Figura nr. 12: Euroregiunea Danubius[53]

[51] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.*, figura 102, p. 258.
[52] Ion Talabă, *op. cit.*, p. 196.
[53] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.*, figura nr. 1072, p. 267.

Euroregiunea Danubius continuă și amplifică obiectivele și posibilitățile analizate anterior în situația Euroregiunii Giurgiu Ruse, dar cadrul geografic, economic și structura demografică sunt extrapolate la nivelul județului Giurgiu[54].

Dunăre-Dobrogea a luat ființă în anul 2002, cu structuri teritoriale din România (județele Ialomița, Călărași și Constanța) și Bulgaria (provinciile Silistra și Dobrici – *figura nr. 13*).

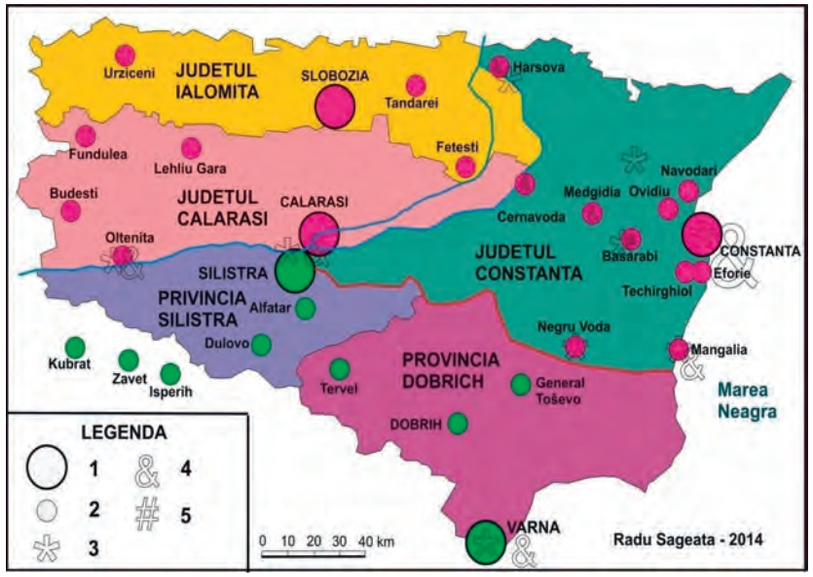

Figura nr. 13: Euroregiunea Dunăre-Dobrogea[55]

Euroregiunea este o structură transfrontalieră puternică. Partea română cuprinde județul Constanța, nod de polarizare transfrontalieră de amploare și de importanță regională majoră, ca port la Marea Neagră. Valoarea nodului de comunicații și a forței economice vor spori în viitor, în raport cu extinderile din axa Rhin-Main-Dunăre, precum și cu extinderea traseului hidrocarburilor dinspre zona Mării Caspice.

În cadrul euroregiunilor din sud, asistăm la implicări semnificative de coeziune la nivelul comunităților locale privind conturarea spațiului

În cadrul euroregiunilor din sud, asistăm la implicări semnificative de coeziune la nivelul comunităților locale privind conturarea spațiului de colaborare, prosperitate și progres specific euroregiunilor amplasate pe frontiera de sud a României, în acord cu politicile Uniunii Europene.

[54] Vasile Bogdan, *op. cit.*, pp. 173-175.

[55] După *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării, loc. cit.*, figura nr. 118, p. 286. (1. - Nuclee de polarizare regională și locală. 2. - Porturi. 3. - Canale navigabile. 4 - Limite administrative. 5 - Frontiere de stat).

de colaborare, prosperitate și progres specific euroregiunilor amplasate pe frontiera de sud a României, în acord cu politicile Uniunii Europene.

Spiritul antreprenorial este semnificativ, prin conturarea și manifestarea unor forme propice ale colaborării comerciale, culturale și administrative, acceptarea valorilor și politicilor UE în domeniul transfrontalier. Se remarcă extinderea experienței pozitive, ca imbold spre rezultate sporite în plan transfrontalier.

CONCLUZII

Instituirea structurilor transfrontaliere este o realitate de dată relativ recentă la nivelul Uniunii Europene. Constituirea euroregiunilor intervine în zone marcate de convulsii istorice ce au învrăjbit și afectat major comunitățile amplasate în preajma granițelor. Prin mecanismele cooperării transfrontaliere se renunță la ura proprie trecutului, trecându-se la o construcție comună, ca soluție utilă, care favorizează edificarea unei Europe a păcii, a destinderii și progresului.

Constituirea euroregiunilor intervine în zone marcate de convulsii istorice ce au învrăjbit și afectat major comunitățile amplasate în preajma granițelor. Prin mecanismele cooperării transfrontaliere se renunță la ura proprie trecutului, trecându-se la o construcție comună, ca soluție utilă, care favorizează edificarea unei Europe a păcii, a destinderii și progresului.

Succesul dorit în implementarea și viitorul euroregiunilor este dependent de o serie de factori, precum voința politică a constituirii de *„punți de legătură”* cu foștii inamici istorici, stimularea experienței și a capacității antreprenoriale, asigurarea suportului multiplu (legislativ, politic, financiar, tehnologic etc.) pentru comunitățile implicate, sprijinirea zonelor paupere și accesarea de fonduri europene, subvenții, donații ori scutiri de taxe, realizate pe mari perioade de timp.

Pentru viitor, apreciem că este necesară optimizarea cadrului legislativ european, racordarea prevederilor dreptului intern la exigențele respective, direcționarea fondurilor planificate spre zonele cu populații paupere și probleme multiple de soluționat, stabilirea de mecanisme simplificate în accesarea fondurilor europene, fluidizarea deciziei locale, coordonarea îndeplinirii efortului practic și lărgirea contextului geopolitic de afirmare a genului de cooperare transfrontalieră. Prin maturitatea efortului de durată, euroregiunile pot deveni factori de progres în viitor.

Din unghiul securității naționale, implicarea euroregiunior poate comporta efecte și aspecte diferite. Dintre efectele pozitive, putem menționa sprijinul creșterii standardului de viață, înnoiriile tehnologice, conservarea tradițiilor, realizarea de facilități critice absolut necesare,

inducerea progresului și a prosperității în zone vitregite. Efectele negative fac referire la dorința de eliminare a frontierelor spațiului românesc, ștergerea indentității naționale, dispariția sentimentului de apartenență la trecutul comun și eliminarea formelor tradiționale din spațiile transfrontalire.

BIBLIOGRAFIE:

1. ***, *Legea nr. 315 din 28 iunie 2004 (reactualizată) privind dezvoltarea regională în România*, publicată în *Monitorul Oficial*, nr. 577 din 29 iunie 2004.
2. ***, *Stadiul actual al reglementărilor naționale și comunitare în domeniul cooperării transfrontaliere*, Editura Primus, Oradea.
3. Academia Română, Institutul de Geografie, *Euroregiunile de cooperare transfrontalieră din bazinul inferior al Dunării* (coord. Radu Săgeată). *Studiu geografic*, Editura Academiei Române, București, 2014.
4. Centrul Român de Politici Europene, *Contribuții la Parteneriatul pentru dezvoltare dintre România și Republica Moldova*, 29 mai 2013, Chișinău.
5. Uniunea Europeană, *Ghidul cooperării transfrontaliere. Euro Dobrogea*, Constanța, 2005.
6. Andrei Balînschi, *Problemele și perspectivele dezvoltării Euroregiunii „Prutul de Sus" în condițiile proceselor integrării europene, în Euroregiunile. Prezent și viitor*, Editura Performantica, Iași, 2005.
7. Vasile Bogdan, *Euroregiuni de cooperare transfrontalieră ale României*, Editura CTEA, București, 2019.
8. Vasile Bogdan, Emanuel-Ştefan Marinescu, *Cooperarea transfrontalieră şi studii de arie. Curs*, Editura CTEA, Bucureşti, 2019.
9. Tiberiu Brăilean, *Dezvoltare regională și cooperare transfrontalieră*, Editura Junimea, Iași, 2007.
10. Felicia Dediu, *Participarea României la realizarea unor inițiative în domeniul cooperării tranfrontaliere regionale*, în Buletinul U.N.Ap. *„Carol I"*, nr. 4/2007.
11. Cristina Dogot, *Romanian Local Administrations and their activities in Carpathian Euroregion*, în *Cross- Border Cooperation. Models of Good Practice in Carpathian Region* (editor Adrian-Claudiu Popoviciu), Editura CH Beck, Oradea, 2014.
12. Adrian Pop (coord.), Dan Manoleli, *Spre o strategie europeană în bazinul Mării Negre. Cooperarea teritorială*, Institutul European din România, București, 2008.
13. Cosmin Sabău, *Efectele benefice ale cooperării transfrontaliere în euroregiuni: Euroregiunea Bihor-Hajdú-Bihar*, Editura Mirton, Timișoara, 2012.
14. Ion Talabă, *România și tematica euroregiunilor*, în *Euroregiunile. Prezent și viitor*, loc. cit.
15. http://www.interreg-danube.eu/
16. http://www.danube-region.eu/.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

NEVOIA PREGĂTIRII ORAȘELOR PENTRU DESFĂȘURAREA OPERAȚIILOR MILITARE

Lect. univ. dr. Sorina-Georgiana RUSU

Universitatea de Arhitectură și Urbanism „Ion Mincu”, București

Urbanizarea are o influență directă asupra domeniului securității și apărării. Operațiile militare tind să se desfășoare, cu o frecvență din ce în ce mai mare, în mediul complex al orașelor contemporane. Pentru a lupta în acest mediu, este necesară, în primul rând, înțelegerea similarităților și a diferențelor orașelor. Fiecare oraș necesită o abordare unică, pornind de la nivelul strategic al planificării până la nivel tactic. Totodată, este nevoie de cooperarea planificatorilor civili și militari pentru a crea un cadru legal comun de proiectare și de apărare a orașelor.

Cuvinte-cheie: urbanizare, planificare civil-militară, oraș inteligent, operații militare în zone urbane, oraș ofensiv.

INTRODUCERE

Modul în care se dezvoltă şi se extind oraşele are o importanţă covârşitoare asupra viitorului existenţei umane. Oraşele se află într-un proces de transformare continuă ce presupune păstrarea unor elemente şi renunţarea la altele, în vederea dezvoltării şi modernizării. Există astăzi o diversitate extraordinară a peisajelor urbane şi acest lucru face ca pregătirea desfăşurării operaţiilor militare în acest mediu să fie dificilă şi plină de provocări.

Conexiunea din ce în ce mai crescută a oraşelor duce la creşterea complexităţii, a interdependenţelor şi a vulnerabilităţilor acestora. Căutarea unor soluţii punctuale, ca răspuns pentru oricare posibilă situaţie de conflict, este o abordare nepotrivită. Abordarea care se impune, în contextul mileniului III, este aceea a prevenţiei, *a gândirii planificării urbane în corelare cu planificarea militară*.

Diversificarea tipologiei inamicului, în contextul escaladării conflictelor generate de acţiuni teroriste, aduce în atenţie și ideea de globalizare a comunicaţiilor, care presupune libera circulaţie a informaţiilor. Deşi pare a fi o virtute a lumii moderne, care ţine de înaltul grad de civilizaţie, această explozie a circulaţiei informaţiilor este una dintre vulnerabilităţile postmodernităţii. Astfel, dihotomia *amic-inamic*, specifică războiului clasic, ar trebui înlocuită cu ideea de protejare permanentă a populaţiei, prin eliminarea conceptului de *linie a frontului* care separa, după cum se ştie, cele două categorii aflate în conflict: *atacatori* şi *atacaţi*[1].

Câteva dintre întrebările pe care analizele preconflict trebuie să le ia în considerare vizează planificarea oraşului pentru o dezvoltare echilibrată şi sigură, metodele de evacuare a oraşului în caz de necesitate iminentă, apărarea oraşului, modul în care ar putea fi atacat şi reconstruit postconflict, obiectivele de protejat în interiorul oraşului, fluxurile vitale interne şi externe ale oraşului.

Diversificarea tipologiei inamicului, în contextul escaladării conflictelor generate de acțiuni teroriste, aduce în atenție și ideea de globalizare a comunicațiilor, care presupune libera circulație a informațiilor. Deși pare a fi o virtute a lumii moderne, care ține de înaltul grad de civilizație, această explozie a circulației informațiilor este una dintre vulnerabilitățile postmodernității.

[1] Sorina Georgiana Rusu, *Planificarea în proiectarea obiectivelor destinate apărării în orașul inteligent*, Editura Paralela 45, Pitești, 2018, p. 109.

URBANIZARE ŞI SECURITATE

La nivel mondial, se semnalează o tranziţie istorică în curs de desfăşurare. Peste jumătate din populaţia globului trăieşte, în prezent, în oraşe, iar rata migraţiei este accelerată. Până în 2030, oraşele vor reprezenta 60% din populaţia lumii şi vor produce 70% din PIB-ul mondial[2]. În fiecare zi, aproximativ 180.000 de oameni de pe glob migrează spre oraşe[3]. Urbanizarea într-un ritm accelerat, în special în ţările în curs de dezvoltare, are efecte asupra modului în care se configurează oraşele şi asupra apărării acestora.

Peste jumătate din populaţia globului trăieşte, în prezent, în oraşe, iar rata migraţiei este accelerată. Până în 2030, oraşele vor reprezenta 60% din populaţia lumii şi vor produce 70% din PIB-ul mondial. În fiecare zi, aproximativ 180.000 de oameni de pe glob migrează spre oraşe. Urbanizarea într-un ritm accelerat, în special în ţările în curs de dezvoltare, are efecte asupra modului în care se configurează oraşele şi asupra apărării acestora.

Oraşele prezintă similarităţi şi caracteristici individuale distincte, unice, care impun o abordare a apărării personalizată. Similarităţile sunt date de elementele de *viaţă urbană* şi de cele de *cadru urban*. Totalitatea activităţilor localizate în oraşe alcătuieşte *viaţa urbană* (activităţi, comportamente), în vreme ce spaţiile aferente localizării alcătuiesc *cadrul urban* (configuraţie spaţială, cultură urbană, politică urbană)[4]. *Viaţa urbană* şi *cadrul urban* se află în interdependenţă, primul element fiind motorul transformării, care poate lua atât forma involuţiei, cât şi forma evoluţiei la nivelul oraşelor.

Așa cum subliniază Le Corbusier, încă din anul 1980, *„Marele oraș comandă totul, pacea, războiul, munca”*[5]. Astăzi, vorbim despre existența unor așezări urbane precum metropola[6] sau megalopolisul[7], medii deosebit de complexe, în care este nevoie de o nouă abordare

[2] United Nations, 2011. World Urbanization Prospects, 2011. Department of Economic and Social Affairs, New York, http:// esa.un.org/unup/pdf/WUP2011_Highlights.pdf., accesat la 14 februarie 2020.

[3] United States Agency for International Development, USAID Policy, octombrie 2013, Sustainable Service Delivery in an Increasingly Urbanized World. 3, https://www.usaid.gov/sites/default/files/documents/1870/USAIDSustainableUrbanServicesPolicy.pdf, accesat la 14 februarie 2020.

[4] Cf. Alexandru M. Sandu, *Teoria sistemelor urbane – partea I*, curs universitar, Editura Institutul de Arhitectură *„Ion Mincu”*, 1975.

[5] Le Corbusier, *Urbanisme,* Flammarion, Paris, 1980, p. 78.

[6] *Marile metropole se definesc prin echipare și prin zonele de influență, acestea din urmă definind un prag al rentabilității necesare pentru echipamentele de înalt nivel (infrastructuri de transport, capacități de primire, instituții de decizie politică, economică și culturală, servicii pentru marile companii internaționale). Există mai multe relații între metropolele internaționale decât între o capitală și orașele din zona sa metropolitană. Mărimea spațiilor metropolitane duce la acutizarea problemelor urbane (segregare, șomaj, insecuritate, presiune funciară și speculă imobiliară, degradarea calității mediului). (J. Bonnet - Marile Metropole Mondiale, 2000).*

[7] *Ansamblu urban gigant, rezultat al unor conurbații multiple și complexe luând forma unui oraș continuu, care s-a format atunci când interstițiile rurale dintre ariile metropolitane au fost înghițite de creșterea urbană.* (C. Zamfir, L. Vlăsceanu, *Dicționar de sociologie*, 1993).

a planificării urbane, relaționată cu asigurarea securității locuitorilor: *„Copleşite de disparităţi, afectate de multiplele dezastre ecologice majore, la care se adaugă diversificarea paletei de conflicte apărute fie pe fondul inechităţilor sociale ce favorizează infracţionalitatea, fie prin escaladarea conflictelor armate de tip terorist, oraşele contemporane trebuie să-şi construiască o componentă de apărare. Sporirea diversităţii etnice, culturale, religioase, comerciale, economice, în general, a devenit spaţiu propice al generării conflictelor, mai ales în zonele în care gestionarea situaţiei la nivel de guvernanţă nu a dovedit diplomaţia necesară într-un astfel de context. Din nefericire, violenţa defineşte unele comunităţi urbane, iar starea de insecuritate este ameninţarea majoră la adresa cetăţeanului paşnic”*[8].

În ultimii ani, în cadrul armatei americane, s-a manifestat o atenţie sporită asupra aşezărilor formate din zeci de milioane de locuitori. În 2014, armata americană a realizat un proiect de cercetare[9] asupra marilor oraşe, care a concluzionat, în esenţă, faptul că armata este *„slab pregătită”* să conducă orice misiune şi să funcţioneze şi într-un astfel de mediu complex.

Oraşul contemporan este dependent de infrastructurile tehnice necesare susţinerii vieţii urbane moderne, aceste elemente făcându-l, totodată, vulnerabil în faţa atacatorilor. Densitatea urbană în creştere, alături de anonimatul pe care marile oraşe îl asigură, face dificilă gestionarea acestor medii, în general, şi în special din punctul de vedere al apărării.

CONFRUNTAREA ARMATĂ ÎN ORAŞELE CONTEMPORANE

Oraşul contemporan este dependent de infrastructurile tehnice necesare susţinerii vieţii urbane moderne, aceste elemente făcându-l, totodată, vulnerabil în faţa atacatorilor. Densitatea urbană în creştere, alături de anonimatul pe care marile oraşe îl asigură, face dificilă gestionarea acestor medii, în general, şi în special din punctul de vedere al apărării. Apar probleme majore atât în privinţa costurilor, cât și a complicării situaţiei generale a clasificării aşezărilor urbane, prin raportare la conceptul de *smart city*[10].

Numărul atacurilor teroriste s-a situat la un nivel relativ scăzut în 2012, cu 6.771 de atacuri la nivel global. Peste numai doi ani, în 2014, numărul de atacuri teroriste s-a dublat, ajungând la 13.463. Majoritatea actelor de terorism au fost localizate în ţările din Orientul Mijlociu, cum

[8] Sorina Georgiana Rusu, *Planificarea și proiectarea obiectivelor destinate apărării în orașul inteligent*, *op. cit.*, p. 58.

[9] Vezi https://api.army.mil/e2/c/downloads/351235.pdf, accesat la 10 februarie 2020.

[10] *Smart* este un cuvânt de origine englezească, al cărui înțeles este inteligent. Cuvântul este și un acronim, care concentrează conceptele de *S*pecificitate, *M*ăsurabilitate, *A*justabilitate, *R*ealizabilitate și *T*imp. Aceste concepte sunt, în același timp, elemente de referință pe care este construit orașul viitorului – *smart city.*

ar fi Irakul, şi în Asia de Sud-Est (Pakistanul), care au suferit 2.965 de atacuri, respectiv 734 de atacuri. Continuând analiza situaţiei şi pentru anii următori, *Action on Armed Violence* concluzionează că, în perioada ianuarie-noiembrie 2016, 236 de atentatori sinucigaşi au acţionat prin detonarea unor încărcături explozive şi au produs moartea a 11.621 de civili, sporind procentul de atacuri sinucigaşe cu 19% şi numărul victimelor cu 78%[11]. Impactul psihologic al acestor atacuri asupra populaţiei este unul foarte puternic emoţional, din cauza efectului de *contagiune mentală şi sugestibilitate* care se propagă extrem de rapid prin mediile de informare online.

Dinamica puterilor economice creează continuu disparităţi şi vulnerabilizează anumite zone[12], fapt care impune propunerea unor soluţii inteligente de protejare a populaţiei şi a resurselor, prin acordarea unei atenţii deosebite investiţiilor în securitate şi apărare. Iată, prin urmare, un argument fundamental pentru conceptul de *urbanizare a războiului* şi susţinerea necesităţii de a crea structuri manageriale specializate care să asigure planificarea inteligentă a oraşelor, având ca efect apărarea populaţiei, a valorilor materiale şi spirituale.

Dinamica puterilor economice creează continuu disparităţi şi vulnerabilizează anumite zone, fapt care impune propunerea unor soluţii inteligente de protejare a populaţiei şi a resurselor, prin acordarea unei atenţii deosebite investiţiilor în securitate şi apărare.

Noul urbanism militar[13] necesită un mod de gândire care presupune preocuparea pentru modalitatea de organizare şi de pregătire a oraşelor în scopul desfăşurării operaţiilor militare în cadrul acestora. Este un proces complex şi multidimensional, deşi componentele sale sunt la fel de vechi ca şi războiul în sine.

DEZVOLTARE URBANĂ INTELIGENTĂ PENTRU ORAŞE MAI SIGURE

Pentru ca orașele să devină mai sigure pentru locuitorii lor, este necesară informarea, educarea și pregătirea populației în ceea ce privește înțelegerea noilor provocări de securitate și în vederea asumării riscului în contextul locuirii în mediul urban.

[11] Sursa: https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/, accesat la 3 februarie 2020.

[12] Creșterea economică a Chinei se așteaptă să încetinească cu până la 4,5% în primele luni ale anului 2020 – cel mai lent ritm de la criza financiară, cauzat de noul coronavirus apărut în Wuhan, COVID-19, și de epidemia care se răspândește în întreaga lume. Vezi https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel/, accesat la 20 februarie 2020.

[13] Fundamentală pentru *noul urbanism militar* este schimbarea paradigmatică ce face din spațiile publice și private ale orașelor, precum și infrastructura acestora – împreună cu populația civilă – o sursă de ținte și amenințări. Vezi Stephen Graham, *Cities under Siege*, *The New Military Urbanism*, Londra, verso, 2010.

În condiţiile ascensiunii oraşelor inteligente, a economiei de spaţiu necesar în cadrul localităţilor, a faptului că aspectul clădirii nu mai este obligatoriu legat de funcţiile pe care aceasta le poate îndeplini şi având în vedere posibilitatea utilizării clădirilor în scopuri multiple (multifuncţionalitate/reconversie funcţională), considerăm că este nevoie de construcţii moderne, flexibile, adaptate şi adaptabile nevoilor de apărare ale oraşelor, dar capabile, în acelaşi timp, să satisfacă atât nevoile forţelor armate într-o manieră rentabilă, cât şi confortul cotidian al locuitorilor în timp de pace. Important este, pentru locuitorii aşezărilor urbane, să simtă şi efectul protecţiei pe care le-o poate oferi spaţiul citadin securizat. În acest context postmodern, apreciem că oraşul are nevoie de construirea şi consolidarea dimensiunii de *intelligence*, cu rolul de intimidare a acţiunilor inamice, glisând spre trecerea de la conceptul de *oraş defensiv* la cel de *oraş inteligent ofensiv*.

În condiţiile ascensiunii oraşelor inteligente, a economiei de spaţiu necesar în cadrul localităţilor, a faptului că aspectul clădirii nu mai este obligatoriu legat de funcţiile pe care aceasta le poate îndeplini, considerăm că este nevoie de construcţii moderne, flexibile, adaptate şi adaptabile nevoilor de apărare ale oraşelor, dar capabile, în acelaşi timp, să satisfacă atât nevoile forţelor armate într-o manieră rentabilă, cât şi confortul cotidian al locuitorilor în timp de pace.

De asemenea, noile standarde pentru clădiri verzi şi inteligente[14] ajută la realizarea construcţiilor în conformitate cu principiile dezvoltării durabile. Fără a avea pretenţia exhaustivităţii, considerăm că, la nivelul *cadrului urban*, pe lângă componentele specifice de apărare, ar trebui să existe preocupări pentru:

- *atenuarea riscurilor cibernetice prin proiectarea inteligentă a* spaţiului cibernetic al oraşului;
- realizarea de construcţii şi infrastructuri flexibile cu un grad ridicat de modularitate, care să permită, în anumite condiţii, utilizarea multiplă, fie în scop civil, fie în scop militar (de către toate categoriile de forţe);
- construirea unor clădiri accesibile şi securizate, conectate cu infrastructura de apărare prin aplicarea de soluţii integrate de mobilitate etc.;
- disimularea construcţiilor militare în ţesutul urban, cu ajutorul materialelor inovative, reducând, astfel, impactul psihologic negativ al prezenţei acestora asupra populaţiei civile[15].

La nivelul elementelor de *viață urbană* se impun:

- analiza comportamentului uman în relație cu prezența clădirilor inteligente (logica umană versus sistemul de control al clădirilor);

[14] Sistemele internaționale de evaluare pentru clădiri verzi și inteligente precum *BREEAM, LEED, Green Globes, Living Building Challenge* etc.

[15] Sorina Georgiana Rusu, *Cerințe militare și civile în procesul de planificare a obiectivelor destinate apărării în localitățile urbane*, în revista *Gândirea Militară Românească*, nr. 1, 2018, p. 77.

- înlocuirea dihotomiei *amic-inamic*, specifică războiului clasic, cu ideea de protejare permanentă a populației;
- educarea și pregătirea populației pentru a înțelege noile provocări de securitate și pentru a acționa în sprijinul forțelor de ordine, fără a se panica și a destabiliza ordinea acțiunilor de apărare.

CONCLUZII

Planificarea spațială a orașelor va suferi modificări substanțiale sub aspectul necesității de a răspunde provocărilor pe care schimbarea conceptelor de „violență” și „violență mascată” o presupune într-un mediu urban. Dezvoltarea tehnologiilor cu dublă utilizare (civil-militară) duce la o simultaneitate periculoasă a utilizării unor instrumente și mijloace de luptă de către civili și militari.

Considerăm că provocările viitoare ale conflictelor armate urbane se vor concentra pe câteva elemente majore. Acestea ar putea fi: multiplicarea amenințărilor mobile, proces susținut de diseminarea informațiilor şi potențialul acces al civililor la diferite tipuri de baze de date; accentuarea fenomenului migrației populației şi a capitalului financiar; posibilitatea izbucnirii unor pandemii şi panica pe care astfel de fenomene o creează în mentalul colectiv (un exemplu, în acest sens, este pandemia provocată de virusul COVID-19), extinderea spațială a confruntărilor în mediul urban prin accentuarea dispersiei de front, în adâncime şi la altitudine, în defavoarea frontului de luptă continuu în mediul urban, specific războaielor clasice, miniaturizarea armelor, aplicând nanotehnologiile şi asigurarea camuflării armelor nou obținute etc.

În acest context, planificarea spațială a orașelor va suferi modificări substanțiale sub aspectul necesității de a răspunde provocărilor pe care schimbarea conceptelor de *violență* şi *violență mascată* o presupune într-un mediu urban. Dezvoltarea tehnologiilor cu dublă utilizare (*civil-militară*) duce la o simultaneitate periculoasă a utilizării unor instrumente şi mijloace de luptă de către civili şi militari.

În contextul lumii contemporane, convingerile ideologice, religioase, precum şi nivelul de educație şi caracteristicile psihologiei maselor au o mare importanță în asigurarea capacității defensive a orașului. Un rol esențial îl au elementele de psihologie a maselor, prin *puterea invincibilă, contagiunea mentală şi sugestibilitatea* care vizează abilitatea comunităților virtuale de a utiliza mijloacele moderne de informare. Utilizarea efectivă a acestora poate constitui atât o amenințare, cât şi o oportunitate, la nivelul securității cibernetice şi la adresa securității mediului fizic[16].

[16] Cf. Sorina Georgiana Rusu, *Planificarea și proiectarea obiectivelor destinate apărării în orașul inteligent*, *op. cit.*

În concluzie, preocuparea pentru modalitatea de organizare şi de pregătire a orașelor în scopul desfășurării operațiilor militare este o nevoie generată de procesul inevitabil, complex şi multidimensional al urbanizării.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

BIBLIOGRAFIE:

1. ***, United Nations, 2011. World Urbanization Prospects, 2011. Department of Economic and Social Affairs, New York.
2. ***, United States Agency for International Development, USAID Policy. Sustainable Service Delivery in an Increasingly Urbanized World. 3, octombrie 2013.
3. J. Bonnet, *Marile Metropole Mondiale*, Editura Institutul European, 2000.
4. Le Corbusier, *Urbanisme*, Flammarion, Paris, 1980.
5. S. Graham, *Cities under Siege*, The New Military Urbanism, Londra, verso, 2010.
6. Sorina Georgiana Rusu, *Cerințe militare și civile în procesul de planificare a obiectivelor destinate apărării în localitățile urbane*, în revista *Gândirea Militară Românească*, Statul Major al Apărării, nr. 1, 2018.
7. Alexandru M. Sandu, *Teoria sistemelor urbane – partea I*, curs universitar, Editura Institutul de Arhitectură *„Ion Mincu”*, București, 1975.
8. Cătălin Zamfir, Lazăr Vlăsceanu, *Dicționar de sociologie*, Editura Babel, București, 1998.

WEBOGRAFIE:

1. https://api.army.mil/e2/c/downloads/351235.pdf
2. https://asc.army.mil/web//wp-content/uploads/2015/01/WinComplexWorld-diagram.jpg
3. http:// esa.un.org/unup/pdf/WUP2011_Highlights.pdf
4. https://mwi.usma.edu/every-city-different-thats-one-size-fits-approach-urban-operations-wont-work/
5. https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/
6. https://www.usaid.gov/sites/default/files/documents/1870/USAIDSustainableUrbanServicesPolicy.pdf
7. https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel/
8. https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel/.

APĂRAREA FIXĂ MARITIMĂ ÎN SECTORUL ROMÂNESC AL MĂRII NEGRE ÎN PERIOADA INTERBELICĂ ȘI ÎNCEPUTUL CELUI DE-AL DOILEA RĂZBOI MONDIAL

Dr. Ion RÎŞNOVEANU

Cercetător științific III, Muzeul Militar Național „Regele Ferdinand I”

În perioada interbelică, factorii politici şi militari cu putere de decizie de la Bucureşti au luat o serie de hotărâri menite să întărească puterea combativă a Armatei Române, în general, a Marinei de Război, din 1931 Marina Regală, în special.

Contextul economic, politic şi geostrategic generat de încheierea Primului Război Mondial şi semnarea aranjamentelor de pace din cadrul Conferinţei de la Paris, care s-a desfăşurat între anii 1919 şi 1920, nu era menit să asigure României liniştea necesară consolidării Statului Naţional Unitar.

Diplomaţiile revizioniste ale Ungariei, Bulgariei dar, mai ales, ale Uniunii Sovietice au făcut ca decidenţii români, atât politici, cât şi militari, să adopte o atitudine vigilentă în raporturile cu statele vecine care, în continuare, emiteau pretenţii teritoriale asupra României.

În ceea ce priveşte apărarea litoralului maritim al României, deşi sumele alocate au fost insuficiente, măsurile luate în acest sens au acoperit, pentru un timp, nevoile Apărării Fixe Maritime. Aceste măsuri vizau ameninţarea unor baterii de coastă cu rolul de a proteja câmpurile de mine din faţa portului Constanţa, dar şi de a respinge o eventuală tentativă de desantare pe apă a trupelor inamice.

Cuvinte-cheie: perioada interbelică, doctrină navală, al Doilea Război Mondial, Apărarea Fixă Maritimă, Comandamentul Marinei Militare.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

CONTEXT INTERNAŢIONAL

Odată înfăptuită unitatea naţională din 1918, Regatul României nu mai avea nicio revendicare teritorială legitimă. Datorită condiţiilor create, în spiritul tradiţiilor naţionale şi în context cu situaţia existentă post-război, conceptul privind dimensiunea maritimo-fluvială a defensivei României reclama, cel puţin pentru început, întrebuinţarea forţelor sale armate limitate la apărarea graniţelor[1].

Din acest motiv, în principal, în perioada interbelică, România a avut o politică navală şi de apărare a zonei de coastă coerentă, însă nu de amploare. Totul a fost condiţionat de noua lungime a litoralului, de aproape 250 km, de contactul direct cu marea deschisă sau oceanul şi de puterea economică generatoare de capacităţi de transport şi de luptă de anvergură.

România a făcut parte din categoria ţărilor cu o preocupare mai redusă pentru accesul la largul mărilor libere, cu flotă comercială şi militară inferioare şi, implicit, cu un grad mai redus de tangentare a resurselor de care au beneficiat acele ţări care au controlat efectiv oceanul planetar.

Rolul artileriei în apărarea litoralului fluvial şi maritim românesc şi importanţa pregătirii ofiţerilor de marină în specialitatea artilerie i-au preocupat pe analiştii militari şi în anii de după Primul Război Mondial.

PRIMELE MĂSURI LUATE DE COMANDAMENTUL MARINEI MILITARE PENTRU ORGANIZAREA APĂRĂRII DE COASTĂ LA ÎNCEPUTUL PERIOADEI INTERBELICE

Rolul artileriei în apărarea litoralului fluvial şi maritim românesc şi importanţa pregătirii ofiţerilor de marină în specialitatea artilerie i-au preocupat pe analiştii militari şi în anii de după Primul Război Mondial. Astfel, comandorul Ioan Bălănescu[2] sublinia, într-o lucrare

[1] Nicolae Koslinski, Raymond Stănescu, *Marina română în al Doilea Război Mondial,* vol. I., Editura Făt-Frumos, București, 1998, p. 19.

[2] Ministerul de Război, *Anuarul Armatei Române pe anul 1920 (ediție provizorie)*, Atelierele Grafice SOCEC&Comp., Societate Anonimă, București, 1921, p. 407. Ioan Bălănescu, comandor în anul 1920, s-a născut la 3 iulie 1878. A absolvit Școala Navală Superioară în anul 1899, fiind înaintat la gradul de sublocotenent la data de 1 iulie. Grade militare obținute în timpul carierei: locotenent (18 mai 1906), căpitan (10 aprilie 1908), locotenent-comandor (10 aprilie 1915), căpitan-comandor (1 septembrie 1917), fiind înaintat la gradul de comandor în anul 1920. Înaintat până la gradul de viceamiral, a fost comandantul Marinei de Război în perioada 1934-1937.

de analiză referitoare la raporturile dintre puterea maritimă şi apărarea naţională, importanţa apărării litoralului prin mijloace fixe, între care menţiona bateriile de coastă[3].

De asemenea, căpitan-comandorul Ioan Izbăşescu[4] şi locotenent-comandorul Alexandru Gheorghiu[5] atrăgeau atenţia, în anul 1920, asupra rolului şi locului artileriei în Marina Militară şi a pregătirii ofiţerilor de marină în această specialitate. Cei doi ofiţeri au precizat că *„artileria are la marină o deosebită importanţă şi este necesar ca fiecare ofiţer, chiar dacă nu este specialist desăvârşit în arma artilerie, să ştie neapărat să utilizeze această armă (...) și, în afară de orice altă specialitate, trebuie să treacă printr-un curs elementar al direcţiilor de tir”*[6].

„Artileria are la marină o deosebită importanţă şi este necesar ca fiecare ofiţer, chiar dacă nu este specialist desăvârşit în arma artilerie, să ştie neapărat să utilizeze această armă și, în afară de orice altă specialitate, trebuie să treacă printr-un curs elementar al direcţiilor de tir”.

Prin Ordinul ministrului de Război nr. 15029 din 24 martie 1921, noua organizare a Marinei Militare cuprindea, printre alte structuri, Apărarea Fixă Fluvială şi Apărarea Fixă Maritimă care, pe lângă serviciul de mine, torpile, staţii T.F.S., aveau în organică şi *tunurile de coastă* sau bateriile de coastă ale Marinei[7].

Apărarea Fixă Fluvială avea în compunerea sa, pe lângă unităţile amintite, şi Grupul şlepurilor armate constituit la 17 noiembrie 1920 în Regimentul Artileriei Fluviale[8].

În cadrul Apărării Fixe Fluviale s-au organizat, pe lângă Grupul şlepurilor armate sau bateriile de coastă plutitoare, denumite astfel în unele documente de epocă, şi baterii flotante, destinate apărării porturilor Galaţi, Brăila şi Sulina. Subunităţile au avut în dotare 14 şlepuri, fiecare armat cu câte un tun. Pe opt şlepuri au fost instalate câte un tun de 152,4 mm, pe patru şlepuri câte un tun de 120 mm, iar pe două

[3] Comandor Ioan Bălănescu, *Puterea maritimă și apărarea națională,* București, f.a., p. 18.
[4] Ministerul de Război, *op. cit*., p. 407. Căpitan-comandorul Ioan Izbășescu s-a născut la data de 3 martie 1881 și a absolvit Școala navală Superioară în anul 1903, fiind înaintat la gradul de sublocotenent la data de 1 iunie. Grade militare obținute în timpul carierei: locotenent (1 iunie 1906), căpitan (1 aprilie 1911), locotenent-comandor (15 august 1916), căpitan-comandor (1 septembrie 1917).
[5] *Ibidem*, p. 410. Locotenent-comandorul Alexandru Gheorghiu s-a născut la 21 septembrie 1890 și a absolvit Academia de Marină din Fiume la 6 iunie 1909, cu gradul de sublocotenent. Grade militare obținute în timpul carierei: locotenent (3 octombrie 1912), căpitan (1 noiembrie 1916), locotenent-comandor (1 septembrie1916).
[6] Căpitan-comandor I. Izbășescu, locotenent-comandor Al.A. Gheorghiu, *Dare de seamă asupra stagiului de stat major în escadra franceză în Mediterana occidentală cu concluziuni și preocupări pentru marina noastră,* București, 1940, p. 62.
[7] Arhivele Militare Române (în continuare, AMR), fond Comandamentul Marinei Militare, dosar 388, ff. 20-21.
[8] *Ibidem*, dosar 290/1920-1921, f. 26.

şlepuri tunuri de 101,6 mm[9]. Cele mai multe dintre aceste nave au fost destinate apărării portului Sulina.

Bateriile flotante, cum mai erau numite, aveau, la 21 decembrie 1920, următoarea compunere: opt şlepuri fiecare cu câte un tun de 152,4 mm la bord, patru şlepuri cu 4 tunuri de 120/50 mm şi două şlepuri cu câte 2 tunuri de 101,6 mm[10]. Tunurile de mare calibru, *Obukov*, de 152,4 mm, au fost capturate în 1918 de la flota rusă dislocată în zona Deltei Dunării în timpul Primului Război Mondial, împreună cu şlepurile la bordul cărora se aflau[11]. Aceste nave armate au fost ancorate în porturile Galaţi şi Brăila, însă şi la Sulina care, şi în perioada interbelică, a reprezentat un punct strategic întărit cu unităţi navale şi artileristice ale Marinei.

Bateriile flotante, cum mai erau numite, aveau, la 21 decembrie 1920, următoarea compunere: opt şlepuri fiecare cu câte un tun de 152,4 mm la bord, patru şlepuri cu 4 tunuri de 120/50 mm şi două şlepuri cu câte 2 tunuri de 101,6 mm. Tunurile de mare calibru, Obukov, de 152,4 mm, au fost capturate în 1918 de la flota rusă dislocată în zona Deltei Dunării în timpul Primului Război Mondial, împreună cu şlepurile la bordul cărora se aflau.

Pentru apărarea dinspre uscat a litoralului maritim, având limite în sud zona Balcic, iar la nord limanul Nistrului, s-a constituit Apărarea Fixă Maritimă, în compunerea căreia se găseau şi bateriile de coastă.

DOTAREA ŞI REORGANIZAREA APĂRĂRII FIXE MARITIME ÎN PERIOADA INTERBELICĂ

Sectorul dedicat Apărării Fixe Maritime cu Cartierul General în garnizoana Constanţa era cuprins între Limanul Nistrului, la nord, şi Balcic-Ecrene, la sud. În noua organizare, Sectorul Maritim nr. 1 Sud, care primise ca arie de responsabilitate zona cuprinsă între Balcic şi Gura Portiţei, avea în compunerea sa şi bateriile de coastă, a căror dislocare pe noul aliniament a început în anul 1926.

Tot în 1926, tunurile de 152,4 mm *Armstrong* de la distrugătoarele N.M.S. MĂRĂŞEŞTI şi N.M.S. MĂRĂŞTI au fost demontate şi debarcate, pentru a fi înlocuite cu altele mai moderne, şi amplasate în Constanţa, la punctul *Tataia*, pe platforma şi cazematele betonate construite de germani în timpul Primului Război Mondial. În această primă baterie de coastă de pe litoral au fost instalate, în anul 1926, patru tunuri de 152,4 mm L/45 *Armstrong* şi de 76,2 mm L/50 *Armstrong*. Tunurile de 152,4 mm erau încadrate cu câte opt servanţi, iar cele de 76,2 mm cu câte şase marinari.

[9] *Idem*, dosar 308/1916, f.160.
[10] *Ibidem*, f. 160.
[11] Relatările plutonierului major Marin Tănase, activ la această baterie din anul 1926 până în anul 1946.

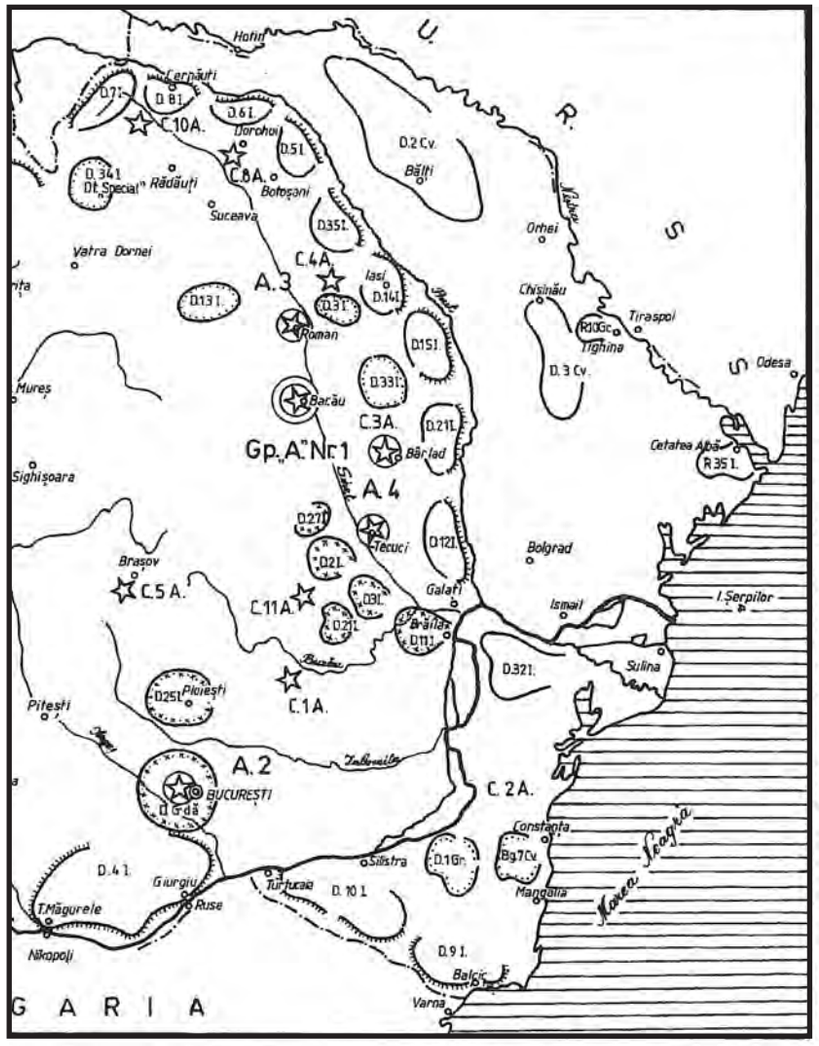

Foto 1: Dispunerea marilor unități ale Armatei Române în vederea apărării Dobrogei și a litoralului românesc în perioada interbelică[12]

În aceeaşi perioadă, pe litoralul maritim s-au făcut studii pe teren pentru a stabili cele mai bune poziţii în vederea amplasării de noi baterii, astfel încât să se asigure o eficientă încrucişare a focului şi o bună apărare a Constanţei şi a fâşiilor de litoral de la nord şi sud de port. În urma studierii informaţiilor centralizate, ofiţerii specialişti

[12] AMR, fond Apărarea Fixă Maritimă, dosar 51/1933-1938, f. 270.

au concluzionat că cele mai corecte puncte erau Midia, Viile Noi, Constanţa şi Agigea. Suprafeţele de teren pe care urmau să fie amplasate noile baterii de coastă au fost declarate *de utilitate publică*, urmând a fi expropriate[13].

În bateria *Tataia* care, ulterior, a primit numele de *Tudor*, se aflau în cazematele betonate depozitele de muniţii ale Diviziei de Mare, aprovizionate de cele centrale de la Hinog, iar mai târziu de cele de la Ţăndărei, care deserveau întreaga Marină.

La această baterie, în anii următori s-au realizat noi amenajări şi dotări. Astfel, în anii 1933 şi 1934, s-au executat lucrări de consolidare a malului litoral în marginea căruia se aflau amplasate aceste tunuri, s-a introdus iluminatul electric, s-au stabilit legături telefonice cu Comandamentul Apărării Fixe Maritime şi s-au amplasat două posturi de mitralieră antiaeriană (AA). În anul 1935, s-a construit, cu mijloace proprii, o centrală de tir şi transmisiuni, s-au introdus sonerii la fiecare din cele patru tunuri de 152,4 mm, putându-se executa, astfel, trageri la comandă.

În vederea economisirii muniţiei de mare calibru la tunurile de 152,4 mm, în baterie s-au montat ţevi de 37 mm, apoi arme de 6,5 mm, pentru trageri de exerciţiu, tir redus[14].

Primul comandant al bateriei *Tataia* a fost locotenentul Dumitru Constantinescu, fiind urmat, printre alţii, de locotenentul Gheorghe Chiriac, locotenentul Ioan Tocineanu, locotenentul Haralambie Stănescu, căpitanul Nicolae Mihalcea şi căpitanul Marin Trache. În această baterie, tunar-şef, de la înfiinţare până în anul 1946, a fost plutonierul-adjutant Marin Tănase, care, în acelaşi timp, a îndeplinit şi funcţia de şef depozit muniţii[15].

Pe litoralul mării s-au întreprins acţiuni pentru montarea altor baterii de coastă în diferite puncte, în funcţie de modul de încrucişare a focului artileriei pentru a cuprinde întregul litoral românesc, precum şi a obiectivelor de apărat. Astfel, în punctul Capul Midia, în anul 1929, prin Înalt Decret, s-a declarat de utilitate publică în interiorul apărării o suprafaţă de 76 058 m^2 din arealul comunei Gargalîc (Corbu), judeţul

Primul comandant al bateriei „Tataia" a fost locotenentul Dumitru Constantinescu, fiind urmat, printre alţii, de locotenentul Gheorghe Chiriac, locotenentul Ioan Tocineanu, locotenentul Haralambie Stănescu, căpitanul Nicolae Mihalcea şi căpitanul Marin Trache. În această baterie, tunar-şef, de la înfiinţare până în anul 1946, a fost plutonierul-adjutant Marin Tănase, care, în acelaşi timp, a îndeplinit şi funcţia de şef depozit muniţii.

[13] *Ibidem.*
[14] Arhiva Muzeului Naţional al Marinei Române (în continuare, AMNMR), *Registrul istoric al Apărării Fixe Maritime*.
[15] *Ibidem*.

Constanţa[16]. Aici au început lucrările de construcţie a amplasamentelor de beton pentru două baterii de 152,4 mm *Obukov*. Cele patru tunuri *Obukov*, de pe şlepurile armate, au stat mulţi ani depozitate în incinta bateriei *Tataia*, până în octombrie 1939, când au fost montate în amplasamentele betonate deja construite.

Bateria era organizată ca un punct fortificat, cu şanţuri şi sârmă ghimpată în jurul ei. Era camunflată în chip de mică fermă, cu grădini de legume. Pentru apărarea AA, avea o secţie de 20 mm. Printre comandanţii bateriei *Mircea*, cum va fi numită, pot fi amintiţi căpitanul Gheorghe Gabroveanu, căpitanul Anton Petriman şi căpitanul Marin Trache.

Un moment important în reorganizarea Marinei de Război a fost reprezentat de anul 1931. După modelul Marii Britanii, prin Decretul Regal nr. 4063 din 15 decembrie 1931, denumirea de Marina de Război s-a schimbat în Marina Regală, iar Comandamentul Marinei Militare a fost redenumit Comandamentul Marinei Regale, cu atribuţii de comandament şi de inspectorat de armă, în structura Ministerului Apărării Naţionale.

Un moment important în reorganizarea Marinei de Război a fost reprezentat de anul 1931. După modelul Marii Britanii, prin Decretul Regal nr. 4063 din 15 decembrie 1931, denumirea de *Marina de Război* s-a schimbat în *Marina Regală*, iar Comandamentul Marinei Militare a fost redenumit Comandamentul Marinei Regale, cu atribuţii de comandament şi de inspectorat de armă, în structura Ministerului Apărării Naţionale[17].

În planurile de pregătire în vederea apărării litoralului au fost angrenate, în deceniul patru, şi bateriile de coastă. Astfel, la o aplicaţie desfăşurată în cursul lunii septembrie 1932 în sectorul Mamaia-Năvodari a luat parte şi o baterie de 77 mm. Prezenţa ei a fost mai mult simbolică, întrucât, neavând muniţie, n-a executat nicio misiune de foc. În cadrul bilanţului aplicaţiei s-a tras, însă, o concluzie importantă, şi anume că bateriile de coastă de calibru mic trebuiau dotate cu mijloace de deplasare rapidă pentru a deveni *„elementul mobil al planului de foc al apărării de coastă”*[18].

O altă baterie de coastă instalată pe litoral a fost cea de la Agigea. Lucrările au început în anul 1932 pentru amplasarea unei baterii de 120 mm *St. Chamond*, dar mult mai târziu, în anul 1939, s-au instalat trei tunuri de 120 mm *Armstrong*, de pe crucişătorul N.M.S. ELISABETA,

[16] AMR, fond Apărarea Fixă Maritimă, dosar 16, f. 193.
[17] Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Florin Stan, Tanța Mândilă, Andrei Vochițu, Ion Rîșnoveanu, *Istoria Statului Major al Forțelor Navale Române. 1860-2010. Monografie*, București, Editura Centrului Tehnic-Editorial al Armatei, 2010, p. 235. Vezi și comandor (r.) (coord..) Anton Bejan, *Dicționar enciclopedic de marină*, Editura Societății Scriitorilor Militari, București, 2006, p. 322.
[18] AMR, fond Apărarea Fixă Maritimă, dosar 51/1933-1938, ff. 156-157.

folosite şi în fortificaţiile de la Turtucaia, în anul 1916. Bateria *Elisabeta*, cum a fost numită, era organizată tot ca un punct fortificat cu şanţuri, postamente şi depozite betonate. Printre comandanţii acestei baterii sunt cunoscuţi căpitanii Gheorghe Costăchescu şi Alexandru Chiriac.

În şedinţa din 7 septembrie 1932, Comitetul Marinei Regale a făcut o analiză atât a situaţiei tehnice a bateriilor de coastă, cât şi a necesarului de unităţi pe regiunile de litoral. La stabilirea necesarului şi dispunerea bateriilor s-au avut în vedere şi misiunile ce trebuiau executate împotriva aviaţei inamice. Din studiile realizate de specialiştii militari a reieşit faptul că, în regiunea Sulina trebuiau amplasate patru tunuri de 250 mm, patru tunuri de 155 mm, patru tunuri de 120 mm, opt tunuri de 100 mm şi 26 de tunuri de 40 mm. În regiunea Taşaul-Constanţa-Tuzla erau necesare patru tunuri de 250 mm, opt tunuri de 155 mm, opt tunuri de 100 mm, precum şi 16 tunuri de 40 mm. De asemenea, în regiunea de sud Tuzla-Ecrene se aprecia că trebuiau amplasate opt tunuri de 100 mm şi opt tunuri de 40 mm.

Costurile financiare ridicate ale bateriilor, dar şi ale lucrărilor de amplasare au determinat Direcţia Marinei din Ministerul de Război să ceară scoaterea din programul de înzestrare a bateriilor de 240 mm ce trebuiau instalate pe cale ferată. Comitetul Marinei Regale nu a agreat modificările cerute la planul de înzestrare şi organizare a bateriilor de coastă. De aceea, în şedinţa din 27 aprilie 1936, specialiştii din cadrul Comandamentului Marinei Regale s-au exprimat în acest sens, mai mult, au afirmat *„dorinţa de a se realiza cât mai repede”*[19].

Dintr-o dare de seamă privind activitatea Apărării Fixe Maritime pe lunile iunie-octombrie 1932 aflăm că, în afară de bateria *Tataia*, care era amplasată judicios, celelalte baterii de coastă aveau o dispunere *„ineficientă cantitativ şi calitativ faţă de zonele sensibile pe care le au de apărat”*[20]. Astfel, bateria *Midia*, din poziţia în care se afla, nu putea acoperi cu foc integral sectorul de la sud de capul Midia, apreciat ca *„cel mai sensibil al coastei”*[21].

Dintr-o dare de seamă privind activitatea Apărării Fixe Maritime pe lunile iunie-octombrie 1932 aflăm că, în afară de bateria „Tataia”, care era amplasată judicios, celelalte baterii de coastă aveau o dispunere „ineficientă cantitativ şi calitativ faţă de zonele sensibile pe care le au de apărat”. Astfel, bateria “Midia”, din poziţia în care se afla, nu putea acoperi cu foc integral sectorul de la sud de capul Midia, apreciat ca „cel mai sensibil al coastei”.

În aceste condiţii, în urma unor studii minuţioase, specialiştii din Comandamentul Marinei Regale au propus mutarea bateriei spre sud

[19] *Ibidem*, ff. 156-157.
[20] *Ibidem*, dosar 33 /1932, f. 101.
[21] *Ibidem*.

cu 500-1.000 m, punct în care *„materialul de 152 mm poate îndeplini misiunea sa esenţială”*[22].

Nici bateria *Viile Noi* nu fusese amplasată în cel mai bun punct pentru apărarea portului Constanţa. Se propunea reamplasarea ei pe terasa inferioară a malului, de unde se puteau executa atât tragerile în condiţii eficiente, cât şi o mascare mai bună. În document se propunea ca şi bateria *Agigea* să fie mutată la circa 600 m N-E.

Comisia care a analizat fâşia de litoral Constanţa-Midia a propus, într-un raport înaintat Diviziei de Mare, mutarea spre sud cu 500-1.000 m a bateriei „Tataia” pentru a acoperi mai bine cu foc sectorul Sud Cap Midia. Cealaltă comisie, care a studiat în teren zona Viile Noi-Mangalia, a propus amplasarea bateriei Vii pe terasa superioară a Vilei Zosima, unde, în timpul ocupaţiei din anii 1916-1918, germanii avuseseră o baterie antiaeriană.

Pe lângă măsurile de reamplasare a bateriilor, în *Darea de seamă* se avansau şi propuneri pentru reorganizarea unităţilor de artilerie de coastă. Acestea trebuiau reunite în două grupuri. Unul urma să coordoneze bateriile de la nord, iar celălalt de la sud de Constanţa, fiecare cu comandament propriu. Totodată, materialul de analiză solicita eşaloanelor superioare luarea unor hotărâri definitive privind punctele de amplasare ale noilor baterii de coastă şi executarea de lucrări în teren.

În a doua parte a lunii august 1933, două comisii au efectuat noi studii pe litoral pentru instalarea bateriilor de coastă. Comisia care a analizat fâşia de litoral Constanţa-Midia a propus, într-un raport înaintat Diviziei de Mare, mutarea spre sud cu 500-1.000 m a bateriei *Tataia* pentru a acoperi mai bine cu foc sectorul Sud Cap Midia. Cealaltă comisie, care a studiat în teren zona Viile Noi-Mangalia, a propus amplasarea bateriei *Vii* pe terasa superioară a Vilei Zosima, unde, în timpul ocupaţiei din anii 1916-1918, germanii avuseseră o baterie antiaeriană. Se propunea, de asemenea, ca, într-o poziţie mai joasă, să se instaleze o baterie cu tunuri de calibru mai mic. Studiind plaja Mangalia, comisia a apreciat că aceasta *poate fi deosebită pentru debarcări* şi a propus efectuarea unei analize speciale în vederea stabilirii mijloacelor de infanterie şi artilerie necesare apărării zonei[23].

De altfel, dintr-un raport al Comandamentului Apărării Fixe Maritime reiese cu claritate că *posibilităţile tactice ale materialului de artilerie al Apărării Fixe Maritime sunt foarte reduse* în comparaţie cu lungimea fâşiei de litoral care trebuia apărată dinspre uscat.

[22] *Ibidem*, f. 23.
[23] *Ibidem*, f. 23. Vezi și AMNMR, *Registrul istoric al Apărării Fixe Maritime*, p. 9.

Din cele 18 tunuri repartizate bateriilor de coastă, numai opt erau montate în teren. Celelalte 10 erau depozitate la bateria *Tataia*, întreţinerea lor efectuându-se cu dificultate, din lipsă de fonduri[24].

Concentrarea pieselor artileristice la *Tataia*, al cărei inventar a sporit în anul 1933 cu câteva tunuri de 152 mm, îngrijora comanda Apărării Fixe Maritime, întrucât, în cazul unui bombardament inamic, puteau fi distruse în totalitate.

O altă problemă semnalată de Apărarea Fixă Maritimă a fost aceea a dificultăţilor de deplasare a tunurilor pe timp nefavorabil de pe o poziţie pe alta, întrucât între baterie şi şoseaua Constanţa-Mamaia nu exista un drum pietruit de legătură[25]. După mai multe intervenţii, s-au obţinut 555 de tone de piatră pentru construirea drumului de acces spre baterie.

Fenomenul eroziunii malurilor din apropierea punctului bateriei *Tataia* a produs Comandamentului Apărării Fixe Maritime o îngrijorare justificată. Luând cunoştinţă de informaţiile cuprinse în rapoartele prezentate, comandantul Diviziei de Mare a ordonat efectuarea unei cercetări în teren. Constatându-se că pericolul este real, s-a propus reamplasarea bateriei pe o altă poziţie, solicitare aprobată de Comandamentul Marinei Regale.

În perioada interbelică, bateria *Tataia* s-a confruntat şi cu alte probleme. Avea nevoie de o remiză, de capote pentru tunurile de 75 mm, de aparate de conducerea tirului la bateria de 76 mm AA, precum şi de muniţie pentru bateria de 77 mm.

Pe linia pregătirii de luptă, rezultatele bateriei *Tataia* au fost apreciate pozitiv. Bunăoară, la 11 septembrie 1933, viceamiralul Vasile Scodrea, comandantul Marinei Regale, aprecia că pregătirea de specialitate era *„mai mult decât mulţumitoare”*[26].

Aceleaşi aprecieri le-a comunicat şi contraamiralul Petre Bărbuneanu, comandantul Diviziei de Mare, la 16 martie 1934. Inspectând bateria, *„a rămas mulţumit de rezultatele obţinute şi a adus laude”*[27], după cum s-a consemnat în *„Registrul istoric al Apărării Fixe Maritime”*[28].

Fenomenul eroziunii malurilor din apropierea punctului bateriei „Tataia” a produs Comandamentului Apărării Fixe Maritime o îngrijorare justificată. Luând cunoştinţă de informaţiile cuprinse în rapoartele prezentate, comandantul Diviziei de Mare a ordonat efectuarea unei cercetări în teren. Constatându-se că pericolul este real, s-a propus reamplasarea bateriei pe o altă poziţie, solicitare aprobată de Comandamentul Marinei Regale.

[24] *Ibidem*, f. 35.
[25] *Ibidem*, f. 37.
[26] AMNMR, *loc. cit.*, p. 9.
[27] *Ibidem*, p. 15.
[28] *Ibidem*.

Inspecţiile celor doi comandanţi au mai avut ca efect şi executarea unor lucrări pe linie logistică. În cursul lunilor aprilie-iunie 1934, la bateria *Tataia* s-a finalizat instalarea reţelei electrice şi telefonice, s-a construit remiza pentru adăpostul tunurilor şi s-au amenajat locaşurile mitralierelor antiaeriane[29].

Întrucât, pentru tunurile de 152,4 mm, nu s-a putut asigura muniţia necesară, în cursul lunii iulie 1934 s-au montat şi ajustat ţevi de 37 mm, cu care s-au executat şi primele trageri de exerciţiu pe timp de zi şi de noapte. La tragerile din noaptea de 3 octombrie 1934 a asistat şi contraamiralul Petre Bărbuneanu, care a felicitat efectivul bateriei pentru modul în care misiunea a fost îndeplinită.

Pentru îmbunătăţirea cadrului de instruire, la 20 octombrie 1934, ordinea de bătaie a Apărării Fixe Maritime a fost modificată. S-au înfiinţat trei companii de pregătire a soldaţilor ce urmau să încadreze bateria 152,4 mm, secţia 77 mm, secţia 76 mm A. şi secţia proiectoare. La bateria *Tataia* s-a înfiinţat un centru de instrucţie pentru centralişti, telemetrişti şi observatorii necesari bateriilor de coastă ale Marinei Regale.

Asigurarea muniţiei necesare a permis ca, în a doua parte a anului 1935, să se execute mai multe exerciţii de tragere, rezultatele lor fiind foarte bune, ca şi în ceilalţi ani[30]. Pe lângă pregătirea tunarilor, tragerile directe şi indirecte executate la bateria *Tataia*, prin intermediul centralei de tir şi al mijloacelor de transmisiuni, şi şedinţele de tragere au permis verificarea constantă a aparaturii.

O problemă care a preocupat conducerea Marinei Regale până în preajma intrării în război a fost întărirea puterii foc a bateriilor de coastă. La 22 ianuarie 1937, Comitetul Marinei a luat, din nou, în dezbatere posibilitatea achiziţionării şi instalarii unei baterii de 240 mm. S-au analizat ofertele firmelor *Bofors* şi *Solothurn*. Problema a fost analizată în şedinţa Comitetului Marinei din 13 octombrie 1937, în care s-a precizat că Marina *„nu poate renunţa la procurarea bateriei de 240 mm”*[31].

Cu toate eforturile depuse, materializate prin rapoarte trimise Ministerului Apărării Naţionale, lipsa fondurilor n-a permis achiziţionarea

O problemă care a preocupat conducerea Marinei Regale până în preajma intrării în război a fost întărirea puterii foc a bateriilor de coastă.
La 22 ianuarie 1937, Comitetul Marinei a luat, din nou, în dezbatere posibilitatea achiziţionării şi instalarii unei baterii de 240 mm.
S-au analizat ofertele firmelor „Bofors” şi „Solothurn”. Problema a fost analizată în şedinţa Comitetului Marinei din 13 octombrie 1937, în care s-a precizat că Marina „nu poate renunţa la procurarea bateriei de 240 mm”.

[29] *Ibidem*, p. 19.
[30] *Ibidem*, pp. 29-30.
[31] AMR, fond Comandamentul Marinei Militare, dosar 1221/1940, f. 764.

şi instalarea unei asemenea baterii. Ea a rămas un deziderat, chestiunea fiind reluată de Comandamentul Marinei Regale la 18 ianuarie 1940, când s-a hotărât încadrarea în planul de înzestrare la urgenţa a treia[32].

Concomitent, s-au făcut noi studii pe litoral vizând atât dispunerea tunurilor, cât şi înzestrarea cu noi baterii. S-a apreciat că, pentru apărarea portului Constanţa, erau necesare şapte-opt baterii, din care patru cu tragere rapidă, două la Constanţa şi una la Agigea. În zona Jibrieni erau necesare cinci baterii, precizându-se că *„lucrările actuale prevăd o singură baterie”*[33]. Studiile au relevat că la Sulina era necesară o baterie cu patru piese, iar la Vâlcov cel puţin o baterie cu acelaşi număr de piese, fiecare baterie trebuind să fie completată cu o mitralieră AA. Studiul aprecia că respingerea unui potenţial adversar se putea realiza cu *22 de piese de artilerie, adică circa şase baterii de 120-150 mm, cu o bătaie de 18-20 km.* În document se preciza că, dacă flota era înzestrată cu două distrugătoare dotate cu 10 piese de artilerie, numărul bateriilor de coastă se putea reduce la trei[34].

Calculele ofiţerilor specialişti din cadrul Comandamentului Marinei Regale au demonstrat că planul de dotare cu cele 22 de piese de artilerie însuma 2.361.084.000 de lei[35].

Conştienţi că bugetul nu putea să asigure această sumă, autorii studiului din anul 1938 propuneau întărirea sistemului bateriilor de coastă cu patru baterii de 150 mm din rezerva artileriei, şase tunuri de 152 mm de la distrugătoarele N.M.S MĂRĂŞTI şi N.M.S. MĂRĂŞEŞTI, patru tunuri de pe crucişătorul N.M.S. ELISABETA, precum şi o baterie de 75 mm[36].

O altă comisie, condusă de contraamiralul Izbăseşcu, a analizat în teren apărarea portului Constanţa. S-a propus comandantului Marinei Regale ca bateria de 75 mm cu tunuri *St. Chammond* să nu fie mutată în punctul *Vii* din sudul oraşului, misiunea acesteia putând fi preluată de o baterie de 47 mm, pe care autorii studiului preconizau *„să fie instalată pe zidul de sud al bazinului de petrol”*[37].

Pentru apărarea portului Constanţa, erau necesare şapte-opt baterii, din care patru cu tragere rapidă, două la Constanţa şi una la Agigea. În zona Jibrieni erau necesare cinci baterii, precizându-se că „lucrările actuale prevăd o singură baterie”. Studiile au relevat că la Sulina era necesară o baterie cu patru piese, iar la Vâlcov cel puţin o baterie cu acelaşi număr de piese, fiecare baterie trebuind să fie completată cu o mitralieră AA.

[32] *Ibidem*, f. 766.
[33] *Idem*, dosar 801 /1938, f. 12.
[34] *Ibidem*, f. 12.
[35] *Ibidem*, f. 17.
[36] *Ibidem*, f. 22.
[37] *Ibidem.*

ORGANIZAREA ARTILERIEI ÎN ZONA COSTIERĂ A ROMÂNIEI LA SFÂRŞITUL PERIOADEI INTERBELICE ŞI ÎNCEPUTUL CELUI DE-AL DOILEA RĂZBOI MONDIAL

Izbucnirea celui de-al Doilea Război Mondial, la 1 septembrie 1939, odată cu invadarea Poloniei de către Germania, şi, mai ales, intrarea României în această conflagraţie la 22 iunie 1941, împotriva Uniunii Sovietice, au impus factorilor politici şi militari de la Bucureşti cu putere de decizie necesitatea de a lua măsuri ample pentru întărirea capacităţii de respingere a unei eventuale tentative de debarcare a inamicului în zona costieră românească de la Marea Neagră.

Izbucnirea celui de-al Doilea Război Mondial, la 1 septembrie 1939, odată cu invadarea Poloniei de către Germania, şi, mai ales, intrarea României în această conflagraţie la 22 iunie 1941 împotriva Uniunii Sovietice, au impus factorilor politici şi militari de la Bucureşti cu putere de decizie necesitatea de a lua măsuri ample pentru întărirea capacităţii de respingere a unei eventuale tentative de debarcare a inamicului în zona costieră românească de la Marea Neagră.

O primă măsură luată de autorităţile militare româneşti a fost legată de reorganizarea unităţilor care formau apărarea costieră. Astfel, prin Ordinul Comandamentului Marinei Regale nr. 663 din 12 martie 1941, s-a constituit Comandamentul Artileriei de Coastă, Mare Unitate care avea misiunea să organizeze şi să conducă sistemul defensiv costier românesc de la Marea Neagră.

La începutul anilor ’40 ai secolului trecut, artileria de coastă românească dispunea de echipament artileristic depăşit fizic şi moral, care nu putea asigura, decât parţial, protecţia câmpului de mine ce înconjura portul Constanţa, cu atât mai puţin respingerea unei misiuni de debarcare a forţelor navale sovietice în această zonă.

De aceea, Misiunea Marinei de Război germane în România, parte a Misiunii Militare germane la Bucureşti, împreună cu ofiţeri specialişti din cadrul Comandamentului Marinei Regale române au conceput un plan de consolidare a sistemului defensiv costier românesc de la Marea Neagră.

În acest sens, alianţa cu Germania a adus cu sine amenajarea unei baterii de coastă germane la sud de Constanţa, în zona localităţii Lazu, bateria *Tirpitz*, precum şi a bateriei mobile *Lange Bruno*, montată pe calea ferată, în zona Mamaia-Sat. Astfel, în iarna anului 1940, au fost aduse la Constanţa şase tunuri model SK L/45 calibru 280 mm, provenind din rezervele pentru cuirasatele germane din clasa *Nassau* din Primul Război Mondial. Trei astfel de piese de artilerie au intrat în organica bateriei *Tirpitz*, amenajată în zona Lazu, celelalte trei fiind

dislocate în organica unei baterii mobile pe calea ferată, la nord de Constanţa[38].

Lucrările specifice de amenajare a bateriei din zona de sud a Constanţei au fost finalizate în primăvara anului 1941, aceasta dispunând şi de tunuri AA calibru 88 mm, tunuri anticar de 75 mm, precum şi de o subunitate motorizată, care avea misiunea de a bloca înaintarea blindatelor pe şenile inamice. De asemenea, întreaga bază era înconjurată de garduri de sârmă ghimpată, fiind deservită de aproximativ 600 de militari.

Bateria mobilă *Lange Bruno*, dispusă pe calea ferată de la nord de Constanţa, în zona Mamaia-Sat, avea misiunea de a opri o eventuală debarcare sovietică pe plaja de la Mamaia, perimetru uşor de abordat datorită plajelor întinse.

Intrate în serviciul activ în martie 1941, cele două baterii aveau ca misiune principală protejarea câmpului de mine din jurul portului Constanţa, dar şi lovirea de la distanţă a navelor sovietice care ar fi atacat zona, fie pentru a produce pagube oraşului şi instalaţiilor portuare, fie pentru forţarea unei debarcări.

Fiecare dintre cele şase tunuri avea o greutate de 40 t, cu o lungime a ţevii de 12 m, cu o cadenţă de trei lovituri pe minut. Muniţia folosită era reprezentată de proiectile în greutate de 300 kg şi o lungime totală de 90 cm.

Bateria *Tirpitz* a acţionat cu foc în situaţie de luptă o singură dată, în ziua de 26 iunie 1941, în timpul unui atac întreprins de o formaţiune de nave din cadrul Flotei sovietice la Marea Neagră, condusă de distrugătoarele grele de comandament HARKOV şi MOSKVA[39].

În timpul acţiunii, la ora 4.22, bateria a executat salve de foc cu toate cele trei tunuri, reuşind, împreună cu forţele româneşti, să respingă atacul sovietic.

Lucrările specifice de amenajare a bateriei din zona de sud a Constanţei au fost finalizate în primăvara anului 1941, aceasta dispunând şi de tunuri AA calibru 88 mm, tunuri anticar de 75 mm, precum şi de o subunitate motorizată, care avea misiunea de a bloca înaintarea blindatelor pe şenile inamice. De asemenea, întreaga bază era înconjurată de garduri de sârmă ghimpată, fiind deservită de aproximativ 600 de militari.

[38] Ioan Damaschin, *Lupta aero-navală de la Constanța din 26 iunie 1941. Cine a scufundat distrugătorul lider MOSKVA?*, Editura Militară, București, 2014, p. 10 și următoarele.

[39] *Ibidem*, p. 22 și următoarele. Vezi și Ioan Damaschin, *Război submarin la Marea Neagră*, Editura Militară, București, 2016, p. 21 și următoarele, și Jürgen Rohwer, *Chronology of the War at Sea. 1939-1945: The Naval History of World War 2*, Naval Institute Press, Annapolis, 2005, p. 83.

CONCLUZII

În perioada interbelică, factorii politici şi militari cu putere de decizie de la Bucureşti au luat o serie de hotărâri menite să întărească puterea combativă a Armatei Române, în general, a Marinei de Război, din 1931 Marina Regală, în special.

Contextul economic, politic şi geostrategic generat de încheierea Primului Război Mondial şi semnarea aranjamentelor de pace din cadrul Conferinţei de la Paris, care s-a desfăşurat între anii 1919 şi 1920, nu era menit să asigure României liniştea necesară consolidării Statului Naţional Unitar.

Diplomaţiile revizioniste ale Ungariei, Bulgariei, dar, mai ales, ale Uniunii Sovietice au făcut ca decidenţii români, atât politici, cât şi militari, să adopte o atitudine vigilentă în raporturile cu statele vecine care, în continuare, emiteau pretenţii teritoriale asupra României.

Diplomaţiile revizioniste ale Ungariei, Bulgariei, dar, mai ales, ale Uniunii Sovietice au făcut ca decidenţii români, atât politici, cât şi militari, să adopte o atitudine vigilentă în raporturile cu statele vecine care, în continuare, emiteau pretenţii teritoriale asupra României.

În ceea ce priveşte apărarea litoralului maritim românesc, toţi cei care au ocupat, în perioada analizată, funcţia de comandanţi ai Marinei de Război, din 1931 Marina Regală, au avut preocupări majore pentru organizarea unui dispozitiv defensiv în zona costieră menit să descurajeze o eventuală agresiune armată venită, în special, din partea Uniunii Sovietice[40].

Deşi sumele alocate au fost, de cele mai multe ori, insuficiente, totuşi măsurile luate au acoperit, pentru un timp, necesarul Marinei de Război în vederea amenajării unor baterii de coastă care aveau rolul de a proteja atât câmpurile de mine din faţa portului Constanţa, cât şi să respingă o eventuală tentativă de desantare pe apă a trupelor inamice.

BIBLIOGRAFIE:

1. ***, Arhivele Militare Române, fond Comandamentul Marinei Militare.
2. ***, Arhiva Muzeului Naţional al Marinei Române, *Registrul istoric al Apărării Fixe Maritime*.
3. ***, Ministerul de Război, *Anuarul Armatei Române pe anul 1920 (ediţie provizorie)*, Atelierele Grafice SOCEC&Comp., Societate Anonimă, Bucureşti, 1921.

[40] Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Florin Stan, Tanța Mândilă, Andrei Vochițu, Ion Rîșnoveanu, *op. cit*., p. 250 și următoarele. Cei care au condus, în această perioadă, Marina Militară, din 1931 Marina Regală, au fost: viceamiralul Constantin Bălescu (1917-1920), contraamiralul Constantin Niculescu-Rizea (1920-1921 interimar și 1921-1925), viceamiraul Vasile Scodrea (1925-1934), viceamiralul Ioan Bălănescu (1934-1937), amiralul Petre Bărbuneanu (1937-1940) și viceamiralul ing. Eugeniu Roșca (1940-1941).

4. Comandor Ioan Bălănescu, *Puterea maritimă şi apărarea naţională,* Bucureşti, f.a.
5. Comandor (r.) Anton Bejan (coord.), *Dicţionar enciclopedic de marină*, Editura Societăţii Scriitorilor Militari, Bucureşti, 2006.
6. Ioan Damaschin, *Lupta aero-navală de la Constanţa din 26 iunie 1941. Cine a scufundat distrugătorul lider MOSKVA?*, Editura Militară, Bucureşti, 2014.
7. Olimpiu-Manuel Glodarenco, Andreea Atanasiu-Croitoru, Florin Stan, Tanţa Mândilă, Andrei Vochiţu, Ion Rîşnoveanu, *Istoria Statului Major al Forţelor Navale Române. 1860-2010. Monografie*, Bucureşti, Editura Centrului Tehnic-Editorial al Armatei, 2010.
8. Căpitan-comandor I. Izbăşescu, locotenent-comandor Al.A. Gheorghiu, *Dare de seamă asupra stagiului de stat major în escadra franceză în Mediterana occidentală cu concluziuni şi preocupări pentru marina noastră,* Bucureşti, 1940.
9. Nicolae Koslinski, Raymond Stănescu, *Marina română în al Doilea Război Mondial,* vol. I., Editura Făt-Frumos, Bucureşti, 1998.
10. Jürgen Rohwer, *Chronology of the War at Sea. 1939-1945: The Naval History of World War 2*, Naval Institute Press, Annapolis, 2005.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

NICOLAE ȘTEFĂNESCU
– ÎN SERVICIUL STATULUI ȘI AL NAȚIUNII ROMÂNE –

Sorin APARASCHIVEI
Academia Națională de Informații „Mihai Viteazul”, București

Deși aproape necunoscut în istoriografia domeniului, Nicolae Ștefănescu face parte din galeria figurilor ilustre ale spionajului și contraspionajului românesc. Și-a început cariera la Poliția de Siguranță, unde a excelat în identificarea și neutralizarea organizațiilor de spionaj bolșevice. A fost șeful Serviciului de Informații Externe pe spațiul URSS din cadrul Direcției Poliției și Siguranței Generale.

Fiindu-i remarcată activitatea, „ca element inteligent și voios”, Mihail Moruzov i-a propus acestuia să treacă la Serviciul „S” al Armatei Române, propunere aceptată în ianuarie 1931, unde va prelua conducerea Secției Contrainformații, având gradul de director. Peste câțiva ani, a fost numit șeful Corpului Detectivilor și directorul Poliției de Siguranță din Direcția Generală a Poliților. Întreaga sa activitate în serviciul statului și națiunii române constituie un model de profesionalism și devotament.

Cuvinte-cheie: informații, Serviciul Secret al Armatei Române, Siguranța Statului, Niky Ștefănescu, Corpul Detectivilor.

DATE BIOGRAFICE

Nicolae Ștefănescu sau Niky, așa cum era cunoscut printre apropiați, s-a născut la 20 septembrie 1896, la Galați. Tatăl său era căpitanul Grigore Ștefănescu, născut la 6 iunie 1871, la Focșani, iar mama sa, Elisabeta (Eliza), a murit de tuberculoză când el era în vârstă de cinci ani, fiind, apoi, crescut de bunica sa pe linie maternă, Ecaterina Croia. Frați și surori nu avea, după cum reiese din documentele de arhivă[1]. A absolvit *„Liceul Vasile Alecsandri”*, din Galați, promoția 1916. Pretindea, *„fără a avea însă pretenția de a fi crezut, că a făcut câțiva ani de drept”*. Probabil că studiase câțiva ani, deoarece *„reușea să facă față în destul de multe probleme care necesitau o cultură mai vastă”*[2]. Vorbea limbile: franceză, rusă, ucraineană, dar cunoștea și unele noțiuni de polonă, germană, italiană și sârbă.

Foto: Nicolae (Niky) Ștefănescu, în ianuarie 1931[3]

Ca înfățișare, Niky era de statură mijlocie, mobil, *„dând impresia de energie și cu un fizic agreabil de tip grecesc”*, talie normală, păr castaniu, fața ovală, ochi căprui, iar ca semn particular avea o cicatrice în regiunea frontală dreaptă. S-a căsătorit cu Iraida Calimans, în ianuarie 1927, profesoară de limba franceză la Gimnaziul de fete din Orhei. Tatăl soției era estonian, ziarist (fost profesor), stabilit la Chișinău.

Evident, ca orice biografie de mare spion, cea a lui Niky Ștefănescu are și ea aspecte de mister. Surse legionare susțineau că Niky s-ar fi folosit în carieră de acte false, de numele unui plutonier mort în război

Nota autorului: Materialul de față reprezintă o cercetare inedită, care are la bază surse documentare primare găzduite de diverse arhive din țara noastră.

[1] Arhiva Serviciului Român de Informații (în continuare, ASRI), dosar nr. 20954, vol. 15, filele 2-4.

[2] ASRI, *ibidem*, *Raport privind pe Niky Ștefănescu*, februarie 1949, ff. 222-225.

[3] *Ibidem*.

și că, la autopsia sa (în noiembrie 1940), s-a *„stabilit că era circumcis”*, înlesnind, astfel, presupunerea că ar fi fost evreu, cu atât mai mult, cu cât soția sa ar fi fost evreică (fostă Calimanson)[4].

ACTIVITATEA ÎN CADRUL SIGURANȚEI STATULUI (1917-1931)

Dumitru C. Dumitru, prieten din copilărie și fost coleg de școală cu Niky Ștefănescu, confia unui superior din Siguranță că, după clasele primare, acesta s-a înscris la Școala elementară, dar, în clasa a II-a, a rămas repetent și nu a mai continuat[5]. Pe timpul Războiului Mondial, Niky a intrat în Siguranța Statului, lucrând, *„sub acoperire”*, la Șantierul Naval din Galați. În decembrie 1917 însă, a *„dezertat”* și s-a *„înrolat”* în *Batalionul revoluționarilor români*, aflat sub conducerea celebrului anarhist Cristian Racovski[6]. Există, astfel, asemănări izbitoare între debutul la Siguranță al lui Niky Ștefănescu și cel al lui Mihail Moruzov. Acesta din urmă a *„abandonat”*, și el, școala în clasa a II-a de liceu, din cauza infiltrării sale în organizația de tineret a iredentei bulgare din Dobrogea, devenind, în anii 1909-1912, om de încredere al aceluiași Cristian Racovski, poziție din care a contribuit la descoperirea activității de spionaj ruso-bulgare din România.

Pe timpul Războiului Mondial, Niky a intrat în Siguranța Statului, lucrând, „sub acoperire”, la Șantierul Naval din Galați. În decembrie 1917 însă, a „dezertat” și s-a „înrolat” în Batalionul revoluționarilor români, aflat sub conducerea celebrului anarhist Cristian Racovski.

Probabil că există un sâmbure de adevăr în toate acestea, deoarece, potrivit *Statului de serviciu* de la Ministerul Apărării Naționale, Niky Ștefănescu a fost angajat la 15 aprilie 1918 direct în funcția de subcomisar la Brigada de Siguranță Tighina din Direcția Poliției și Siguranței Generale a Statului (DPSG), post ce presupunea deja o anumită experiență și studii. Ca polițist, el a ocupat succesiv următoarele funcții și posturi: de la 1 iulie 1919, subprefect la jud. Cetatea Albă; din 1 mai 1920, comisar special aj. la Brigada de Siguranță Tighina; din 1 mai 1921, comisar sp.aj. la Brig. Sig. din Hotin; din mai 1922, la Brig. Sig. Tighina; din martie 1923, la Brig. Sig. din Cetatea Albă; din martie 1923, la Brig. Sig. din Tighina; din martie 1924, la Sig. din Hotin; de la 1 iulie 1924, a devenit subcomisar cl. I la Brig. Sig. din Hotin; din 1 octombrie 1924, la Sig. din Tighina; din 1 octombrie 1925, la Brig.

[4] *Ibidem*, ff. 222-225.
[5] *Ibidem*, ff. 103-107.
[6] ASRI, dosar nr. 10988, vol. 1, f. 134.

Sig. din Iași; din 1 februarie 1926, la Sig. din Tighina; din 1 octombrie 1926, comisar special la Inspectoratul de Siguranță Chișinău – ca șef al Serviciului de Siguranță la Hotin; de la 1 noiembrie 1928, șef al Serviciului de Cercetări – Inspectoratul de Siguranță Chișinău, până la 1 ianuarie 1931, când a demisionat[7].

Însă, ceea nu se arată în *statul de serviciu* este faptul că Niky Ștefănescu era șeful *Serviciului de Informații Externe* al DPSG pe spațiul sovietic. Or, numirea într-o asemenea funcție denotă că personajul era un specialist desăvârșit în cunoașterea și combaterea activității subversive duse de statul sovietic împotriva României. Documentele de arhivă relevă că Niky a coordonat peste Nistru o puternică rețea informativă și contrainformativă, legătura cu agenții făcându-se printr-un sistem ingenios de *„curieri”* acoperiți drept *„contrabandiști”*. Astfel, elemente precum Tarak, Vladimir Sabuc sau Gr. Ozarciuc sunt menționate că utilizau în misiunile încredințate *„dovezi date de comisarul ajutor Niky Ștefănescu prin care se permite circulația în tot județul”*[8]. Un raport al DPSG din 12 ianuarie 1923 arată că *„mai mulți astfel de indivizi cu rol dubios au fost descoperiți și semnalați Inspectoratului de Siguranță Cernăuți (...), fără a se ști prin ce împrejurări au trecut la sovietici”*[9].

Documentele de arhivă relevă că Niky a coordonat peste Nistru o puternică rețea informativă și contra-informativă, legătura cu agenții făcându-se printr-un sistem ingenios de „curieri” acoperiți drept „contrabandiști”. Astfel, elemente precum Tarak, Vladimir Sabuc sau Gr. Ozarciuc sunt menționate că utilizau în misiunile încredințate „dovezi date de comisarul ajutor Niky Ștefănescu prin care se permite circulația în tot județul”.

Printre principalele elemente informative care alcătuiau rețeaua lui Niky Ștefănescu se afla și Ilie Grigorovici Guțuleac sau Huțuleac (zis *„Ilinca”*), o figură aparte, *„un spion de rasă”*, cum îl caracterizau cei care îl cunoșteau, devenit și *„una dintre nestematele”* lui Mihail Moruzov. Născut în anul 1895, în Galiția poloneză (jud. Starojineț), ucrainean, Ilie Guțuleac cunoștea limbile rusă, germană, polonă, ucraineană și română. Fost locotenent în armata austriacă, a luptat în armata naționalistului ucrainean Simeon Petliura și, apoi, în cea a lui Anton Denikin. În aprilie 1920, Guțuleac a venit în România, unde a intrat ca agent în cadrul rezidenței Biroului francez de informații militare din Cernăuți, fiind exploatat concomitent și de DPSG, și de Biroul II militar român. Guțuleac avea o *„bandă de ucraineni”*, care avea legături cu altele din URSS. Rezidentul lui Guțuleac din punctul

[7] ASRI, dosar nr. 20954, vol. 15, *Statul de serviciu* de la Ministerul Apărării Naționale, întocmit în ianuarie 1931 de Mihail Moruzov, Șeful Serviciului *„S”*, filele 226-229 și 245.
[8] ASRI, fond P, dosar 10998, vol. 1, fila 137.
[9] *Ibidem*, fila 136.

Camenița-Podolsk reușise să recruteze o funcționară de la GPU (poliția politică sovietică). În anii 1926-1927, Guțuleac apare ca fiind *„șeful Centrului de Informații al Armatei române de la Atachi-Soroca”*, având misiunea de a controla activitatea *centrului sovietic de spionaj* de la Iaruga, condusă de un anume Keppler[10]. Una dintre sarcinile lui Guțuleac, acoperit și el drept *„contrabandist”*, era constituirea de *„comandouri”* ce aveau ca misiune atacarea unor poștalioane sau depozite bancare în scopul obținerii rublelor necesare plății agenturii noastre și a celei *„aliate”* de peste Nistru[11]. Pe de altă parte, interesul organelor noastre speciale pentru obținerea de valută sovietică este un indicator al existenței acestei agenturi, ce trebuia plătită în moneda locală pentru a nu fi compromisă. Pe atunci, rublele se obțineau greu și din cauză că România și URSS nu aveau relații oficiale. De altfel, acest model acțional a fost preluat de Niky și oamenii săi chiar de la regimul sovietic, ale cărui comandouri atacau instituțiile statului român și răspândeau teroarea în dreapta Nistrului.

Prin utilizarea unor tactici și metode variate, parte din „contrabandiștii” lui Niky Ștefănescu au reușit să se infiltreze în cadrul diverselor organizații ale statului sovietic, de unde primeau instrucțiuni și reveneau în România ca „agenți sovietici”. Ca urmare, organele noastre speciale reușiseră să dețină un anumit control informativ asupra celulelor comuniste paramilitare înființate de spionajul sovietic pe teritoriul nostru național.

Cert este că, prin utilizarea unor astfel de tactici și metode, parte din *„contrabandiștii”* lui Niky Ștefănescu au reușit să se infiltreze în cadrul diverselor organizații ale statului sovietic, de unde primeau instrucțiuni și reveneau în România ca *„agenți sovietici”*. Ca urmare, organele noastre speciale reușiseră să dețină un anumit control informativ asupra celulelor comuniste paramilitare înființate de spionajul sovietic pe teritoriul nostru național.

Referindu-se la activitatea sa din această perioadă, Niky Ștefănescu consemna, la 18 iulie 1924, către șefii săi (cu ocazia unei promovări): *„În trecut, am dus o viață nestabilă și nu lipsită de pericole (țin să arăt că am lucrat la Biroul de Cercetări comuniste, atât la Brigăzile din Hotin și Tighina, cât și la Inspectoratul de Siguranță din Chișinău), cu care ocazie am făcut arestări și cercetări în toată Basarabia, **operațiuni de unde nu-mi amintesc să fi lipsit focurile de armă** și din care cred că Statul a câștigat (...)”*[12].

Faptele și bravura lui Niky Ștefănescu în serviciul țării sunt confirmate și de șeful Brigăzii de Siguranță Hotin, care a ținut să evidențieze

[10] ASRI, D, dosar 10988, vol. 1, fila 186.
[11] *Ibidem*, cota arhivistică 10988, vol. I, fila 134.
[12] ASRI, dosar nr. 20954, vol. 18, f. 121.

următoarele în *Foaia calificativă* a acestuia: *„Vechi și foarte bun ofițer de poliție, specialist în cercetări. A condus și conduce cu multă pricepere **Serviciul de informații externe**; înzestrat în toate acțiunile sale cu mult tact și discernământ, menținându-și o linie de conduită demnă atât în raporturile cu personalul de serviciu, cât și cu publicul în afară de serviciu. Este foarte conștiincios și punctual la serviciu. Prin zelul cum a organizat **Serviciul de informații externe**, a putut face legătura cu oameni din Ucraina prin care a supravegheat bandele teroriste din Basarabia, fapt ce a dus la descoperirea organizației teroriste și a depozitului de munițiuni sovietice din comuna Zorojani, județul Hotin. Pentru această reușită, a fost propus spre decorare, după însuși ordinul verbal al domnului ministru Tătărescu, de către Inspectoratul General de Siguranță Cernăuți. Prin aceleași mijloace, s-au descoperit gazdele grupei teroriste de sub conducerea individului Puiu, care, de trei ani, se găsește în serviciul GPU din Cernăuți [rezidența, n.a.] și care a operat în nordul Basarabiei, afacere care se instrumentează în prezent tot de către acest ofițer de Poliție. Nota generală de calificare: foarte bun”*[13].

Sugestiv pentru pericolele la care erau expuși agenții români este și *nota* prin care *comandamentul* Batalionului I/8 Vânători se interesa la *„dl Niky Ștefănescu dacă agentul din Ucraina care a dat informații despre depozitul de la Zorojani trăiește sau face parte din cei doi agenți omorâți de bolșevici la 3 decembrie 1924”*[14].

RĂSCOALA DE LA TATAR-BUNAR: ATAC SOVIETIC ASUPRA STATULUI ROMÂN

La Serviciul de Informații Externe, Niky Ștefănescu îi avea ca șefi de echipe și pe Gheorghe Stârcea, Mihail Cărare, Ion Ajocu și N. Georgescu. Împreună au avut o contribuție importantă la contracararea și neutralizarea rebeliunii sovietice de la Tatar-Bunar (Tătărăști)[15] – cel mai puternic atac extern asupra statului român de după război. Erau însă pregătiți. Informațiile arătau că la Viena a avut loc *Congresul*

La Serviciul de Informații Externe, Niky Ștefănescu îi avea ca șefi de echipe și pe Gheorghe Stârcea, Mihail Cărare, Ion Ajocu și N. Georgescu. Împreună au avut o contribuție importantă la contracararea și neutralizarea rebeliunii sovietice de la Tatar-Bunar (Tătărăști) – cel mai puternic atac extern asupra statului român de după război.

[13] Pe larg în Pavel Moraru, *Serviciile secrete și Basarabia, Dicționar 1918-1991*, Editura Militară, București, 2008, p. 291.
[14] ASRI, dosar nr. 20954, vol. 18, f. 151.
[15] Pe larg în Sorin Aparaschivei, *Sistemul național de informații de la Regulamentul Organic și până după Războiul de Reîntregire Națională*, Editura Militară, București, 2018, pp. 411 și urm.

„Răscoala de la Tatar-Bunar nu a fost opera Partidului Comunist din România și nici o manifestare spontană prosovietică și antiromânească a populației locale din Basarabia. Ea a fost declarată de împrejurări externe în următoarele scopuri: la Conferința sovieto-română de la Viena, delegatul URSS a condiționat reluarea raporturilor dintre România și URSS de un plebiscit în Basarabia, adoptând o temă net revizionistă”.

agenților militari sovietici, sub președinția lui Egoroff, comandantul trupelor sovietice de pe Frontul de Sud, în speță comandantul frontului român, care a dat ordinul pentru provocarea revoluției bolșevice în Basarabia. Iar *„dacă răscoala va deveni generală în Basarabia,* ***trupe neregulate din armata sovietică, concentrată la granița română, vor fi trecute peste graniță”***[16]. Astfel, atacul sovietic contra statului român a început la 12 septembrie 1924, când târgușorul Nicolaevka din jud. Ismail a fost atacat de o bandă formată din 25-30 de indivizi mascați, care au pătruns în sat și i-au împușcat pe primar (Jancovski), pe soția acestuia și doi jandarmi (Ion Costin și Gh. Chirvase). Sătenii au fost adunați în târg (circa 1.000 de persoane), unde li s-a citit un *manifest* semnat de Terente Colomeez, din satul Tașlâc, prin care acesta îi îndemna să lupte contra burgheziei române: *„Bandiții spuneau despre ei că nu sunt bandiți ordinari, ci fac parte din trupele sovietice venite să lupte contra burgheziei române”*. Apoi, au atacat comunele Cișmea, Tatar-Bunar (Tătărăști), Vâlcov, Periprava, Nerusai etc.

Trupele române au intervenit și au purtat lupte crâncene cu bandiții, care erau foarte bine dotați, fiind capturate mii de pistoale și puști noi de proveniență sovietică și germană, tunuri de asalt (demontabile), sute de grenade, bărci cu motor etc. Sute de bandiți au fost arestați și judecați. Ancheta a stabilit că acțiunea a fost îndreptată în mod cert contra statului român, fiind organizată și finanțată de către conducerea sovietică de la Moscova.

Referindu-se la cauzalitatea acestor evenimente, Niky Ștefănescu era de părere că: *„Răscoala de la Tatar-Bunar nu a fost opera Partidului Comunist din România și nici o manifestare spontană prosovietică și antiromânească a populației locale din Basarabia. Ea a fost declarată de împrejurări externe în următoarele scopuri: la Conferința sovieto-română de la Viena, delegatul URSS a condiționat reluarea raporturilor dintre România și URSS de un plebiscit în Basarabia, adoptând o temă net revizionistă. La argumentele istorico-etnografice ale valabilității actului Unirii, invocate de delegatul României și susținute cu simpatie de toate țările civilizate, URSS a opus o teorie politico-socială, susținând că Basarabia s-ar fi pronunțat pentru un regim sovietic. Cum a solicita*

[16] ASRI, D, dosar nr. 8348, filele 7-13.

anexarea Basarabiei ar fi însemnat să denaturezi cu cinism realitățile, acest delegat a cerut, pur și simplu, autonomia Basarabiei. Eșecul suferit de delegații sovietici, care, în lipsă de argumente, au rupt tratativele, a avut adânci repercusiuni atât în opinia publică mondială, cât și în sufletul populației Rusiei. Statele europene acuzau URSS de obstrucție și șicanare în relațiile internaționale, iar în Rusia se comenta extrem de nefavorabil tendința de izolare a republicii față de vecini. Pentru a justifica restabilirea tezei susținute de delegații comuniști, era necesară o acțiune de răsunet internațional care să se producă în Basarabia. Alegerea regiunii subiectului acestei provocări nu se poate considera un simplu hazard. Ea a fost determinată tocmai de împrejurarea că acolo exista o populație minoritară, ruși și bulgari, care nu începuseră să se asimileze. ***Organizarea rebeliunii a fost încredințată nu țăranilor basarabeni, ci unor emisari sovietici care au fost pregătiți timp de șase luni în materie de instruire, conducere și tacticile războiului civil*** *[hibrid, n.a.].* ***Armamentul, banii și chiar literatura și ștampilele unităților revoluționare au fost făcute în Rusia****. Reușita și chiar eșecul rebeliunii de la Tatar-Bunar trebuiau să confirme valabilitatea punctului de vedere al URSS la Conferința de la Viena.* ***Rebeliunea a eșuat lamentabil, ieșind în evidență tocmai imixtiunea statului sovietic în organizarea acestei revolte*** *[subl.a.]”*[17].

Eșecul sovietic de la Tatar-Bunar rămâne și un indicator al performanțelor atinse de sistemul nostru național de informații, care a fost capabil să se opună celui mai periculos sistem de spionaj din lume.

Pe de altă parte, eșecul sovietic de la Tatar-Bunar rămâne și un indicator al performanțelor atinse de sistemul nostru național de informații, care a fost capabil să se opună celui mai periculos sistem de spionaj din lume.

ORGANIZAREA COLABORĂRII INFORMATIVE ÎN BASARABIA

În Basarabia, Niky Ștefănescu a continuat să se ocupe de activitatea și colaborarea informativă externă între organele DPSG și cele ale Armatei Române, aici începând activitatea și Mihail Moruzov, care preluase organizarea aparatului tehnic al Serviciului *„S”* al Armatei Române. Tot Niky Ștefănescu avea în responsabilitate corelarea organelor noastre informative cu cele ale rezidenților aliate ale *British*

[17] ASRI, dosar nr. 8724, *„Chestiunea Basarabiei, 1930-1939”*, vol. 1, f. 62; Niky Ștefănescu, *cauzele rebeliunii de la Tatar-Bunar*, *raport către Consiliul de Miniștri*, 17 noiembrie 1936, document ce poartă avizul lui Mihail Moruzov.

Intelligence Service și Biroului II francez (informațiile militare) care operau pe spațiul sovietic (sarcinile erau împărțite, pentru a nu exista suprapuneri).

Prin natura acestor atribuții și sarcini, Niky Ștefănescu lucra mai mult la Chișinău, acoperit ca *„șef al Serviciului de Cercetări”*, însă, potivit unui document intern din 1 noiembrie 1928, el ocupa aici funcția de șef al **Biroului de Informații al Inspectoratului General al Basarabiei**[18].

Printre reperele activității sale din această perioadă se află descoperirea, în martie 1928, a organizației de spionaj sovietic care își avea reședința în comuna Nagoreni, jud. Hotin. Ancheta a stabilit că organizația era condusă de un anume Gh. Draganiuc, care lucra după directivele date de *Biroul de Spionaj* sovietic din Camenița-Podolsk (Ucraina), având legături și cu alte centre de spionaj sovietic din România, unde erau plătiți rezidenții pentru spionaj – toate acestea fiind identificate și neutralizate[19]. Plecând de la acest caz, Niky Ștefănescu a reușit recrutarea lui Vasile Botnariuc (alias Vasile Dogaru), unul dintre liderii Partidului Comunist din România. Acesta a furnizat informații exacte asupra existenței, componenței, organizării și activității tuturor organizațiilor comuniste din nordul Basarabiei. Au fost arestați zeci de agenți ai celulelor paramilitare comuniste, unii instruiți în școli speciale din URSS, fiind descoperite numeroase case conspirative, articole de propagandă și mari cantități de arme, muniții și explozivi[20].

Poate cel mai important caz anchetat de Niky Ștefănescu, ca șef al Serviciului de Cercetări, a fost cel al comisarului Constantin Tibacu. Niky arăta că a descoperit cazul plecând de la o altă pistă, un anume Al. Caramanov, curier sovietic, ocazie cu care „a descoperit întreaga organizație de spionaj de sub președinția lui Tibacu”.

Dar, poate cel mai important caz anchetat de Niky Ștefănescu, ca șef al *Serviciului de Cercetări*, a fost cel al comisarului Constantin Tibacu. Niky arăta că a descoperit cazul plecând de la o altă pistă, un anume Al. Caramanov, curier sovietic, ocazie cu care *„a descoperit întreaga organizație de spionaj de sub președinția lui Tibacu”*[21]. Iată, pe scurt, faptele: Constantin Tibacu a fost prefect al jud. Cetatea Albă (1922) și, apoi, șef de birou la Inspectoratul de Siguranță Chișinău[22], deci coleg cu Niky Ștefănescu. În anul 1928, cu ocazia reorganizării

[18] ASRI, dosar nr. 20954, vol. 4, 1 noiembrie 1941, *anchetă Moruzov*, f. 103.
[19] *Ibidem*, vol. 18, f. 120.
[20] ASRI, D, dosar nr. 4702, filele 100-113.
[21] ASRI, dosar nr. 6771, *„Spionaj sovietic, 1942”*, f. 41.
[22] Despre *Cazul Tibacu-Caramanof* au scris mai toate ziarele vremii, vezi *„Dimineața”* din 10 mai 1930, *„Universul”* sau *„Lupta”*.

Siguranței Generale a Statului, postul lui Tibacu de la Chișinău a fost desființat, acesta fiind repartizat la un departament din București. Dar, cum familia i-a rămas la Chișinău, noua lume nu-i era deloc familiară lui Tibacu. Singur și presat de griji financiare, încerca din răsputeri să se adapteze noilor condiții. Salariul abia dacă îi ajungea, în jur de 8-9.000 lei/lună, fiind împărțit între nevoile zilnice, chirie și familia rămasă departe. Într-o zi din septembrie 1928, lui Tibacu i-a apărut în cale Granic (nume conspirativ Craiu sau Olmozov), un fost coleg de la Siguranța din Chișinău, despre care știa că părăsise serviciul și se stabilise cu familia la Berlin. Surprins să-l vadă, Tibacu s-a împrietenit cu el. Granic i-a povestit că a părăsit, între timp, Germania și lucrează în București, la o mare companie comercială germană, fiind foarte bine plătit. După câteva întâlniri, Tibacu s-a lăsat convins să fie ajutat cu bani de prietenul său mult mai bine plătit. A împrumutat, cu chitanțe, diverse sume, pe care le-a folosit ca să-și vadă familia la Chișinău. Apoi, într-o zi, Granic i-a spus lui Tibacu adevărul: *că, de fapt, este agent sovietic și că are misiunea de a-l recruta*. Văzând că Tibacu se opune, Granic l-a amenințat cu chitanțele compromițătoare și cu faptul că va fi ucis de agenții GPU care-l însoțesc. Astfel, Constantin Tibacu a devenit agent sovietic. Soția sa, Reghina, născută în Polonia, era o femeie foarte frumoasă, iar faptul că l-a ajutat pe soțul ei în activitatea de trădare i-a făcut pe anchetatori că creadă că aceasta i-a fost *„livrată”* de sovietici lui Tibacu, fiind și ea condamnată la șase luni de închisoare.

Într-o zi din septembrie 1928, lui Tibacu i-a apărut în cale Granic (nume conspirativ Craiu sau Olmozov), un fost coleg de la Siguranța din Chișinău, despre care știa că părăsise serviciul și se stabilise cu familia la Berlin. Surprins să-l vadă, Tibacu s-a împrietenit cu el. Granic i-a povestit că a părăsit, între timp, Germania și lucrează în București, la o mare companie comercială germană, fiind foarte bine plătit. După câteva întâlniri, Tibacu s-a lăsat convins să fie ajutat cu bani de prietenul său mult mai bine plătit.

Pentru testare și inițiere, Tibacu s-a deplasat la rezidența sovietică din Istanbul, unde s-a întâlnit cu Visevold Balițki[23], șeful GPU ucrainean. Aici, seara petreceau în hoteluri luxoase, iar ziua, Tibacu era instruit în domeniul cifrului și al metodelor folosite de sovietici, totul decurgând foarte bine, avându-se în vedere că Tibacu era deja un profesionist în domeniu. Balițki i-a comunicat lui Tibacu că va trebui să facă orice este posibil pentru a se infiltra în cercul de apropiați al lui Eugen Cristescu, director în Siguranța Statului. Salariul lui Tibacu a fost stabilit la 20.000 de lei lunar, plătiți anticipat, iar dacă avea realizări, putea ajunge la 80.000 lei lunar. Banii veneau via Berlin, unde, mai nou, se mutase și sediul Centralei Sovietice care se ocupa de România.

[23] La 1 august 1931, Balitsky Visevold Apolenovici a fost mutat în conducerea GPU Moscova, în locul său, la GPU din Ucraina, a fost numit Stanislav Redens, de origine poloneză.

Toamna lui 1928 și primăvara lui 1929 au reprezentat pentru Tibacu o muncă intensă pentru a-și mulțumi noii șefi. În seara de 15 mai 1929, Tibacu chefuia cu șefii săi sovietici la Berlin, unde se afla pentru câteva zile pentru noi instrucțiuni. Unul dintre sovietici, amețit de băutură, i-a mărturisit lui Tibacu că Inspectoratul General de Siguranță Chișinău era infiltrat cu sovietici, că fiecare din rapoartele secrete ale Inspectoratului era bătut la mașină în trei exemplare: unul rămânea la Inspectorat, al doilea pleca la Direcția din București, iar cel de-al treilea ajungea direct la... Moscova! Apoi, surprinzător, Tibacu a avut ocazia să-i cunoască pe mai mulți dintre foștii săi colegi de la Inspectoratele de Siguranță din Basarabia și Bucovina care lucrau, acum, pentru sovietici.

Pe la sfârșitul anului 1929, sovieticii i-au dat ordin lui Tibacu să sustragă de la Siguranța din București dosarul lui Constantin Dobrogeanu-Gherea, vechi anarhist rus refugiat în România, despre care sovieticii au aflat că fusese denunțat Siguranței de câțiva lideri ai Partidului Comunist din România.

La Berlin, Tibacu a primit ca noi însărcinări întocmirea de liste cu personalitățile române din ministere și Siguranța Generală care ar fi putut fi racolate de sovietici și bine plătite. De exemplu, pentru Eugen Cristescu, în caz că putea fi racolat, sovieticii au prevăzut un salariu lunar de 100.000 de lei. De altfel, pe urma lui Eugen Cristescu, GPU l-a pus pe agentul Kirilov, care avea sarcina de a-l racola. Când Constantin Tibacu i-a răspuns acestuia că treaba este imposibilă, Kirilov i-a replicat lui Tibacu că: *„Sovietele au oameni în România la care el nici nu poate gândi și nici nu-i poate bănui, care au să încerce atragerea lui Cristescu”*.

Sovieticii se mai interesau și de Mihail Moruzov și Vintilă Ionescu (șeful contraspionajului din Siguranță), Tibacu fiind chestionat dacă-i cunoaște pe aceștia. A răspuns negativ, deși Tibacu, fiind din Tulcea, îl știa pe Mihail Moruzov, cu care fusese chiar coleg de școală (ambii aveau mame de etnie bulgară, n.a.). Conform lui Tibacu, sovieticii erau îngrijorați de agilitatea inspectorului general Vintilă Ionescu, pe care-l considerau *„cel mai priceput funcționar al Siguranței române”*.

Pe la sfârșitul anului 1929, sovieticii i-au dat ordin lui Tibacu să sustragă de la Siguranța din București dosarul lui Constantin Dobrogeanu-Gherea, vechi anarhist rus refugiat în România, despre care sovieticii au aflat că fusese denunțat Siguranței de câțiva lideri ai Partidului Comunist din România (vezi, mai sus, Vasile Botnariuc, n.a.). Vinovații trebuiau aflați și atrași în URSS pentru a fi pedepsiți. Cum treaba era extrem de grea, dosarul aflându-se închis în fișetul personal la lui Eugen Cristescu, la București a sosit și Balițki. Planul însă nu a putut fi pus în aplicare și Tibacu a ratat contactele cu legăturile sale din București. Îngrijorat, el a plecat la Chișinău.

În noaptea de 8 februarie 1930, după investigații și filaje care au durat luni de zile, Niky Ștefănescu și agenții Siguranței din Chișinău i-au bătut la poartă pentru a-l aresta. Constantin Tibacu a fost condamnat la 10 ani de temniță (fiind eliberat în anul 1938). La anchetă, acesta a încercat să-și minimizeze activitatea, dar Niky Ștefănescu și Serviciul său au stabilit că acesta a lucrat sub coordonarea unor persoane importante din spionajul sovietic: Leplievscky, din Harkov, șeful GPU din toată Ucraina; Vladimir Petrovici Karaolin, șeful de informații externe (INO) din Harkov; Vladimir Maximovici Piescariov, șeful informațiilor externe din Odessa[24].

Însă, ancheta din cazul Tibacu nu s-a oprit aici și a zguduit întreaga conducere a Inspectoratului General de Siguranță al Basarabiei. Pe fir au intrat Mihail Moruzov și Serviciul *„S”* al Armatei Române, care au stabilit că principal vinovat era și Zaharia Husărescu, șeful Inspectoratului de Siguranță Basarabia, care a fost schimbat din funcție.

În noaptea de 8 februarie 1930, după investigații și filaje care au durat luni de zile, Niky Ștefănescu și agenții Siguranței din Chișinău i-au bătut la poartă pentru a-l aresta. Constantin Tibacu a fost condamnat la 10 ani de temniță (fiind eliberat în anul 1938). La anchetă, acesta a încercat să-și minimizeze activitatea, dar Niky Ștefănescu și Serviciul său au stabilit că acesta a lucrat sub coordonarea unor persoane importante din spionajul sovietic.

CARIERA ÎN SERVICIUL „S”(ECRET) AL ARMATEI ROMÂNE (1931-1940)

Faptul că Niky Ștefănescu colabora tot mai strâns cu organele informative ale Armatei Române, în speță cu Mihail Moruzov, nu era deplin agreat de unii șefi din Siguranță. Niky Ștefănescu a fost acuzat de tot feluri de abuzuri[25]. În acest context, la sfârșitul anului 1930, Mihail Moruzov i-a făcut o ofertă de nerefuzat. Demisia lui Niky Ștefănescu a provocat un adevărat șoc atât în Siguranță, cât și în opinia publică; până și ziarul de limba rusă *„Slova Basarabiei”* titrând: *„Ștefănescu este unul din **stâlpii** Siguranței, el a descoperit o mulțime de organizații de spionaj și comuniste. A fost decorat cu câteva ordine. În zilele acestea, a fost decorat a doua oară cu ordinul Coroana României, iar plecarea lui din Siguranță a fost ceva neașteptat chiar și pentru șefii lui. Inspectorul General Maimuca a trimis o telegramă la București, cerând a nu se da curs demisiei lui Ștefănescu”*[26].

[24] ASRI, fond D, dosar nr. 7328, referitor la *Activitatea SSI român despre activitatea serviciului de informații sovietic în România, Bulgaria, Turcia, Ungaria, Austria (...) anii 1918-1942,* filele 44-53 și altele.
[25] Pe larg, despre acestea, în Pavel Moraru, *Serviciile secrete și Basarabia, Dicționar 1918-1991*, *op. cit.*, p. 290.
[26] *Ibidem*, p. 293.

Așadar, de la 1 ianuarie 1931, Niky Ștefănescu a trecut la Secția a II-a din Marele Stat Major al Armatei Române, unde, de ceva timp, Mihail Moruzov organiza și conducea Serviciul *„S”* – o instituție mixtă (militari și civili) adaptată amenințărilor de tip hibrid (politico-militare) proliferate de statul sovietic la adresa integrității teritoriului și regimului politic din România.

De la 1 ianuarie 1931, Niky Ștefănescu a trecut la Secția a II-a din Marele Stat Major al Armatei Române, unde, de ceva timp, Mihail Moruzov organiza și conducea Serviciul „S” – o instituție mixtă (militari și civili) adaptată amenințărilor de tip hibrid (politico-militare) proliferate de statul sovietic la adresa integrității teritoriului și regimului politic din România.

Conform *statului de serviciu* de la Ministerul Apărării Naționale (întocmit de Mihail Moruzov), Nicolae Ștefănescu – conspirativ *„I. Popescu”* – a fost numit în funcția de șef de echipă la Serviciul Secret al Marelui Stat Major. Următoarele funcții îndeplinite de acesta au fost: de la 1 iulie 1934, Director Clasa a II-a (Decizia nr. 833 *S*[ecret]); de la 1 aprilie 1937, Director Clasa I (Decizia nr. 355 *S*) până în ziua de 5 septembrie 1940, când a fost destituit. La rubrica *diverse* din același document s-a adăugat: *„N. Ștefănescu a fost trecut în cadrul descoperit la 22 noiembrie 1933, prin Ordinul de zi nr. 141 al Marelui Stat Major”*[27].

La Marele Stat Major al Armatei Române, Niky Ștefănescu a început activitatea în cadrul *Centrului de Informații Chișinău („B”)* ca ajutor și prim-colaborator al șefului centrului, maiorul Constantin A. Râpeanu. Raza de acțiune a Centrului *„B”* se întindea pe lungul Nistrului, de la Atachi-Soroca până la Cetatea Albă, având ca singur obiectiv: *cunoașterea situației politice și militare a URSS*. Niky lucra direct cu șefii de agenturi din Soroca, Orhei, Lăpușna, Tighina și Akerman (Cetatea Albă). Pe lângă informatorul Vasile Botnariuc amintit mai sus, era ajutat și de Dora Constantinescu, fostă cântăreață la operele din Paris și Londra, care era gazdă, la conacul moșiei sale din comuna Târnava, jud. Soroca, a diferite persoane din lumea mondenă a Capitalei, printre care doamna Seletzki, din faimoasa afacere Skoda (în care statul român a aflat jocul dublu al cehoslovacilor în relația lor de *„aliați”* cu România). Niky continua să lucreze și cu Ilie Guțuleac, cu grecul Gheorghe Caragunopolus – *„care avea urme de gloanțe la cap dintr-o captură a sa la Ovidiopol – Ucraina și din care a reușit să scape rănit”*[28], cu Niculae Cociubei (*Prințul*) – unul dintre cei mai buni spioni pe spațiul sovietic, conspirativ *„Arghir”*, acesta făcând parte din aristocrația rusă, culegând informații din rândul emigrației ruse la Varșovia, Viena, Hamburg și Berlin.

Ca amuzament, Niky Ștefănescu îl utiliza ca informator și pe celebrul tenor de talie mondială Gogu Ștefănescu. Acesta concerta la *„Radio București”* și efectua frecvent turnee în Italia, Franța și chiar în Rusia sovietică, de unde aduna informații pentru Niky Ștefănescu și Mihail Moruzov. Deși, în actele de la Marele Stat Major, nu figurează ca având vreun frate, Niky și Gogu se *„afișau”* în această ipostază pe la diverse evenimente mondene, marele tenor afirmând unor apropiați că era *„sponsorizat de fratele mai mare din Siguranță”*[29].

PRINCIPALELE DIRECŢII DE ACŢIUNE ÎN FRUNTEA SERVICIULUI „S” AL ARMATEI ROMÂNIEI

La venirea lui Niky Ștefănescu la Serviciul *„S”* al Armatei Române, Secția II (Contrainformații) era condusă de un anume *„Vasea Potapov”*, nepot al lui Mihail Moruzov, despre care cunoscătorii afirmau că *„a murit mai târziu într-un ospiciu”*. Probabil că acesta era conspirativul lui Gheorghe Moruzov, vechi agent al Siguranței și fiu al preotului Simeon Moruzov, frate cu Mihail.

Abia în anul 1932, Niky Ștefănescu a preluat conducerea Secției Contrainformații din Serviciul *„S”*, mai cu seamă latura contraspionajului[30]. El era ajutat aici de comisarul Gheorghe Comșa, trecut și el în cadrul armatei. La Serviciu, Niky Ștefănescu era socotit ca fiind primul funcționar după Mihail Moruzov: *„Când era cazul unei misiuni mai dificile, care depășea atribuțiile de contrainformații, lui Niky Ștefănescu i se încredința. După cum, atunci când era o problemă mai complicată, Moruzov, care, de obicei, nu se sfătuia cu nimeni, se sfătuia cu el”*[31].

În anul 1932, Niky Ștefănescu a preluat conducerea Secției Contrainformații din Serviciul „S”, mai cu seamă latura contraspionajului. El era ajutat aici de comisarul Gheorghe Comșa, trecut și el în cadrul armatei. La Serviciu, Niky Ștefănescu era socotit ca fiind primul funcționar, după Mihail Moruzov.

Prioritatea lui Niky Ștefănescu a rămas *„problema sovietică”*. La 20 mai 1933, el a întocmit un referat în care avertiza că sovieticii își reorganizau aparatul de spionaj, sens în care au inițiat colaborări contra României și cu spionajul italian: *„Din informațiile pe care le avem, reiese că sovietele au creat la Viena un Centru de Spionaj, Propagandă și Agitație, a cărui rază de activitate este România,*

[27] ASRI, fond P, dosar 20954, vol. 15, filele 226-229.
[28] Arhivele Naționale ale României (în continuare, ANR), Inv. 2349, DGP (Direcția Generală a Poliției), dosar nr. 58/1920.
[29] ASRI, dosar D, cota arhivistică 10 988, vol. I, fila 134.
[30] ANR, Inv. 2379, dosar nr. 6/1929, *declarație* – Victor Siminel, f. 7.
[31] ASRI, dosar nr. 20954, vol. 15, ff. 222-225.

Iugoslavia și Peninsula Balcanică. Centrul este camuflat pe lângă Ambasada sovietică din Viena și are trei secții: 1) Secția Comunistă; 2) Secția de Agitație, în sânul minorităților balcanice, inclusiv în România și Iugoslavia; 3) Secția de Spionaj. Primele două secții au conducători speciali, subordonați reprezentantului sovietic, cea de a treia secție s-a creat prin colaborarea în materie de spionaj a Razvedupr-ului [spionajul militar, n.a.] cu Serviciul de Spionaj italian. Pentru a duce la îndeplinire această misiune, secția se folosește ca acoperire de reprezentanții agențiilor TASS și IMPRECOR; își mai dau concursul și casele SCHENKER CO. [germană]; DERUT [societate ruso-germană] și RATO [societate austro-rusă], toate au sedii sau filiale la Viena. De ajutor este și MOPR [Ajutorul Roșu Internațional] și societatea INTURIST"[32].

Ca reacție la cleștele informativ sovietic, Niky Ștefănescu avea drept strategie plierea contraspionajului român pe spionajul sovietic în toate centrele de difuzare a acestuia.

Ca reacție la cleștele informativ sovietic, Niky Ștefănescu avea drept strategie plierea contraspionajului român pe *spionajul sovietic în toate centrele de difuzare a acestuia, inclusiv prin penetrarea acestuia la el acasă*, în URSS. Pentru aceasta, Serviciul *„S"* trebuia să-și extindă parteneriatele externe de colaborare și schimb de informații.

Ca urmare, în iunie 1933, Niki Ștefănescu s-a întâlnit la Belgrad cu generalul Romanovsky și colonelul Durov, foste cadre ale armatei țariste (ruși albi) retrase în Iugoslavia, în scopul unei înțelegeri informative antisovietice. Niky Ștefănescu îi raporta lui Mihail Moruzov următoarele: *„Gl. Romanovsky, cât a fost șef al Marelui Stat Major Rus, a utilizat o serie de agenți care locuiesc azi în diferite țări din Europa. După lovitura de stat din octombrie 1917, a întrerupt legătura cu aceștia, dar, în anul 1932, împreună cu Durov, a reluat legătura cu o parte dintre aceștia și au adunat o serie de materiale. Cred că se poate avea încredere în Romanovsky, iar Durov, care pare specialist în informații, este acela care dirijează activitatea aparatului informativ al generalului Romanovsky. Durov este un om abil, șiret și sensibil la informațiile care i se dau. (…) La un moment dat, le-am cerut celor doi să-mi predea aparatul lor informativ [inclusiv pe spațiul sovietic, n.a.], arătându-le imensul serviciu ce-l pot aduce ideologiei antisovietice. (…) Am observat că aparatul informativ al lui Romanovsky a reușit să*

[32] ASRI, fond D, dosar nr. 7181, *Activitatea Kominternului și spionajul sovietic în România și alte țări, 1925-1940*, filele 148-149.

se introducă în Legația sovietică [din Viena, n.a.] și că poate procura informații și fotografii cu privire la activitatea sovietelor în România. S-a căzut de acord ca finanțarea agenților de la Viena să nu aibă caracterul unei salarizări, pentru a nu transforma în profesioniști pe acești oameni care activează doar de dragul ideii. Durov a propus ca activitatea agenturii să fie dirijată de la Belgrad, însă i-am replicat că aceasta ar putea crea probleme cu iugoslavii. S-a ajuns la soluția ca Durov să plece la Viena și să predea agentura lor de la Legația sovietică delegatului nostru la Viena, care va avea sarcina să o instruiască pe loc. Romanovsky mi-a spus că are legături și la Praga, însă trebuie verificate, că mai are legături în orașele sovietice: Kiev, Tiflis, Rostov, Vladicaucaz și Odessa. Romanovsky mi-a comunicat că s-a convins de starea reală a relațiilor româno-ruse și ar fi dispus să înceapă activitatea în această direcție cu condiția să se asigure completa discreție, iar din materialul obținut lui să-i revină partea privitoare la starea spiritelor din Armata Roșie și în rândul UTC, iar materialele militare să revină în întregime românilor"[33].

Dinspre Bulgaria, Niky Ștefănescu a stabilit că principalul pericol pentru România îl reprezenta Organizația Revoluționară Dobrogeană, de orientare comunistă, susținută și finanțată clandestin atât de guvernul bulgar, cât și de cel din URSS.

Apoi, Niky Ștefănescu s-a deplasat în Turcia, încheind și aici un *acord de colaborare* informativă antisovietică. S-a convenit ca schimbul de informații între Serviciul *„S"* al Armatei Române și Siguranța Generală din România, respectiv Direcția Siguranței Generale din Turcia, să aibă loc *„conform contrapropunerilor"* părții turce din *„adresa nr. 229 din 20 octombrie 1933",* referitoare la *„cifrarea corespondenței telegrafice"*[34].

Dinspre Bulgaria, Niky Ștefănescu a stabilit că principalul pericol pentru România îl reprezenta Organizația Revoluționară Dobrogeană (DRO), de orientare comunistă, susținută și finanțată clandestin atât de guvernul bulgar, cât și de cel din URSS. Activitatea DRO era coordonată de secția a II-a a Marelui Stat Major al armatei bulgare, care organizase, la Silistra, un *„centru de spionaj, propagandă și teroare"*, pus sub *„ordinele"* avocatului Asparuh Aidemirski, președintele DRO, și a lui Kiril Mauloff, fost deputat bulgar în Parlamentul României, plecat la vecini în anul 1928 și angajat la Marele Stat Major bulgar. Cum, în toamna anului 1933, acest centru începuse deja o acțiune

[33] *Ibidem*, *Referat*, 19 iunie 1933, întocmit de Niky Ștefănescu, șeful *Secției Contrainformații*, filele 151-153.

[34] ASRI, fond D, dosar nr. 9279, vol. 1, fila 158.

virulentă contra României, problema a fost preluată de Serviciul *„S”* și Mihail Moruzov. De remarcat că, în chestiunea DRO, Mihail Moruzov o controla informativ chiar pe soția fostului senator *„bulgar”* Hristu Toncof din Bazargic, la origine rusoaică[35].

COLABORAREA DINTRE SERVICIUL „S” ŞI SERVICIUL DE INFORMAŢII AL ARMATEI GERMANE (ABWEHR)

În ceea ce privește Germania, primele colaborări și schimburi de informații între Serviciul „S” român și Serviciul de informații al armatei germane (Abwehr) au avut loc în cazul agentului sovietic Peter Urban. În decembrie 1936, acesta a fost depistat de Serviciul „S” în momentul când încerca să intre în contact cu ofițeri din Marele Stat Major român și cu membri ai Legației Germaniei la București spre a-și oferi serviciile.

În ceea ce privește Germania, primele colaborări și schimburi de informații între Serviciul *„S”* român și Serviciul de informații al armatei germane *(Abwehr)* au avut loc în cazul agentului sovietic Peter Urban. În decembrie 1936, acesta a fost depistat de Serviciul *„S”* în momentul când încerca să intre în contact cu ofițeri din Marele Stat Major român și cu membri ai Legației Germaniei la București spre a-și oferi serviciile. Niky Ștefănescu a cercetat cazul și a stabilit că respectivul era în realitate Akoș Domany, sas din Brașov, condamnat, în urmă cu doi ani, pentru fals. Aflat în închisoare (la Aiud), Domany l-a cunoscut pe Emil Bodnăraș, venit, în anul 1934, din URSS, fraudulos în România și care activa intens în *Secția Română* a Serviciului de spionaj sovietic și în *Internaționala Comunistă*. Sesizând că Akoș Domany era german de origine, Emil Bodnăraș (cu mamă de origine germană) l-a recrutat și l-a prezentat, apoi, Legației sovietice prin fratele său, Emanoil Bodnăraș. Legația sovietică l-a instruit pe Domany să se prezinte la Legația germană din București și să caute să se infiltreze în Marele Stat Major german, solicitând o întrevedere cu personaje importante sub motivul că are ceva stringent de comunicat care interesează Înaltul Comandament German. În plasa spionajului sovietic a căzut Von Pochammer, consilier la Legația germană din București, care, auzind despre ce era vorba, l-a trimis pe Domany la Berlin, comunicând Centralei sale că respectivul are legături cu Serviciul de spionaj sovietic și că dorește să furnizeze informații importante Marelui Stat Major german. De la Berlin, Domany a fost trimis la București cu pașaport german, pe numele Urban. Aici, el a încercat să ia legătura cu Serviciul *„S”* român, dându-se drept trimis al Marelui Stat Major german. Prin acest plan, preciza ulterior Mihail

[35] ASRI, dosar nr. 10 998, vol. II, f. 202.

Moruzov, sovietele doreau să-l prezinte pe Urban germanilor ca pe un troțkist (Leon Troțki era în conflict cu Stalin, n.a.) și să-l infiltreze, astfel, în Marele Stat Major german și în Serviciul *„S”* român, cărora să le livreze materiale *pregătite* de Moscova și, totodată, să strângă *„dovezi compromițătoare”* privind *legăturile ascunse* româno-germane, pe care să le prezinte Franței și Marii Britanii pentru a deteriora relațiile României cu aceste state. La percheziție, s-a găsit asupra lui Urban și un extras dintr-un plan sovietic asupra *tacticii insurecției armate în România* (lupta de stradă), document elaborat de Emil Bodnăraș cu concursul agenților sovietici. S-a mai stabilit că Emil Bodnăraș lua contact, din închisoare, cu Moscova, prin Legația sovietică de la București, care-i trimitea bani și instrucțiuni prin fratele său. Tot Emanoil era cel care ducea la Legația sovietică rapoartele lui Emil din închisoare asupra situației reale a Partidului Comunist din România în urma arestărilor, precum și alte date despre comuniști și spionii sovietici arestați[36].

O altă împrejurare care a dus la cimentarea colaborării noastre informative cu germanii a fost „cazul Dorman”, petrecut în iarna anilor 1936-1937. Dorman (numele era conspirativ), fost colonel țarist, s-a dat drept „reprezentant” al guvernului mexican pentru a face unele achiziții de avioane vechi de la statul român, în valoare de sute de milioane de lei.

După finalizarea anchetei în acest caz, Niky Ștefănescu s-a deplasat în Germania pentru a avertiza în chestiune *Abwehr*-ul și, dacă germanii erau deschiși, să fie încheiat un *acord de colaborare informativă* (antisovietică) între serviciul german și Serviciul *„S”* din România.

O altă împrejurare care a dus la cimentarea colaborării noastre informative cu germanii a fost *„cazul Dorman”*, petrecut în iarna anilor 1936-1937. Dorman (numele era conspirativ), fost colonel țarist, s-a dat drept *„reprezentant”* al guvernului mexican pentru a face unele achiziții de avioane vechi de la statul român, în valoare de sute de milioane de lei. Dar, Serviciul *„S”* român a descoperit că Dorman se afla, de fapt, în serviciul de spionaj sovietic, iar avioanele achiziționate luau drumul Spaniei, unde serveau pentru dotarea brigăzilor bolșevice (internaționale) care luptau în *războiul civil* din această țară. Românii au descoperit că Dorman efectuase deja achiziții similare și în Germania, informând, în acest sens, *Abwehr*-ul. La Berlin a plecat tot Niky Ștefănescu, ocazie cu care a fost primit și de conducerea *Gestapo* (poliția politică a regimului lui Adolf Hitler)[37].

[36] Sursă consultată de autor într-o colecție privată.
[37] ASRI, dosar nr. 20954, vol. 1-21.

La începutul lui ianuarie 1937, Niky Ștefănescu s-a deplasat incognito la Berlin, pentru a fixa o întâlnire cu șefii spionajului german. În luna următoare, o echipă a Serviciului *„S”*(ecret) al Armatei Române a făcut o vizită cu caracter strict secret la sediul *Abwehr*-ului, sub *„motivul” procurării de aparate tehnice necesare Serviciului*, dar cu scopul real: *stabilirea unor contacte de cooperare informativă pe Frontul de Est* (antisovietic) *cu partea germană*. Deși era *„subșeful Serviciului Secret și șeful Secției de Contrainformații”*, adică numărul 2 în Serviciul *„S”* după Moruzov, de această dată, Niky Ștefănescu s-a prezentat părții germane drept un simplu *„funcționar civil, specialist în chestiuni militare ale Frontului de Est”*, probabil sub conspirativul *„I. Popescu”*. Pentru a deruta partea germană, acesteia i-a fost prezentat ca șef oficial al echipei române maiorul Ionescu-Micandru Constantin, însoțit de cpt. ing. Dumitru Son și cpt. ing. Mihai Șerbănescu (românii bănuiau că și ofițerii germani aveau nume conspirative)[38].

La 21 februarie 1937, Niky Ștefănescu și echipa sa au asistat la parada „Zilei Eroilor”, eveniment la care a participat însuși Adolf Hitler, însoțit de mareșalul August von Mackensen. Una dintre concluziile părții române era că „schimbul de informații militare privind URSS, făcut în cel mai strict secret, a fost sincer și fără rezerve, iar în viitor, cantitatea și calitatea vor crește; că autoritățile germane, pentru a avea informații cât mai multe asupra URSS, vor fi dispuse la un aranjament precis și durabil”.

Niky Ștefănescu a luat contact cu maiorul von Krienitz, care s-a recomandat a fi *„ajutorul”* amiralului Wilhelm Canaris – șeful Secției Informații din Marele Stat Major al Armatei Germane *(Abwehr)*. Partea română a vizitat și sediul *Gestapo*, unde a fost primită de dr. Best, care și-a arătat deplina satisfacție pentru acest început de colaborare, mai ales că Rusia sovietică avea graniță comună cu România, și a propus ca ing. Son și ing. Șerbănescu[39] să facă practică la Berlin, la *Gestapo*, și să folosească aparatele acestuia. La 21 februarie 1937, Niky Ștefănescu și echipa sa au asistat la parada *„Zilei Eroilor”*, eveniment la care a participat însuși Adolf Hitler, însoțit de mareșalul August von Mackensen. Una dintre concluziile părții române era că *„schimbul de informații militare privind URSS, făcut în cel mai strict secret, a fost sincer și fără rezerve, iar în viitor, cantitatea și calitatea vor crește; că autoritățile germane, pentru a avea informații cât mai multe asupra URSS, vor fi dispuse la un aranjament precis și durabil”*[40].

[38] ASRI, D, dosar nr. 3694, filele 20-32, *Darea de seamă asupra călătoriei la Berlin, 12-24 februarie 1937*.

[39] La 1 noiembrie 1936, ing. cpt. Mihai Șerbănescu a devenit ajutor al șefului *Serviciului Tehnic* din Serviciul *„S”* și, împreună cu ing. cpt. Son, au procedat la dotarea Serviciului cu mașini, aparate și materiale tehnice moderne pe care le-au procurat din Germania.

[40] ASRI, D, dosar nr. 3694, filele 20-32, *Darea de seamă asupra călătoriei la Berlin, 12-24 februarie 1937*; sau ANR, Inv. 2379, dosar nr. 24/1937, f. 23 și urm.

REORGANIZAREA SECȚIEI CONTRAINFORMAȚII

În ceea ce privește *organizatorul* și *formatorul* Niky Ștefănescu, iată câteva impresii ale lui Eugen Cristescu: *„Niky Ștefănescu, fire inteligentă și întreprinzătoare, a scos Secția Contrainformații din rutină, reorganizând-o complet, a introdus o serie de inovații tehnice și i-a adus aici pe Scarlat Grigoriu, Ștefan Enescu și Nicolae Stănescu”*, viitoare nume grele în contraspionajul românesc. La reorganizare, *„contribuie în mare măsură și Marele Stat Major, atât ca directive și plan de căutare, cât și în dotarea cu personal*[41]*. Echipele de contraspionaj erau conduse direct de Niky Ștefănescu. Cele pentru curente subversive se aflau sub coordonarea lui Gheorghe Comșa; cele de filaj, conduse de Albu [nume real Gheorghe Untăreanu] – Rizescu [Constantin] etc. Ele aveau în componență echipe volante, cu organizare aparte, de asemenea și echipe pentru supravegherea și filajul misiunilor diplomatice străine. De pildă, pentru supravegherea misiunii diplomatice a URSS, Niky Ștefănescu și Mihail Moruzov au alcătuit o echipă specială, formată din cele mai bune elemente. Totodată, echipele Serviciului „S” au infiltrat cu elemente informative speciale aproape întreg aparatul nostru diplomatic din străinătate. Ca urmare – sublinia Eugen Cristescu –, ‹Secția Contrainformații devine foarte puternică, posedând un personal numeros, temeinic format la Școala de cadre a Serviciului S, după cele mai moderne metode de instruire›”*[42].

Niky Ștefănescu, fire inteligentă și întreprinzătoare, a scos Secția Contrainformații din rutină, reorganizând-o complet, a introdus o serie de inovații tehnice și i-a adus aici pe Scarlat Grigoriu, Ștefan Enescu și Nicolae Stănescu.

Mai completăm că toată această reorganizare s-a făcut temeinic și după criterii raționale, științifice, după consultarea unui vast material documentar asupra altor servicii de informații, mai cu seamă a datelor privind organizarea *British Intelligence Service*, Biroul II-francez și a FBI american, plus datele culese asupra serviciilor de informații vecine: polonez, ungar, bulgar, sârb și cehoslovac.

Însă, această activitate a întâmpinat opoziția crâncenă a Ministerului de Externe, îndeosebi pe cea a lui Nicolae Titulescu, care, în anii 1934-1936, era factorul dominant al diplomației noastre și care acuza Serviciul *„S”* că, prin infiltrarea în aparatul de externe al țării,

[41] ASRI, dosar nr. 17474, vol. 1, diverse *declarații* făcute de Eugen Cristescu, filele 5-V.

[42] *Ibidem*, filele 7-45.

nu se respectă *„principiile diplomatice”*[43]. Or, Mihail Moruzov, care nu agrea pro-sovietismul arătat de Titulescu și nu dorea niciun fel de relații cu regimul sovietic, a canalizat aproape întreaga activitate informativă și contrainformativă a Serviciului *„S”* împotriva URSS. Încă din prima zi de la reluarea relațiilor diplomatice cu sovieticii (decembrie 1934), Legația acestora din București a fost supusă unei stricte supravegheri și filaj, acțiune condusă personal de Niky Ștefănescu[44]. De asemenea, o echipă de supraveghere *„antisovietică”*, sub conducerea lui Niky Ștefănescu, se deplasa frecvent la Legația Regală a României de la Geneva, la sediul Ligii Națiunilor, unde activa Titulescu, purtând asupra sa o *„valiză diplomatică blindată”* care avea inclus un post de radio-emisie[45].

Afacerea Butenko: la 6 februarie 1938, Hrisanfovici Theodor Butenko, abia numitul însărcinat sovietic cu afaceri al Legației sovietice în România, a dispărut de la locuința sa particulară. A doua zi, la orele 16.00, Vladimir Bodrov, atașat de presă și reprezentant al „TASS”, dar și cel care asigura supravegherea contrainformativă a personalului sovietic, s-a prezentat la Ministerul Afacerilor Externe al României pentru a semnala „dispariția” diplomatului.

Nicolae Titulescu a protestat față de această *„suspectare”* a activității sale și, văzând că nu era posibilă înlăturarea echipei de supraveghere, a cerut măcar ca respectiva echipă să fie condusă de Gheorghe Cristescu, fratele lui Eugen Cristescu, de la Siguranță. Gheorghe Cristescu se afla la Paris de mai mulți ani, trimis de Moruzov, pentru desăvârșirea specializării sale tehnice în cadrul Serviciului *„S”*. Titulescu avea încredere în Gheorghe Cristescu, pe care îl vedea ca pe un element format la școala franceză, iar Franța, la vremea aceea, dezvoltase relații cu sovieticii. Prin Niky Ștefănescu, Gheorghe Cristescu reușise fotocopierea clandestină a *Protocoalelor Dezarmării pentru Conferința de la Geneva*, care, la ordinul lui Moruzov, au fost predate personal lui Nicolae Titulescu, fiindu-i de mare ajutor diplomatului român în negocierile anevoioase la care a participat[46].

AFACEREA BUTENKO

Afacerea Butenko: la 6 februarie 1938, Hrisanfovici Theodor Butenko, abia numitul însărcinat sovietic cu afaceri al Legației sovietice în România, a dispărut de la locuința sa particulară. A doua zi, la orele 16.00, Vladimir Bodrov, atașat de presă și reprezentant al *„TASS”*, dar și cel care asigura supravegherea contrainformativă a personalului sovietic, s-a prezentat la Ministerul Afacerilor Externe al României pentru a semnala *„dispariția”* diplomatului.

În următoarele zile, presa sovietică și guvernul sovietic au atacat virulent din toate direcțiile, amenințând autoritățile române cu intervenția armată pentru a-l *„elibera pe tov. Butenko”*, caracterizat drept *„un prieten personal al tovarășului Stalin, răpit de imperialiștii de la București”*[47].

Apoi, stupoare: la 14 februarie 1938, presa italiană a anunțat că Butenko se află la Roma și că a plecat din proprie inițiativă, din cauză că urma să fie suprimat de un agent al GPU (poliția politică sovietică).

Dar, iată, pe scurt, faptele acestui episod: Serviciul *„S”* avea date certe că GPU urma să-l înlăture pe Butenko (prin agentul Vasile Thumanov, sosit în acest sens de la Legația sovietică din Praga). Planul sovietic prevedea un *ultimatum* și, eventual, o intervenție armată pentru ocuparea Basarabiei. Prevenit de partea română, Butenko a *„dezertat”* și a stat ascuns vreme de patru zile acasă la Mihail Moruzov (str. Sofia nr. 17), unde a fost interogat de Niky Ștefănescu cu privire la rețelele informative sovietice în România, agenți de influență etc. De asemenea, Th. Butenko a lăsat mai multe scrisori (olografe), în care și-a exprimat motivele gestului. Una dintre ele i-a fost adresată Regelui Carol al II-lea, scrisoare din care redăm următorul pasaj: *„Sire, părăsind granițele țării, destinele căreia sunt încredințate Augustelor Voastre mâini, sunt profund fericit că numai pe teritoriul ei m-am deșteptat din apăsatul vis rău bolșevic ce-mi sfâșia inima de câțiva ani. (…) În activitatea mea viitoare și în calitate de intelectual ucrainean, doritor de fericire pentru acest popor martir, aș fi foarte fericit dacă aș putea aduce cel mai mic serviciu Majestății Voastre, încredințat fiind că între Ucraina dezrobită de bolșevici și Regatul Majestății Voastre se vor stabili legături de strânsă prietenie și de înțelegere reciprocă. (…) Sire, la 6 februarie, ora 7 seara, eu, șeful misiunii sovietice din București, am părăsit pentru totdeauna clădirea Legației URSS, pentru a cădea la Augustele Voastre picioare, rugând pe Majestatea Voastră să-mi acorde refugiul și aducându-Vă spovedania mea, din care se va vedea cum eu, cetățean rus, în vârstă de 33 ani, am fost târât pe calea*

[43] *Ibidem*.
[44] *Ibidem*.
[45] *Ibidem*.
[46] *Ibidem*.
[47] ASRI, dosar nr. 20954, vol. 14, ff. 150 și urm.

infernală a bolșevismului, cât și motivele care m-au determinat să mă rup de voie de ei. Persoana Mea (...)”[48]. Mai mult, Regele Carol al II-lea l-a primit în secret pe Th. Butenko.

Mai reiese din documente că, inițial, Butenko a cerut protecția guvernului Octavian Goga, dar protestul Moscovei a fost atât de energic, încât, pentru a detensiona situația, guvernul nostru a demisionat și a fost nevoie să se negocieze urgent cu puteri mai mari, Italia și Germania, pentru preluarea lui Butenko.

La 10 februarie 1938, la punctul de frontieră Jimbolia, în tabelul referitor la trecerile de persoane spre Iugoslavia apare numele *„Niky Ștefănescu, director, supus român”*, însoțindu-l pe un anume *„Mircea Ioan Dobrescu, cu pașaportul nr. 255014/938, eliberat de Ministerul de Interne”*, nimeni altul decât... celebrul Theodor Butenko, ambii călători având ca destinație Roma!

La 10 februarie 1938, la punctul de frontieră Jimbolia, în tabelul referitor la trecerile de persoane spre Iugoslavia apare numele „Niky Ștefănescu, director, supus român”.

Dar, în ciuda evidențelor, sovieticii continuau să susțină că Th. Butenko nu a fugit, ci a fost răpit și ucis, iar că individul aflat în custodia autorităților italiene nu era adevăratul Butenko. Astfel, la cererea autorităților italiene, Niky Ștefănescu a repetat vizita la Roma pentru a-l *„recunoaște”* pe Theodor Butenko. S-a păstrat raportul către Mihail Moruzov, unde Niky Ștefănescu descrie scurta reîntâlnire cu Butenko și surpriza acestuia de a vedea figuri *„cunoscute”*.

Totuși, cu prilejul celei de a doua deplasări la Roma, pe baza relațiilor deja create, Niky Ștefănescu, în numele Serviciului *„S”* al Armatei Române, a semnat cu omologii italieni un *acord de cooperare informativă antisovietică*. Despre această misiune, Niky i-a raportat lui Moruzov: *„Am fost la Roma să verific identitatea lui T. Butenko, ocazie cu care, în data de 20 februarie 1938, am luat contact cu șeful Serviciului de Informații al armatei italiene, Cavalerul Santo Emanuele, cu care am discutat necesitatea unei colaborări în fața pericolului comun pe care-l reprezintă agitațiile Moscovei (...). Am stabilit, apoi, posibilitatea întreprinderii unor acțiuni comune în vederea contracarării continuelor uneltiri și provocări sovietice, preconizând cu dl Santo Emanuele un schimb de informații asupra următoarelor chestiuni: activitatea politică și informativă a sovietelor în străinătate, directivele pentru greve*

[48] *Ibidem.*

și sabotaj; activitatea sovietică și identificarea legăturilor în străinătate ale sovietelor; organizarea și dislocarea Armatei Roșii (...)”. Pe acest raport, Mihail Moruzov a semnat și a pus următoarea rezoluție: *„Am considerat că această legătură este necesară, având în vedere nevoile Serviciului „S” pentru conlucrări cu interese comune”*[49]. Succesul misiunii din Italia este confirmat în iunie 1938, când, în secret, a avut loc vizita în România a generalului italian Valle, șeful Marelui Stat Major al armatei italiene, însoțit de Della Porta, atașatul militar italian la București. La întoarcere, generalul italian a trimis Marelui Stat Major al armatei române o scrisoare de felicitare pentru dl Nicolae Ștefănescu, pentru modul în care s-a ocupat de buna desfășurare a vizitei[50].

Succesul misiunii din Italia este confirmat în iunie 1938, când, în secret, a avut loc vizita în România a generalului italian Valle, șeful Marelui Stat Major al armatei italiene.

Tot în această perioadă, notăm că Niky Ștefănescu a fost trimis de Mihail Moruzov să negocieze *acorduri de colaborare informativă* și cu omologii din Iugoslavia, Grecia și Turcia. De pildă, la 22 iunie 1938, Niky Ștefănescu a primit din partea statului iugoslav *„Coroana Iugoslaviei”*, prin Decret al Regelui Iugoslaviei (comunicare făcută părții române de către locotenent-colonelul iugoslav Stropnik – adresa nr. 45889 din 27 ianuarie 1939, Marele Stat Major, Secția a II, către Serviciul Secret)[51].

La 7 februarie 1940, Niky Ștefănescu se afla iar în Iugoslavia, de această dată pentru semnarea unui acord de colaborare și schimb de informații între Serviciul *„S”* român și Siguranța iugoslavă. Intermediar a fost ambasadorul Victor Cădere, care a stabilit contactele necesare cu dl Vlascalin, *Subsecretar de Stat însărcinat cu conducerea Siguranței iugoslave*[52].

LA CONDUCEREA CORPULUI DETECTIVILOR ȘI, APOI, LA CONDUCEREA SIGURANȚEI GENERALE

Intensificarea riscurilor și amenințărilor externe la adresa României a determinat conducerea statului să caute o nouă formulă de eficientizare a sistemului național de informații. Niky Ștefănescu, considerat a fi un bun cunoscător și al realităților din Siguranța Statului,

[49] *Ibidem*, f. 152.
[50] *Ibidem*, f. 232.
[51] *Ibidem*, fila 234.
[52] ASRI, dosar nr. 9060, vol. 2, ff. 5-7; dosar nr. 20954, vol. 4, *privind ancheta Moruzov*, fila 401.

a fost delegat, în aprilie 1937, cu preluarea Corpului Detectivilor[53] (oficial, el a fost numit prin *decizia* de ministru nr. 22 267 din august 1938). Prin lege, Corpul Detectivilor avea ca atribuții culegerea de informații prin toate mijloacele: filaj, informatori, interceptări telefonice și de corespondență etc. din cadrul: partidelor politice extremiste; organizațiilor minorităților naționale, mișcărilor iredentiste; legațiilor străine; urmărirea suspecților de spionaj; asigurarea pazei și protecției familiei regale și a unor demnitari[54].

Prin lege, Corpul Detectivilor avea ca atribuții culegerea de informații prin toate mijloacele: filaj, informatori, interceptări telefonice și de corespondență etc. din cadrul: partidelor politice extremiste; organizațiilor minorităților naționale, mișcărilor iredentiste; legațiilor străine; urmărirea suspecților de spionaj; asigurarea pazei și protecției familiei regale și a unor demnitari.

Din punct de vedere operativ, prin numirea lui Niky Ștefănescu, Corpul Detectivilor (organ al Ministerului de Interne) se subordona acum Serviciului *„S”* (organ al Ministerului Apărării Naționale), sens în care Niky îi trimitea zilnic raportul lui Moruzov și la care se prezenta pentru directive mai importante.

Și la Corpul Detectivilor, Niky Ștefănescu s-a dovedit a fi un excelent organizator, în special pe zona informativă. Dovadă stau rapoartele vremii, astfel: *„La Siguranță, Niky Ștefănescu a adus un suflu nou, în bună parte acesta fiind mentalitatea de la Serviciul Secret, sporită cu aportul său personal. Fără a intra în detalii, este suficient a se afirma că* ***cel mai complet aparat de informații interne, politice, diplomatice și economice, care fusese până atunci în România, era cel creat la Siguranță de Niky Ștefănescu*** *[subl.a.]. La această performanță a fost ajutat de capacitatea sa profesională, care crescuse, de autoritatea instituției, de faptul că avea un ajutor prețios în persoana lui Valeriu Ionescu, detașat la Serviciul Secret, cât și de fondurile mari ce-i fuseseră puse la dispoziție”*[55].

Așa-numitul *„stat major”* al lui Niky Ștefănescu la Corpul Detectivilor era format din oameni aduși și formați de el: Paul Abramovici, Tică Gheorghiu, Nicolae Baicu, Petrovici, Borcea, Oproiu, Taflaru, Ghițescu, Wirth, Costel Petrescu, Nae Georgescu, Mănăilă, Curelea etc[56].

Drept urmare, succesele Corpului Detectivilor se țineau lanț: Niky Ștefănescu a salvat, *„în 10-12 rânduri”*, viața Regelui Carol al II-lea, iar după alte versiuni, chiar de mai multe ori, la care, în tot atâtea rânduri, legionarii încercaseră să atenteze: *„Nu se poate preciza în amănunt unde este meritul lui Niky Ștefănescu și dacă prima informație care a dus la înlăturarea atentatului, la fiecare dintre aceste cazuri, nu venea de la însuși Mihail Moruzov; dar, în orice caz, instrumentarea tehnică a afacerii a fost întotdeauna meritul lui Niky Ștefănescu”*[57].

Alteori, o *echipă specială* a Corpului Detectivilor *„îi lichida fizic pe complotiști”*, ceea ce astăzi nu poate fi trecut cu vederea, deși nici la serviciile occidentale nu lipsesc astfel de exemple. Din această *echipă* făcea parte și Gheorghe Comșa, care, deși angajat la Serviciul *„S”*, participa la *„operațiile grele ale Direcției Generale a Poliției”*. Oamenilor coordonați de Niky Ștefănescu nu le scăpa nici activitatea desfășurată de Partidul Național-Țărănesc și cel Liberal, aceasta fiind raportată uneori la interval de câteva ore distanță de când se producea vreun fapt în interiorul acestor partide istorice. Deosebit de aceasta, nu scăpa vigilenței lui Niky Ștefănescu nici *„activitatea germanilor, etnici și pașaportari, împreună cu cea a organizațiilor lor și* ***se spunea că poate nici la Berlin nu exista o evidență mai strictă a activității lor decât era la Direcția Generală a Poliției*** *[subl.a.]. Identic, și viața economică, cu toate combinațiile și dedesubturile diferitelor societăți, era tot atât de atent raportată, urmărindu-se pas cu pas infiltrația capitalului german, cu combinațiile sale politice, cât și rivalitatea acestuia cu cel apusean”*[58].

*

Dar, cu toată această vigilență, unele evenimente politice nu au putut fi împiedicate, deși informații existau. La sfârșitul lui iunie 1940, guvernul sovietic a somat România să renunțe la Basarabia, amenințând cu invazia armată. Ungaria și Bulgaria amenință, și ele, România. Regele Carol al II-lea cere Germaniei să garanteze hotarele noastre. Sistemul nostru național de informații trece de la *starea de pace* la cea *de război*, intrând sub coordonarea militarilor. Ca urmare, prin Decizia ministrului de Interne nr. 46303 din 4 iulie 1940, Nicolae Ștefănescu, detașat ca șef al Corpului Detectivilor, este delegat cu conducerea

La sfârșitul lui iunie 1940, guvernul sovietic a somat România să renunțe la Basarabia, amenințând cu invazia armată. Ungaria și Bulgaria amenință, și ele, România. Regele Carol al II-lea cere Germaniei să garanteze hotarele noastre. Sistemul nostru național de informații trece de la starea de pace la cea de război, intrând sub coordonarea militarilor.

[53] *Idem*, dosar nr. 20954, vol. 12, f. 228.
[54] Pe larg, despre acest subiect, în Sorin Aparaschivei, *Corpul Detectivilor – Scotland Yard-ul românesc*, disponibil pe www.Historia.ro.
[55] ASRI, dosar nr. 20954, vol. 15, ff. 222-225; Valeriu Ionescu, șef de grupă la Serviciul S, apoi SSI, i-a supravegheat pe comuniști, s-a sinucis prin împușcare după 23 august 1944 (n.a.).
[56] *Idem*, dosar 10998, vol. 1, fila 142.
[57] *Idem*, dosar nr. 20954, vol. 15, ff. 222-225.
[58] *Ibidem.*

Direcției Poliției de Siguranță din Direcția Generală a Poliției[59]. La 13 iulie același an, este emis decretul de lege nr. 49477-S, prin care are loc contopirea Direcției Generale a Polițiilor cu Corpul de Jandarmi și Prefectura Poliției Capitalei într-un organ unic, cu denumirea de *Direcția Generală a Poliției și Siguranței Statului*. Niky Ștefănescu a fost însărcinat la conducerea acestei instituții[60].

Dar, lucrurile continuau să se precipite. În următoarele luni, *Gestapo*, iar nu *Abwehr* are cuvântul de spus în România. Conducerea Germaniei mizează pe *mișcarea legionară*. La 1 septembrie 1940, prin Decizia cu nr. 61765-S, Niky Ștefănescu a fost retras din toate funcțiile deținute la *Siguranță* și a revenit la postul său de titular din Serviciul *„S”* al Armatei Române[61].

CONCLUZII: SFÂRȘITUL ȘI AMINTIREA LUI NIKY ȘTEFĂNESCU

„Niky Ștefănescu a reprezentat un elev reușit al lui Mihail Moruzov, care, la învățămintele maestrului său, a adăugat o experiență polițienească proprie și randamentul unei inteligențe vioaie, cu multe posibilități de adaptare la situații diferite.”

La 6 septembrie 1940, Mihail Moruzov și Niky Ștefănescu sunt arestați și închiși la Jilava, unde, în noaptea de 26/27 noiembrie din acel an, au fost asasinați de legionari[62]. Amenințată de legionari, Iraida Ștefănescu a părăsit Bucureștiul și s-a mutat în Basarabia, la Orhei. O *notă* a Serviciului Special de Informații din România (fostul Serviciu *„S”*) arată că, pe timpul ocupației sovietice a Basarabiei, aceasta ar fi intrat în atenția organelor sovietice de informații. După 23 august 1944, Iraida Ștefănescu a făcut mai multe demersuri pentru ca statul român să-i acorde o pensie de urmaș[63].

Aceasta este, pe scurt, biografia lui Niky Ștefănescu, unul dintre cei mai mari profesioniști pe care i-a avut spionajul și contraspionajul românesc. Însemnătatea sa pentru acest domeniu se relevă și de următoarea mărturie de arhivă: *„Niky Ștefănescu a reprezentat un elev reușit al lui Mihail Moruzov, care, la învățămintele maestrului său, a adăugat o experiență polițienească proprie și randamentul unei inteligențe vioaie, cu multe posibilități de adaptare la situații diferite.*

[59] *Ibidem*, f. 92.
[60] *Ibidem*, f. 96.
[61] *Ibidem*, f. 99.
[62] ASRI, dosar nr. 10998, vol. 1, f. 129.
[63] *Idem*, dosar nr. 20954, vol. 15, filele 287.

***Nu a avut convingeri politice** și, așa cum în Basarabia a urmărit mișcarea comunistă, tot așa a urmărit la București pe legionari; **orientarea sa fiind numai după interesele Statului**. (...) Cei care au luat contact cu el au avut de câștigat în rapiditatea soluționării problemelor și executarea fără atitudini personale a misiunilor primite din partea ordinii stabilite”*[64].

Pentru meritele excepționale în serviciul statului și națiunii române, Niky Ștefănescu a fost apreciat la cel mai înalt nivel, fiind onorat cu diverse decorații, printre care: *„Bărbăție și Credință Clasa I”, „Cavaler al Ordinului Coroana României”, „Ofițer al Ordinului Coroana României”, „Crucea de Război Franceză”.*

SURSE BIBLIOGRAFICE:

1. ***, Arhivele Naționale ale României, Inv. 2349, *Direcția Generală a Poliției*, dosarele nr.: 58/1920; 6/1929; 24/1937.
2. ***, Arhiva Serviciului Român de Informații, dosarele nr.: 3694; 4702; 6771; 7181; 7328; 8348; 8724; 9060; 9279; 10998; 17474; 20954 etc.
3. Pavel Moraru, *Serviciile secrete și Basarabia, Dicționar 1918-1991*, Editura Militară, București, 2008.
4. Sorin Aparaschivei, *Corpul Detectivilor – Scotland Yard-ul românesc*, disponibil pe: www.Historia.ro.
5. Sorin Aparaschivei, *Sistemul național de informații de la Regulamentul Organic și până după Războiul de Reîntregire Națională*, Editura Militară, București, 2018.

[64] *Ibidem*, ff. 222-225.

MISIUNEA NAVALĂ FRANCEZĂ ÎN ROMÂNIA – EFORTURI PENTRU SEMNAREA UNOR CONTRACTE DE ÎNZESTRARE NAVALĂ LA ÎNCHEIEREA PRIMULUI RĂZBOI MONDIAL –

Drd. Dan-Dragoș SICHIGEA

Șef Secție Muzeu Mangalia, Muzeul Național al Marinei Române

La încheierea Primului Război Mondial, organismul militar al României se resimțea după efortul depus și a intrat într-o etapă de reorganizare a structurilor sale. În ceea ce privește componenta navală a sistemului național de securitate, intrarea în posesia litoralului Basarabiei creștea și mai mult presiunea pe Divizia de Mare, care trebuia să primească toată atenția factorilor de decizie ai Marinei Române pentru perioada următoare. Drept urmare, Inspectoratul Marinei a căutat noi variante de dezvoltare a parcului de nave de care dispunea, prin contacte cu ofițerii de marină străini aflați în diferitele misiuni în România. Cei mai activi au fost reprezentanții Misiunii Navale Franceze, care au propus mai multe tipuri de nave militare Marinei Române în anul 1919.

Cuvinte-cheie: Inspectoratul Marinei, Misiunea Navală Franceză, Marina Militară, dragoare, Royal Navy.

ÎNCEPUTURILE MISIUNII FRANCEZE

Încă din 1916, Franța a organizat, în cadrul Misiunii Militare din România, și o componentă navală, care avea ca obiective modernizarea micii Marine Române și, mult mai important pentru interesele Parisului, eficientizarea conducerii operațiilor pe Dunăre împotriva Puterilor Centrale. Pentru această misiune au fost trimiși în România trei ofițeri: căpitanul Belloy de Saint-Liénard (Șeful Misiunii Navale) și locotenenții Berg de Breda și Bahezre de Lanley[1].

Rezultatele concrete ale prezenței specialiștilor francezi în rândul marinarilor români au fost, mai degrabă, limitate. Ieșirea României din război prin Pacea de la Buftea-București a consemnat sfârșitul acțiunilor navale pe Dunăre, fără prea multe evenimente și cu reușite minore.

Poziția strategică a României oferea perspective viabile. Cu atât mai mult, cu cât, alături de importanța arterei comerciale care era Dunărea, proximitatea Rusiei merita o atenție deosebită pentru interesele franceze în estul Europei.

Interesul francez în aspectele navale care priveau România a revenit, însă, după reintrarea ei în război și avea să continue în următorii ani, perioadă în care România încearcă să-și recapete teritoriile pierdute și să-și consolideze poziția de stat național. Ca posibil aliat într-un conflict în Marea Neagră, Bucureștiul nu promitea prea multe din punct de vedere naval. Marina Română nu deținea forțe maritime substanțiale și, în ciuda planurilor de expansiune, ofițerii de marină francezi aveau destule indicii să suspecteze că nu vor exista fondurile necesare pentru o creștere serioasă a potențialului de luptă român la Marea Neagră, cel puțin pe termen scurt și mediu. Poziția strategică a României însă oferea perspective viabile. Cu atât mai mult, cu cât, alături de importanța arterei comerciale care era Dunărea, proximitatea Rusiei merita o atenție deosebită pentru interesele franceze în estul Europei. La concluzii similare a ajuns și Marina Britanică (Royal Navy), care s-a grăbit să recupereze avansul luat de Franța în chestiunea influenței navale în Marea Neagră.

Comparativ cu pașii făcuți de partea britanică, Franța a investit mult mai multe resurse în menținerea influenței în Marina Română,

[1] Patrick Boureille, *„Les relations navales franco-roumaines (1919-1928): les illusions perdues”*, în *Revue historique des armées*, 244/2006, p. 2.

fără a obține însă rezultatele anticipate. Până în vara anului 1920, Marea Britanie a reușit să trimită o misiune militară navală la București, care a funcționat în paralel cu cea franceză, recuperând astfel din avantajul pe care îl avusese Franța prin instalarea propriei misiuni în timpul Primului Război Mondial. Mai mult, prin faptul că misiunea britanică a fost acreditată pe lângă Ministerul de Război, în vreme ce misiunea Franței era acreditată pe lângă Directorul Superior al Marinei, putem aprecia că Franța a intrat într-un con de umbră în raporturile cu Marina Română.

Încă din februarie 1919, conducerea Marinei Române a solicitat sprijinul Misiunii Navale Franceze pentru organizarea unui serviciu de dragaj pe coastele României, după ce apelurile la celelalte Puteri Aliate nu au primit un răspuns favorabil. Ca și în cazul acestor cereri, conducerea Marinei dorea să-i fie cedate ori măcar împrumutate nave de dragaj, pe care să le utilizeze cu echipaje proprii în misiunile de dragaj.

Se explică deci de ce Misiunea Navală Franceză a căutat metode de a redeveni relevantă în zona Dunării și a Mării Negre. Una dintre ele, cu posibile consecințe negative neprevăzute pentru poziția navală franceză în zonă, a fost participarea ofițerilor de marină francezi la proiectul de reorganizare a Marinei Române, la încheierea Primului Război Mondial. Din rapoartele căpitanului O´Neill, care i-a luat locul lui Belloy la sfârșitul anului 1919, Directorul Superior și Inspectorul Marinei, contraamiralul Constantin Bălescu, nu a apreciat cooperarea directă a ofițerilor de marină francezi cu Guvernul României, trecând peste poziția conducerii Marinei, la reorganizarea ei după război[2].

IDEEA VÂNĂTOARELOR DE SUBMARINE

Un aspect în care Misiunea Navală Franceză s-a bucurat de un oarecare succes și unde a putut să-i depășească pe rivalii ei britanici a fost misiunea de dragare a minelor rămase pe fluviu, dar și pe mare, în urma barajelor instalate între anii 1916 și 1918. De la plecarea navelor dragoare ale Puterilor Centrale, România nu a fost capabilă să ofere siguranța navigației decât pe Dunăre, și aceasta cu mari eforturi[3].

Încă din februarie 1919, conducerea Marinei Române a solicitat sprijinul Misiunii Navale Franceze pentru organizarea unui serviciu de dragaj pe coastele României, după ce apelurile la celelalte Puteri Aliate nu au primit un răspuns favorabil. Ca și în cazul acestor cereri, conducerea Marinei dorea să-i fie cedate ori măcar împrumutate nave de dragaj, pe care să le utilizeze cu echipaje proprii în misiunile de dragaj. Partea română dorea să profite de intenția Franței de a face unele sacrificii pentru a-și consolida poziția la Marea Neagră.

[2] *Ibidem*, p. 3.
[3] Arhivele Militare Naționale Române (AMNR), fond Comandamentul Marinei Militare, dosar 270, f. 71.

Dovada acestei intenții era tocmai decizia de a păstra navele dragoare pe care le avea în acea zonă chiar și pe timp de pace, pentru a continua serviciul de dragaj.

La nivelul conducerii Inspectoratului Marinei de la București nu existau îndoieli cu privire la necesitatea de a se crea unități de dragoare la Marea Neagră, nu numai pentru a asigura rutele de navigație de care depindea relansarea economică a țării, ci și, așa cum arăta contraamiralul Bălescu, pentru a se evita ca Puterile Aliate să *„organizeze singure controlul zonelor minate în apele și porturile noastre”*[4]. Era o chestiune de prestigiu național ca România să nu depindă de nave străine, motiv pentru care s-a cerut operarea dragoarelor de către echipaje românești, în eventualitatea în care ar fi fost împrumutate. Pentru un stat care își propunea să se afirme ca o putere demnă de luat în seamă la Marea Neagră, nu era acceptabil ca dragajul apelor teritoriale să fie realizat de forțe navale străine: *„ar însemna deci a chema și a primi o protecție străină în apele și porturile noastre, care poate să ne conducă la obligațiuni costisitoare și servitudini umilitoare”*[5]. Este foarte posibil ca afirmațiile contraamiralului Bălescu să fi fost făcute în relație cu cele două misiuni străine, franceză și britanică, ai căror membri se implicau în diferitele proiecte de dezvoltare ale Marinei Române, un amestec pe care conducerea l-a resimțit în mod deosebit.

Era o chestiune de prestigiu național ca România să nu depindă de nave străine, motiv pentru care s-a cerut operarea dragoarelor de către echipaje românești, în eventualitatea în care ar fi fost împrumutate. Pentru un stat care își propunea să se afirme ca o putere demnă de luat în seamă la Marea Neagră, nu era acceptabil ca dragajul apelor teritoriale să fie realizat de forțe navale străine.

Planul Marinei Române era de a continua negocierile începute deja cu Franța pentru achiziționarea canonierelor tip *„Chiffone”*, care se vor concretiza prin intrarea în serviciu, în decembrie 1919, a patru astfel de nave[6], și să se folosească de bunăvoința astfel obținută pentru a primi, sub formă de împrumut, mai multe nave de dragaj franceze. Dacă s-ar fi ajuns la concretizarea planului, Marina Română ar fi dispus de trei *„divizii de vase dragă-mine”*[7], cu următoarea componență:

- prima unitate, în zona cea mai nordică amenințată, având sediul la Sulina, cu două canoniere dotate cu echipamente de dragaj, plus șase vedete dragoare în zona Sulina-Akerman;

[4] *Ibidem*, f. 69.
[5] *Ibidem*, f. 70.
[6] Georgeta Borandă, *„Nave de luptă românești – breviar”*, în Ion Ionescu, Georgeta Borandă, Marian Moșneagu, *Noi contribuții la istoria Marinei Militare Române*, Editura Muntenia&Leda, Constanța, 2001, p. 145.
[7] AMNR, fond Comandamentul Marinei Militare, dosar 270, f. 70.

- la sud, la Constanța, o a doua *„divizie dragă-mine”*, cu același număr și același tip de nave; zona ei de acțiune era Constanța-Balcic;
- o unitate de rezervă, compusă tot din două canoniere și șase vedete[8].

Se observă că Inspectoratul miza, la momentul iulie 1919, când a fost pregătit acest plan, pe șase canoniere-dragoare, dar, în cele din urmă, Marina Română a putut să achiziționeze numai patru astfel de nave.

Marina americană dorea un vânător de submarine ieftin și robust, dar având corpul din lemn, capabil să atingă viteze de 17-18 noduri. Raza sa de acțiune a fost proiectată să fie de maximum 1.500 de mile, iar armamentul inițial a constat dintr-un tun naval de 76 mm, un altul de 57 mm și trei mitraliere. Experiențele anterioare cu navele anti-submarin au arătat că ele nu se puteau limita la acțiuni în apele de coastă și trebuiau să fie capabile să-și urmărească țintele mult în larg.

În paralel, Șeful Misiunii Navale Franceze în România, căpitanul Belloy de Saint-Liénard, era implicat în diferitele variante de mărire a parcului de nave, la care lucra conducerea Marinei Române pentru a-și întări prezența la Marea Neagră. Ca urmare a diferitelor solicitări ale părții române, care căuta oferte avantajoase pentru a achiziționa nave capabile să contribuie la apărarea coastelor maritime, au apărut mai multe contracte, ocazie cu care au fost vehiculate diferite variante de nave franceze ca posibile achiziții.

Tot în vara anului 1919, spre exemplu, profitând de prezența vedetelor anti-submarin franceze pe Dunăre, Inspectorul Marinei, contraamiralul Constantin Bălescu, a putut vizita una dintre aceste nave, cu numărul de bordaj *„C 27”*[9].

Navele respective erau, de fapt, de fabricație americană, proiectul debutând în 1917, atunci când amenințarea submarinelor germane era la apogeu. Marina americană dorea un vânător de submarine ieftin și robust, dar având corpul din lemn, capabil să atingă viteze de 17-18 noduri. Raza sa de acțiune a fost proiectată să fie de maximum 1.500 de mile, iar armamentul inițial a constat dintr-un tun naval de 76 mm, un altul de 57 mm și trei mitraliere. Experiențele anterioare cu navele anti-submarin au arătat că ele nu se puteau limita la acțiuni în apele de coastă și trebuiau să fie capabile să-și urmărească țintele mult în larg. În aceste condiții, s-a decis să se reducă din viteza maximă și să se crească fiabilitatea mașinilor, oferind, totodată, proiectului mai multă stabilitate[10].

Navele, care au avut indicativul *„S.C.” (Submarine chaser)*, erau foarte rezistente, în ciuda corpului din lemn, și peste 200 astfel

[8] *Ibidem*, f. 70.
[9] *Ibidem*, f. 84.
[10] Norman Friedmann, *U.S. Small Combatants, including PT-boats, sub chasers, and the brown-water navy: an illustrated design history*, Naval Institute Press, Annapolis, 1987, p. 27.

de vedete au traversat Atlanticul în Europa, în timpul războiului. Cel mai mare dezavantaj era, totuși, dimensiunea mică a navei, ceea ce făcea ca viața la bordul ei să fie dificilă. S-au făcut încercări de adaptare pentru misiuni de dragaj pe mare, fără succes însă. Ca dragor de fluviu, ele se descurcau foarte bine[11].

Marina americană a semnat contractul pentru construcția navelor în aprilie 1917, mizând pe 355 de unități până la 1 ianuarie 1918. Cifra a fost aproape atinsă, motiv pentru care s-au putut livra Franței 50 de nave, plus alte 50 la 1 ianuarie 1918. Până la sfârșitul războiului, Statele Unite au construit 441 de vedete, dintre care 133 au fost transferate aliaților lor[12]. În serviciul Marinei americane, navele au fost folosite din Anglia până în insula Corfu, în baze precum Otranto și Gibraltar. Unele vedete au asigurat paza convoaielor care transportau trupe americane în Atlantic, de pe coasta estică a Statelor Unite până în Bermuda, în zone unde acționau submarine germane. În Marea Mediterană, în condiții mai apropiate de cele pe care urmau să le întâlnească în Marea Neagră, vânătoarele de submarine erau grupate câte trei și detectau submarinele inamice prin triangulație, folosind hidrofoanele din dotare. Navele inamice erau, apoi, atacate cu bombe anti-submarin[13].

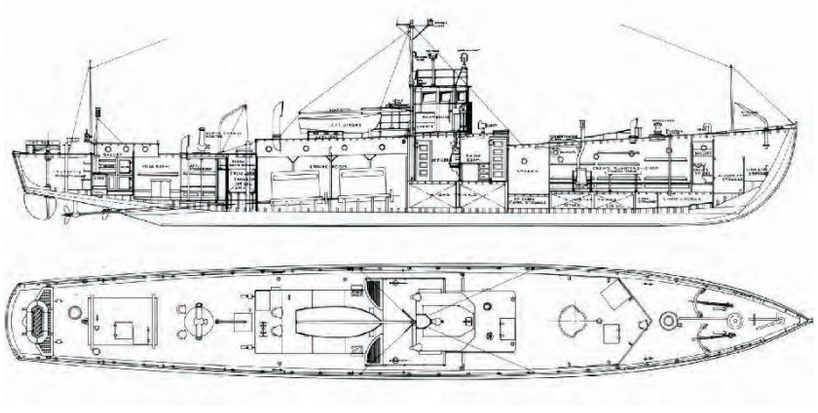

Foto 1: Planul vânătoarelor de submarine americane tip „S.C.”[14]

[11] *Ibidem*, p. 31.
[12] Vezi https://www.subchaser.org/statistics, accesat la 16 aprilie 2020.
[13] Norman Friedmann, *op. cit.*, p. 32.
[14] Sursa foto: Norman Friedmann, *U.S. Small Combatants, including PT-boats, sub chasers, and the brown-water navy: an illustrated design history*, *op. cit.*, p. 28.

Rezultatele analizei Inspectorului Marinei au fost transmise la Ministerul de Război și ele ilustrau anxietatea care caracteriza conducerea Marinei în acea perioadă de tranziție de la starea de război la cea de pace. Lipsa dotărilor moderne reprezenta principala grijă a Inspectoratului, mai ales că la granița răsăriteană se puteau anticipa cu ușurință conflicte generate de tensiunile cu Rusia. Marina Militară trecea printr-o etapă de transformări importante, ca toate structurile Armatei, iar o parte semnificativă din aceste modificări trebuiau să includă dezvoltarea parcului de nave al Diviziei de Mare. Marina traversase anii războiului fără o protecție reală a coastelor maritime, o situație care a fost declarată intolerabilă pe viitor, mai ales că, prin unirea cu Basarabia, România a intrat în posesia unui litoral imens în raport cu forțele de care dispunea.

Lipsa dotărilor moderne reprezenta principala grijă a Inspectoratului, mai ales că la granița răsăriteană se puteau anticipa cu ușurință conflicte generate de tensiunile cu Rusia. Marina Militară trecea printr-o etapă de transformări importante, ca toate structurile Armatei, iar o parte semnificativă din aceste modificări trebuiau să includă dezvoltarea parcului de nave al Diviziei de Mare.

Concluzia inspecției sumare la care a fost supusă vedeta vânătoare de submarine era una pozitivă, Inspectorul Marinei fiind de părere că *„acest vas ne-ar fi de cel mai mare ajutor nu numai în împrejurările actuale, dar și pentru viitor, oricare ar fi organizarea și importanța marinei noastre de mâine”*[15]. Contraamiralul Bălescu făcea referire la procesul de reorganizare prin care trecea Marina Militară după demobilizarea de la finalul războiului, în primul rând prin trecerea accentului dezvoltării de la Divizia de Dunăre la cea de Mare. Totodată, primii doi ani, între 1919 și 1921, au fost marcați de căutări pentru noi formule de organizare, în stare să compenseze lipsa fondurilor, care s-au dovedit insuficiente să acopere chiar și nevoile minimale ale Marinei.

În ceea ce privește Divizia de Mare, aceasta urma să joace rolul de pivot al Marinei, majoritatea înzestrărilor fiind destinate acestei mari unități. Toate analizele forurilor conducătoare ale Marinei au arătat că ea nu poate acționa *„cu o mână legată la spate”*, așa cum s-a întâmplat între anii 1916 și 1918, când, la Marea Neagră, România nu a avut practic nicio navă de luptă, iar bateriile de coastă au fost reduse la limită. Din punctul de vedere al unor analiști militari, absența investițiilor în nave pentru Divizia de Mare a fost o greșeală strategică importantă[16].

[15] AMNR, fond Comandamentul Marinei Militare, dosar 270, f. 84.

[16] Andreea Atanasiu-Croitoru, *„Forța navală maritimă a României între cele două războaie mondiale”*, în *Analele Dobrogei*, serie nouă, nr. X-XIII, 2009-2012, Muzeul de Istorie Națională și Arheologie Constanța, p. 72.

Într-un raport către Ministerul de Război, din data de 4 iulie 1919, Șeful Biroului Marinei din cadrul Marelui Cartier General arăta situația dificilă, aproape disperată, provocată de absența oricăror forțe navale române la Marea Neagră. Pusă în fața perspectivei retragerii comandamentului naval aliat și rămasă singură, fără protecție, România era amenințată de flota bolșevică, formată din trei distrugătoare și două submarine, cu baza la Odessa[17]. Cu toate că aceasta nu își atinsese nivelul de investiții din anii următori, faptul că Marina Română nu avea *„niciun mijloc de a face cel puțin paza coastelor”*, ba chiar mai mult, nu putea împiedica minarea căilor navigabile, însemna că legăturile cu aliații din Occident puteau foarte ușor să fie tăiate. Singura soluție, în accepțiunea Biroului Marinei de la Marele Cartier General, împărtășită și de Comandamentul Marinei, era să se solicite Comandamentului naval aliat patru distrugătoare de 1.000 de tone, 12 vânătoare de submarine și 12 hidroavioane[18]. Raportul considera o soluție de rezervă, amintind de canonierele care s-au cumpărat din Franța[19], care puteau fi puse în serviciu rapid și utilizate ca dragoare și nave de pază. Acest plan, de a solicita cedarea sau măcar împrumutarea de distrugătoare aliate, a fost abandonat, dar canonierele franceze au reprezentat, o perioadă mare de timp, alături de distrugătoarele tip *„M”*, singurele nave de război maritime ale României.

Singura soluție, în accepțiunea Biroului Marinei de la Marele Cartier General, împărtășită și de Comandamentul Marinei, era să se solicite Comandamentului naval aliat patru distrugătoare de 1.000 de tone, 12 vânătoare de submarine și 12 hidroavioane.

Vedetele vânătoare de submarine propuse de Marina Franceză urmau să satisfacă mai multe nevoi ale flotei române la Marea Neagră; mai presus de orice, ele reprezentau promisiunea unor întăriri de care Marina Română avea nevoie disperată, într-o zonă pe care trebuia să o controleze fără să dispună de mijloacele necesare. Deja Inspectoratul Marinei primise informații despre programul de dezvoltare al flotei de submarine sovietice din Marea Neagră. De altfel, în raportul către superiorii lui, contraamiralul Bălescu făcea aluzie la numărul mare de submarine pe care U.R.S.S. le construia în șantierele maritime, menționând *„amenințarea dinspre Rusia”*, un pericol în fața căruia mijloacele anti-submarin ale Marinei Române erau aproape inexistente[20].

[17] AMNR, fond Direcția 5 Marină, dosar 386/1919-1920, f. 703.

[18] *Ibidem*, f. 704.

[19] Andreea Atanasiu-Croitoru, *„Canoniera Locotenent-comandor Eugen Stihi – o călătorie cât un centenar”*, în Corneliu Postu, Petrișor Florea, Cornel Popescu (coord.), *Armata Română și Marea Unire*, studii și articole prezentate la Sesiunea națională de comunicări științifice, Pitești, 26 iulie 2018, Editura Militară, București, 2018, pp. 366-368.

[20] AMNR, fond Comandamentul Marinei Militare, dosar 270, f. 85.

Dat fiind tonajul redus al vedetelor, precum și armamentul limitat, caracteristici care făceau să scadă eficacitatea lor în apărarea unor coaste extinse, conducerea Marinei a concluzionat că se impunea achiziționarea unui număr considerabil de astfel de nave pentru a se putea acționa în grupuri cât mai mari. Dotarea cu mijloace de detecție a submarinelor era slabă, astfel că, în scopul acoperirii unor suprafețe extinse, Inspectoratul își propunea să înființeze trei escadrile a câte șase nave. La rândul lor, escadrilele urmau să fie împărțite în grupuri de câte trei vedete și repartizate în cele trei puncte importante din Dobrogea: Constanța, Sulina și Gura Chiliei[21]. Cu încă șase nave de rezervă, totalul pe care Inspectoratul dorea să îl comande se ridica la 24 de unități.

Dotarea cu mijloace de detecție a submarinelor era slabă, astfel că, în scopul acoperirii unor suprafețe extinse, Inspectoratul își propunea să înființeze trei escadrile a câte șase nave. La rândul lor, escadrilele urmau să fie împărțite în grupuri de câte trei vedete și repartizate în cele trei puncte importante din Dobrogea: Constanța, Sulina și Gura Chiliei.

Din cauza lipsei de material flotant la Marea Neagră, misiunile pe care aceste nave le-ar fi îndeplinit nu s-ar fi limitat la lupta anti-submarin. Marina trebuia să apere un litoral maritim cu o întindere considerabilă și era obligată să apeleze la bastimente flexibile, atribuind deci vedetelor și misiuni de patrulare, de respingere a infiltrărilor agenților străini, mergând chiar până la posibilitatea trimiterii lor în *„incursiuni de informații în apele inamice”*, acțiuni în care viteza relativ mare a vânătoarelor de submarine se putea dovedi prețioasă[22].

Alte sarcini pe care navele franceze de origine americană le-ar fi putut avea în serviciul Marinei Române includeau transporturi de trupe și materiale de-a lungul coastei Mării Negre, deși Inspectorul Marinei recunoștea că dimensiunea redusă a vedetelor limita capacitatea acestora de a îndeplini astfel de sarcini. Se avea în vedere și rolul de comunicație între forțele terestre și cele navale, dar Inspectoratul era mai degrabă interesat de utilizarea vedetelor pe timp de pace, când ele ar fi putut fi *„foarte prețioase pentru poliția navigației și stârpirea contrabandei”*[23]. În concluzie, recomandarea conducerii Marinei Române era de a se obține 24 de vedete anti-submarin din Franța.

Seria intervențiilor pe lângă Ministerul de Război pentru soluționarea problemelor cauzate de lipsa navelor în sectorul maritim a continuat cu un apel al Direcției Marinei, în care se trecea în revistă situația generală a câmpurilor de mine amplasate în zona porturilor române.

[21] *Ibidem*.
[22] *Ibidem*.
[23] *Ibidem*, f. 86.

Chestiunea era una foarte serioasă și a fost agravată de retragerea unităților de dragoare Aliate, care reușiseră să reducă pericolul pe care minele neexplodate îl reprezentau pentru navigația comercială. Marina Română nu dispunea decât de trei nave, improvizate pentru misiuni de dragaj: *„Basarab”*[24], *„Rareș”* și *„Ungheni”*, care puteau acționa însă doar pe Dunăre. La Mare, deși responsabilitatea înlăturării minelor cădea în sarcina statului român, nu au existat posibilități de a întreprinde ceva concret în acest sens[25].

ALTE TIPURI DE NAVE OFERITE MARINEI ROMÂNE

În aceste condiții, contactele cu Misiunea Navală Franceză au continuat. În paralel cu negocierile pentru achiziționarea canonierelor tip *„Frippone”* (care au dus la cumpărarea a doar patru unități, nu șase, așa cum dorea partea franceză)[26], francezii au oferit alte tipuri de nave, în principal vedete rapide, adaptate pentru dragaj. În august 1919, Franța a început să-și retragă navele de pe coasta de vest a Mării Negre și de pe Dunăre, așteptând ca Guvernul României să grăbească negocierile și să trimită o ofertă pentru ele[27]. Conducerea Marinei Române era la curent cu această stare a lucrurilor, deoarece reprezentanții Misiunii Navale Franceze au discutat despre convingerea lor că, dată fiind „*lipsa completă de apărare a litoralului”*, România va apela la navele franceze pentru a *„crea sâmburele forței navale care, prin dezvoltarea viitoare, să asigure hegemonia pavilionului nostru în Marea Neagră”*, după cum se exprima căpitan-comandorul Ioan Bălănescu, șeful Direcției Marinei[28]. Desigur, Marina Română nu putea să spere și nici nu își propunea să ajungă la o poziție hegemonică în Marea Neagră, dar exprimarea, evident preluată de la ofițerii francezi, relevă o strategie de marketing la care apela misiunea navală, care miza pe temerile României față de superioritatea navală evidentă a Rusiei.

În paralel cu negocierile pentru achiziționarea canonierelor tip „Frippone”, francezii au oferit alte tipuri de nave, în principal vedete rapide, adaptate pentru dragaj. În august 1919, Franța a început să-și retragă navele de pe coasta de vest a Mării Negre și de pe Dunăre, așteptând ca Guvernul României să grăbească negocierile și să trimită o ofertă pentru ele.

Cu toate acestea, Misiunea Navală Franceză a oferit alte alternative în ceea ce privește dezvoltarea parcului de nave, mai ales dragoarele de care avea nevoie Marina Română. Dintre navele pe care Franța dorea

[24] Navă cu zbaturi, construită în anul 1893 la Șantierul Naval din Linz. În timpul războiului a făcut parte din Grupul Port Mine-Dragă Mine al Apărărilor sub Apă. Vezi Georgeta Borandă, *op. cit*., p. 139.
[25] AMNR, fond Comandamentul Marinei Militare, dosar 270, f. 69.
[26] Pentru patru milioane de franci. Vezi Patrick Boureille, *op. cit*., p. 3.
[27] AMNR, fond Comandamentul Marinei Militare, dosar 270, f. 87.
[28] *Ibidem*.

să le vândă României se disting două dragoare, special concepute pentru acest tip de misiuni, și nu nave adaptate: *„Gres”* și *„Marbre”*. Ele erau din clasa *„Granit”* și au fost lansate la apă în anul 1918, deci erau de construcție recentă. Caracteristicile navelor erau: deplasament 360 t, lungime 57 m, lățime 8 m, pescaj 2 m, armament – un tun de 120 mm și unul de 75 mm[29]. Dragoarele au fost și ele vizitate de oficiali ai Marinei Române la Galați, cu rezultate pozitive, ele făcând parte din grupurile de nave franceze care acționau pe Dunăre și în Marea Neagră.

Alături de aceste dragoare, Marina Franceză mai dorea să renunțe și la două nave din clasa *„Herse”*, de model mai vechi, din 1913/1914, anume *„Rateau”* și *„Coquelicot”*, ceva mai mici decât cele din clasa *„Granit”*. Cu un deplasament de 255 t și dotate cu 2 piese de 47 mm, ele reprezentau o alternativă mai ieftină. Tot la capitolul nave cu tonaj redus, căpitanul O´Neill a sugerat ca Marina Română să achiziționeze canoniere de tip *„Decidée”*, din clasa *„Surprise”*. Aceste canoniere au fost folosite în mare parte în acțiunile navale din colonii. Nava propusă României a petrecut perioada 1914-1917 în Indochina, iar între anii 1917 și 1918 a apărat coastele Siriei[30].

Căpitanul O´Neill a sugerat ca Marina Română să achiziționeze canoniere de tip „Decidée”, din clasa „Surprise”. Aceste canoniere au fost folosite în mare parte în acțiunile navale din colonii. Nava propusă României a petrecut perioada 1914-1917 în Indochina, iar între anii 1917 și 1918 a apărat coastele Siriei.

Foto 2: Canoniera „Decidée”[31]

[29] *Ibidem*, f. 91.
[30] Robert Gardiner (coord.), *Conway´s all the World´s Fighting Ships 1906-1921*, Conway Maritime Press, Londra, 1985, p. 196.
[31] Sursa foto: http://servimg.com/image_preview.php?i=57&u=11930999#, accesat la 14 martie 2020.

Armamentul canonierei era considerabil: 2 tunuri de 100 mm, 4 de 65 mm și un tun de 37 mm, în vreme ce deplasamentul era de 630 de tone, iar echipajul se ridica la 100 de oameni[32].

Cea mai spectaculoasă idee a căpitanului O´Neill a fost însă ca Marina Română să preia, contra unui cost redus, crucișătorul protejat *„Jurien de la Gravière”*, lansat în 1899 și finalizat în 1903[33]. Un proiect nereușit al Marinei Franceze, crucișătorul era considerat prea slab înarmat, cu doar opt piese de 164 mm, 10 x 47 mm, 6 x 37 mm și două tuburi lans-torpile de 450 mm[34]. Artileria principală era dispusă câte o piesă în turele blindate la prova și la pupa, iar celelalte șase, câte trei în cazemate, în fiecare bord. Problemele erau limitate la artileria considerată insuficientă pentru o navă de 5.600 t; nava era relativ înceată, atingând cu dificultate 21 de noduri, față de 23, conform proiectului. Compartimentul motoarelor era înghesuit, iar nava, în general, nu ținea bine marea. Nu este nicio surpriză deci că, la fel ca celelalte tentative de a oferi bastimente României, nici această idee a Misiunii Navale Franceze nu s-a concretizat.

Cea mai spectaculoasă idee a căpitanului O´Neill a fost ca Marina Română să preia, contra unui cost redus, crucișătorul protejat „Jurien de la Gravière”, lansat în 1899 și finalizat în 1903. Un proiect nereușit al Marinei Franceze, crucișătorul era considerat prea slab înarmat, cu doar opt piese de 164 mm, 10 x 47 mm, 6 x 37 mm și două tuburi lans-torpile de 450 mm.

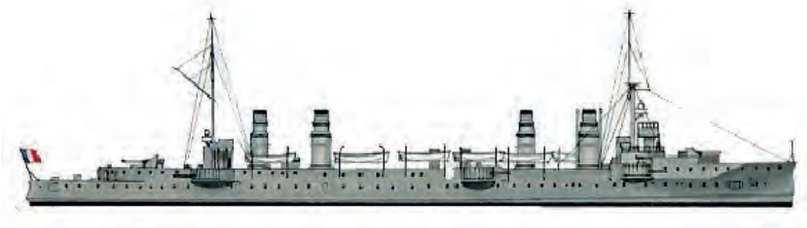

Foto 3: Crucișătorul „Jurien de la Gravière”[35]

CONCLUZII

După încheierea Primului Război Mondial, Franța s-a străduit să întrețină relații bune cu Marina Română, în vederea obținerii de avantaje strategice în zona de est a Europei, dar mai ales la Marea Neagră. Situația volatilă din Rusia i-a determinat pe conducătorii francezi să păstreze și chiar să extindă misiunea navală în România,

[32] Vezi http://www.navypedia.org/ships/france/fr_of_surprise.htm, accesat la16 aprilie 2020.
[33] Patrick Boureille, *op. cit.*, p. 3.
[34] Fred T. Jane (coord.), *Jane´s Fighting Ships 1905/1906, A reprint of the 1905/1906 Edition of Fighting Ships*, Arco Publishing Company, New York, 1970, p. 123.
[35] Sursa foto: https://www.naval-encyclopedia.com/ww1/France/jurien-de-la-graviere/, accesat la 16 aprilie 2020.

luând în calcul posibilele acțiuni militare de sprijinire a albgardiștilor. Concomitent, misiunea s-a confruntat cu rivalitatea neașteptată din partea Marii Britanii, care a trimis propriii specialiști pe lângă Marina Română.

Deși a beneficiat de experiența acumulată în timpul războiului și de relațiile create în cei trei ani de conflict armat împreună cu aliații români, Misiunea Navală Franceză s-a confruntat cu dificultăți în a-și îndeplini scopurile de consolidare a poziției franceze în cadrul Inspectoratului Marinei de la București. Ezitarea părții române, fricțiunile din timpul războiului, îndreptarea ofițerilor români către alți furnizori de armament naval, toate au contribuit la o experiență mai degrabă frustrantă pentru reprezentanții Misiunii Navale Franceze.

Cu toate acestea, ofițerii de marină francezi au depus eforturi semnificative în încercarea de a oferi micii Marine a României o serie de nave, unele ușor demodate, altele mai noi, cu care să se formeze nucleul unei forțe la Marea Neagră.

BIBLIOGRAFIE:

1. ***, Arhivele Militare Naționale Române, fond Comandamentul Marinei Militare.
2. Patrick Boureille, *„Les relations navales franco-roumaines (1919-1928): les illusions perdues”*, în *Revue historique des armées*, 244/2006.
3. Andreea Atanasiu-Croitoru, *„Canoniera Locotenent-comandor Eugen Stihi – o călătorie cât un centenar”*, în Corneliu Postu, Petrișor Florea, Cornel Popescu (coord.), *Armata Română și Marea Unire*, studii și articole prezentate la Sesiunea Națională de comunicări științifice, Pitești, 26 iulie 2018, Editura Militară, București, 2018.
4. Andreea Atanasiu-Croitoru, *„Forța navală maritimă a României între cele două războaie mondiale”*, în *Analele Dobrogei*, serie nouă, nr. X-XIII, 2009-2012, Muzeul de Istorie Națională și Arheologie Constanța.
5. Norman Friedmann, *U.S. Small Combatants, including PT-boats, sub chasers, and the brown-water navy: an illustrated design history*, Naval Institute Press, Annapolis, 1987.
6. Robert Gardiner (coord.), *Conway´s all the World´s Fighting Ships 1906-1921*, Conway Maritime Press, Londra, 1985.
7. Fred T. Jane (coord.), *Jane´s Fighting Ships 1905/1906*, *A reprint of the 1905/1906 Edition of Fighting Ships*, Arco Publishing Company, New York, 1970.

8. Ion Ionescu, Georgeta Borandă, Marian Moșneagu, *Noi contribuții la istoria Marinei Militare Române*, Editura Muntenia&Leda, Constanța, 2001.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

WEBOGRAFIE:

1. www.naval-encyclopedia.com.
2. www.subchaser.org
3. www.navypedia.org.

Președintele României

Dorind a răsplăti meritele

revistei

„Gândirea militară românească"

cu ocazia împlinirii a 140 de ani de existență, pentru rezultatele de excepție obținute în sistematizarea teoretică a gândirii militare naționale și pentru contribuția fundamentală adusă la edificarea concepțiilor strategice care au susținut transformarea profundă a Armatei României la nivelul standardelor operaționale ale Alianței Nord-Atlantice,

Conferă Ordinul „Meritul Cultural"

în gradul de Cavaler categoria F „Promovarea culturii"

Dat în București la 24-08-2004

Președintele României

Ministrul Culturii și Cultelor — Ion Iliescu — Cancelarul Ordinelor

Decret nr. 646 Din 24-08-2004

Brevet MC/ nr. Cav/ F/ 2 Nr. crt. 76755

Ordinul *„Meritul Cultural"* în grad de *„Cavaler"*, categoria F – *„Promovarea culturii"* (Decretul Prezidențial nr. 646 din 24.08.2004)

Președintele României

Dorind a răsplăti meritele

Revistei

Gândirea Militară Românească

în semn de recunoaștere a contribuției fundamentale la edificarea conceptelor strategice care au susținut construcția militară națională și transformarea profundă a Armatei României,

Conferă

Ordinul „Meritul Cultural" în grad de „Ofițer", Categoria F - „Promovarea culturii".

Președintele României

Ministrul — Traian Băsescu — Cancelarul Ordinelor

Decret nr. 483 din 30.06.2014

Brevet MC Of/ Inv. IV Nr. crt. 100229

Ordinul *„Meritul Cultural"* în grad de *„Ofițer"*, categoria F – *„Promovarea culturii"* (Decretul Prezidențial nr. 483 din 30.06.2014)

gmr.mapn.ro
facebook.com/gmr.mapn.ro