

ISSN 2537-1363
ISSN-L 2537-1363

REVISTA ACADEMIEI DE ȘTIINȚE ALE SECURITĂȚII NAȚIONALE ANUL V, 2020 NR.1 (08)

RASSN



Revista Academiei de Științe ale Securității Naționale

NR. 1/2020

ȘTIINȚE MILITARE

INFORMAȚII ȘI SECURITATE NAȚIONALĂ

ORDINE PUBLICĂ

CONSILIUL ȘTIINȚIFIC

Prof.univ.dr. **Pricopie Remus** – președinte

Prof.dipl.eng, **Pavel NEČAS**, PhD, MBA, dr.h.c., Faculty of Political Science and International Relations, University of Matej Bel, Slovakia;

Prof. assit. **Jan RAJCHEL** – University of Natural Sciences and Humanities, Polonia;

Prof. **Miroslav KELEMEN**, Tehnical University of Košice, Slovakia;

Prof.univ.dr. **George MAIOR**

Prof.univ.dr. **Vasile DÎNCU**

Prof.univ.dr. **Gabriel-Florin MOISESCU**

Prof. univ. dr. **Adrian CURAJ**

Prof. univ. dr. **Gheorghe TOMA**

Prof. univ. dr. **Teodor FRUNZETI**

Prof. univ. dr. **Ion MITULETU**

Prof. univ. dr. **Cristian POPESCU**

Prof. univ. dr. **Gheorghe BOARU**

Prof. univ. dr. **Gheorghe BĂRBULESCU**

Prof. univ. dr. **Sorin CÎMPEANU**

Prof. univ. dr. **Viorel BUȚA**

Prof. univ. dr. **George ȚICAL**

Prof. univ. dr. **Adrian IACOB**

Prof.univ.dr. **Costel DUMITRESCU**

Prof.univ.dr. **Țuțu PIȘLEAG**

Conf.univ.dr. **Diana Elena ȚUȚUIANU**

Conf. univ. dr. **Florin Neacșa**

Dr. **Petru TĂGOREAN**

Colegiu de redacție

Redactor-șef - Prof.univ.dr. **Gheorghe BOARU**

Redactor-șef adjunct - Prof.univ.dr. **George-Marius ȚICAL**

Membri

Prof.univ.dr. **Ion Mitulețu**

Prof.univ.dr. **Țuțu Pișleag**

Conf.univ.dr. **Diana-Elena Țuțuianu**

Nelușa Solbă

Secretar redacție - Conf.univ.dr. **Florin Neacșa**

*Revista
Academiei de Științe
ale Securității Naționale*

*Editată de Academia de Științe ale Securității
Naționale*



Revistă indexată în baze de date internaționale
(SRN, ResearchBib, Scipio)

ISSN 2537-1363
ISSN-L 2537-1363



CUPRINS

EDITORIAL	5
<i>Gl.bg.(rtr.) prof.univ.dr. Gheorghe TOMA</i>	
CORONACRIZA – PROVOCĂRI PENTRU VIITOR	8
<i>Gl. mr. (r) prof.univ.dr. Gabriel-Florin MOISESCU</i>	
PANDAMIA DE CORONAVIRUS ȘI SECURITATEA CIBERNETICĂ.....	19
<i>Col.(rtr.) prof.univ.dr. Gheorghe BOARU</i>	
LIDER ȘI LEADERSHIP MILITAR	44
<i>Col.(r.) prof.univ.dr. Ion MITULEȚU</i>	
SCHIMBĂRI ALE PARADIGMEI STRATEGICE GLOBALE ÎN URMA BREXITULUI.....	62
<i>Prof. univ. dr. Costel DUMITRESCU</i>	
PANDEMIA DE CORONAVIRUS – RISC SAU AMENINȚARE LA ADRESA SECURITĂȚII NAȚIONALE, REGIONALE ȘI GLOBALE?	74
<i>Gl. mr. (r) prof.univ.dr. Gabriel-Florin MOISESCU</i> <i>Lt. col. lector univ.dr. Bogdan-Cezar CHIOSEAUA</i>	
DESPRE SECURITATEA NAȚIONALĂ ÎN NOUL CONTEXT MONDIAL.....	83
<i>Drd. Ion-Sorin MOLDOVAN</i>	



DE LA ATRIBUȚIE LA MISIUNE.
OPERAȚIONALIZAREA ATRIBUȚIILOR JANDARMERIEI (I)..... 91
Prof.univ.dr. Țuțu PIȘLEAG

BREXIT – ȘI VIITORUL POLITICII EXTERNE
ȘI DE SECURITATE COMUNĂ A UNIUNII EUROPENE 107
Lt. col. lector univ.dr. Bogdan-Cezar CHIOSEAUA

INFORMAȚIA PENTRU APĂRARE ÎN CONTEXTUL
CONFRUNTĂRII INFORMAȚIONALE117
Drd. Ion-Sorin MOLDOVAN



EDITORIAL

NOI VREMURI / NOI ACTORI (I)

Planeta noastră este un „*sat planetar*”, cu economii și interese din ce în ce mai legate între ele. Războaiele din diferite zone ale lumii, în special din Orientul Mijlociu, problemele interne, lupta împotriva criminalității, controlul granițelor și pandemiile, toate sunt situații greu de gestionat, necesită evaluări continue și atente din partea instituțiilor cu rol în asigurarea apărării și securității naționale.

În toate aceste probleme (crize punctuale) într-un fel sau altul a fost și va fi implicată și armata. Apărarea și securitatea națională se abordează astăzi din perspectivă sistemică. Securitatea este un concept multidimensional (politic, diplomatic, militar, economic, științific, informațional, cultural, social ș.a.), omniprezent și omnidirecțional, fiecare domeniu luându-și măsuri de promovare a intereselor specifice fiecăruia.

Putem afirma faptul că politica de securitate și apărare națională, promovată de factorul politic, trebuie să țină cont de faptul că legăturile vitale între sectoarele (dimensiunile) securității și apărării naționale determină funcționarea lor optimă. Dar acest lucru trebuie bine înțeles de toți factorii de decizie, să nu ne aducem aminte numai în situații limită (cum se întâmplă și astăzi). Echilibrul sistemului și funcționarea optimă a acestuia este fundamentată teoretic și asigurată practic prin măsuri pentru promovarea intereselor naționale fundamentale și apărarea lor împotriva oricăror agresiuni, amenințări, riscuri și vulnerabilități.



Prezentul pe care specialiști îl percep tinde spre un nou sistem internațional, o altă așezare a statelor în structura mondială de putere, crucială pentru fizionomia și pentru viitorul omenirii. Înțelegerea și definirea corectă a riscurilor, amenințărilor, pericolelor și vulnerabilităților generează securitatea națională extinsă.

Amenințările globale nu s-au micșorat, ci s-au modificat. Pericolul unui război a fost înlocuit, cel puțin în Europa, cu o mulțime de factori de risc, a căror importanță variază de la o regiune la alta. Și totuși, instabilitatea s-a extins. Conflictele au devenit din ce în ce mai explozive, se evidențiază sub o paletă largă de crize cu caracter social, etnic, religios, economic, și chiar rivalității interstatale și intrastatale, la care se adaugă pandemia la nivel mondial.

În condițiile în care conflictele și crizele sunt de genul celor amintite, planificatorii militari trebuie să adapteze și să reprojeteze structurile militare în mod corespunzător și, totodată, să găsească tactici și strategii prin care să contracareze noua gamă de amenințări. Toți sunt conștienți că, în prezent, are loc o extensie considerabilă a conceptului, care să exprime interacțiunea factorilor politici, economici, militari, tehnologici, culturali, juridici ș.a.

Construcția destinului României, Europei și lumii în general, va depinde de aptitudinile și capacitățile polilor de putere, actuali și viitori, cu maximă eficiență în problemele globale, dar și de capacitatea de armonizare a intereselor pe diferite spații. Apreciem și faptul că o eliminare/diminuare a rolului de pol de putere va dăruia întreaga arhitectură de securitate, indiferent cât de favorabil sau generos ar fi scenariul geopolitic, geostrategic și geoeconomic pentru care s-a proiectat.

Analizele geopolitice la nivel global arată faptul că, la intervale periodice (nu mai mult de o jumătate de secol), s-a desfășurat și se desfășoară un proces de regândire și redefinire a relațiilor internaționale. Principalele rezultate ar trebui să fie reducerea probabilităților de confruntare, realizarea unui climat de parteneriat și colaborare, toate având



ca obiectiv modelarea arhitecturii de securitate. Dar de fiecare dată s-a constatat menținerea unor riscuri și amenințări la adresa statelor, inclusiv a României, a unor factori de risc nemilitari, asimetrici, asincroni și neconvenționali, cu un potențial destul de mare de pericol pentru securitatea globală, regională, zonală și locală.

Ca urmare, realitatea contemporană impune factorilor politici să dispună permanent de forțe și mijloace pregătite, profesioniste, disponibile, adaptate realităților pentru gestionarea crizelor. *Forțele Armate nu sunt nici mai bune nici mai rele decât factorii politici care le stabilesc sarcinile și le fixează misiunile.*

Avem nevoie de o voință politică și o viziune pe termen lung, de coeziune națională și pragmatism. Este nevoie să prevedem din timp crizele de orice natură, să avem specialiști și forțe profesionale în combaterea crizelor interne, cu scopul de a asigura securitatea și apărarea națională extinsă. Pornind de la această realitate contemporană, accentuăm ca necesară studierea și cunoașterea detaliată a fenomenului crizelor, a metodelor de acțiune destinate gestionării și combaterii acestora.

Gl.bg.(rtr.) prof.univ.dr.Gheorghe Toma



CORONACRIZA – PROVOCĂRI PENTRU VIITOR!

CORONACRISIS – CHALLENGES FOR THE FUTURE

Gl. mr. (r.) prof.univ.dr. Gabriel-Florin MOISESCU
Membru titular al Academiei de Științe ale Securității Naționale,
E-mail: moisescu.gbrl@gmail.com

Rezumat: Pandemia de coronavirus este considerată de către specialiști un eveniment de tip Lebăda Albă și/sau Rinocerul Gri. Prin impactul său major, acesta a „paralizat” autoritățile statelor din întreaga lume o perioadă de timp, fapt ce a determinat ca acestea să acționeze „fiecare pentru el”.

Ulterior, au fost puse în mișcare mecanismele de colaborare și cooperare ale Uniunii Europene, Alianței Nord Atlantice, parteneriatelor etc.

Funcționarea autonomă a statelor în perioada aceasta este propunerea noastră pentru ca nici un stat, în situații de criză, să nu devină o povară pentru celelalte.

Cuvinte cheie: Pandemie, tip de eveniment, autoritățile statului, perioada, funcționare autonomă, industrie națională de securitate.

Abstract: Coronavirus pandemic is considered by specialists a White Swan and/or a Gray Rhino. Through its major impact, it has „paralyzed” the authorities of all the states in the world for a certain period which created the need that each of these should act „on its own and for itself”.

Subsequently, collaboration and cooperation mechanisms started to be put into motion, such as those of the European Union, the North Atlantic Treaty Organization, partnerships etc.

The autonomous functioning of states in this period is our proposition so as no state, in crisis circumstances, might become a burden to the others.

Keywords: pandemic, type of event, state authorities, period, autonomous functioning, national security industry.

În aceste zile, când iei contact cu lumea reală, trăiești cu impresia că te-ai întors în timp. Lumea parcă stă pe loc. Numai tehnologia ne readuce în prezent și ne amintește că suntem în secolul al XXI-lea. Zici că suntem actorii unui film de science-fiction: oameni cu măști și mănuși de protecție care stau la distanță unii de alții pentru a-și procura bunuri de strictă



necesitate și medicamente, echipaje de poliție și jandarmi precum și ale Ministerului Apărării Naționale la intersecțiile importante, ambulante etc. Există o tensiune pe care o resimți cumva în aer, creată de acest virus ucigaș, COVID-19, care a apărut din neant și va dispărea probabil în același fel.

Pe canalele Veneției, altădată supraaglomerate de gondole pline cu turiști, delfinii se joacă în voie într-o apă din ce în ce mai curată, iar lebedele „răsufală ușurate” de parc-ar spune: „În sfârșit e liniște în habitatul nostru!”.

Natura „respiră” și își continuă „viața ei”, avertizându-ne însă că în interacțiunea dintre ființa umană și „ea” trebuie să existe un echilibru, că a acorda mediului importanța cuvenită trebuie să fie o prioritate absolută a omenirii.

Așa arată lumea în care trăim noi astăzi!

În ce tip de eveniment se poate încadra pandemia? De ce s-a ajuns aici? Unde suntem acum? Cum am putea depăși aceste vremuri? Ce ar trebui să facem pentru ca așa ceva să nu se mai întâmple? sunt întrebări la care ne propunem să oferim răspunsuri în actualul demers.

Pandemia de coronavirus a fost considerată inițial ca eveniment de tip Lebăda Neagră, care conform autorului teoriei, Nassim Nicholas Taleb are trei atribute¹: caz izolat; cu impact major; predictibilitate retrospectivă („...”, natura umană ne-a făcut să născocim explicații pentru apariția sa, după ce acest lucru s-a întâmplat, făcându-l explicabil și predictibil”²).

Exemple³ de Lebede Negre sunt următoarele: ascensiunea lui Hitler și Al Doilea Război Mondial, dispariția precipitată a blocului sovietic, răspândirea internetului, criza financiară din 1987, atacul terorist din 11 septembrie 2001.

Însuși autorul teoriei neagă faptul că pandemia de coronavirus ar fi fost un eveniment de tip Lebăda Neagră și afirmă că acum este o Lebăda Albă⁴ întrucât aceasta ar fi putut fi prevenită⁵.

¹ Nassim Nicholas Taleb, *LEBĂDA NEAGRĂ*, impactul foarte puțin probabil, Editura Curtea Veche, București, 2009, pp. 14-15.

² *Ibidem*, p.14.

³ *Ibidem*.

⁴ N.A. Lebăda Albă este un eveniment rar, neprevizibil și cu efecte pozitive; Lebăda Gri sunt evenimente a căror efecte pot fi prevăzute până la un anumit punct dar a căror apariție este improbabilă; conform [<https://descopera.org> >teoria-l...], accesat la 02.04.2020.



Din punctul de vedere al analistei americane Michele Wueker, metafora care i s-ar potrivi mai bine acestui tip de eveniment ar fi Rinocerul Gri, care corespunde unei amenințări care putea să aibă loc cu o probabilitate destul de mare și cu un foarte mare impact, dar care a fost însă neglijată⁶.

Spre deosebire de Taleb, Nouriel Roubini, cel care a prezis criza din 2008, nu consideră crizele financiare ca fiind Lebede Negre, ci le aseamănă uraganelor, care sunt rezultatul predictibil al unui cumul de vulnerabilități economice și financiare și greșeli politice. Potrivit acestuia, pandemia ar putea arunca economia globală într-o criză mai mare decât cea din 1929-1933⁷.

Urmare a celor mai sus prezentate, considerăm că pandemiei, ca tip de eveniment, i se pot atribui atât metafora de Lebădă Albă cât și cea de Rinocerul Gri, întrucât aceasta prezintă caracteristicile identificate de către autorii lor.

Ne alăturăm, în același timp, punctului de vedere al analistei Michele Wueker, care aprecia faptul că, a face ceva pentru a îndrepta lucrurile pe care le vedem în fața noastră („a acorda atenție Rinocerului Cenușiu”) ar însemna o utilizare mult mai bună a timpului decât a localiza Lebedele Negre⁸.

De ce s-a ajuns aici?

În primul rând, din cauza unei profunde conectivități care, alături de atenția insuficientă acordată mediului, reprezintă o altă problemă cu care azi lumea se confruntă⁹.

Apoi, sindromul încrederii, în sensul că mie/nouă nu ni se poate întâmpla așa ceva, a determinat o lipsă de asumare, în timp oportun, de responsabilități și implicare a guvernelor din întreaga lume care, la rândul ei

⁵ Nassim Nicholas Taleb, interviu pentru Bloomberg, conform [<https://romania.europalibera.org>>d...], accesat la 02.04.2020.

⁶ N.A. Rinocerul Gri este un animal masiv de două tone, cu cornul orientat către tine, călcând pământul și pregătindu-se de atac-și, cel mai important, oferindu-ți șansa de a acționa (Michele Wueker în articolul pentru Washington Post. Metafora a fost folosită pentru criza financiară din Grecia din anul 2012).

⁷ *Ibidem*.

⁸ [<https://revistasinteza.ro>>profe...], accesat la 02.04.2020.

⁹ [<https://romania.europalibera.org>>d...], accesat la 02.04.2020.



a condus la amânarea luării unor decizii privind limitarea extinderii și oprirea pandemiei¹⁰.

În același timp nu s-a ținut cont, în etapa inițială, de efectele acesteia în plan economic, de faptul că nu se poate separa combaterea pandemiei de problemele economice, întrucât acestea nu sunt două universuri paralele¹¹.

De asemenea, se evidențiază că guvernele, companiile și corporațiile nu au nici o scuză pentru a nu se fi pregătit pentru un asemenea tip de eveniment¹².

Potrivit specialiștilor¹³, informații au existat încă din anul 2019, când epidemiologii și experții în sănătate avertizau că lumea este „răscoaptă” pentru următoarele pandemii și că traficul global, schimbările climatice și rezistența la antibiotice a făcut omenirea mai vulnerabilă.

În același an, Departamentul Serviciilor Naționale de Informații din SUA făcea un apel global prin care avertiza că SUA și întreaga lume vor rămâne vulnerabile în fața următoarei pandemii sau a unei boli contagioase, cu efecte grave asupra economiei mondiale și a resurselor internaționale.

În același sens, unii analiști¹⁴ sunt de părere că pandemia ar fi putut fi prevenită dacă în data de 26 ianuarie, când s-a lansat anunțul că trebuie oprită din fașă, s-ar fi acționat extrem de rapid.

Nimeni nu-și poate permite să caute vinovații în aceste vremuri, însă, suntem de părere că greșelile făcute în ceea ce privește combaterea pandemiei trebuie înlăturare și noi, omenirea, trebuie să strângem rândurile pentru a învinge împreună acest virus insidios și ucigător.

Unde suntem acum?

Acum ne aflăm în situația¹⁵ în care aproape jumătate de planetă se află izolată la domiciliu, cu un număr al infectărilor care se apropie de un milion și cu un bilanț al deceselor de 40.000, din care jumătate dintre ele în Italia și Spania. Avem de-a face cu cea mai mare criză umanitară după cel

¹⁰ [<https://romania.europalibera.org>>d...], accesat la 02.04.2020.

¹¹ [<https://revistasinteza.ro>>profe...], accesat la 02.04.2020.

¹² *Ibidem*.

¹³ Michele Wueker, [<https://revistasinteza.ro>>profe...], accesat la 02.04.2020.

¹⁴ Nassim Nicholas Taleb, [<https://romania.europalibera.org>>d...], accesat la 02.04.2020.

¹⁵ Secretarul general al Organizației Națiunilor Unite, Antonio Guterres, conform [<http://romania.europalibera.org>], accesat la 02.04.2020.



de-al Doilea Război Mondial care va conduce, probabil, la o recesiune ce nu poate fi comparată cu nimic din trecutul recent¹⁶.

Uniunea Europeană, „inertă” pentru o perioadă de timp, ca și celelalte organizații mondiale și regionale, are în vedere un plan de redresare comună¹⁷ care, din nefericire, a produs puternice diviziuni între statele din Sud și cele din Nord (Italia și Spania au propus o împărțire a instrumentelor de datorie – „coronabonduri” – însă Germania, alături de alte state din Nord, a respins această idee de asumare a datoriilor provocate de pandemie).

NATO s-a reunit (târziu din punctul nostru de vedere, tot după o perioadă de timp) pentru prima dată printr-o legătură video securizată (02.04.2020) și, prin secretarul său general, a declarat că sprijină prin forțele sale armate națiunile în lupta lor pentru stoparea crizei de coronavirus (s-a răspuns solicitărilor Italiei și Spaniei prin faptul că a mediat ca Spania să primească rezerve medicale din partea Republicii Cehia, iar Turcia să trimită un avion cu materiale și echipamentele medicale în Spania și Italia)¹⁸.

De asemenea, prin vocea unui înalt oficial¹⁹ al său, consideră actuala criză o amenințare la adresa securității globale, un risc de securitate diferit dar nu mai puțin periculos și insidios, precum și faptul că, mobilizarea resurselor de securitate, în special cele economice, reprezintă o lecție în privința viitoarelor investiții în sectorul de securitate²⁰.

În ceea ce privește țara noastră, în timp ce autoritățile chineze se luptau cu virusul, clasa noastră politică se lupta pentru putere, gândind probabil, potrivit sindromului mai sus amintit, că virusul este undeva departe și nouă nu ni se poate întâmpla nimic.

Ulterior, când Organizația Mondială a Sănătății (OMS) a declarat pandemia, am început să dăm semne că ne-am trezit (tot după o perioadă de timp), s-a renunțat la alegerile anticipate și avem un guvern cu drepturi depline.

¹⁶ Secretarul general al Organizației Națiunilor Unite, Antonio Guterres, conform [<http://romania.europalibera.org>], accesat la 02.04.2020.

¹⁷ Secretarul general al Organizației Națiunilor Unite, Antonio Guterres, conform [<http://romania.europalibera.org>], accesat la 02.04.2020.

¹⁸ [evz.ro], accesat la 02.04.2020.

¹⁹ N.A. Este vorba despre Mircea Geoană, secretarul general adjunct al N.A.T.O.; [www.rador.ro > N.A.T.O.], accesat la 02.04.2020.

²⁰ *Ibidem*.



În momentul în care scriem aceste rânduri, România se află în Stare de Urgență, decret semnat de Președintele României la 16.03.2020, în urma Hotărârii Consiliului Suprem de Apărare a Țării (CSAT) nr.30/2020 și a declarării pandemiei de către OMS, la data de 11.03.2020²¹, și a intrat în Scenariul 4 de alertă (peste 2000 de cazuri de persoane infectate).

Nici o țară din lume nu a fost pregătită să facă față de la început acestui virus, specialiștii învățând din mers, adaptându-se în permanență la modul de evoluție, precum și la mutațiile acestuia.

Amânarea luării deciziilor de către autorități, viteza mare de propagare a virusului, impactul major, imprevizibilitatea evoluției, au făcut ca cea mai mare parte a sistemelor de sănătate, indiferent de nivelul de dezvoltare a statului respectiv, să fie surprinse nepregătite să facă față acestui tip de eveniment pe termen mediu și lung, întrucât nu au avut suficiente echipamente de protecție (mănuși, măști, combinezoane, ochelari), aparatură medicală (pentru testare, ventilatoare etc), teste, medicamente, paturi, mijloace de transport specializate, resursa umană de specialitate etc.

De ce s-a întâmplat așa ceva?

Pentru că, din punctul nostru de vedere, aproape în întreaga lume, problema obținerii de profit a luat-o cu mult înaintea celei de rezolvare a problemelor sociale, fapt pentru care ne alăturăm opiniei unui reputat analist care spunea că „Originea acestei crize este o disfuncționalitate colosală a pieței și a politicilor neoliberale care au intensificat problemele socio-economice”²².

Așa s-a ajuns în situația în care Germania nu poate ajuta Grecia dar Cuba ajută țările europene²³.

Cum putem depăși aceste vremuri?

În primul rând, noi suntem de părere că autoritățile statului trebuie să aibă o conducere unică (în țara noastră, în ciuda faptului că există, potrivit

²¹ [[https://, presidency.ro](https://presidency.ro)> media], accesat la 30.03.2020.

²² Naom Chomsky, interviu cu tema „Coronavirus – what is at stake” acordat lui Srećko Horvat la DiEM25-TV din Arizona, la 28 martie 2020; conform [<https://internal.diem25.org>>events], accesat în 03.04.2020; [m.youtube.com], accesat la 03.04.2020.

²³ Naom Chomsky, interviu cu tema „Coronavirus – what is at stake” acordat lui Srećko Horvat la DiEM25-TV din Arizona, *op.cit.*



legii, asemenea organisme – Comitetul Național pentru Situații Speciale de Urgență, Grupul de Comunicare Strategică din subordinea acestuia, Comitetele Județene pentru Situații de Urgență etc. – acestea sunt „bruiate” de o implicare excesivă a autorităților locale).

În al doilea rând, trebuie să existe o „voce unică” (credem că este momentul în care politicianismul ar trebui să dispară din toate discursurile și oamenii politici să-și respecte angajamentele pe care și le-au asumat față de țară și cetățenii ei).

Apoi, ar trebui să ne protejăm oamenii din „linia întâi”, personalul medical, și să le asigurăm tot ceea ce au nevoie.

În același timp, autoritățile trebuie să ia măsuri economice și fiscal-bugetare, cu prioritate în sprijinul angajaților, în scopul asigurării continuității în funcționare a economiei și păstrării locurilor de muncă, absolut necesare pentru o repornire rapidă în perioada postpandemie.

De asemenea, trebuie să respectăm normele transmise de autorități cât și măsurile de prevenție corespunzătoare, însă nu numai unii, ci toți, pentru că înconștiența și prostia sunt universale, iar împotriva prostiei „zeii înșiși” luptă în zadar²⁴.

Și, nu în ultimul rând, este extrem de important ca forțele destinate să vegheze în permanență la respectarea legii.

Un corolar al celor mai sus prezentate ar putea fi cuprins în patru cuvinte: responsabilitate, implicare, solidaritate și respect.

Ce ar trebui să facem pentru ca așa ceva să nu se mai întâmple?

Faptul că trăim într-un sistem politic internațional, care este o anarhie, în care trăsătura principală este suveranitatea, stare structurală care favorizează relațiile competitive²⁵, într-o lume care suferă de prea multă conectivitate, atunci când apare un asemenea tip de eveniment, statele sunt practic „paralizate” pentru o perioadă de timp pe care noi o estimăm a fi cuprinsă între 6 și 12 săptămâni.

²⁴ N.A. Este vorba despre romanul lui Isaac Asimov, *Zeii înșiși*, Editura Teora, București 1993. Autorul dedică această carte omenirii „și speranței că războiul împotriva prostiei va fi câștigat într-o bună zi” (p.2). Cuprinsul lucrării este constituit din trei părți: partea întâi – *împotriva prostiei...*; partea a doua – *zeii înșiși...*; partea a treia: *luptă în zadar*.

²⁵ Barry Buzan, *Popoarele, statele și frica – O agendă pentru studii de securitate în epoca de după războiul rece*, Editura Cartier, Ediția a doua, Chișinău, 2014, pp. 153, 155.



În această perioadă, reacția autorităților este orientată spre interior, către proprii cetățeni, către propriile sisteme de sănătate, politica internă fiind preponderentă față de politica externă. Este etapa în care se constată că avem nevoie de o mulțime de lucruri și fiecare încearcă să-și rezolve cum poate ceea ce-i lipsește prin economia națională sau/și prin importuri. Însă apar blocajele în transportul internațional, întrucât fiecare stat și-a luat propriile măsuri privind restricționarea circulației persoanelor și a transporturilor de bunuri de tot felul. În acest timp, la nivelurile global, regional și național, cererea depășește oferta la produsele de care cetățenii statelor au nevoie și apare un nou blocaj, precum și o creștere a prețurilor. Este perioada în care noi apreciem că atât competiția cât și colaborarea și cooperarea au tendințe de scădere spre minim, este perioada „fiecare pentru el”.

După depășirea acesteia, încep să se pună în mișcare mecanismele de colaborare și cooperare (în cadrul UE, NATO, parteneriatelor strategice, acordurilor bilaterale etc.), se iau decizii economico-financiare și de altă natură care vizează cetățenii țărilor membre/partenere și economiile acestora, se manifestă o oarecare intrare în normalitate. Este perioada în care noi considerăm rămânerea competiției la un nivel minim și o tendință de creștere importantă, spre maxim, în dreptul colaborării și cooperării. Aceasta nu înseamnă rămânerea competiției la minim întrucât se va manifesta pregnant, cu o tendință de creștere spre maxim, în domeniul cercetării, pentru descoperirea vaccinului/tratamentului care să salveze oamenii de acest virus.

Identificarea perioadei de timp așa cum am perceput-o și descrisă mai sus, ne-a determinat să formulăm concluzia conform căreia, indiferent din ce uniune, alianță, parteneriat face parte, fiecare stat, la apariția unui asemenea tip de eveniment, va trebui să treacă printr-o perioadă în care trebuie să-și desfășoare activitatea autonom, perioadă pe care am denumit-o „funcționare autonomă”.

De aceea, propunem ca autoritățile din țara noastră să ia măsuri care să conducă la funcționarea pe teritoriul național a unor capacități de producție care să asigure utilitățile de bază, produse de strictă necesitate, echipamente de protecție, aparatură medicală, teste, medicamente etc.

Oportunitățile apar nu numai din competiție ci și în situații de criză, ceea ce ar trebui să dea de gândit clasei noastre politice în ceea ce privește modificarea profilului țării noastre, care nu este de țară industrializată și, în



același timp, să acorde o atenție deosebită agriculturii care poate deveni unul din „motoarele” economiei naționale.

În acest sens, autoritățile române ar trebui să investească din ce în ce mai mult în economia națională și să stimuleze în același timp prin măsuri economico-financiare, realizarea de investiții în capacități de producție a marilor concerne internaționale.

De asemenea, ar trebui identificate din rândul capacităților de producție existente, cele în măsură să realizeze reconversia într-un timp relativ scurt, pentru a produce ceea ce avem nevoie.

Și nu în ultimul rând, aceste capacități de producție ar trebui să facă parte din industria națională de securitate.

Sintagma „utilități și produse de strictă necesitate” poate fi dezvoltată în Ghidul Strategiei Naționale de Apărare a Țării, iar capacitățile de producție cu destinația „funcționare autonomă” a statului să fie stabilite și ulterior cuprinse într-un plan (Plan de capacități de producție), anexă la Planul de implementare a strategiei.

„Funcționarea autonomă” a statului presupune și regândirea sistemului național de sănătate publică, crearea unui fond financiar de rezervă, intangibil și la dispoziția autorităților pentru astfel de situații, alături de constituirea și menținerea unui stoc cu materialele și produsele mai sus amintite, în cadrul rezervelor statului.

Ceea ce supunem atenției în continuare se încadrează, din punctul nostru de vedere, în efectele benefice ale unui eveniment de tip „Lebăda Albă”, precum și în unul din atributele evenimentelor de tip „Rinocerul Gri”, adică a face ceva pentru a îndrepta lucrurile pe care le vedem în fața noastră.

În acest sens, considerăm că trebuie să aibă loc o restructurare a strategiilor politice globale/regionale care să nu permită virusului COVID-19 să afecteze relațiile din interiorul uniunilor, alianțelor, parteneriatelor.

Pe termen lung, este importantă stoparea „virusului” egoismului aparent, întrucât în această perioadă fiecare stat este obligat să se descurce singur, deoarece ceilalți nu-l pot ajuta, iar situația în care apare, să fie blocat de „vaccinul” colaborării și cooperării.

Această perioadă, în care ne așteptăm la o dinamică mai rapidă a relațiilor din interiorul UE, NATO, parteneriatelor etc., nu trebuie să dea naștere „virusului” ruperii relației și a „virusului” destrămării.



Dimpotrivă, ea ar trebui definită, formalizată prin noi reguli, astfel încât țările membre/partenere să nu se simtă izolate și abandonate, să nu nască orgolii și temeri extremiste, temeri sociale firești în perioade dificile și să nu fie tentate de „mirajele” unor ajutoare care, pe termen lung, nu sunt lipsite de capcane.

De aceea țările membre ale UE, NATO, partenere, trebuie să sprijine prin măsuri economico-financiare dezvoltarea unor capacități de producție care să asigure fiecărui membru „funcționarea autonomă” până la punerea în mișcare a mecanismelor de colaborare și cooperare.

Întocmirea planului de capacități de producție ar trebui să aibă loc până la nivelul UE/NATO, iar abordarea pe care noi o considerăm a fi mai eficientă, este de la parte la întreg.

Trebuie să se găsească un echilibru între mecanismele pieței libere și regulile de securitate, să se stabilească până unde merg regulile pieței libere și când intră în acțiune regulile de securitate, până unde se poate merge cu anumite măsuri ce pot fi privite ca fiind autoritare, astfel încât principiile fundamentale ale democrației să nu fie afectate pe termen mediu și lung.

„Funcționarea autonomă” este necesară fiecărui stat pentru a nu deveni o povară pentru celelalte state membre ale uniunii/alianței.

Funcționând autonom dar împreună, vom fi mai puternici!

Este nevoie, de asemenea, de schimbarea modului de a comunica a autorităților care să nu mai permită crearea de false așteptări. Aceasta trebuie să ne învețe pragmatismul și să ne „vaccineze” împotriva așteptărilor umane și societale neîmplinite, ca să știm exact ce putem face noi înșine și ce și când trebuie să așteptăm de la ceilalți.

Neavând așteptări și cunoscând exact care sunt posibilitățile de ajutor din partea celorlalți, poți combate eficient fake-news-urile și poți avea o comunicare corectă și directă cu membrii propriei societăți. Deci oamenii vor ști cum, când și până când să se ajute singuri și care este momentul când se vor putea baza și pe ceilalți parteneri.

Dacă cetățenii sunt informați corect privind planul care se pune în aplicare și văd că măsurile sunt corecte, atunci nu se va instaura sentimentul de nesiguranță socială ale cărui urmări vor fi extrem de greu de înlăturat pe termen mediu și lung.

Oamenii vor fi tentați să dea ascultare și credibilitate celor care par a li se adresa direct și a le înlătura temerile. Acest fapt ar trebui să conducă și la stoparea „contaminării” cu „virusul” „Cine este vinovat?”.



Da, coronavirusul „...”, este o oportunitate de resetare a mentalității, de a pune aceste riscuri evidente în față²⁶ și va trece „...”, dar partea bună ar putea fi că va face oamenii să se gândească la ce fel de lume dorim²⁷.

Dacă nu, și așa ceva are șanse mari să se întâmple, întrucât autoritățile statelor și-ar pune sub semnul întrebării eficiența propriilor sisteme social-economice și politico-ideologice, o posibilă viitoare luptă la nivel global ne va găsi la fel de nepregătiți ca acum.

Criza va trece și va începe o nouă competiție, și cine va reuși să repornească primul „motoarele” economiei va fi probabil deținătorul supremației mondiale.

Bibliografie

1. Barry, Buzan *Popoarele, statele și frica – O agendă pentru studii de securitate în epoca de după războiul rece*, Editura Cartier, Ediția a doua, Chișinău.
2. Isaac, Asimov *Zei înșiși*, Editura Teora, București 1993.
3. Nassim, Nicholas, Taleb *LEBĂDA NEAGRĂ, Impactul foarte puțin probabilului*, Editura Curtea Veche, București, 2009.
4. *** <http://descopera.org/teoria-l>.
5. *** <http://romania.europalibera.org/d>.
6. *** <https://revistasinteza.ro/profe...>
7. *** evz.ro.
8. *** www.rador.ro/NATO.
9. *** <https://www.presidency.ro/media>.
10. *** <https://internal.diem25.org/events>.
11. *** m.youtube.com.

²⁶ Michele Wueker, [<https://revistasinteza.ro/profe...>], accesat la 02.04.2020.

²⁷ Naom Chomsky, [<https://internal.diem25.org/events>], accesat în 03.04.2020; [m.youtube.com], accesat la 03.04.2020.



PANDAMIA DE CORONAVIRUS ȘI SECURITATEA CIBERNETICĂ

CORONAVIRUS PANDAMIA AND CYBERSECURITY

Col. (rtr.) prof. univ. dr. Gheorghe BOARU

Membru titular al Academiei de Științe ale Securității Naționale,

Membru titular al Academiei Oamenilor de Știință din România

E-mail: boarugheorghe@yahoo.com

Rezumat: În această perioadă de criză sanitară gravă de nivel mondial, generată de Coronavirus, organizațiile din sistemul de securitate și apărare națională, dar și o parte dintre cele civile, continuă activitatea în sistem online de la domiciliu sau în sistem telemuncă. Prin acest nou tip de activitate, preponderent online, organizațiile pot crea, din neatenție, o breșă de atac mai largă pentru actorii amenințării cibernetice. În această perioadă „escrocheriile coronavirus” sunt în creștere.

În acest articol voi încerca să atenționez asupra câtorva moduri de a vă proteja Internetul, rețeaua și dispozitivele (devices-urile) proprii. Putem considera acest articol ca fiind un ghid general simplificat menit să surprindă esența a ceea ce aveți nevoie. Sunt prezentate 33 de recomandări practice doar pentru calculatoare nu și pentru telefoane mobile.

De fapt, indiferent dacă este vorba despre COVID-19 sau de o altă situație de criză, nu neapărat sanitară, aceste sugestii consolidează bunele practici și obiceiuri de securitate.

Cele 33 sfaturile sunt chiar concrete și practice și pot fi excelente pentru apărarea împotriva înșelătoriei / exploatării / atacurilor diferite. Urmând sfaturile prezentate în acest ghid de supraviețuire, este posibil să rămâneți neafecțați în fața hackerilor și să le zădărniciți acțiunile înainte să aibă șanse de a vă penetra rețeaua informatică.

Cuvinte cheie: securitate software, hacker, amenințări cibernetice, parole, confidențialitate, pirații Internetului.

Abstract: In this period of serious global health crisis, generated by Coronavirus, the organizations in the national security and defense system, but also some of the civil ones, continue their activity in the online system from home or in the telework system.

Through this new type of activity, mainly online, organizations can inadvertently create a wider breach of attack for cyber threat actors. During this period, "coronavirus's scams" are on the rise.



In this article I will try to warn you about some ways to protect your Internet, network and your own devices. We can consider this article as a simplified general guide designed to capture the essence of what you need. 33 practical recommendations are presented only for computers and not for mobile phones.

In fact, whether it is COVID-19 or another crisis situation, not necessarily a health one, these suggestions reinforce good security practices and habits.

The 33 tips are even concrete and practical and can be excellent for defending against various scams / exploitation / attacks. Following the tips in this survival guide, you may remain unaffected by hackers and thwart their actions before they stand a chance of penetrating your computer network.

Keywords: *software security, hackers, cyber threats, passwords, privacy, Internet's pirates.*

Introducere

Invazia Coronavirusului (COVID-19) a cuprins și surprins scena mondială. În momentul elaborării acestui articol, majoritatea țărilor importante au confirmat multe cazuri grave și au fost înregistrate foarte multe decese. România nu a fost exclusă din această criză sanitară gravă.

Decretarea stării de urgență, a stării de alertă și recunoașterea pandemiei în România a dus la impunerea unor restricții sociale fără precedent, a obligat la noi modalități de desfășurare a activităților sociale și a vieții oamenilor.

Astfel, o parte dintre instituțiile de stat și cele private, care și-au continuat activitatea online, au adoptat una dintre formele cunoscute: telemunca și/sau lucrul de acasă.

Continuând îndeplinirea sarcinilor de serviciu în sistem online angajații (conducătorii organizațiilor și operatorii) pot uita că trebuie să ia unele măsuri speciale tehnice și organizatorice și vulnerabilizează astfel confidențialitatea informațiilor cu care operează în acest spațiu cibernetic

Conștientizând importanța și dependența de acest spațiu cibernetic, a trebuit să i se asigure o securitate sporită, atât lui cât și sistemelor informatice și de comunicații care operează cu informații. Avem astfel în vedere că „...în analiza unei activități informaționale militare, informația poate fi considerată „materie primă”, „scop”, „țintă”, „armă” și că protejarea acesteia este cu atât mai importantă și mai complexă”¹.

¹ Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare „Carol I”, București, 2018, p. 6.



Prin acest nou tip de activitate, de acasă, organizațiile pot crea, din neatenție, o zonă de atac mai largă pentru actorii amenințării cibernetice (Cyber Threat Actors - CTA).

Departamentele IT din instituțiile aparținând domeniului securității și apărării naționale trebuie să rămână vigilente, deoarece la nivelul cel mai de bază, malware-urile și instrumentele de hacking, au devenit, de asemenea, mai ușor disponibile, permițând celor fără condiții de codare să le înțeleagă și să le utilizeze corect.

„Existența acestui mediu virtual sau „spațiul cibernetic, recunoscut ca mediu de conflict, se bazează pe exploatarea cu succes a dependenței de date și informații”, manifestată la nivelul structurilor militare, cu atât mai mult cu cât acestea acționează într-un mediu de conflict hibrid. Pe lângă automatizarea acțiunilor și digitalizarea forțelor militare, societatea civilă a contribuit și contribuie major la creșterea dimensiunii și definirea spațiului cibernetic ca cel de-al cincilea mediu de conflict, alături de mediul terestru, aerian, maritim și cosmic”².

În cazul creării acestor breșe de securitate, hackerii criminali și rețelele subterane pot exploata această situație pentru a profita de țintele vulnerabile și sistemele lor de infrastructură.

În această perioadă „escrocheriile coronavirus” sunt în creștere. Acestea includ acțiuni a mulți dintre aceiași înșelători profesioniști în domeniul cibersecurității care au mai fost văzuți. Pot părea noi, dar de fapt sunt la fel. Principala diferență este că sunt „încoronați”.

Domeniul IoT (**I**nternet **o**f **T**hings- Internetul lucrurilor)³, care este în prezent în atenția specialiștilor în IT are acum două aplicații majore, cele din spațiul de consum și cele din industrie (organizații civile și/sau militare). Numai în acest an au fost publicate zeci de lucrări științifice privind IoT,

² Gheorghe BOARU, Benedictos IORGA, *IMPLICAȚIILE PARTICIPĂRII FORȚELOR MILITARE ROMÂNEȘTI LA OPERAȚIILE DE TIP COALIȚIE, ASUPRA EVOLUȚIEI ȘI DEZVOLTĂRII SISTEMULUI MILITAR NAȚIONAL DE COMUNICAȚII ȘI INFORMATIC*, Editura SITECH, Craiova, 2020, p. 236.

³ IoT (**I**nternet **o**f **T**hings) este o definiție destul de largă, acoperind în esență orice dispozitiv care este capabil să comunice cu alte dispozitive pe Internet. În fiecare zi, tot mai multe aparate și obiecte se conectează la Internet. Aceasta înseamnă oportunități mai mari pentru atacurile cibernetice. Cu cât IoT este mai dezvoltat, cu atât există și mai multe probleme de securitate a informațiilor și sistemelor informaționale.



autorii⁴ fiind de pe toate continentele. Toate lucrările au în atenție și securitatea acestor sisteme.

În ghidul cu recomandări sunt incluse o gamă largă de scheme de atac precum phishing, produse de răscumpărare (ransomware) și reclame false. Guvernele, întreprinderile și persoanele fizice trebuie să-și dea seama de ele și să caute modalități de a rămâne în siguranță.

Datorită acestei „furtuni”, puteți deveni o țintă. Poate aveți multe lucruri valoroase în informațiile pe care le caută hackerii. Protejați-le!, protejați-le căutând modalități de a vă consolida securitatea. La nivel instituțional „*caracterul global și multidimensional al problemei de asigurare a securității informațiilor, cu recunoașterea necesității ca guvernarea securității să fie dezvoltată spre a combate amenințarea cibernetică și că, în această acțiune, trebuie să fie angajate mult mai multe niveluri, actori, instituții și persoane implicate în ecosistemul cibernetic*”⁵.

În acest articol voi încerca să atenționez asupra câtorva moduri de a vă proteja Internetul, rețeaua și dispozitivele (devices-urile) proprii. Acest articol acoperă subiecte precum e-mail, parole și securitate software. Poate părea prea general, dar toate aceste sfaturi sunt excelente pentru apărarea împotriva înșelătoriei / exploatării / atacurilor diferite. De altfel problema nu este deloc nouă. „*Astfel, în anul 1985, un militar chinez în vârstă de 25 de ani, Shen Weiguang, a scris un eseu intitulat „Războiul informațiilor”. În această lucrare el vorbea despre noțiuni ca „frontiera informațiilor”,*

⁴ Huimin Lu, *Cognitive Internet of Things: Frameworks, Tools and Applications*, Series: Studies in Computational Intelligence 810, Publisher: Springer International Publishing, Year: 2020; Mohammad Ali Jabrael Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdzadeh, Farhad Norouzi, *Towards the Internet of Things: Architectures, Security, and Applications*, Series: EAI/Springer Innovations in Communication and Computing, Publisher: Springer International Publishing, Year: 2020; Sheng-Lung Peng, Souvik Pal, Lianfen Huang, *Principles Of Internet Of Things (IoT) Ecosystem: Insight Paradigm*, Series: Intelligent Systems Reference Library Vol. 174, Publisher: Springer, Year: 2020; Srikanta Patnaik, *New Paradigm Of Industry 4.0: Internet Of Things, Big Data & Cyber Physical Systems*, Series: Studies In Big Data Vol. 64, Publisher: Springer, Year: 2020; Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*, Publisher: Apress, Year: 2020.

⁵ Col. (ret.) prof.univ.dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană*, Revista Academiei de Științe ale Securității Naționale, nr. 2/2017, p. 68.



„fabrica de informații”, „armata informaționalizată”, „poliția informațiilor”, „lupta la domiciliu” și descria informația ca trăsătură atotcuprinzătoare a societății”⁶.

De fapt, indiferent dacă este vorba despre criza COVID-19 sau de o altă situație de urgență, aceste sugestii consolidează bunele practici și obiceiuri de securitate.

Eu nu pot afirma cu dovezi că virusul SARS-CoV-2 este produs în laborator, de către X sau Y actor mondial și folosit ca „armă biologică”, dar pot afirma cu certitudine că virușii informatici sunt rezultatul muncii unor informaticieni iscușiți care, pentru un anumit interes individual sau de grup, produc pagube directe sau colaterale unor utilizatori normali dar care nu cunosc sau nu respectă regulile „de igienizare” de bază.

La nivel național reglementările specifice protecției informațiilor definesc suficient de clar domeniul. Strategia de securitate cibernetică a României definește securitatea cibernetică ca fiind „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic”⁷.

Puteți alege să implementați oricare dintre aceste sfaturi sau cel puțin să înțelegeți raționamentul din spatele lor. Aceste sugestii se concentrează pe practici și lucruri pe care le puteți face chiar acum.

Putem considera acest articol ca fiind un ghid general simplificat menit să surprindă esența a ceea ce aveți nevoie. Dacă considerați necesar puteți aprofunda informarea și chiar să continuați cercetarea. Responsabilitatea revine pe umerii fiecăruia dintre noi. Să ne reamintim de ce a spus fostul președinte american Abraham Lincoln: „Nu poți evita responsabilitatea de mâine, eludând-o astăzi”.

Supunem atenției o serie de reguli privind unele obligații personale ale utilizatorilor de Internet, sub forma unui ghid cu 33 de recomandări, așa

⁶ Col. (r.) prof. univ. dr. Gheorghe BOARU, *RĂZBOIUL INFORMAȚIONAL – UN OBIECTIV AL SECURITĂȚII NAȚIONALE*, Revista Academiei de Științe ale Securității Naționale nr.2/2019, p. 29.

⁷ Hotărârea nr. 271/2013 pentru aprobarea *Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013, p. 7.



cum mai sugerează și un autor avizat⁸, dar și sfaturi adaptate la situația românească generată de Coronavirus.

Securitatea cibernetică - Recomandări pentru utilizatori

1. Adoptați parole mai puternice

Numele de utilizator și parolele slabe sunt adesea una dintre cele mai bune breșe pentru ca hackerii să intre în conturile vulnerabile.

Foarte mulți utilizatori folosesc parole de genul „1234” sau „11111”. Parolele slabe pot fi ghicite sau forțate brutal.

Soluția este de a stabili propriul procedeu pentru a crea parole noi. Amestecați caractere speciale, cifre și litere, caractere speciale pentru a adăuga complexitate contului. În plus, încercați să nu utilizați aceleași parole de mai multe ori. În acest fel, dacă un cont este spart, celelalte nu vor fi afectate.

2. Alegeți politici de confidențialitate prudente

Deoarece site-urile web schimbă în mod constant modul în care utilizatorii se conectează și cum le sunt colectate și stocate datele. Regulamentul general privind protecția datelor (GDPR) și alte cadre legale, a stabilit cum companiile au fost nevoite să actualizeze modul în care își colectează datele. Site-urile web vor examina datele pentru a identifica tendințele și a prezice comportamentul utilizatorilor.

Ce se poate face? De fiecare dată când vă conectați la un site web, vizitați pe site-ul lor pagina de confidențialitate. Citiți politicile lor cu privire la modul în care colectează datele dumneavoastră și ce fac cu acestea. Căutați specificul și jargonul tehnic.

Dacă site-urile web pe care le vizitați și le cumpărați nu au o politică de confidențialitate, considerați că este posibil să fie un semnal de alertă.

3. Anticipați atacurile ciberneticice

Hackerii caută în permanență modalități de a crea breșele în sistemele informatice. Atacurile ciberneticice se petrec în fiecare zi. O mare parte din acestea se întâmplă prin intermediul automatizării computerizate.

⁸ LEVI WEST, *The Coronavirus Cybersecurity-Survival Guide-Top Tips to Protect You From A Cyber Attack*, 2020.



Ce se poate face? Dacă atacurile cibernetice pot avea loc în orice moment, atunci utilizatorii trebuie să-și actualizeze și să-și apere sistemele cât mai repede posibil. Rulați software antivirus în mod automat. Scațați toate fișierele noi pe care le descărcați pentru a vă asigura că nu au malware. Nu instalați niciodată nimic cu care nu sunteți familiarizat și mai ales care vi se pare ciudat (binevoitor, salvator, ieftin sau chiar gratuit).

Blocați informațiile dumneavoastră valoroase prin parolare. Toate sistemele de operare vă permit să ascundeți și fișiere.

4. Evitați ofertanții dubioși

„Meseriașii” în oferte tentante creează în Internet un sentiment de urgență și penurie, pentru anumite produse, pentru a-i determina pe utilizatori să cumpere urgent produse (false), să descarce software-ul gratuit (infectat) sau să introducă informațiile cardului de credit pe site-urile false.

Ce trebuie să faceți? Nu intrați în panică. Aceste Site-uri și „vânzătorii” sunt configurați cu bunuri „noi” care nu există. Acestea pot crea false oferte dar care de fapt nu există în realitate. Ei pot promite chiar o cură pentru imunizare sau tratament la COVID-19 (tratamente naturiste, medicamente, vaccinuri,...). Cineva încerca să vândă sprayuri anti Covid-19. Interesant, nu? Feriți-vă de reclame suspecte și promisiuni prea tentante pentru a fi adevărate.

Clickbait (Click - momeală) este una dintre cele mai ieftine modalități prin care hackerii și vânzătorii își recoltează informațiile dar și bani în mod fraudulos. Se vor prezenta adesea ca oferte super avantajoase. De exemplu, s-au făcut oferte de teste Covid la un preț de 100-150 lei comandate pe Internet. Aceste oferte sunt foarte tentante mai ales că, spun ei, pot fi utilizate acasă și se obține rezultatul urgent. Se speculează emoția momentului, în condițiile când aceste testări oficiale nu prea s-au făcut la populație (din motive tehnice dar și politice), și se pot obține, în mod fraudulos bani fără ca aceste comenzi să se poată onora conform generoasei ofertei.

În această perioadă a pandemiei și a Ordonanțelor militare de urgență, când școala se desfășoară online, Internetul este încărcat cu lecții și jocuri online interactive (texte, grafice, filmulețe,...) ceea ce deschide o bună șansă a răuvoitorilor internați să penetreze sistemele și să folosească momentul pentru Hacking. „Pirații Internetului” exploatează momentul și-și fac treaba nestingheriți dacă nu a-ți luat măsurile corespunzătoare de



securizare a divaces-urilor pe care le folosiți. Există chiar și un steag al acestora (în mai multe variante) care au însă ca element comun stindardul piraților (vezi Figura 1).

Figura 1. Steagul piraților pe fundalul cerului albastru

De altfel prin însăși definiția sa, conceptul de **Hacker** înseamnă, ... *un expert în informatică, care se ocupă cu studiul în profunzime al programelor informatice (sisteme de operare, aplicații), adesea folosind tehnici de inginerie inversă (demontare), cu scopul de a obține cunoștințe care nu sunt accesibile publicului larg. Cei ce folosesc aceste cunoștințe în scopuri ilegale, pentru a compromite securitatea sistemelor informatice sau a aplicațiilor, sunt de fapt **crackeri** (spărgători), însă în percepția publicului (formată de obicei de mass-media) noțiunile de hacker și cracker adesea se confundă*⁹.

Din publicațiile de specialitate¹⁰, cele mai recente, am desprins concluzia că un hacker poate fi definit ca „*Persoană care se folosește de computere pentru a obține neautorizat informații sau pentru a manipula sisteme informatice sau a obține avantaje materiale în mod ilegal*”.

5. Faceți copii de rezervă a datelor

Legea lui Murphy spune că „*dacă ceva poate să meargă prost, va merge*”¹¹. Ca utilizator, ar trebui să aveți o copie de încredere a datelor dumneavoastră păstrate bine în cazul în care ceva nu merge corect. Numărul de motive ar putea varia de la distrugerea fizică a calculatorului dumneavoastră până la defectarea hardware la atacul cibernetic. Nu știi

⁹ [<https://ro.wikipedia.org/wiki/Hacker>].

¹⁰ Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Publisher: Harvard University Press, Year: 2020; Vinny Troia, *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*, Publisher: Wiley, Year: 2020; Aditya Gupta, *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things*, Publisher: Apress, Year: 2019; Jim Kou, *Hacking: The Practical Guide to Become a Hacker | Field Manual for Ethical Hacker Including Ethical Hacking with Kali Linux*, Publisher: Independently published, Year: 2019.

¹¹ [https://www.academia.edu/21702040/Legile_Lui_Murphy], cap. 3.



niciodată când smartphone-ul sau hard disk-ul computerului dumneavoastră ar putea muri. O a doua „viață” va remedia rapid această situație.

Ce puteți face? Gândiți-vă la datele pe care le aveți și la ce anume este important. Clasați-le de la cel mai important la cel mai puțin important pentru a stabili ordinea în care să faceți backup. După ce ați făcut acest lucru, stocați-vă datele pe un sistem de rețea cloud fiabil și pe un alt dispozitiv / sistem pe care îl aveți. Asigurați-vă că vă sunt cele mai nimerite memorii externe pentru dumneavoastră (CD-uri, DVD-uri, BD-uri, Stick-uri, Hard disk-uri externe,...).

Recomandarea este să faceți backup-uri în mod regulat și în mod continuu.

6. Atenție la Phishing

Phishing-ul este o altă tactică populară folosită de hackeri pentru a obține acces la sistemul victimei. Phishingul implică *masquerading* (deghizarea, ascunderea identității reale) ca parte de încredere în încercarea de a-ți fura informațiile. Aceștia se pot preface că sunt compania ta preferată, șeful sau chiar prietenii tăi. Cea mai populară metodă de livrare este prin e-mail, dar se poate întâmpla prin orice formă de comunicare electronică.

Ce poți face? Dacă sesizezi ceva ciudat, fii atent și verifică dacă : calitatea e-mailului este aceeași? E ceva ciudat în el? Multe e-mailuri de tip phishing vă vor solicita informații personale și vă va convinge să răspundeți înapoi. Companiile de renume nu cer aceste informații într-un e-mail.

Nu răspundeți niciodată la aceste comunicări. Phishingul este simplu, dar este unul dintre cele mai periculoase tipuri de atacuri.

Phishingul are diferite tipuri de forme. Din cauza costurilor reduse de trimitere a acestuia, hackerii trimit de regulă scheme de phishing pentru a-și prinde victimele. Voi descrie pe scurt două dintre cele mai comune forme de phishing.

Pescuitul cu sulita. Acesta este un tip sofisticat de phishing care vizează o persoană anume și un cont de e-mail. În această situație particulară, hackerul știe cam totul despre victimă. Aceștia pot studia chiar comportamentul victimei și pot determina cel mai bun moment al zilei pentru a-l prinde într-un moment prielnic atacului. Când se lansează un atac de phishing sulită, acesta va părea foarte real și relevant.



Vânătoarea de balene este un tip de phishing care vizează managementul și nivelurile de conducere ale unei organizații. Hackerii își vor face cercetările pe platformele de social media precum *LinkedIn*¹² și identifică partenerii cu care lucrează.

Concomitent, atunci când trimit e-mailuri, hackerii pot încorpora, de asemenea, link-uri sau atașamente relevante pentru operațiunile zilnice ale unei organizații. Când este deschis, acesta va compromite un sistem prin malware (precum un virus sau un *Keylogger*¹³).

Limitați informațiile private când puteți și cât de mult puteți.

7. Verificați e-mailurile de două ori

De ce este important: cybercriminalii știu că obiectivele lor potențiale ar putea ceda panicii și impulsului. Datorită acestei posibilități, ei știu că atunci când trimit un e-mail rău intenționat, există o șansă crescută de deschidere.

Ce puteți face? Ori de câte ori primiți un e-mail în căsuța de e-mail, verificați expeditorul și adresa de e-mail pe care le utilizează. Asigurați-vă că pe acea adresă de e-mail a-ți mai primit și trimis e-mailuri și mai înainte. Cybercriminalii pot înregistra un domeniu fals și pot adăuga caractere pentru a părea legitime. De exemplu, *user@un.org* este domeniul oficial al Națiunilor Unite. Nu este probabil să vă trimită e-mailuri de pe adresele de e-mail *user@un-safety.net* sau *user@un-usa.com*.

8. Verificați ortografia și gramatica

De ce este important: poate părea evident, dar o mulțime de hackeri fac greșeli de ortografie și gramatică atunci când comunică cu potențialele ținte. Mulți hackeri sunt internaționali și au învățat engleza ca a doua sau a treia limbă (dacă ne referim la mesajele în engleză). Multe dintre amăgelile lor pot suna în mod ciudat sau pot include fraze pe care un vorbitor nativ le-ar folosi foarte rar.

¹² *LinkedIn* este o rețea de socializare orientată spre mediul profesional cu ajutorul căruia orice utilizator își poate găsi un loc de muncă sau un angajator poate găsi profesionistul de care are nevoie.

¹³ Un *Keylogger*, numit uneori apăsător de taste sau monitor de sistem, este un tip de tehnologie de supraveghere folosită pentru monitorizarea și înregistrarea fiecărei apăsări operate pe tastatura unui computer. Software-ul *Keylogger* este disponibil și pentru smartphone-uri, cum ar fi dispozitivele Apple iPhone și Android.



Ce puteți face? Dacă primiți ceva suspect de la prieteni, colegi de muncă, foști camarazi etc., luați în considerare frazarea. Este o exprimare ciudată, penibilă? Mesajul a fost trimis la o oră anormală pentru conversație? Comunică acesta cu voi în mod normal, în acest fel. Limba română este complexă și, în acest caz, este un lucru bun pentru că falșii camarazi se pot demasca singuri prin exprimări nefirești limbii noastre. Dacă textul mesajelor este într-o altă limbă de circulație internațională (cum ar fi engleza) atunci apălați la un translator sau la o persoană care cunoaște subtilitățile acestei limbi străine.

Nimeni nu este perfect. Aceasta îi include și pe hackeri.

9. Evitați planurile (hărțile) false de Coronavirus

Hărțile și graficele sunt una dintre cele mai bune modalități de a face ca o poveste să poată fi credibilă. Ori de câte ori mass-media încearcă să redea starea actuală a virusului, acestea vor prezenta deseori o hartă geografică sau vizualizări de date, sub formă de cifre sau reprezentări grafice, pentru a vă oferi o imagine cât mai relevantă a ceea ce se întâmplă.

Datorită încrederii populației în aceste forme de informare, hackerii au copiat formatul sau au încorporat link-uri rău intenționate pentru a recolta informații de la dumneavoastră.

Ce poți face? Marchează-ți sursele oficiale și cunoscute, astfel încât să puteți apăla doar la acestea atunci când este nevoie. Sursa voastră de informare trebuie să fie organizațiile de știri de reputație și site-urile oficiale. Nu subestimați niciodată creativitatea unui hacker!

10. Nu deschideți e-mailuri suspecte

Tot timpul primim e-mailurile nesolicitate și neașteptate. Ele sunt trimise sub formă de știri, reclame avantajoase sau anunțuri importante. Acestea poate par tentante dar evident că nu trebuie să faceți clic pe e-mailurile suspecte, dar totuși se mai întâmplă uneori și i se poate întâmpla oricui. Deschiderea lor poate oferi informații hackerilor, chiar dacă clic-ul a fost dat din curiozitate. De exemplu, ei pot afla unde te afli și chiar te pot localiza.

Ce puteți face ? Raportați orice e-mailuri care vin clandestin în căsuța de e-mail, autorităților și furnizorului de servicii de e-mail.

Configurați un alt cont de e-mail pentru a-l utiliza ca buffer între contul nou creat și contul dumneavoastră principal.



După configurarea, activați o funcție de e-mail de previzualizare care izolează conținutul contului dumneavoastră.

11. Nu faceți clic pe Link-uri suspecte

Chiar dacă deschideți un e-mail de la un contact de încredere sau o sursă, hackerii vă pot compromite în continuare. De fapt, de multe ori compromis mai întâi prietenii sau familia, deoarece acest lucru crește șansa ca tu să le citești e-mailurile. Cu toate acestea, le poate fi greu să compromită aceste conturi. În schimb, ceea ce ar putea face este să redirecționeze hyperlink-urile web (linkurile albastre) pe care le vedeți în e-mailuri către o altă locație pe care o controlează. Un cont fals pe site-ul web al unei companii de socializare sau a băncii dumneavoastră de exemplu.

Ce poți face? Evitați să faceți clic pe linkurile directe în care au fost încorporate e-mailuri. Copiază legătura, altfel cunoscută sub numele de Uniform Resource Locator (URL) și pune-o printr-un scanner URL. Site-uri precum *virustotal.com* și *sucuri.net* sunt populare din acest motiv.

Legăturile rău intenționate sunt unul dintre cei mai comuni vectori pentru a păcăli victimele.

De ce este important să nu faceți clic pe Link-uri suspecte: legăturile sunt un numitor comun pentru hackeri pentru a obține un acces neautorizat. Hackerii vor folosi adesea link-uri scurtate care te redirecționează către site-uri web dăunătoare.

Linkurile scurtate folosesc un număr de caractere cu o lungime foarte mică. Cu toate acestea, hackerii și-au dat seama că este greu pentru cineva să vadă și să verifice o legătură, deoarece aceste legături le prezintă un anumit nivel de confuzie.

Ce se poate face? Când primiți link-uri suspecte, examinați-le pe fiecare dintre ele. Utilizați scanere URL pentru a le scana și verifica dacă sunt rău intenționate. În ciuda formei sale, în final, este totuși o legătură. Dacă trebuie, deschideți e-mailul înainte de a copia și insera link-ul în scannerul URL pentru a stabili dacă acesta este în siguranță.

12. Descărcați programe de securitate

Un instrument de securitate este necesar întotdeauna pentru protecția sistemelor tale informatice. Acest instrument trebuie să includă o suită de protecții precum antivirus, anti-spyware și un firewall puternic. Fiecare este un parte necesară a apărării tale.



Ce poti face? Aflați ce vă puteți permite și care este prețul. Puteți găsi o mulțime de programe antivirus și anti-spyware bune, dar multe dintre cele mai solide și actualizate instrumente necesită abonament. Numai dumneavoastră decideți care este cel mai convenabil produs atât ca preț cât și ca servicii de protecție oferite.

13. Atașamentele prin e-mail pot fi periculoase

Atașamentele rău intenționate pot fi un mod eficient de infectare a sistemelor informatice ale unui utilizator. Fișierele atașate, deși sunt simple, pot găzdui și malware executiv care vă poate compromite rapid informațiile. Nu contează dacă este un document, o foaie de calcul sau chiar o imagine. Toate aceste lucruri pot fi dăunătoare.

Ce poti face? Dacă aveți o setare pentru a descărca automat atașamente, opriți-l imediat. Asigurați-vă că se așteaptă orice atașament primit. De exemplu, dacă un coleg de serviciu a spus că a trimis un fișier specific, atunci știi că va veni. Totuși, scanează fiecare fișier așa cum ajunge, pentru a-ți oferi liniștea sufletească de care ai nevoie. Nu crede în instinctele tale, verifică orice fișier chiar dacă altădată (înainte de pandemie) nu o făceai.

14. Evitați eterna cerere de răscumpărare (Ransomware-ul)

Ransomware-ul (răscumpărarea) este una dintre principalele amenințări cibernetice fiind folosit pentru amenințarea victimelor. Ransomware este un tip de malware care blochează toate datele victimei și le criptează astfel încât să nu poată avea acces la ele. Aceasta infectează calculatoarele în multe moduri, dar deschiderea atașamentelor de e-mail sau vizitarea site-urilor deja infectate sunt două dintre cele mai importante căi.

Odată infectat, hackerii vor cere apoi drept răscumpărare bani (Euro, USD sau criptomonede uzuale) sau, dacă nu, ei vor face publice datele sau le va șterge pe toate.

Ce poti face? Vă amintiți cum v-am recomandat să vă faceți backup cu datele? Backup-urile proaspete sunt una dintre cele mai bune apărări pentru datele dumneavoastră. Dacă ei vă vor șterge datele, puteți reveni la copia de rezervă și continuați să operați normal.

Ransomware-ul este un tip de amenințare extrem de eficientă.

Tratează-l foarte serios!



15. Asigurați-vă că este instalat cel mai recent firmware

Firmware-ul este software încorporat pe hardware-ul dumneavoastră care să-l ajute să ruleze. Mulți utilizatori de Internet nu actualizează firmware-ul activat pe routerul lor. Aceasta expune rețeaua lor la defectele de securitate care pot fi utilizate de către atacatorii care exploatează utilizatorii de la distanță.

Ce puteți face? Conectați-vă la software-ul de gestionare Wi-Fi și executați o actualizare pe routerul dumneavoastră. Instalați cel mai recent software dacă știți că aveți unul depășit. Verificați dacă routerul dumneavoastră se actualizează automat sau dacă îl puteți seta să facă actualizări automate. În plus, apălați la furnizorul de servicii Internet pentru sfaturi suplimentare despre routerul și rețeaua Wi-Fi. Extindeți-vă la alte dispozitive, mai moderne, după cum este necesar.

16. Așteptați-vă că media socială va fi copleșitoare în această perioadă de pandemie

Trăim într-o economie informațională. Noi suntem dependenți de Internet pentru a înțelege ce se întâmplă. Primul lucru oamenii merg deseori la social media. Social media este cel mai larg vector de a infecta utilizatorii de media. O mulțime de conturi sunt false (administrare de bots de computer) și există o mulțime de știri distractive care vă vor consuma timpul necesar sarcinilor obligatorii pentru care sunteți acasă (lucrul de acasă).

Ce puteți face? Minimizați retweet-urile (re-postările unui Tweet) și postările la numai cele relevante. Urmăriți doar un număr limitat de surse pentru știri. *Semnalați și raportați orice fel de conturi false!*

17. Clipuri false prin intermediul DeepFakes (falsuri profunde)

Streaming media este un material multimedia care este în permanență primit și prezentat unui utilizator final în timp ce este livrat de un furnizor.

Streaming-ul este o sabie cu două tăișuri. Pe de o parte, știința datelor și învățarea automată ne-au permis să găsim rapid videoclipurile pe care le considerăm relevante și informative. Cu toate acestea, hackerii și manipulatorii de social media au creat, de asemenea, videoclipuri false numite deepfakes.

Un deepfake înseamnă că un videoclip este modificat în așa fel încât să pară a fi un videoclip autentic. De exemplu, chipul unei persoane



într-un videoclip este schimbat cu chipul altcuiva. Datorită codificării, aceasta înseamnă că videoclipurile sunt foarte convingătoare și reale. Acest lucru permite hackerilor să controleze conversații naționale și dezbateri online. Este o înșelăciunea de cea mai bună calitate.

Ce puteți face? În videoclipurile care sunt suspecte sau par ireale, gândiți-vă de două ori. Verificați videoclipul pentru a vedea dacă există o lumină care nu este corectă sau dacă videoclipul nu este sincronizat. Multe videoclipuri deepfake sunt apropiate, dar nu exacte. De obicei, este ceva greșit pentru că nici algoritmii care creează aceste videoclipuri nu sunt perfecți.

Când aveți îndoieli, „săpați” mai adânc!

18. Atenție la acțiuni de caritate false pentru Coronavirus

Apar noi site-uri web care sunt în calitate de organizații de caritate înregistrat cu o combinație de cuvinte precum „alinare” sau „victime”.

Aceste cuvinte sunt menite să emane emoții ilicite din partea utilizatorilor. Multe dintre aceste domenii sunt dăunătoare și vor arunca software-ul pe computer pentru a-ți spiona conturile și activitatea web.

Ce poți face? Dacă aveți de gând să donați pentru ajutor de urgență, verificați toate organizațiile de caritate înainte de a face acest lucru. Faceți cercetări ample asupra potențialului organizației de caritate la care puteți face donații. Examinați înregistrările lor pentru a vedea recenziile lor și căutați documentații clare despre istoricul lor.

19. Ferește-te de huliganii cibernetici (Cyberbullies)

Atmosfera Internetului Wild West are Internet oferit și răufăcătorilor care pot găsi o nouă modalitate de a hărțui pe alții, postând în mod anonim informații răutăcioase. Uneori, aceste comentarii se pot transforma în acțiuni fizice și pot avea consecințe chiar în viața reală.

Ce poți face? Ca să te descurci cu un cyberbully, există o serie de lucruri pe care le puteți face. Limitați informațiile dumneavoastră personale astfel încât să le fie greu să vă facă rău sau să vă expună online.

Vă vor prezenta adesea pe Google sau vă vor căuta pe site-urile paginilor albe pentru a afla cine sunteți în viața reală și să vă posteze online pentru ca toți să vă vadă. Orice ai face, nu escalada situația răspunzând cu ostilitate. În cele din urmă, documentați-vă și înregistrați toată activitatea pe care o desfășurați. Acest lucru vă va ajuta cu acțiuni legale și raportare în cazul în care alegeți acest lucru.



20. Furtul de identitate

Milioane de oameni au fost afectați de furtul de identitate. Furtul informațiilor de identificare personală (**Personally Identifiable Information-PII**), cum ar fi datele de contact, documentele de călătorie și data nașterii oferă un număr util de modalități prin care ciberneticii pot câștiga bani. Când introduceți detalii în orice sistem informațional, riscați ca un hacker să vă fure informațiile și să le folosească pentru acțiuni frauduloase.

Ce puteți face? Evitați să dați PII decât numai dacă trebuie.

Este greu să stabilești cât de sigure sunt informațiile tale la bancă, la magazinul alimentar etc. Ai o singură identitate. Cu atât mai mult trebuie să o puteți proteja.

Monitorizați-vă creditul și pregătiți-vă să îl înghețați în orice moment.

21. Implementați autentificarea cu doi factori

De ce este important: autentificarea cu doi factori este un mecanism în care trebuie prezentate două tipuri diferite de informații pentru a avea acces la un cont. De exemplu, pentru a intra în contul dumneavoastră bancar, poate fi necesar să furnizați ca parolă și un cod special unic care este livrat de telefonul dumneavoastră (Mobile Token). Acest nivel suplimentar de securitate face dificilă compromiterea contului dumneavoastră chiar dacă parola proprie este listată undeva pe Dark Web.

Ce puteți face? Treceți peste toate aplicațiile și serviciile pe care le-ați utilizat, în special a celor legate de informațiile financiare. Verificați dacă fiecare dintre acestea are autentificare cu doi factori. Încercați să o activați pe cât mai multe aplicații. Este posibil să fie un inconvenient și să vă consume timp din ziua ta de muncă, dar merită să o faci pentru a nu avea probleme atunci când oprești un hacker în demersul lui distructiv.

Dincolo de autentificarea cu doi factori, există și cu trei sau patru factori de autentificare.

22. Aflați despre Scareware

Prin definiție, *scareware* care înseamnă înspăimântare, speriere sau înșelare, este un tip de malware care are scopul de a valorifica anxietatea utilizatorului.

Scareware face acest lucru prin lansarea unui mesaj terifiant care va amenința un utilizator să facă ceva împotriva interesului său. Cel rău va cere bani în schimb.



Ce poți face? Antivirusul este bun pentru scanarea tipului de amenințare.

Scareware este o amenințare cunoscută, iar companiile antivirus de renume au construit protecții împotriva acestui tip de amenințare. Asigurați-vă că accesați doar site-urile web de încredere și să nu vă fie frică. O mulțime de sperieturi au fost reutilizate de mai multe ori. Este posibil ca odată să o facă vulnerabilă.

23. Deconectați-vă frecvent!

Personal, poate vă place să rămâneți, uneori, conectat un timp prea lung. Este bine ca după ce să încheiați sesiunea de lucru să ștergeți datele de acreditare când a-ți terminat. Acest lucru vă ajută să restrângeți fereastra de atac pe care o are un hacker. De fapt, mulți hackeri folosesc deturnarea sesiunilor (credențiale stocate prea mult timp) ca o modalitate de a fura identitatea cuiva.

Ce puteți face? Deconectați-vă de orice servicii de care aveți nevoie numai atunci când sunteți în lucru, în special pentru informațiile financiare. Funcțiile de conectare automată care salvează conturile ar trebui să fie dezactivate. Indiferent dacă este pe laptop sau online, acest tip de funcții oferă atacatorilor un avantaj dacă închei lucrul prin a pierde controlul.

24. Mențineți comunicarea cu angajatorul

Acesta este mai mult, este mai mult pentru cei care lucrează de acasă. Dacă tot lucrați, cel mai bine este să nu vă izolați, să fiți în pas cu evoluțiile continue și modificările de politici de securitate. Evoluțiile inundă piața informaticii în fiecare minut.

Ce poți face? Elaborati o listă de contacte la locul de muncă și obțineți adrese e-mail, număr de telefon și alte date de contact. Păstrați o listă cu toate întrebările pe care le aveți. De exemplu, căutați clarificări cu privire la modul de înregistrare a orelor și a ceea ce este considerat lucru de la domiciliu. Aflați, de asemenea, cine este contactul desemnat pentru probleme specifice, cum ar fi problemele de asistență. Fiți la curent cu problemele IT care vă vor oferi un ritm bun de lucru, fără incidente de securitate.

Munca de la distanță, care poate dura mai mult decât s-a discutat inițial, poate extinde vulnerabilitatea atacului pe care un hacker îl poate exploata.



25. Nu toate VPN-urile sunt sigure

Rețelele private virtuale sau VPN-urile sunt o modalitate comună de a cripta un trafic pe Internet. Datorită necesității de a lucra de la domiciliu sau de a proteja informațiile, multe articole de știri sugerează utilizarea unei VPN (*Virtual Private Network*).

Problema este că nu toate VPN-urile sunt în siguranță, multe dintre ele fiind conduse de hackeri.

Ce puteți face? Dacă decideți să utilizați un VPN, asigurați-vă că a fost revizuit de alții. Unele dintre VPN-urile mai bune au sute de recenzii, chiar premii. Este necesar să plătiți pentru serviciile lor dacă doriți un serviciu de calitate.

26. Rețelele publice Wi-Fi sunt vulnerabile

Ori de câte ori vă conectați la un Wi-Fi¹⁴ dintr-o rețea publică, expuneți datele dumneavoastră altcuiva. Aceasta se poate întâmpla când se face telemuncă din locații străine. Spre deosebire de rețeaua proprie pe care o utilizați acasă, nu veți ști cine se conectează la o rețea publică anume la un moment dat. Hackerii pot să se amestece în conexiune și să vă fure informațiile.

Ce puteți face? În general, evitarea rețelelor publice este cel mai bun mod de a proceda. Pur și simplu nu aveți suficient control asupra lor nu știți ce se întâmplă. Cu toate acestea, dacă sunteți obligat să vă conectați la unul dintre ele, cel mai bine este să nu accesați site-uri web sensibile la identitatea dumneavoastră online (servicii bancare online, conturi de socializare etc.). Dezactivați partajarea fișierelor și asigurați-vă că vă deconectați din toate conturile când ați terminat.

27. Scanați fișierele noi

Am precizat acest lucru cu atașamente de e-mail, dar aceeași preocupare se extinde și la toate noile fișiere pe care le primiți în sistemul dvs. Ar putea fi de pe Internet, dar ar putea fi și de pe o unitate USB sau CD. Toate fișierele noi ar trebui să parcurgă același proces.

Ce puteți face? Imediat ce obțineți un fișier nou, izolați fișierul și scanați-l. Dacă descărcați și utilizați instrumentele de securitate, atunci puteți face *clic dreapta* pe fișier și *scan*. Asigurați-vă că software-ul

¹⁴ *Wi-Fi* este o tehnologie radio folosită deseori la implementarea rețelelor locale de calculatoare de tip rețea locală fără fir (*Wireless Local Area Network, WLAN*).



dumneavoastră antivirus este actualizat pentru a vă asigura că este eficient la detectarea semnăturilor malware cunoscute.

Mai bine în siguranță decât să vă pară rău!

28. Opriți răspândirea dezinformării

Toți suntem bombardați cu informații și dezinformare.

Ce puteți face? Fiți gata să semnalizați, să notați și să le spuneți și altora despre aceste informații inexacte de pe Internet. Transmiteți informațiile periculoase canalelor corespunzătoare (autorităților) pentru a vedea dacă se pot lua măsuri. Există o mulțime de companii din sectorul privat care vă vor răspunde rapid și vă vor prelua cu ușurință informațiile dumneavoastră. Gândiți-vă la voluntariatul online sau apelând la unele organizații pentru a vă oferi asistența.

29. Pregătiți-vă și instruiți-vă în domeniul securității informatice

În timp ce poate părea o formare de sensibilizare în materie de securitate, pregătirea reprezintă un adevărat beneficiu pentru dumneavoastră. Pregătirea vă crează fundamentul pentru combaterea acestor amenințări. Există întotdeauna o nouă tendință apărând în lupta pentru cibersecuritate și ar trebui să le luați în serios atunci când apar.

Ce puteți face? Căutați online companii și furnizori de renume care oferă instruire de sensibilizare. O mulțime de antrenamente sunt oferite gratuit, mai ales cu mai mulți „studenți” acasă. Gândiți-vă la timpul pe care îl puteți dedica și dacă se potrivește nivelului dumneavoastră de cunoștințe. Alege unul sau două cursuri de formare comparându-le pe ambele pentru a afla cele mai bune practici de care ai nevoie.

30. Luați un Manager de parolă

Un manager de parole este un alt instrument pe care îl puteți descărca pentru a vă ajuta să urmăriți toate parolele pe care le utilizați.

Cu toate acestea, nu este o soluție completă și finală. Utilizatorii vor avea pe parcursul vieții sute de parole. Managerii de parole își organizează parolele și îi eficientizează conturile.

Ce puteți face? Examinați instrumentele gratuite și plătite de managerii de parole. Gama gratuită nu va oferi numărul de funcții solide pe care le-ați plătit, dar le veți putea obține rapid și nu vi se va sparge contul bancar.



Companiile de administrare a parolelor au adesea o opțiune gratuită disponibilă. Folosiți ce credeți că este potrivit pentru dumneavoastră.

Managerii de parole sunt și ei vulnerabili.

Nu puneți niciodată toate ouăle într-un singur coș!

31. Avertizați-i și pe alții

Din când în când, este posibil să vedeți că ceva este suspect online. În timp ce s-ar putea să nu-i cădeți victimă, așteptați-vă ca și alții să fie în pericol. Sunteți în măsură să faceți diferența.

Ce puteți face? Raportați orice credeți că este suspect pe canalul adecvat. Dacă a sosit prin e-mail, raportați-l furnizorului de e-mail. Dacă este prin intermediul rețelelor de socializare, raportați-l companiei tehnologice care administrează serviciul respectiv. Mai bine în siguranță decât să vă pară rău.

Miliarde de înregistrări au fost furate și compromise. Acest număr va continua să crească pe măsură ce dependența de Internet crește.

32. Urmăriți prețurile

Multe bunuri și servicii care au fost cândva ușor disponibile acum au devenit rare. Acest lucru a creat o piață cu practici de preț supraumflate. Unii vânzători (jefuitori), în pandemie, vând hârtie igienică, mănuși și măști de protecție,...., dezinfectanți cu prețuri înzecite.

Datorită acestei dinamici, hackerii care au site-uri de configurare vor încerca să ademenească cumpărătorii cu mărfuri care nu există. Acestea se numesc escrocherii *nondelivery* (nedistribuibile).

Ce puteți face? Cercetați toate site-urile web înainte să intrați în aceste informații de oferte. Este o opțiune sigură să mergeți doar la furnizorii de la care ați mai cumpărat și altădată și în care aveți încredere. Cred că știți că unii dintre acești vânzători suspecți nu pot livra niciodată bunurile pe care le căutați pentru că, de fapt, nici nu le au.

33. Când puteți, încurajați obiceiurile bune, nu ezitați!

Învățați multe lucruri interesante din acest articol și din experiențele dumneavoastră. Dacă aveți o mulțime de cunoștințe pentru a le oferi altora, ajutați-i și pe alții să beneficieze de asta.

Ce puteți face? Când discutați cu alții despre cum să fiți mult mai siguri privind protecția informațiilor, vedeți dacă există ceva cu care îi puteți ajuta sau puteți fi ajutat. Nu vă fie teamă să le oferiți câteva dintre sfaturile din acest articol.

Cunoașterea este putere!



Concluzii

Urmând sfaturile prezentate în acest ghid de supraviețuire, este posibil să rămâneți neafecțați în fața hackerilor și să le zădărniciți acțiunile înainte să aibă chiar o șansă de a vă penetra rețeaua.

La nivel național, în deplin acord cu acțiunile europene, a fost aprobată, în februarie 2015, *Strategia Națională privind Agenda Digitală pentru România 2020*¹⁵, care definește patru domenii de acțiune dintre care amintesc doar primul domeniu, care este: e-Guvernare, Interoperabilitate, *Securitate Cibernetică*, Cloud Computing și Social Media.

Indiferent dacă este vorba despre amenințări cibernetice generale sau amenințări cibernetice cu teme „Corona”, puteți avea liniștea sufletească de care aveți nevoie pentru a putea lucra în continuare și să aveți încrederea de care aveți nevoie pentru a supraviețui în aceste timpuri în schimbare.

Pentru domeniul securității și apărării naționale, conform aprecierilor unor specialiști militari contemporani, exprimate într-o lucrare de specialitate, „*pe lângă lipsa frontierelor, la nivelul noului mediu de manifestare al societății umane, se suprapun alte caracteristici, precum anonimatul acțiunilor întreprinse, lacunele legislative și nu în ultimul rând posibilitatea desfășurării de activități și acțiuni în mediul virtual permanent, din orice loc, nefiind condiționate de o prezență fizică sau de disponibilitatea unor resurse financiare și tehnice majore*”¹⁶.

Aceste recomandări vă pot ajuta direct. Astfel veți fi pregătiți în avans. Asta pentru că veți avea un software actualizat care va scana amenințările pe măsură ce „inamicii” vor încerca să intre în sistemul dumneavoastră. Calculatorul pe care îl utilizați va detecta protecția anti-spyware și anti-virus pentru a face carantină și să izoleze fișierele care sunt vizate a fi afectate.

Veți ezita să vă oferiți informațiile personale și financiare altora. Identitatea pe care o aveți este valoroasă, iar furtul de identitate este ceva de care veți fi mereu avertizat să fiți vigilent.

¹⁵ *Strategia Națională privind Agenda Digitală pentru România 2020* a fost aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.

¹⁶ Gheorghe BOARU, Benedictos IORGA, *op.cit.*, p. 239.



Nu vă veți teme când aveți de-a face cu un e-mail, deoarece știți diferitele moduri în care hackerii vă pot afecta. Fie că va fi prin suliță phishing, link-uri încorporate și fișiere dăunătoare, sunteți avertizat că sunteți în fața unei amenințări.

Astfel veți avea capacitatea de a-i ajuta pe ceilalți colegi la timpul potrivit dacă au nevoie.

Indiferent dacă este vorba de consiliere și raportare de știri false, sunteți înarmați cu informațiile necesare pentru a identifica manipularea.

Și poate cel mai important dintre toate, veți fi inspirat să aflați mai multe despre cibersecuritate. Opinia dvs. despre tehnologie și apreciere pentru aceasta a crescut și a câștigat toate acestea într-un mod rapid și concis. În acest mod veți fi mulțumit că ați făcut Internetul mai sigur, și că într-o situație critică puteți face diferența – în favoarea securității informațiilor cu care operați.

Consider că experții noștri (civili și militari), trebuie să găsească cele mai potrivite căi de exploatare a capacităților proprii dezvoltate, specifice războiului, pentru utilizare în cibernetică, precum și tehnologia și doctrinele necesare pentru a ne apăra împotriva atacurilor cibernetice.

După opinia președintelui Consiliul de revizuire a investițiilor străine David Irvine BA (Hons)¹⁷, ..., *Răspunsul la amenințările cibernetice va fi complicat, nu în ultimul rând, deoarece profilaxia rămâne inevitabil inventivitatea celor care folosesc Internetul pentru a face rău.*

Acesta va implica soluții tehnice sofisticate pentru a ne proteja dispozitivele cibernetice conectate împotriva infiltrărilor și a activității dăunătoare; aceasta va implica schimbări culturale sau de comportament în modul în care reacționăm la amenințările din spațiul cibernetic; aceasta va implica legislație care să forțeze industria și furnizorii de servicii informatice să protejeze atât confidențialitatea, cât și viabilitatea infrastructurii critice care acum depinde de spațiul cibernetic”¹⁸.

¹⁷ David Irvine BA (Hons)- Președinte al Consiliului de revizuire a investițiilor străine, AO (din 2017), Director general la Organizația australiană de informații de securitate (2009–2014), Director general la Serviciul Secret de Informații Australian (2003–2009).

¹⁸Henry Prunckun, *Cyber Weaponry - Issues and Implications of Digital Arms*, Series: Advanced Sciences and Technologies for Security Applications, Publisher: Springer International Publishing, Year: 2018, p. VIII.



Trebuie să dedicăm mai mult efort intelectual pentru a analiza impactul acestei tehnologii, vulnerabilitățile pe care le creează și modalitatea optimă de atenuare a vulnerabilităților. Acest efort intelectual trebuie să se îndrepte și către dimensiunile etice și morale și obligațiile organelor abilitate ale statului de a proteja intimitatea și siguranța cetățenilor săi împotriva catastrofelor ce pot fi produse de atacatorii cibernetici

Bibliografie

1. * * * Hotărârea nr. 271/2013 pentru aprobarea *Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013.
2. * * * *Strategia Națională privind Agenda Digitală pentru România 2020*, aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.
3. Col. (ret.)
prof.univ. dr.
Gheorghe Boaru *Securitatea cibernetică în Uniunea Europeană*, Revista Academiei de Științe ale Securității Naționale, nr. 2/2017.
4. Col. (r.) prof.
univ. dr.
Gheorghe
BOARU *RĂZBOIUL INFORMAȚIONAL – UN OBIECTIV AL SECURITĂȚII NAȚIONALE*, Revista Academiei de științe ale Securității Naționale nr.2/2019.
5. Gheorghe
Boaru,
Iulian Marius
Iorga *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare „Carol I”, București, 2018.
6. Gheorghe
BOARU,
Benedictos
IORGA *IMPLICAȚIILE PARTICIPĂRII FORȚELOR MILITARE ROMÂNEȘTI LA OPERAȚIILE DE TIP COALIȚIE, ASUPRA EVOLUȚIEI ȘI DEZVOLTĂRII SISTEMULUI MILITAR NAȚIONAL DE COMUNICAȚII ȘI INFORMATIC*, Editura SITECH, Craiova, 2020.
7. Ben Buchanan *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Publisher: Harvard University Press, Year: 2020.



8. Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler
Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment, Publisher: Apress, Year: 2020.
9. Aditya Gupta
The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, Publisher: Apress, Year: 2019.
10. Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdzadeh Farhad Norouzi
Towards the Internet of Things: Architectures, Security, and Applications, Series: EAI/Springer Innovations in Communication and Computing, Publisher: Springer International Publishing, Year: 2020.
11. Alexander Klimburg
National Cyber Security-Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), Publication, Tallinn, 2012.
12. Jim Kou
Hacking: The Practical Guide to Become a Hacker / Field Manual for Ethical Hacker Including Ethical Hacking with Kali Linux, Publisher: Independently published, Year: 2019.
13. Huimin Lu
Cognitive Internet of Things: Frameworks, Tools and Applications, Series: Studies in Computational Intelligence 810, Publisher: Springer International Publishing, Year: 2020.
14. Srikanta Patnaik
New Paradigm Of Industry 4.0: Internet Of Things, Big Data & Cyber Physical Systems, Series: Studies In Big Data Vol. 64, Publisher: Springer, Year: 2020.
15. Sheng-Lung Peng, Souvik Pal, Lianfen Huang
Principles Of Internet Of Things (IoT) Ecosystem: Insight Paradigm, Series: Intelligent Systems Reference Library Vol. 174, Publisher: Springer, Year: 2020.
16. Henry Prunckun
Cyber Weaponry - Issues and Implications of Digital Arms, Series: Advanced Sciences and Technologies for Security Applications, Publisher: Springer International Publishing, Year: 2018.
17. Vinny Troia
Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques, Publisher: Wiley, Year: 2020.



18. LEVI WEST *The Coronavirus Cybersecurity-Survival Guide-Top
Tips to Protect You From A Cyber Attack*, 2020.
19. * * * https://www.academia.edu/21702040/Legile_Lui_Murphy.
20. * * * <https://ro.wikipedia.org/wiki/Hacker>.



LIDER ȘI LEADERSHIP MILITAR

LEADER AND MILITARY LEADERSHIP

Col. (r.) prof.univ.dr. Ion MITULEȚU

Membru titular al Academiei de Științe ale Securității Naționale,

E-mail: mituletuion@yahoo.com.

Rezumat: Mediul de securitate actual, multidimensional, înalt tehnologizat, interconectat și interdependent, marcat de amenințări difuze care generează instabilitate, dezechilibre și surprize strategice, determină schimbări de paradigmă în abordarea conceptelor de lider și leadership militar.

La modul general, liderul militar este persoana vizionară care dispune de pregătirea, experiența, competența și abilitatea de anticipare, inovare, motivare și mobilizare a subordonaților în vederea îndeplinirii unui scop (obiectiv, misiune).

Leadershipul poate fi abordat ca sistem, relație și artă în cadrul organizației militare și presupune abilitatea de a conduce, bazată pe creativitate, inovație, convingeri și motivații, precum și pe capacitatea de a mobiliza și influența subordonații în îndeplinirea unor obiective comune.

Domeniile de valorificare a competențelor liderului militar sunt: conceptual, organizatoric; pregătirea personalului de conducere și instruirea forțelor; integrarea tehnologiilor performante în structura forțelor; susținerea acțiunilor militare.

Rolul leadershipului performant în procesul operației militare vizează planificarea, pregătirea, executarea și evaluarea acesteia.

Pentru prevenirea și contracararea crizelor și conflictelor potențiale din mediul operațional multidimensional este nevoie de lideri militari vizionari, creativi și competenți, precum și de un leadership performant, orientat către oportunități.

Cuvinte cheie: lider militar, cultură organizațională, leadership vizionar, leadership participativ, leadership orientat către oportunități, procesul operației militare.

Abstract: The current security environment, which is multidimensional, high-tech, interconnected and interdependent, is marked by diffuse threats that generate instability, imbalances and strategic surprises which generate paradigm shifts in approaching the concepts of leader and military leadership.

Generally speaking, the military leader is a visionary person, who has the training, experience, competence and ability to anticipate, innovate, motivate and mobilize subordinates in order to achieve a goal (objective, mission).



Leadership can be approached as a system, relationship and art within the military organization and involves the ability to lead, based on creativity, innovation, beliefs and motivations, as well as on the ability to mobilize and influence subordinates in achieving common goals.

The domains of valorization of the competences of the military leader are: conceptual and organizational the training of the management personnel and the training of forces; integrating high-performance technologies into the force structure; supporting military actions.

The role of effective leadership in the process of military operation is aimed at its planning, preparation, execution and evaluation.

In order to prevent and counteract potential crises and conflicts in the multidimensional operational environment, visionary, creative and competent military leaders as well as high performance-oriented leadership are needed.

Keywords: *military leader, organizational culture, visionary leadership, participatory leadership, opportunity-oriented leadership, military operation process.*

Abordări teoretice

Mediul de securitate actual, multidimensional, înalt tehnologizat, interconectat și interdependent, marcat de amenințări difuze care generează instabilitate, dezechilibre și surprize strategice, determină schimbări de paradigmă în abordarea conceptelor de lider și leadership militar.

În acest context, cunoașterea și înțelegerea complexității mediului de securitate, precum și necesitatea transformării relativismului în oportunitate în procesul decizional, impun o abordare pragmatică a procesului de formare, pregătire și dezvoltare a unei noi generații de lideri militari vizionari, competenți și motivați, capabili să desfășoare un leadership performant în tot spectrul crizelor și conflictelor potențiale.

Atitudinile, aptitudinile, deprinderile și competențele liderului militar sunt potențate numai în interiorul unei organizații (structuri militare) care dispune de acea cultură ce descrie caracterul unui grup de oameni, modul de gândire și de acțiune a acestora¹.

Astfel, cultura organizațională trebuie privită ca un sistem de interacțiuni și comportamente interumane, bazat de comunicare, încredere și

¹ Simon Sinek, *Liderii mănâncă ultimii: de ce unele echipe lucrează bine împreună, iar altele nu*, Editura Publică, Ediția a 2-a Rev, București, 2017, p. 207.



cooperare, unde liderul militar motivează și influențează subordonații în materializarea viziunii sale.

În acest sens, la modul general, apreciem că *liderul militar* este persoana care dispune de pregătirea, experiența și capacitatea de anticipare, inovare, motivare și mobilizare a subordonaților în vederea îndeplinirii unui scop (obiectiv, misiune).

În sens restrâns, liderul militar este persoana care acționează proactiv în toate situațiile, dispune de abilitatea de a crea o viziune și are capacitatea de a motiva și inspira subordonații în materializarea acesteia.

Acest lucru presupune din partea liderului să manifeste empatie, încredere și responsabilitate în relațiile cu subordonații pentru realizarea viziunii sale, contribuind astfel la dezvoltarea unei culturi credibile în cadrul organizației militare.

Atitudinea liderului în relațiile interumane este potențată de prestigiul personal de care dispune în interiorul și exteriorul organizației².

Liderii militari trebuie să aibă capacitatea de a lucra în echipă și de a armoniza interesele acesteia, de a-și asuma riscuri și a fi responsabili în toate situațiile, de a recunoaște valoarea celorlalți și de a le stimula inițiativa. În acest sens, liderul trebuie să dispună de aptitudinile și competențele necesare pentru a înțelege, anticipa și vizualiza acțiunile organizației militare în vederea gestionării noilor provocări existente în mediul operațional.

Rezultă faptul că, esența activităților și acțiunilor liderului are la bază generarea condițiilor necesare, la nivel decizional, uman și tehnic, care să garanteze succesul organizației militare în îndeplinirea misiunilor, realizarea efectelor și a obiectivelor stabilite.

În prezent, apariția unor mutații bruște și neanticipate în mediul de securitate, precum și dezvoltarea componentei informaționale și cibernetice, produc transformări asupra liderului militar privind cunoașterea și aplicarea unor metode moderne de leadership în procesul decizional.

Leadershipul înseamnă abilitatea de a conduce sau arta conducerii, bazată pe convingeri și motivații, precum și capacitatea de a mobiliza subordonații la desfășurarea unei activități.

² Gustave Le Bon, *Psihologia mulțimilor*, Editura Anima, București, 1937, p. 77.



În acest sens, leadershipul generează schimbare prin creativitate și inovație, realizându-se în cadrul unui grup motivat, care acceptă îndeplinirea unor obiective comune.

Leadershipul poate fi abordat în trei ipostaze: *proces*; *relație*; *artă*.

În primul rând, leadershipul constituie un *proces* prin care o persoană poate influența un grup de indivizi în realizarea unui obiectiv comun³.

Leadershipul reprezintă capacitatea de a determina persoanele din cadrul unei organizații să acționeze, aflându-se în relație directă cu capacitatea de a influența comportamentul oamenilor⁴.

În al doilea rând, leadershipul este o *relație* între un lider și subordonați, caracterizată prin încredere reciprocă și se manifestă prin capacitatea acestuia de a coagula și mobiliza energiile în jurul unei acțiuni colective⁵.

În al treilea rând, leadershipul este *artă* bazată pe știință, care generează stiluri de conducere moderne și cuprinde principii, metode și procedee specifice, alături de abilitățile liderului bazate pe viziune, creativitate, charismă, prestigiu, comunicare verbală și deschidere la nou.

Din ansamblul teoriilor și modelelor abordate în lucrările de specialitate, vom analiza următoarele tipuri de leadership militar: transformățional; bazat pe valori; vizionar; participativ; în era digitală; orientat către oportunități.

Leadershipul militar transformățional presupune un grad ridicat de motivare a subordonaților, bazat pe inspirație, stimulare și înțelegere a comportamentului uman, în scopul îndeplinirii cu randament maxim a unor obiective comune⁶.

În acest sens, calitățile liderului militar, bazate pe charismă, motivație, stimulare intelectuală și prestigiu individual, coroborate cu nivelul culturii organizaționale, generează un leadership transformățional

³ <http://onisimbn.ro/sinoiputem/assets/rolul-leadershipului.pdf>, accesat la data de 12.03.2020.

⁴ *Ibidem*.

⁵ buzdugan.com.ro/blogmanagement/?p=2172, accesat la data de 03.03.2020.

⁶ Dr. Constantin Moștoflei, dr. Petre Dușu, *Liderul militar în România*, București, Editura Universității Naționale de Apărare „Carol I”, 2007, pp. 38-39.



performant, orientat către crearea unei viziuni, acceptată și realizată de subordonați.

Leadershipul militar bazat pe valori are în vedere respectarea legilor, principiilor, intereselor și obiectivelor care reglementează activitățile desfășurate în Armata României.

Astfel, valorile care trebuie respectate vizează responsabilitatea, capacitatea de integrare în mediul militar și de adaptare la riscuri, amenințări și vulnerabilități⁷.

De aceea, leadershipul militar bazat pe valori presupune un grad înalt de coeziune în cadrul organizației, o conduită ireproșabilă, respectarea elementelor specifice eticii și prezervarea intereselor de securitate în toate situațiile.

Leadershipul militar vizionar motivează și convinge subordonații să participe activ la respectarea unor principii și idealuri comune.

La baza acestui tip de leadership stă viziunea, motivația și dinamismul personal al liderului.

De asemenea, leadershipul militar vizionar se bazează pe gândire strategică și sistemică, viziune multilaterală, spirit de colaborare, adaptabilitate și autocunoaștere⁸.

Numai prin aceste caracteristici, leadershipul militar vizionar capătă coerență în elaborarea unor documente ce includ scenarii și ipoteze de lucru, în cadrul cărora sunt anticipate fenomenele specifice și determinate tendințele și perspectivele evoluției acestora.

Leadershipul militar participativ presupune implicarea într-o măsură mai mare sau mai mică a subordonaților în luarea deciziilor.

De regulă, liderii militari asigură un leadership participativ prin consultarea subordonaților și evaluarea opiniilor acestora în procesul de planificare a operațiilor.

Totodată, acest tip de leadership presupune participarea membrilor organizației la procesul de luare a deciziei prin consultarea acestora și acceptarea ideilor și expertizei lor⁹.

⁷ Dr. Constantin Moștoflei, dr. Petre Duțu, *Op.cit.*, pp. 40-41.

⁸ <https://leaders.ro/modelul-de-leadership/>, accesat la data de 12.03.2020.

⁹ <https://virtualboard.ro/teorii-de-leadership-participativ-situational/>, accesat la data de 12.03.2020.



Astfel, lucrul în echipă în cadrul comandamentelor, estimarea compartimentelor în diferitele faze ale planificării, formularea unor cursuri de acțiune care sunt evaluate și comparate, propunerea cursului de acțiune care îndeplinește condițiile considerate a fi optime în vederea formulării deciziei de către comandant, constituie elemente ale unui stil participativ de leadership militar.

Totodată, leadershipul militar participativ vizează delegarea unor atribuții și responsabilități către subordonați pe termen scurt, mediu sau lung.

Leadershipul militar în era digitală are în vedere dezvoltarea fără precedent a tehnologiilor informaționale și cibernetice, integrate și interconectate în cadrul structurilor militare.

În acest sens, era digitală crează noi modele de leadership bazat pe inovare, capacitate de analiză, originalitate, viziune, putere de decizie, comunicare, intuiție și responsabilitate.

Leadershipul militar orientat către oportunități reprezintă corolarul celorlalte forme de leadership, deoarece presupune dezvoltarea unor abilități de adaptare la mediul de securitate, de anticipare și prevedere a evoluției fenomenelor militare.

Astfel, leadershipul militar trebuie să aplice un diagnostic corect fenomenului respectiv, să identifice amenințările și vulnerabilitățile, să anticipeze și să determine tendințele de evoluție și, pe această bază, să formuleze opțiunile de răspuns care să fie credibile, flexibile și oportune.

Leadershipul orientat către oportunități stimulează performanța și dezvoltă cultura organizației militare¹⁰.

De aceea, apreciem că leadershipul militar bazat pe oportunități este cea mai flexibilă formă de leadership, perfect adaptabil, rezilient și eficient în arta conducerii, planificarea operațională și procesul de luare a deciziei.

Aceste abordări teoretice constituie motivația pentru evaluarea domeniilor de valorificare a competențelor liderului militar și a rolului leadershipului în procesul operației militare.

¹⁰ <https://www.srac.ro/ro/stiri/semnificatia-rolul-si-importanta-leadership-ului-cadrul-noilor-standarde-pentru-sistemele-de>, accesat la data de 12.03.2020.



Domenii de valorificare a competențelor liderului militar

Liderii militari își manifestă gradul de competență în funcție de locul pe care îl ocupă în cadrul sistemului de apărare, la nivel strategic, operativ, respectiv tactic.

În acest sens, vom detalia domeniile de valorificare a competențelor liderului militar la nivel strategic, pentru a identifica și dezvolta conceptele care definesc securitatea și apărarea națională.

Modalitatea în care vor fi valorificate domeniile de competență ale liderului militar la nivel strategic se bazează pe următoarea schemă logică: lider competent – oameni motivați și mobilizați – utilizarea tehnologiei informaționale și cibernetice – exploatarea caracteristicilor sistemelor de armamente și echipamentelor militare moderne – leadership performant – misiuni îndeplinite – obiective realizate.

În acest context, vor fi abordate sintetic domeniile de valorificare a competențelor liderului militar în scopul creșterii rezilienței în desfășurarea unui leadership performant care să asigure perfecționarea sistemului de apărare.

Domeniile în care liderul militar este pregătit pentru valorificarea competențelor dobândite sunt: *conceptual; organizatoric; pregătirea personalului de conducere și instruirea forțelor; integrarea tehnologiilor performante în structura forțelor; susținerea acțiunilor militare*¹¹.

La nivel *conceptual*, liderul militar participă la dezvoltarea, armonizarea și adaptarea cadrului normativ la realitățile și nevoile organismului militar, în condițiile existenței unui mediu operațional fluid, incert și imprevizibil. Totodată, un lider cu experiență, viziune, imaginație și inițiativă, înțelege imperativele momentului privind necesitatea dezvoltării conceptelor specifice contracarării noilor forme de conflict (neconvențional, asimetric, non-cinetic și hibrid).

Un alt element important vizează capacitatea liderului de a dezvolta procesul de implementare a standardelor NATO în cadrul structurilor proprii și de participare la asigurarea interoperabilității în acțiunile militare.

Pentru a elabora o concepție credibilă în domeniul apărării, liderul militar vizionar identifică raporturile ce se stabilesc între amenințări și opțiunile de răspuns, între utilizarea mijloacelor hard și soft, între

¹¹ *Strategia militară a României*, București, 2016, pp. 9-10.



înțelegerea mediului operațional multidimensional și capabilitățile necesare modelării spațiului de luptă, proiectării și angajării forțelor.

În acest sens, liderul militar, prin capacitatea de gândire și reflecție, își valorifică experiența, viziunea și creativitatea în identificarea oportunităților care să conducă la elaborarea unor strategii inteligente și a unor doctrine militare novatoare.

Aceste documente instituționale sprijină liderul în identificarea priorităților, stabilirea obiectivelor, motivarea subordonaților și anticiparea evoluției fenomenului militar, în vederea participării la elaborarea unor scenarii și ipoteze strategice prin care sunt stabilite capabilitățile necesare și dezvoltate variantele de acțiune ale forțelor în diferite situații operative.

Scenariile și ipotezele strategice presupun din partea liderului prevedere, analiză și responsabilitate în orientarea subordonaților, în scopul elaborării planurilor operaționale de întrebuințare a forțelor în acțiunile militare.

Un rol important al liderului militar se manifestă în modul în care reușește să motiveze echipa de specialiști în înțelegerea intenției și viziunii sale, în vederea elaborării planurilor de contingentă și a celor militar-strategice.

Planul de contingentă are la bază situații ipotetice din zona de interes strategic, fiind dezvoltat la un nivel suficient care să permită evaluarea tipului prognozat de operație și identificarea naturii și dimensiunii capabilităților necesare.

Planul militar-strategic este destinat gestionării unei crize posibile în plan național sau la nivel NATO, prin intervenția forțelor destinate apărării naționale sau colective.

Această abordare pragmatică permite aprecierea faptului că, liderul este un creator de plusvaloare operațională și formator al altor lideri, capabili să înțeleagă și să dezvolte domeniul militar la nivel conceptual¹².

La nivel *organizatoric*, liderul își poate valorifica competențele prin implicarea creativă și inovativă în dezvoltarea și perfecționarea structurii de forțe, având la bază principiile stipulate în documentele instituționale care reflectă concepția de apărare în context național și multinațional.

Astfel, apreciem faptul că, liderul militar trebuie să dispună de viziune, competență organizațională și de abilitatea de a crea o echipă pentru

¹² <https://www.danieltanase.com/lider/>, accesat la data de 12.03.2020.



a putea coordona utilizarea unor metode științifice de proiectare, dezvoltare și perfecționare a structurilor de forțe¹³.

În acest sens, liderul militar vizionar, care are abilitățile necesare pentru motivarea și inspirarea subordonaților, poate concepe arhitectura organizatorică a structurii de forțe în următoarea manieră mixtă: *pe bază de riscuri, amenințări și vulnerabilități; în raport de capabilități; orientată către oportunități.*

În prima categorie, structurile de forțe trebuie concepute, dimensionate și dezvoltate pentru a răspunde eficient la toată gama amenințărilor din mediul de securitate.

Abilitatea liderului militar de a conduce echipa în proiectarea structurii de forțe care să răspundă eficient amenințărilor, constă în capacitatea acestuia de a identifica tendințele și evoluțiile mediului de securitate pentru a sesiza situațiile în care apar mutații bruște și neanticipate generatoare de surprize strategice.

În acest sens, liderul militar orientează echipa către proiectarea unor *structuri de nucleu* care să fie completate în situația apariției unor amenințări inedite, pentru a fi evitată producerea unor surprize strategice.

Privind a doua categorie, structurile de forțe trebuie concepute, dimensionate și dezvoltate pentru a asigura capabilitățile necesare gestionării și soluționării oricăror situații cu potențial de risc care pot crea vulnerabilități în mediul de securitate.

În acest context, liderul militar direcționează echipa în sensul identificării și proiectării acelor capabilități care să integreze forțele și mijloacele necesare desfășurării operațiilor militare în spectrul complet.

În a treia categorie, structurile de forțe trebuie concepute, proiectate și dezvoltate având în bază criteriul orientării către oportunități.

În acest sens, liderul militar identifică oportunitățile din mediul de securitate, stabilește prioritățile, anticipează tendințele și orientează echipa către proiectarea unor structuri de forțe mobile, flexibile și adaptate, capabile să afere un răspuns eficient la crizele și conflictele potențiale.

Totodată, identificarea oportunităților oferă motivarea stabilirii *pachetelor de forțe* destinate participării la operațiile multinaționale în context aliat sau în cadrul unor coaliții.

¹³ <http://mihaicurteanu.blogspot.com/2014/09/ce-inseamna-leadership-si-care-sunt-calitatele-unui-leader.html>, accesat la data de 12.03.2020.



Privind *pregătirea personalului de conducere și instruirii forțelor*, liderul militar își valorifică experiența, cunoștințele și competențele în vederea regândirii și implementării documentelor privind instruirea forțelor în Armata României în consens cu prevederile NATO în domeniu.

În acest sens, liderul militar vizionar direcționează echipa în sensul elaborării unui program multianual de pregătire a personalului de conducere și instruire a forțelor, astfel încât, pe termen mediu să se desfășoare toată gama exercițiilor în mediul operațional extins, în context național și multinațional.

Având în vedere noile forme de manifestare a conflictelor, liderul militar identifică prioritățile și oportunitățile de pregătire a comandamentelor și de instruire a forțelor, punând accentul pe desfășurarea unor exerciții complexe la nivel înrunit, integrat și multinațional, în mediul operațional extins.

În funcție de tipologia scenariilor și ipotezelor strategice elaborate, liderul militar direcționează echipa în planificarea unor exerciții care să aibă ca scop verificarea capacității comandamentelor și nivelului instruirii forțelor în operațiile neconvenționale, asimetrice, non-cinetice și hibride.

Totodată, liderul militar își valorifică abilitățile și competențele în modul în care motivează, convinge și influențează activitatea echipei în elaborarea documentelor de conducere a exercițiilor și în asigurarea desfășurării eficiente a acestora pentru îndeplinirea misiunilor și realizarea scopurilor de către structurile implicate.

Având în vedere importanța care se acordă instruirii prin simulare, liderul militar trebuie să fie antrenat să-și folosească creativ experiența în planificarea, pregătirea și desfășurarea exercițiilor de acest tip în diverse situații operative, cu structura de forțe desemnată.

La finalizarea unui ciclu de pregătire a comandamentelor și instruire a forțelor, liderul militar trebuie să dispună de abilitatea și competența de a desprinde și valorifica lecțiile învățate rezultate din desfășurarea exercițiilor la nivel național și multinațional.

Privind *integrarea tehnologiilor performante în structura forțelor*, liderul militar trebuie să dispună de cunoștințele și competențele necesare pentru a orienta subordonații în înțelegerea locului și rolului sistemelor și armamentelor moderne și infrastructurii informaționale în cadrul organizației militare, precum și a modului de exploatare a acestora pentru obținerea succesului în îndeplinirea misiunilor.



În acest sens, liderul își valorifică abilitățile și competențele profesionale în motivarea subordonaților pentru înțelegerea avantajelor integrării tehnologiilor moderne în cadrul structurii de forțe și dezvoltarea deprinderilor acestora de a le exploata judicios, asigurând astfel, condițiile necesare pentru obținerea superiorității informaționale, decizionale și în plan acțional în desfășurarea eficientă a acțiunilor militare.

O problemă importantă care trebuie să fie mereu în atenția liderului militar vizează modul în care vor fi dezvoltate sistemele de comandă și control prin integrarea și interconectarea tehnologiei informaționale, care să asigure desfășurarea unui proces decizional colaborativ, oportun și credibil.

Privind *susținerea acțiunilor militare*, liderul trebuie să fie preocupat în permanență pentru îmbunătățirea înzestrării structurii de forțe cu sisteme de armamente, echipamente de luptă și materiale performante.

De asemenea, trebuie să înțeleagă necesitatea achiziționării și înzestrării forțelor cu armamente și echipamente militare compatibile și interoperabile cu cele existente în cadrul NATO, pentru a desfășura în comun exerciții și misiuni de luptă, în context multinațional.

Un lider militar competent și responsabil formulează cerințe operaționale, convinge și conștientizează subordonații să acționeze pentru achiziționarea și înzestrarea structurii de forțe cu sisteme și echipamente militare performante, precum și cu tehnologii informaționale, care să asigure îndeplinirea cu succes a misiunilor la nivel național și multinațional.

Rolul leadershipului în procesul operației militare

Leadershipul înseamnă creativitate și inovație, precum și abilitatea de a conduce o structură de forțe prin viziune, convingere și influențare în vederea atingerii unui obiectiv comun.

Totodată, leadershipul reprezintă arta de a conduce oameni prin utilizarea unor metode de convingere, folosind mijloace necoercitive, având ca finalitate îndeplinirea obiectivelor stabilite în comun.

Rezultă de aici o îmbinare a stilurilor de conducere a unei structuri de forțe folosind un leadership vizionar, participativ și orientat către oportunități.

În acest context, apreciem rolul important al leadershipului în procesul operației militare care vizează *planificarea, pregătirea, executarea și evaluarea acesteia*¹⁴.

¹⁴ S.M.G.-3, *Manualul de planificare a operațiilor*, București, 2016, p. 31.



Planificarea operațională constituie un proces complex, în cadrul căruia funcționează un leadership vizionar, orientat către oportunități, bazat pe capacitatea liderului de a motiva și determina oamenii să acționeze și pe abilitatea de a influența comportamentul personalului din comandament în luarea unei decizii eficiente și în elaborarea unui plan/ordin de operații credibil.

Totodată, planificarea operațională presupune un leadership participativ, deoarece liderul consultă și implică personalul de conducere din comandament în fiecare fază a procesului, având ca finalitate luarea deciziei, elaborarea concepției și a planului de operații.

Aplicarea unui stil de conducere care vizează un leadership performant presupune existența unei culturi strategice în cadrul comandamentului, formată în timp, ce presupune cunoaștere, experiență, înțelegere și gândire novatoare, spirit de echipă dezvoltat, abilități și competențe de lucru în mediul informațional și cibernetic.

Un leadership vizionar în planificare presupune integrarea și interconectarea instrumentelor și mecanismelor de analiză pentru a realiza un raport optim între diagnoză și prognoză, între vulnerabilitate și oportunitate, precum și între responsabilitățile liderului și atribuțiile delegate în cadrul compartimentelor comandamentului.

Dacă diagnoza vizează cunoașterea situației reale prin determinarea identității fenomenului respectiv, prognoza presupune anticiparea și evaluarea tendințelor de evoluție și perspectivelor de dezvoltare a acestuia.

Vulnerabilitățile sunt consecințele unor disfuncționalități sau deficiențe care pot diminua eficiența sistemului de comandă și control și pot favoriza manifestarea unor riscuri și amenințări asupra structurii de forțe.

Oportunitățile vizează elementele de succes identificate în mediul operațional și care, exploatate judicios, pot atenua vulnerabilitățile și potența activitățile pentru luarea unei decizii eficiente care să avantajeze acțiunile proprii, să asigure producerea efectelor preconizate, îndeplinirea obiectivelor și realizarea stării finale dorite.

În acest sens, un leadership vizionar identifică vulnerabilitățile existente în cadrul sistemului propriu și al mediului operațional, determină oportunitățile, stabilește structura de forțe necesară și formulează opțiunile de răspuns pentru contracararea amenințării.



Privind responsabilitățile liderului și delegarea unor atribuții, ca formă de leadership participativ, considerăm că trebuie să existe un echilibru între limita minimă care presupune consultare și cea maximă care vizează acceptarea expertizei personalului de conducere, astfel încât liderul să beneficieze de estimările și propunerile subordonaților, dar să-și asume pe deplin responsabilitatea și autoritatea luării deciziei.

Leadershipul performant vizează motivarea și stimularea personalului de conducere pe orizontală, în cadrul comandamentului, pentru a desfășura o activitate eficientă, dar și pe verticală, prin dezvoltarea încrederii, abilităților și competențelor subordonaților, utilizând ca procedeu planificarea colaborativă, menită să scurteze durata procesului de luare a deciziei și de elaborare a documentelor de conducere la nivel multieșalon.

Pregătirea operației militare constituie un proces coordonat în cadrul căruia leadershipul are un rol important în realizarea în timp scurt a capacității de luptă a forței în scopul îndeplinirii obiectivelor stabilite în planul de acțiune.

În acest sens, leadershipul se adresează direct structurii de forțe prin capacitatea liderului de a comunica, motiva și mobiliza subordonații în vederea executării cu succes a misiunilor primite.

Totodată, pregătirea operației militare presupune aplicarea unui leadership participativ în cadrul căruia liderul coordonează activitățile de instruire. Persoanele din comandament care au primit sarcini prin delegarea responsabilității asigură desfășurarea instruirii conform planului, iar subordonații acționează pentru cooperarea forțelor și sincronizarea misiunilor.

În această etapă, leadershipul vizează desfășurarea activităților care să asigure utilizarea eficientă a puterii de luptă prin executarea repetițiilor, organizarea și modelarea forței pentru îndeplinirea misiunii primite, instruirea, antrenarea și transmiterea sarcinilor către subordonați și verificarea modului de înțelegere a conținutului acestora.

Rolul leadershipului în executarea repetițiilor vizează stimularea, determinarea și mobilizarea forței pentru exersarea acelor procedee care dinamizează și potențează acțiunea. Astfel, repetițiile reflectă capacitatea și abilitatea liderilor de a direcționa acțiunile către neutralizarea centrului de greutate al adversarului, în vederea realizării efectelor stabilite și îndeplinirii obiectivelor precizate prin misiune. De asemenea, aplicarea unui leadership performant pe timpul executării repetițiilor, bazat pe capacitatea de



comunicare, integrare, coordonare și sincronizare a acțiunilor forței, asigură indicatorii necesari realizării puterii de luptă care să permită devansarea adversarului și potențarea executării misiunilor.

Organizarea și modelarea forței pentru îndeplinirea misiunii primite implică un leadership participativ orientat către nevoia de asigurare a resurselor necesare. În acest sens, leadershipul eficient presupune desfășurarea, coordonarea și simularea unor acțiuni prin care organizarea forței pentru misiune să fie dimensionată corect în raport cu efectele și obiectivele stabilite.

Această abordare corelativă a raportului dintre dimensionarea structurii de forțe și amploarea misiunii are în vedere aplicarea unui leadership eficient, care să ofere condițiile de succes în operația militară.

Instruirea și antrenarea subordonaților constituie un proces de durată care se desfășoară înainte de planificarea operației militare, însă se intensifică pe timpul pregătirii acesteia.

În această etapă, leadershipul orientează instruirea și antrenarea forței către coordonarea, cooperarea și sincronizarea acțiunii componentelor de forțe în vederea aplicării sinergice a puterii de luptă.

Astfel, apreciem rolul leadershipului în abilitatea și capacitatea de a mobiliza, convinge și încuraja personalul în executarea unor exerciții care să reflecte mediul operațional fizic sau virtual, să permită identificarea oportunităților și acțiunea sincronizată a forței pentru îndeplinirea misiunii.

Totodată, un leadership vizionar presupune motivarea și convingerea forței să execute instruirea cât mai aproape de realitate, să exerseze formele adecvate de manevră, să sincronizeze acțiunile componentelor sistemului de lovire, să realizeze protecția multidimensională și logistica întrunită.

Transmiterea misiunilor către subordonați și verificarea modului de înțelegere a conținutului acestora se bazează pe planul de acțiune elaborat în cadrul comandamentului.

Pentru a verifica modul de înțelegere a conținutului misiunilor primite de către subordonați, leadershipul vizează elaborarea unui plan de control adecvat precizărilor liderului.

Executarea operației militare este momentul culminant al confruntării, când toate energiile fizice, cognitive și morale acționează sinergic pentru obținerea succesului¹⁵.

¹⁵ S.M.G.-3, *Manualul de planificare a operațiilor*, București, 2016, pp. 80-81.



În acest sens, leadershipul vizează mobilizarea forței, exploatarea oportunităților, susținerea moralului, încurajarea și responsabilizarea subordonaților în aplicarea planului de operații pentru angajarea adversarului și îndeplinirea misiunilor primite.

În această etapă, leadershipul sprijină execuția operației prin inițiativă, dinamism, flexibilitate și inventivitate în gândire și acțiune.

De asemenea, leadershipul vizionar trebuie să identifice la timp amenințările care pot vulnerabiliza misiunea forțelor proprii, să acționeze pentru reducerea acestora și să exploateze oportunitățile care asigură succesul.

Astfel, apreciem faptul că, rolul leadershipului în dinamica operației devine foarte important, deoarece mobilizează, încurajează și potențează coordonarea și sincronizarea permanentă a forței în executarea misiunilor și îndeplinirea obiectivelor stabilite.

Abilitatea și capacitatea de adaptare permanentă a procedeeleor de luptă la situația concretă, reducerea efectelor desincronizării, valorificarea informațiilor de interes și flexibilitatea acțională sunt condiții de succes, generate de aplicarea unui leadership vizionar.

Totodată, un leadership eficient vizează direcționarea subordonaților către respectarea schemei de manevră, angajarea țintelor de interes ale adversarului, menținerea protecției forțelor și viabilității sprijinului logistic.

În acest sens, leadershipul presupune creativitate și inovație în poziționarea avantajoasă a forței, care să-i permită realizarea manevrei dominante, astfel încât, adversarul să fie surprins și devansat în acțiune, iar obiectivele să fie cucerite cu rapiditate.

Totodată, leadershipul trebuie să sprijine și să susțină concentrarea efortului asupra elementelor esențiale ale misiunii care converg către centrul de greutate al adversarului, deoarece numai anihilarea acestuia asigură succesul operației militare.

Schimbarea situației operative pe timpul executării misiunilor presupune, din partea leadershipului, desfășurarea unor activități pentru ajustarea planului și elaborarea unor noi ordine fragmentare, astfel încât acțiunile să aibă continuitate, dispozitivul de luptă să-și mențină dinamismul și suplețea, iar tempoul să fie susținut, în concordanță cu obiectivele stabilite.



Capacitatea de anticipare, experiența și gândirea creativă favorizează adaptarea forței la noile situații create în spațiul de luptă, fără a necesita executarea unor manevre și re poziționări de amploare sau complicate și fără a modifica substanțial obiectivele inițiale planificate.

Toate condițiile de succes nu pot fi realizate fără un leadership vizionar, participativ și orientat către oportunități care să valorifice informațiile și produsele de informații din spațiul de interes, să obțină superioritatea informațională și să susțină potențarea acțiunilor în tot spectrul operației militare.

Evaluarea operației militare este procesul prin care leadershipul verifică modul de îndeplinire a misiunilor și concordanța dintre conținutul planului și nivelul de executare a acțiunilor în spațiul de luptă¹⁶.

Astfel, apreciem rolul important al leadershipului în evaluarea operației, deoarece rezultatele obținute în urma desfășurării acestei activități pot fi valorificate în planificarea acțiunilor viitoare, eliminându-se, pe cât posibil, neconcordanțele, suprapunerile, desincronizările și disfuncționalitățile în executarea misiunilor de către structurile de forțe.

De fapt, în procesul de evaluare a operației, leadershipul realizează feedback-ul între planul de acțiune și modalitatea în care s-a executat misiunea, oferind un set de lecții învățate care vor fi valorificate în planificarea operației militare viitoare.

Liderul are rolul de a coordona și direcționa personalul de conducere din comandament în vederea constituirii unei structuri specializate care să cuantifice consecințele și efectele acțiunilor desfășurate în zona de operații.

În acest sens, leadershipul determină și orientează persoanele desemnate în stabilirea indicatorilor de eficacitate și de performanță care să măsoare rezultatele obținute pe timpul executării acțiunilor, în raport cu conținutul planului, gradul de realizare a efectelor și a obiectivelor stabilite inițial.

Stabilirea indicatorilor de evaluare a operației militare vizează aplicarea unui leadership bazat pe oportunități, caracterizat prin suplețe, flexibilitate și creativitate pentru a măsura corect eficiența și performanța structurilor de forțe pe timpul executării misiunilor.

Totodată, leadershipul orientat către oportunități trebuie să asigure optimizarea procesului de evaluare a operației militare prin utilizarea unor

¹⁶ S.M.G.-3, *Manualul de planificare a operațiilor*, București, 2016, p. 166.



criterii relevante, iar produsele rezultate să determine un feedback real, care să conducă la îmbunătățirea activității personalului de conducere din comandament în planificarea acțiunilor viitoare.

Concluzii

Mediul de securitate dinamic, fluid și instabil, generator de amenințări difuze, situații în care apar mutații bruște și neașteptate, precum și surprize strategice, determină schimbări de paradigmă în abordarea conceptelor de lider, leadership și organizație militară.

Liderul militar este persoana care dispune de prestigiu, capacitate intelectuală, abilitate motivațională și competență profesională de anticipare, inovare și mobilizare a membrilor unei organizații în vederea îndeplinirii unui obiectiv.

În acest sens, liderul este înzestrat cu viziune, gândește sintetic și proactiv, manifestă empatie, motivează și influențează subordonații fără a utiliza metode coercitive și dispune de abilitatea de a dezvolta capacitatea personalului din cadrul organizației în materializarea concepției sale pentru îndeplinirea obiectivelor stabilite.

De aceea, se afirmă faptul că liderul este persoana care dispune de abilități, experiență, caracter și loialitate față de organizație și angajează echipa în realizarea viziunii sale.

Leadershipul abordat ca sistem interuman, ca relație dintre cel ce conduce și cei ce acceptă să fie conduși și ca artă de a conduce, presupune din partea liderului viziune, creativitate, inovație, convingere și motivație, precum și capacitatea de a mobiliza și influența subordonații în îndeplinirea unor obiective comune.

Dacă cea mai importantă trăsătură a liderului militar este capacitatea acestuia de a motiva și mobiliza participanții la desfășurarea unor activități, cea a leadershipului înseamnă ierarhie, creativitate și inovație în conducerea organizației.

Ca un corolar al stilurilor de conducere, apreciem că leadershipul orientat către oportunități corespunde cel mai bine diagnosticării mediului de securitate actual, identificării amenințărilor și vulnerabilităților, diminuării disfuncționalităților și incertitudinilor și formulării opțiunilor interinstituționale de răspuns, care să fie flexibile, credibile și eficiente.



Față de complexitatea mediului de securitate și multitudinea elementelor componente, aplicarea unui leadership performant în procesul operației militare constituie garanția obținerii succesului în îndeplinirea misiunilor.

La final, apreciem faptul că problematica atât de complexă a domeniului abordat ar trebuie revăzută, regândite și redefinite conceptele în contextul schimbărilor de paradigmă și aplicate noile principii în scopul dezvoltării și perfecționării direcțiilor de valorificare a competențelor liderului militar și creșterii rolului leadershipului în procesul operației militare.

Bibliografie

1. * * * *Strategia Militară a României*, București, 2016.
2. * * * S.M.G.-3, *Manualul de planificare a operațiilor*, București, 2016.
3. Dr. Constantin, *Liderul militar în România*, - București: Editura Moștoflei,
dr. Petre, Duțu Universității Naționale de Apărare „Carol I”, 2007.
4. Gustave, *Psihologia mulțimilor*, Editura Anima, București,
Le Bon 1937.
5. Simon, Sinek *Liderii mănâncă ultimii: de ce unele echipe lucrează bine împreună, iar altele nu*, Editura Publica, Ediția a 2-a Rev, București, 2017.
6. * * * buzdugan.com.ro/blogmanagement/?p=2172
7. * * * <http://onismbn.ro/sinoiputem/assets/rolul-leadershipului.pdf>
8. * * * <https://leaders.ro/modelul-de-leadership/>
9. * * * <https://danieltanase.com/lider/>
10. * * * <http://mihaicurteanu.blogspot.com/2014/09/ce-inseamna-leadership-si-care-sunt-calitatile-unui-leader.html>
11. * * * <https://virtualboard.ro/teorii-de-leadership-participatil-situational/>
12. * * * <https://www.srac.ro/ro/stiri/semnificatia-rolul-si-importanta-leadership-ului-cadrul-noilor-standarde-pentru-sistemele-de>



SCHIMBĂRI ALE PARADIGMEI STRATEGICE GLOBALE ÎN URMA BREXITULUI

THE SHIFT OF THE GLOBAL STRATEGIC PARADIGM FOLLOWING BREXIT

Prof. univ. dr. Costel DUMITRESCU

Membru titular al Academiei de Științe ale Securității Naționale,

E-mail: dumitrescuco1@gmail.com

Rezumat: Numărătoarea inversă a început. Uniunea Europeană este la răscruce de drumuri, deoarece Marea Britanie a părăsit UE. Marea Britanie și UE nu au ajuns la un acord privind condițiile de ieșire și, de preferință, un nou acord comercial. Ambele părți au parcurs un drum imprevizibil. În ciuda faptului că principalul nostru scenariu era ieșirea Marii Britanii din UE la 31 octombrie 2019, acest lucru s-a realizat la data de 31 ianuarie 2020. Începând cu această dată, Regatul Unit a putut începe eliminarea sau introducerea legilor UE, dacă se dorește.

Cuvinte cheie: peisaj politic; nivel de trai; șomaj; criză; piață comună; potențial economic; echilibru; impact financiar.

Abstract: The countdown has started. The European Union is right at the crossroads, as Great Britain has left the EU. Great Britain and the EU have neither reached an agreement regarding the conditions for exit nor signed a new commercial deal as it would have been preferable. Both parties involved have followed an unpredictable pathway. Despite the fact that the main scenario anticipated the exit of Great Britain from the EU on October 31st 2019, this was accomplished on January 31st, 2020. Starting with that date, the United Kingdom was free to start eliminating or introducing EU laws according to its interests.

Keywords: political landscape; standard of living; unemployment; crisis; common market; economic potential; balance; financial impact.

Introducere

Brexitul este un moment de cotitură istorică, ale cărui rădăcini au trecut de șaptezeci de ani. Consecințele sale vor avea un efect de lungă durată. Decizia Angliei de a lansa Brexitul nu a șters subiectul dezbătut la UE, ci a stârnit cu adevărat noi controverse și a împărțit țara mai



ireconciliabil ca niciodată. Beneficiile presupuse ale Brexit rămân vagi, dar problemele sale economice sunt concrete. La rândul său, UE se confruntă cu o criză existențială.

După opinia unui cunoscător, din interior, al domeniului¹ mitul ireversibilității și pretenția de a întruchipa destinul manifest al Europei au dispărut. UE pierde un membru important, eficient și puternic din punct de vedere economic.

Autorul, care însuși a lucrat ca diplomat la Ambasada Germaniei din Londra, arată în această carte cum ar putea avea loc referendumul pentru Brexit și cum trebuie evaluat rezultatul. Ce abordări urmărește Theresa May cu cabinetul său pentru a implementa votul alegătorilor? Care sunt perspectivele de viitor pentru Regatul Unit? Ce consecințe ar putea avea plecarea sa pentru UE în ansamblul său, dar mai ales pentru Germania?

Răspunsurile la aceste întrebări stau la baza analizelor și diagnosticărilor captivante și vii ale acestui autor dar și ale multor analiști politici contemporani.

Referendumul din Marea Britanie cu privire la ieșirea din UE a generat nenumărate recenzii, publicații și opinii inter pares. Toate aceste poziții converg într-un singur sens - Marea Britanie și UE au intrat într-o etapă de dinamică imprevizibilă și au adăugat o serie întreagă de variabile noi, deși deseori încă confuze, pentru situația deja dificilă din Europa și din lume.

În comunitatea experților s-a dezvoltat un consens relativ cu privire la prognozele dezvoltării evenimentelor, care se prezumă a fi următoarele: cu cât persistă incertitudinea, cu atât consecințele vor fi mai grave pentru toți actorii implicați și cu atât vor fi mai negative și directe și indirecte efectele asupra proceselor de integrare, precum și asupra pieței globale. În același timp, Brexitul a creat o realitate nouă, neprevăzută, în care este posibil să se schimbe rolurile în procesele regionale și globale ale unor state, inclusiv al Rusiei și al statelor dintre ea și UE.

¹ Rudolf G. Adam, *BREXIT: Eine Bilanz*, Publisher: Springer Fachmedien Wiesbaden, Year: 2019. N.a. Autorul, care însuși a lucrat ca diplomat la Ambasada Germaniei din Londra, arată în această carte cum ar putea avea loc referendumul pentru Brexit și cum trebuie evaluat rezultatul.



Opinii privind Brexitul

La prima vedere, referendumul a devenit o combinație a calculelor politice de scurtă durată create pentru simpatia opiniei publice, a cărei influență asupra dinamicii politice a fost din nou subestimată. În același timp, argumentele raționale în favoarea beneficiilor integrării, liberei circulații a persoanelor, a capitalurilor și a serviciilor în Europa nu au fost suficiente pentru a depăși echilibrul în favoarea susținătorilor menținerii aderării la UE.

Discursurile despre Brexit oferă un caleidoscop al perspectivelor despre modul în care acestea au influențat rezultatul acestu fenomen socio-politic european.

Lucrând cu o mare varietate de date, de la discursuri politice până la Twitter și o gamă largă de metode, autorii lucrării *Discourses of Brexit*² prezintă cea mai detaliată examinare a discursurilor din jurul referendumului britanic al UE și a evenimentelor conexe.

Analiza acestor discursuri oferă o înțelegere cuprinzătoare a tratamentului discursiv al Brexit-ului, oferind în același timp investigații detaliate despre cum a fost negociat Brexit-ul în diferite contexte, atât pentru specialiștii în geopolitică cât și pentru toți cei interesați să dezvolte înțelegerea lor, despre referendum.

Referendumul a jucat un alt rol important - a aprobat în cele din urmă argumentele populiștilor și euroscepticilor din „mainstream”-ul politic, care de curând părea că, atunci când nu este capabil să arunce o umbră serioasă pe calea europeană a britanicilor, devine marginal.

Cu toate acestea, atitudinea prudentă față de instituțiile europene nu este un slogan pentru Marea Britanie, ea există atât timp cât există și ideea unei Europe unite și nu este prima dată când ea se face simțită, mai ales în timpul campaniilor electorale. Mai mult decât atât, forțarea Euroscepticismului nu a fost întotdeauna asupra Partidului Conservator.

La începutul anilor '80 ieșirea Marii Britanii din Comunitatea Economică Europeană a devenit unul dintre punctele de program ale Partidului Laburist, însă au fost forțați să o abandoneze după o înfrângere

² Veronika Koller, Susanne Kopf, Marlene Miglbauer, *Discourses Of Brexit*, Publisher: Routledge, Year: 2019.



zdrobitoare din 1983 de la conservatorii conduși de „progresista euro-sceptică” Margaret Thatcher. Mai mult decât atât, guvernul conservator, condus de Harold Macmillan, a făcut pașii istorici către integrarea europeană în anii '60, astfel încât preferințele partidului în acest caz nu au tipare clare.

După intrarea în vigoare a Tratatului de la Maastricht în 1993, partidele de conducere au pledat pentru continuarea integrării europene, preferând să modereze criticile față de Bruxelles și căutând condiții speciale pentru Londra. Deși printre conservatorii de la începutul anilor 2000 s-au făcut încercări de a se apropia de euroscepticii continentali, aceștia nu au fost susținuți nici de liderii și nici de majoritatea partidului (inclusiv David Cameron).

Singura forță politică care nu numai că a aderat la o poziție anti-europeană deschisă, ci și-a construit programul în jurul acesteia, a fost Partidul Independenței Regatului Unit (PNC). A fost fondat în 1991 de o serie de intelectuali universitari și personalități publice care s-au opus Tratatului de la Maastricht. Timp de cincisprezece ani, PNSK a atras mai des atenția tabloidelor decât politicieni de vârf și experți serioși. Cu toate acestea, acest lucru a continuat până în 2006, când carismaticul Nigel Farage a devenit liderul partidului. În fața lui N. Farage, PNSK a făcut o mică revoluție în peisajul politic aparent stabil al Marii Britanii, reușind să se bazeze pe voturile alegătorilor și grupuri sociale disparate, opunându-se nu numai integrării europene, dar și afluxului de străini, globalizării, corporațiilor transnaționale etc.

N. Farage și asociații săi nu s-au temut să folosească retorica populistă, apelând la restricționarea migrației, la restabilirea Marii Britanii și la ruperea cu burocrația de la Bruxelles. A fost un set de sloganuri antiliberale, pe fondul consecințelor crizei din 2008-2009. S-au bucurat de o popularitate crescândă în toată Europa. Succesul PNSK (în mai multe campanii regionale, iar în alegerile pentru Parlamentul European din 2014, s-a clasat înaintea celor trei mari partide britanice, câștigând 28%) a provocat numeroase scindări atât între conservatori, cât și pentru laburiști. Drept urmare, a existat o consolidare a pozițiilor facțiunilor extreme atât la dreapta, cât și la stânga, ai căror lideri erau Boris Johnson și, respectiv, Jeremy Corbyn.



John F. Kennedy spunea: „*Alegătorii ne votează pentru că au încredere în judecățile noastre și în capacitatea noastră de a înțelege care sunt interesele națiunii. Aceasta înseamnă că, ori de câte ori este posibil, ar trebui să conducem, să informăm, să corectăm și uneori chiar să ignorăm opinia publică*”³. Însuși faptul anunțării unui referendum privind ieșirea Marii Britanii din UE a fost rezultatul falimentului unor conservatori moderați britanici conduși de premierul David Cameron. Ei credeau că ar putea face față simultan euroscepticilor lor din propriul partid, precum și acelei părți a societății pentru care globalizarea și integrarea sunt sinonime cu eșecul economiei britanice și cu declinul națiunii.

Deși statisticile arată că de-a lungul anilor de aderare a Marii Britanii la UE, situația economică din țară nu s-a deteriorat deloc: PIB-ul pe cap de locuitor a crescut de la 5.500 de lire sterline în 1998 la aproape 7.000 în 2015, iar numărul de companii private în 2015 a atins un nivel record de 5,4 milioane, comparativ cu 3,5 milioane în 2000. Rata șomajului, depășind contextul negativ al anilor 2008–2012, a revenit în 2014 la un 6% confortabil, care este comparabil cu sfârșitul anilor '90, și mult mai bine decât cele mai puternice fluctuații de pe piața forței de muncă din anii 1970-1980.

Mulțumită presei britanice, a apărut un stereotip potrivit căruia marile companii erau în favoarea păstrării calității de membru în UE, în timp ce Brexitul era susținut întreprinderile mici, dar acest lucru nu este în întregime adevărat. Dacă întreprinderile mari au susținut într-adevăr aproape complet ideea de a continua calea europeană, atunci în comunitatea întreprinderilor mici și mijlocii a apărut o scindare. Mulți dintre reprezentanții săi au considerat normele și standardele europene prea complexe și au pledat pentru o mai mare libertate față de birocrația europeană. Cu toate acestea, în mare parte datorită standardelor europene, economia britanică din ultimul sfert de secol a devenit mai competitivă și a reușit să depășească efectele numeroaselor recesiuni și crize din anii 1970-1980.

Cu toate acestea, la final, confruntarea dintre susținătorii rămânerii Marii Britanii în UE și părăsirea ei nu s-a transformat într-o bătălie de argumente raționale, ci într-o luptă normală pentru voturi - cu campanii masive de manipulare de masă, spectacole vii ale politicianilor și

³ Kennedy JF, *Profiles in Courage*, Published by Harper & Row, NY, 1956, p. 15.



celebrităților și spectacole colorate, precum parada navei pe Tamisa. Dar a existat o tendință periculoasă în spatele acestor campanii - dependența de opinia publică într-un moment în care erau necesare decizii serioase și bine gândite din partea conducerii superioare.

Este interesant faptul că printre regiunile care au votat cel mai activ pentru ieșire s-au numărat Anglia și Țara Galilor, care au suferit obiectiv din cauza efectelor piețelor neregulate și a economiilor bugetare. Cu toate acestea, astfel de argumente au fost greu utilizate de liderii Brexit. Dimpotrivă, campania lor s-a bazat pe critica la adresa Uniunii Europene și a migrației, ca principalele motive pentru scăderea nivelului de trai și creșterea șomajului.

Este evident că în perioadele de criză publicul tinde către răspunsuri mai simple și mai inteligibile. Care ar fi rezultatul unui referendum, de exemplu în Germania, dacă ar exista un vot privind problema asistenței financiare acordate Greciei? Ce ar recomanda cetățenii francezi dacă sunt întrebați cu privire la restricționarea migrației din țările arabe? Răspunsurile ar fi evidente pentru majoritatea, dar ar fi corecte pentru aceste țări și pentru Europa?

Un referendum în Marea Britanie a fost o demonstrație evidentă a potențialului democrației disfuncționale. S-a utilizat un plebiscit în momentul în care a fost necesară o procedură parlamentară echilibrată, cu consultări active ale tuturor grupurilor interesate. Lipsa unor consultări serioase și a unei lucrări de specialitate atentă a condus la faptul că a treia economie europeană nu a avut un plan clar de acțiune în cazul retragerii din Uniunea Europeană.

În principiu, instabilitatea este inerentă piețelor - acestea răspund la orice criză internațională cu explozii de volatilitate. Cu toate acestea, Brexitul a devenit o criză neobișnuită pentru piețe. Disponibilitatea britanicilor de a abandona regulile de joc acceptate a servit ca o nouă variabilă, în raport cu care piețele, inclusiv britanicii, nu pot în niciun caz să dezvolte o poziție fără echivoc. Astăzi, principalele instituții economice, state și companii din lume sunt obligate să lucreze simultan cu mai multe scenarii - de la pozitiv, la extrem de negativ. Posibilitatea implementării acestor scenarii depinde de o serie de factori, care sunt asociați în principal cu viteza și eficiența găsirii unui nou status-quo între Londra și Bruxelles.



Cu toate acestea, este evident prematur să spunem că Brexitul va da naștere unei noi crize economice globale.

Unele aspecte economice ale Brexitului

Scenariile catastrofale sunt în mod tradițional populare în mass-media, dar economia britanică are o marjă imensă de siguranță. Acest lucru este confirmat de întărirea lirei și de o scădere vizibilă a panicii la bursele din primele săptămâni după șocul rezultatelor referendumului. FMI a scăzut, într-adevăr, prognoza pentru creșterea economică globală pentru 2017 cu 0,1%, iar pentru zona euro cu 0,2%. Cu toate acestea, aceste calcule sunt încă de natură foarte speculativă, deoarece totul va depinde de aceleași scenarii și negocieri cu Bruxellesul. De asemenea, acum este imposibil de prezis cât vor costa consecințele Brexitului pentru economia britanică. Institutul de cercetare financiară din Londra, cu o lună înainte de vot, a stabilit o gamă cuprinsă între 74 de miliarde de lire sterline și un excedent de 30 de miliarde de lire sterline, în funcție de evoluția situației. Cifrele sunt atât de diferite încât niciun economist serios nu poate numi chiar costul aproximativ al „Brexit”.

Cu toate acestea, zona euro are astăzi riscuri mai distincte asociate cu starea de incertitudine a sectorului financiar din Italia și cu operațiunile periculoase la Deutsche Bank. În cazul scenariilor negative pentru sistemele bancare italiene și germane, acestea vor avea un efect mult mai rapid asupra economiei europene. Problemele structurale ale șomajului ridicat, ale productivității scăzute și ale dinamicii slabe a creditelor nu au dispărut. Brexitul a adăugat doar incertitudinea economică din regiune, ceea ce ar putea crește povara asupra sectorului financiar. Uniunea Europeană, care a ratat investițiile britanice în bugetul său (aproximativ 15 milioane de lire sterline pe an), va fi obligată să le compenseze în detrimentul altor țări membre, în primul rând Germania.

Cei care văd ca fiind o strategie bine gândită despărțirea de Bruxelles în afara Uniunii Europene, consideră că Marea Britanie va fi scutită de povara problemelor sistemice din Europa continentală și își va putea îmbunătăți în mod independent economia. Principala vulnerabilitate a acestei poziții este aceea că independența în lumea modernă este o categorie condiționată. Nu există piețe independente pentru servicii, sisteme



financiare, industrie inovatoare etc. Deci, întrebarea este, ce parte din noul întreg va dori să devină Marea Britanie?

Cel mai optimist scenariu descris în campania *Out* implică următoarele: după ce a primit dreptul de a încheia în mod independent acorduri comerciale, țara nu va rămâne doar în zona de liber schimb cu UE (sau va încheia acorduri separate cu aceasta pe sectoarele economice), ci va extinde în mod semnificativ și aria de influență, crearea de noi piețe economico-financiare cu principalele economii ale lumii - Statele Unite, China, India etc. Acest lucru ar trebui să transforme Marea Britanie într-un hub comercial și financiar unic, noua Elveție sau Singapore. Una dintre nuanțele unui posibil nou acord între Londra și Bruxelles este aceea că este practic imposibil să obții acces gratuit la piețele financiare ale UE fără să fii membru al blocului. În special, Elveția, care are o pondere mai mare a serviciilor financiare în PIB decât Marea Britanie, are un deficit comercial cu UE în ceea ce privește serviciile financiare - poziția unui partener privilegiat nu este încă echivalentă cu apartenența deplină.

Unicitatea Marii Britanii înainte de Brexit a fost aceea că țara a servit ca punte de investiții între Uniunea Europeană și restul lumii. Regatul Unit a reprezentat mai multe investiții directe decât întreaga UE combinată. Potrivit unui studiu Ernst & Young din 2015, majoritatea investitorilor (72%) au declarat că principalul avantaj al Regatului Unit este accesul liber pe piața europeană. Cu alte cuvinte, investitorii au considerat statul insular nu doar ca obiectiv al investiției, ci și ca o zonă de tranzit majoră. Susținătorii retragerii din UE au încercat până acum să nu convingă investitorii mondiali că acest lanț nu va merge nicăieri în viitor.

Cu toate acestea, acest lucru va necesita încheierea unui acord unic cu Bruxelles, care nu are analogie în Europa. Acesta ar trebui să prescrie simultan accesul gratuit pe o piață unică și să restricționeze circulația persoanelor (adică migrația) - unul dintre punctele principale ale campaniei *Out*. Dacă fracțiunea victorioasă a conservatorilor euro-sceptici și a altor forțe socio-politice care au pledat pentru retragerea din UE abandonează acest punct populist, vor pierde sprijinul părții „supărate” a populației și își vor amortiza propriile eforturi.

Într-un anumit sens, acesta a fost cel mai dificil și adevăratul motiv pentru care procesul de negociere s-a desfășurat cu greutate, întrucât Bruxellesul, Berlinul și Parisul nu au fost de acord cu faptul că un astfel de



punct ca „oamenii” poate fi eliminat din conceptul de liberă circulație. La urma urmei, aceasta va însemna o încălcare sau necesitatea unei revizuirii parțiale a fundamentelor legale ale Uniunii.

Câteva consecințe mondiale

Pentru țările din afara UE, și în mod special pentru Rusia, consecințele pe termen scurt ale Brexitului vor fi, cel mai probabil, de natură indirectă, prin fluctuații ale piețelor de materie primă și fluctuații valutare cauzate de incertitudinea evenimentelor ulterioare. Poate că unele companii mari care tranzacționează în mod tradițional la Bursa de la Londra vor dori să evite volatilitatea financiară și să suspende tranzacționarea sau să vândă o parte din activele lor. În același timp, trebuie menționat că tendința pentru întreprinderile din fostul spațiu sovietic de a părăsi Bursa de la Londra a apărut clar cu mult înainte de referendum și a fost cauzată de motive complet diferite: o scădere globală a prețurilor materiilor prime, pierderea interesului unui număr de investitori-cheie în activele rusești pe fundalul unei noi runde de turbulențe geopolitice și economice, stagnarea economică în Rusia.

În multe privințe, unii dintre acești factori nefavorabili au impus în 2015 eliminarea firmelor Uralkali, Polyus și Eurasia BC. În cele din urmă, unele companii ce acționau pe plan intern în Rusia (de exemplu, Otkritie Bank) și-au exprimat dorința de a transfera comerțul pe piețele asiatice atractive. Cu toate acestea, nu sunt așteptate plecarea celorlalte companii ruse de pe Bursa de la Londra (31 în total), fiind dezvoltate legături prea strânse de la mijlocul anilor 2000 între directorii de afaceri ruși și finanțatorii londonezi. Dacă dobânda continuă să scadă, cauza se pare că nu este în Rusia, ci la investitorii străini frustrați, iar în acest caz, transferul comerțului către Hong Kong, Shanghai sau Singapore este puțin probabil să salveze aceste companii de o pierdere de lichiditate.

Un număr semnificativ de politicieni occidentali de vârf care au susținut campania *In*, inclusiv David Cameron, au spus că Moscova va fi prima care va beneficia de ieșirea britanică și de slăbirea UE. Acest argument, care este destul de pueril din punct de vedere rațional, ar fi putut fi o încercare de a da un răspuns foarte simplu la întrebarea de ce ieșirea din UE este rea.



În ceea ce privește extinderea sau ridicarea treptată a sancțiunilor împotriva Rusiei, Brexitul probabil joacă un rol, dar nu unul decisiv. În realitate, durata acestora este extinsă de către toți membrii UE, în unanimitate. Chiar dacă nu mai există un vot oficial al Regatului Unit la instituțiile europene, vor exista și alte țări dispuse să ia o poziție dură împotriva Rusiei; în același timp, părerea Marii Britanii ca un actor regional important în orice caz nu va dispărea.

Cu toate acestea, astăzi situația se dezvoltă mai probabil în direcția opusă - tot mai multe grupuri politice importante și reprezentanți de afaceri din statele membre ale UE declară necesitatea slăbirii regimului de sancțiuni. Dacă aceste grupuri câștigă aderenți în masa critică, în special în economiile de frunte ale Uniunii, atunci s-ar putea obține efectul invers prognozat. Evident, Marea Britanie - indiferent dacă a fost în UE sau în afara ei începând cu 31 ianuarie 2020 - cu greu ar fi putut sau va putea inversa această situație.

Cu toate acestea, regimul sancțiunilor este, în orice caz, un fenomen temporar pentru relațiile ruso-europene. Un alt lucru este mai important - modul în care Rusia și Uniunea Europeană vor construi relațiile strategice în viitor și ce rol poate juca Brexitul în această dinamică. În ultimii ani, Rusia a luat o poziție destul de pasivă (în funcție de conotație) în ceea ce privește integrarea europeană. Incertitudinea predominantă politico-militară, adesea mărginită de isterie, nu adaugă fundamentele raționale pentru o implicare mai profundă a Rusiei.

Evident, un scenariu de unificare între Uniunea Eurasiatică și Uniunea Europeană, care a fost criticat în mod repetat și care încă suscită diverse comentarii, are încă un potențial enorm, însă punerea sa în aplicare necesită voință politică și eforturi serioase ale experților. Deși astăzi elita rusă și-a îndreptat în mare măsură atenția către o altă uniune - cu Centura economică a drumului mătăsii, aceasta nu înseamnă că Rusia va refuza participarea la procesele de integrare în Occident.

În acest sens, Brexitul creează o nouă paradigmă care nu a fost încă dezvoltată. Oricât de ciudat ar părea, acest pas încă obscur și în mare măsură populist al cercurilor politice individuale din Marea Britanie este capabil să schimbe semnificativ spațiul regional și să deschidă posibilități pentru noi oportunități, inclusiv pentru Rusia și Turcia.



Concluzii

În contextul schimbării elitelor conducătoare din Marea Britanie, căutarea de noi paradigme de dezvoltare de către Uniunea Europeană, interacțiunea activă a proiectelor de integrare (scenarii de parteneriat transatlantic), conducerea rusă și cea turcă ar trebui să se gândească nu la obținerea influenței puterii, ci la beneficiul lui Smith (raționalism economic), aceasta fiind o nouă realitate.

Într-o perioadă în care Europa a intrat într-o fază de incertitudine, Moscova ar trebui să înceapă să studieze nu numai riscurile, ci și potențialele avantaje - în ceea ce privește noile formate pentru cooperarea comercială și financiară cu Londra, oportunități pentru o inversare constructivă în relațiile cu Uniunea Europeană și reducerea tensiunii geopolitice. Până în prezent, în mediul analitic, au fost făcute doar încercări timide de a înțelege potențialul apropierei economice cu Marea Britanie, independent de Bruxelles sau revizuirea relațiilor cu UE, unele dintre ele părănd simple scenarii.

Brexitul creează într-adevăr oportunități, atât pentru Moscova, cât și pentru Ankara, dar nu din punctul de vedere al unei presupuse slăbiri a UE, pe care insistă politicienii occidentali, ci din punctul de vedere al reformării spațiului economic european în care Rusia, ca principal vector energetic, ar putea să dezvolte o participare în condiții favorabile pentru ea și pentru Europa.

Acest articol abordează câteva dintre cele mai importante aspecte ale Brexit-ului, care au fost mereu prezente în dezbaterile publice, dar care, până în prezent, nu au fost suficient în atenția publiciștilor.

Pentru a rezolva acest decalaj, într-o lucrare care a reunit contribuția unui grup internațional de autori⁴ se oferă un tratament cuprinzător și multidisciplinar al acestui subiect. Mai precis, colaboratorii, savanții din Marea Britanie și din întreaga Europă, oferă relatări diverse despre rolul parlamentelor regionale, naționale și europene și cetățenilor din perspectivele dreptului, științei politice și studiilor europene.

⁴ Thomas Christiansen, Diane Fromage, *Brexit and Democracy: The Role of Parliaments in the UK and the European Union*, Series: European Administrative Governance, Publisher: Springer International Publishing; Palgrave Macmillan, Year: 2019.



Dincolo de furnizarea unei examinări cuprinzătoare a controlului Brexitului, articolul folosește ideile obținute din aceste experiențe pentru un studiu al relațiilor social-politice din Uniunea Europeană, în general, examinând echilibrul, sau lipsa acestuia, între guverne și parlamente. În acest fel, rămân în atenția noastră unele dintre întrebările de lungă durată, într-adevăr perene, despre efectele dispozițiilor constituționale și ale practicii politice în contextul democrației europene.

Bibliografie

1. Rudolf G. Adam *Brexit: Causes and Consequences*, Publisher: Springer, Year: 2020.
2. Rudolf G. Adam *BREXIT: Eine Bilanz*, Publisher: Springer Fachmedien Wiesbaden, Year: 2019.
3. Thomas Christiansen, Diane Fromage *Brexit and Democracy: The Role of Parliaments in the UK and the European Union*, Series: European Administrative Governance, Publisher: Springer International Publishing; Palgrave Macmillan, Year: 2019.
4. Duță, Paul *Europa lărgită, politica europeană de vecinătate și spațiul comun de securitate externă*, în Impact Strategic, nr.2/2005.
5. Duță, Paul; Grațian, Lupu *Europa de la dezideratul unificării la OSCE și Uniune*, Colecția Politică și Apărare Națională nr. 11, Editura Continent, Sibiu, 2006.
6. Kennedy JF *Profiles in Courage*, Published by Harper & Row, NY, 1956.
7. Veronika Koller, Susanne Kopf, Marlene Miglbauer *Discourses Of Brexit*, Publisher: Routledge, Year: 2019.



**PANDEMIA DE CORONAVIRUS – RISC SAU AMENINȚARE
LA ADRESA SECURITĂȚII NAȚIONALE,
REGIONALE ȘI GLOBALE?**

**CORONAVIRUS PANDEMIC – RISK OR THREAT TO NATIONAL,
REGIONAL AND GLOBAL SECURITY?**

Gl. mr. (r.) prof.univ.dr. Gabriel-Florin MOISESCU

Membru titular al Academiei de Științe ale Securității Naționale,

E-mail: moisescu.gbrl@gmail.com

Lt. col. lector univ.dr. Bogdan-Cezar CHIOSEAU

Academia Forțelor Aeriene „Henri Coandă”

E-mail: b.chioseaua@gmail.com

Rezumat: Apariția și evoluția epidemiei de coronavirus și transformarea ei ulterioară în pandemie, precum și modul de răspuns de până acum al autorităților, pe etape, la criza generată de către aceasta, ne-a determinat să supunem atenției necesitatea stabilirii unor clarificări privind încadrarea ei ca risc sau amenințare la adresa securității naționale/regionale/globale, utilizând drept fundament teoretic elemente ale gândirii de securitate occidentale și naționale.

Cuvinte cheie: *pandemie de coronavirus, securitate, amenințare, risc, vulnerabilitate, strategie de securitate națională, strategie de securitate internațională.*

Abstract: *The appearance and evolution of coronavirus epidemic and its subsequent transformation into a pandemic, as well as the response of authorities – in stages – to the crisis it generated have prompted us to address this issue. Thus, we have felt the need to establish clarifications regarding its definition as a risk or a threat to national/regional/global security, using as theoretical background elements of Western and national security thinking.*

Keywords: *coronavirus pandemic, security, threat, risk, vulnerability, strategy of national security, strategy of international security.*

Pandemia de coronavirus reprezintă o încercare pentru prezentul omenirii, dar ceea ce contează sunt provocările pe care aceasta le generează pentru viitor.



Vom ști să răspundem la aceste provocări?

Dintre aceste provocări am optat pentru a încerca să răspundem la întrebarea: *Pandemia reprezintă un risc sau o amenințare la adresa securității naționale/regionale/globale?*

Chiar dacă nu există o definiție unanim acceptată a securității, cea formulată de cercetătorii¹ Școlii de la Copenhaga a reușit să organizeze Teoria Relațiilor Internaționale în jurul acestui concept², întrucât a abordat problematica securității din perspectiva sistemică, folosind nivelurile de analiză în termeni de scară spațială, de la individ la sistem prin intermediul statului și sectoarele de analiză ca fiind văzute printr-un sistem de lentile, care focalizează sau estompează tipurile de relație și activitate: militară, politică, economică, socială și de mediu.

Conform teoriei, insecuritatea națională reprezintă o combinație de amenințări și vulnerabilități – unde amenințările sunt din afara sistemului și vulnerabilitățile din interiorul acestuia³ - iar opțiunea de a acționa asupra cauzelor vulnerabilităților se numește strategie de securitate națională, în timp ce alegerea de a acționa pentru reducerea sau micșorarea amenințărilor se numește strategie de securitate internațională⁴.

Dacă ne referim la obiectul acțiunii potrivit celor două opțiuni, în urma distincției cheie dintre amenințări și vulnerabilități, se apreciază faptul că, în timp ce vulnerabilitățile sunt destul de concrete, amenințările sunt mai greu de controlat datorită raportului subiectiv-obiectiv dintre indivizi, precum și a dificultății de a le deosebi pe cele cu impact asupra securității naționale de cele rezultate din mediul competitiv internațional⁵.

De asemenea, trebuie comparată probabilitatea de îndeplinire a unei amenințări cu consecințele determinate de aceasta⁶ de profunda

¹ N.A. Este vorba despre Barry Buzan care, alături de Ole Waever și Jaap de Wilde, sunt reprezentanți ai Școlii de la Copenhaga care are drept obiect de studiu securitatea.

² N.A. Ole Waever despre Barry Buzan, conform Barry Buzan, *Popoarele, statele și frica O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Ediția a doua, Editura Cartier, Chișinău, 2014, p. III.

³ *Ibidem*, p. 120.

⁴ *Ibidem*, p. 333.

⁵ *Ibidem*, pp. 122-123.

⁶ N.A. Ole Waever despre Barry Buzan, conform Barry Buzan, *Popoarele, statele și frica. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Ediția a doua, Editura Cartier, Chișinău, 2014, p. 144.



ambiguitate a amenințărilor⁷, precum și de faptul că ele pot avea loc în toate sectoarele (domeniile, dimensiunile) mai sus amintite.

În acest sens, se subliniază faptul că, amenințările ecologice, ca și celelalte tipuri de amenințări, pot aduce prejudicii bazei fizice a statului într-o măsură suficientă pentru a-i amenința ideea și instituțiile⁸.

Alinierea gândirii românești de securitate la cea occidentală precum și necesitatea lărgirii conceptului s-au materializat în țara noastră prin promovarea în cadrul Strategiei Naționale de Apărare a Țării (S.N.Ap.Ț.) pentru perioada 2015-2019, a conceptului de securitate națională extinsă (S.N.E.).

Aceasta are la bază democrația constituțională și respectul mutual dintre cetățeni și stat și adaugă la patru din domeniile mai sus menționate – militar, economic, social și de mediu, ultimul fiind doar amintit nu și dezvoltat – pe cele de ordine publică, informații, contrainformații și securitate, educație, sănătate, energetic, financiar, diplomatic, management al situațiilor de criză și infrastructuri critice⁹.

Constatăm în acest punct al demersului nostru faptul că din cadrul conceptului S.N.E. lipsește dimensiunea politică, - și ne întrebăm de ce? – întrucât elaborarea și punerea în aplicare a politicilor în toate domeniile aparțin clasei politice, iar problema securității unui stat este o chestiune de percepție, iar dacă percepțiile sunt greșite pot genera consecințe dramatice¹⁰.

Drept urmare, propunem ca în S.N.Ap.Ț. pentru perioada 2020-2025, care urmează să fie elaborată în acest an, în cadrul conceptului S.N.E. să fie introdusă dimensiunea politică, iar celelalte dimensiuni să fie abordate într-o succesiune care să evidențieze importanța lor în cadrul sistemului național de securitate.

⁷ N.A. Ole Waever despre Barry Buzan, conform Barry Buzan, *Popoarele, statele și frica. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Ediția a doua, Editura Cartier, Chișinău, 2014, p. 150.

⁸ *Ibidem*, p. 139.

⁹ *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume*, Administrația Prezidențială, București, 2015, p. 9.

¹⁰ N.A. Aprecierile aparțin lui Robert Jervis, conform Radu-Sebastian Ungureanu, *Conceptul de securitate*, în Andrei Miroiu, Radu-Sebastian Ungureanu (coord.), *Manualul de relații internaționale*, Editura Polirom, București, p. 182.



În S.N.Ap.Ț., definițiile amenințării și vulnerabilității se încadrează în distincția cheie dintre acestea, iar riscul este definit ca fiind posibilitatea de manifestare a unui eveniment incert cu impact direct sau indirect asupra securității naționale¹¹.

În plus, în scopul creării unui cadru conceptual comun, acestea sunt abordate și în Ghidul strategiei¹².

Din punct de vedere medical, epidemia reprezintă dezvoltarea rapidă a unei boli contagioase, în cadrul unei populații, de cele mai multe ori de origine infecțioasă, determinată de o endemie sau poate surveni pentru prima dată¹³.

Pandemia este o epidemie care se extinde pe un teritoriu foarte mare, cuprinzând mai multe țări, continente¹⁴.

Inițial, la debut (nu se știe cu precizie când și unde a avut loc acesta), COVID-19 a provocat o epidemie care, ulterior, s-a transformat în pandemie.

Conform S.N.Ap.Ț., pandemia constituie un risc cu probabilitate redusă dar cu impact major, alături de confruntările militare de joasă intensitate, dar persistente în timp, de fluxurile migratorii generate de catastrofe naturale și dezastre ecologice¹⁵.

Însă un risc generează de cele mai multe ori o criză, iar managementul inadecvat al unei astfel de situații – perioadă de tensiuni, de tulburări, de încercări (adesea decisive) care se manifestă în societate¹⁶ - poate determina transformarea riscului în amenințare la adresa securității naționale.

Autoritățile române, în scopul prevenirii răspândirii virusului COVID – 19 și realizării managementului consecințelor, au instituit starea de urgență pe o perioadă de 30 de zile¹⁷ prin care a fost restrâns exercițiul

¹¹ Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019*, op. cit., p. 23.

¹² *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*, Administrația Prezidențială, București, 2015, pp.12, 15, 17.

¹³ [www.csid.ro>*Dictionar medical*], accesat la 13.04.2020.

¹⁴ [dexonline.ro/*definitie/pandemie*], accesat la 13.04.2020.

¹⁵ Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019*, op. cit., p. 25.

¹⁶ [<https://dexonline.ro>>*definitie>criza*], accesat la 13.04.2020.

¹⁷ N.A. A intrat în vigoare pe data de 16 martie 2020, data publicării în Monitorul Oficial al României, Partea I.



anumitor drepturi și s-au stabilit două categorii de măsuri: măsuri de primă urgență, cu aplicabilitate imediată (Anexa 1 din Decret) care acoperă domeniile de activitate ordine publică, economie, sănătate, muncă și protecție socială, justiție, afaceri externe etc.; măsuri cu aplicabilitate graduală (Anexa 2 din Decret)¹⁸.

Se observă deci că, prin măsurile luate, într-o perioadă de timp de aproximativ 6 săptămâni de la apariția primului caz de infectare cu coronavirus, autoritățile au răspuns la o criză – criză de sănătate publică – generată de un risc (pandemia) acționând asupra cauzelor vulnerabilităților sistemului național de sănătate publică (sistemul de securitate națională) în scopul limitării efectelor acesteia.

Prin decizia luată (dimensiunea politică) au fost angrenate mecanismele sistemului național de răspuns la criză (celelalte dimensiuni ale conceptului S.N.E.) și în dinamica evoluției crizei s-a realizat ceea ce avem și ceea ce nu avem pentru a face față unei asemenea situații.

Ulterior, după o perioadă de timp în care țările membre s-au orientat cu prioritate spre „interiorul” lor, Uniunea Europeană a început să colaboreze cu aceasta pentru a da un răspuns coordonat menit să limiteze răspândirea virusului.

În această direcție, s-au restricționat temporar călătoriile neesențiale către U.E. timp de 30 de zile, este descurajată deplasarea cetățenilor europeni în afara U.E., Consiliul a activat mecanismul integrat al U.E. pentru un răspuns politic la crize (IPCR), Comisia Europeană și Consiliul facilitează contactul permanent și coordonarea ministerelor naționale relevante, președintele Consiliului European organizează conferințe cu liderii U.E., Centrul European de Prevenire și Control al Bolilor (ECDC) publică pentru populația U.E. evaluări rapide ale riscurilor și actualizări epidemiologice¹⁹.

De asemenea U.E. s-a angajat să combată dezinformarea și să colaboreze cu țările membre pentru asigurarea de echipamente, promovarea cercetării pentru tratamente și vaccinuri (140 mil. €), sprijinirea locurilor de

¹⁸ [www.pwc.ro], accesat în 10.04.2020; Pe data de 6 aprilie 2020, Președintele României a anunțat că va prelungi Starea de Urgență cu încă 30 de zile, până pe 16 mai 2020 (conform [<https://romania-eurolibera.io/>], accesat la 10.04.2020).

¹⁹ [<https://www.consilium.europa.eu/c/>], accesat la 09.04.2020.



muncă, a întreprinderilor și a economiei (37 md. €), iar Banca Europeană a anunțat un program de achiziții de urgență în valoare de 750 md. €²⁰.

Reacția a fost lentă – din punctul nostru de vedere – și din partea N.A.T.O. care, începând cu 02.04.2020, prin secretarul său general, l-a numit pe comandantul suprem al Forțelor Aliate din Europa (SACEUR) să coordoneze sprijinul necesar în vederea combaterii virusului prin furnizarea de: profesioniști în domeniul sănătății; paturi de spital și medicamente esențiale; personal medical, materiale și echipamente esențiale din surse civile și militare; cunoștințe și resurse medicale, științifice și tehnologice²¹.

Drept urmare a succesiunii de evenimente prezentate mai sus, la care se adaugă modalitatea de răspuns la criza generată de pandemie în prima etapă – de la identificarea primului cetățean român infectat cu COVID-19 și până la intrarea în funcțiune a mecanismelor de răspuns la criză ale U.E. și N.A.T.O. – în cea de-a doua etapă, odată cu intervenția N.A.T.O. și U.E., s-a acționat, după părerea noastră, pentru reducerea și micșorarea unei amenințări (sistemul internațional de securitate).

Prin urmare, evoluția pandemiei pe „traiecul” risc-criză-amenințare a determinat autoritățile statului român să acționeze într-o primă etapă asupra cauzelor vulnerabilităților (strategia de securitate națională).

De aceea, noi considerăm că în prima etapă pandemia a fost un risc la adresa securității naționale care, în etapa a doua, s-a transformat în amenințare.

Așadar, managementul inadecvat al unui risc a generat transformarea acestuia în amenințare la adresa securității naționale, cu efecte nebănuite asupra domeniilor securității.

Și asta nu este tot. Întrucât amenințarea s-a „îndeplinit”, statele, regiunile, continentele, omenirea se află acum într-un adevărat „război” cu un „inamic” care te poate „ataca” oriunde și oricând, invizibil, care nu are gust, miros, pe care uneori îl simți și alteori nu, care nu ține cont de poziția geografică, geografia teritoriului, nivelul de dezvoltare economică, tipul de relație (amic, inamic, neutru), politicile de securitate ale statelor „țintă”, care a „cucerit” stat după stat, regiune după regiune, continent după continent,

²⁰ [<https://www.consilium.europa.eu/c...>], accesat la 09.04.2020.

²¹ N.A. Declarația adoptată de miniștrii de externe ai țărilor membre ale N.A.T.O. în urma reuniunii din 02.04.2020, conform [<https://www.euroactiv.ro/extern/n...>], accesat la 09.04.2020.



fără a întâmpina o reacție suficient de puternică pentru a putea fi oprit pe un anumit „aliniament”.

Este un „conflict” între om și mediu, în care omul nu a avut suficiente informații despre capacitățile, strategiile și intențiile „inamicului” pentru a realiza o reacție corespunzătoare și până acum nu a apărut „comandantul” care, cu resursele avute la dispoziție, să folosească conceptele adecvate de ducere a „acțiunilor militare” (arta comandantului) încât să atingă obiectivul propus (înfrângerea „inamicului”).

Caracteristicile „agresiunii” (viteza de propagare, mutațiile virusului – de la o țară la alta, de la o regiune la alta, de la un continent la altul - dimensiunea, amploarea, intensitatea, efectele produse) și reacția autorităților de la toate nivelurile (național/regional/global) la aceasta, demonstrează încă odată faptul că, securitatea sănătății ființei umane este relativă și nu absolută, că a-ți asigura „singur” securitatea este aproape imposibil, sistemul internațional de securitate rămânând opțiunea de dorit.

Este „ceva” cu care omenirea nu s-a mai întâlnit în trecutul recent, cu efecte extrem de dificil de cuantificat asupra tuturor domeniilor securității naționale, regionale și globale.

În același timp cu „lupta” statelor lumii cu virusul COVID-19, sunt „semne” că s-a mai declanșat una, și anume cea pentru identificarea „vinovatului” de ceea ce se întâmplă astăzi.

Astfel, președintele S.U.A. vorbește despre „virusul chinezesc”, oficialii chinezi pretind că acesta a fost adus în China de către americani, cu prilejul desfășurării la Wuhan a Jocurilor Mondiale Militare, în perioada 18-27 octombrie 2019, un raport arată că turiștii europeni și nu asiatici au adus virusul la New York²².

De asemenea, sunt informații conform cărora, Institutul de Virusologie din Wuhan ar fi desfășurat experimente pe mamifere capturate la o distanță de 1600 km. depărtare, în regiunea Yunnan, experimente care au fost sponsorizate cu 3,7 mil. \$ de către guvernul american, că laboratorul ar fi de fapt sursa originală a virusului și nu piața de animale din Wuhan²³.

²² N.A. Este vorba de un raport publicat în New York Times, conform [<https://m.digi24.ro...>SUA>], accesat la 12.04.2020.

²³ [<https://m.mediafax.ro>externe>po..>], accesat la 12.04.2020.



În același sens, un înalt oficial american, întrebat miercuri 08.04.2020 dacă China a ascuns informații despre răspândirea virusului, a declarat că nu este momentul acum pentru represalii, dar este încă timp pentru claritate și transparență²⁴.

Și, nu în ultimul rând, președintele S.U.A. a tăiat finanțarea pentru Organizația Mondială a Sănătății (O.M.S.), pe care o consideră vinovată pentru răspândirea virusului.

Și, probabil, că această luptă va continua, chiar dacă omenirea trebuie să facă față atât coronavirusului cât și crizei economice pe care o „vedem” și o „simțim” cu toții.

Așa cum secolul XX a făcut față provocărilor economice cu două școli mari de gândire economică, cea a lui John Maynard Keynes și Milton Friedman care au arătat, prima, rolul intervenționismului statal în echilibrarea politicilor economice ale pieței libere și a dezechilibrelor provocate de aceasta – iar cea de-a doua, rolul banilor și a echilibrelor financiar-bancare, secolul XXI are în față un nou tip de criză economică, cu noi provocări, neîntâlnite până acum, astfel încât va trebui să preia elementele favorabile din teoriile economice existente.

Marea provocare economică este aceea de a găsi o nouă politică macroeconomică, un „New Deal” al epocii noastre pe care, asemenea președintelui american Franklin Delano Roosevelt, să avem tăria de a o implementa, de a înțelege că ea nu va fi perfectă de la început ci doar perfectibilă pe parcurs, dar să ne ajute să găsim punctele de echilibru între muncă și profit, piață liberă și reglementări impuse de stat, între nevoia de finanțare și capitaluri.

Parafrazând teoria lui Friedman privind „așteptările raționale”, poate că asta este ceea ce așteaptă secolul XXI de la noi, să avem „așteptări raționale” de la noi înșine și de la autoritățile statale, în toate domeniile vieții economico-sociale.

Întrucât demersul nostru a pornit de la nevoia unor clarificări privind încadrarea pandemiei de coronavirus ca risc sau amenințare la adresa securității naționale, regionale și globale, considerăm că rămâne la latitudinea autorităților politice și militare naționale, ale N.A.T.O. și U.E.,

²⁴ N.A. Secretarul de stat Mike Pompeo, conform [<https://caleaeuropeana.ro/covid-19-secretarul-de-stat-al-SUA-mike-po...>], accesat la 13.04.2020.



ca, în urma unei analize profunde, să ia decizia corespunzătoare care să modifice sau nu locul pandemiei în documentele fundamentale care privesc securitatea.

Bibliografie

1. Barry, Buzan *Popoarele, statele și frica – O agendă pentru studii de securitate în epoca de după războiul rece*, Ediția a doua, Editura Cartier, Ediția a doua, Chișinău.
2. Andrei, Miroiu; Radu-Sebastian, Ungureanu (coord.) *Manualul de relații internaționale*, Editura Polirom, București, 2006.
3. *** *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume*, Administrația Prezidențială, București, 2015.
4. *** *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*, Administrația Prezidențială, București, 2015.
5. *** www.csid.ro>Dictionar medical
6. *** <https://dexonline.ro>
7. *** www.pwc.ro
8. *** <https://www.consilium.europa.eu>>c...
9. *** <https://www.euroactiv.ro>>extern>po...
10. *** <https://m.digi24.ro>>...>SUA
11. *** [ttps://m.mediafax.ro](https://m.mediafax.ro)>externe>po...
12. *** <https://www.caleaeuropeana.ro>>covid-19-secretarul-de-stat-al SUA-mike-po...



DESPRE SECURITATEA NAȚIONALĂ ÎN NOUL CONTEXT MONDIAL

ON NATIONAL SECURITY IN THE CURRENT WORLD

Drd. Ion-Sorin MOLDOVAN

E-mail: moldovan.ion.sorin@gmail.com

Rezumat: *Trăind într-o epocă marcată de o dinamică deosebită, ne confruntăm cu o lume a insecurității, în care se remarcă înaintea de toate prăbușirea sau alterarea sistemelor de valori tradiționale, care una după alta devin tot mai desprinse de realitate și mai greu de aplicat; este o lume conflictuală în care formele de confruntare devin însă tot mai atipice, arsenalul mijloacelor de luptă îmbracă forme tot mai puțin convenționale. În acest context foarte complicat, se constată o stringentă, imperioasă nevoie de securitate, indiferent dacă această tendință se exprimă din partea actorilor statali sau a indivizilor; totodată, remarcăm în momentul de față o continuă tendință a lumii de a stabili o nouă stare de echilibru. Aceasta într-o situație fără precedent, pe fondul procesului tot mai intens de globalizare dar și al unei dezvoltări tehnologice fără precedent. Se poate afirma că toate procesele și fenomenele clasice legate de securitate vor căpăta în noul context noi forme și caracteristici, astfel încât vom putea vorbi despre formarea unui climat de securitate cu totul și cu totul nou, care impune modificarea paradigmatelor în scopul de a identifica soluțiile eficiente.*

Cuvinte cheie: *securitate, securitate națională, apărare națională, informații, ordine publică.*

Abstract: *Living in an age marked by special dynamics, we are facing a world of insecurity, in which we notice first and foremost the collapse or alteration of traditional value systems, which one after the other are becoming more detached from reality and harder to apply; it is a conflictual world in which the forms of confrontation are becoming increasingly atypical, the arsenal of the means of combat taking less conventional forms. In this very complicated context, there is a pressing, urgent need for security, whether this tendency is expressed by state actors or individuals; at the same time, we are noticing at present a continuous tendency of the world to establish a new state of equilibrium. This is happening in an unprecedented situation, against a background of not only an increasingly intense process of globalization but also of an unprecedented technological development. It can be said that all the classic processes and phenomena related to security will acquire new forms and characteristics in the new context, so that we might be able to talk about forming an absolutely new security climate, which requires changing paradigms in order to identify effective solutions.*



Keywords: *security, national security, national defense, intelligence, public order.*

Introducere

În cadrul literaturii de specialitate și sub influența normală a actelor normative și a altor documente oficiale, dintre care se remarcă în special Strategia Națională de Securitate elaborată de Președinție, ca izvor principal de drept în acest domeniu, s-a încercat deseori definirea sintagmei de „securitate națională”. Putem observa cum strategiile anterioare anului 2015 au căutat să prevadă definiții clare ale conceptului. În mod interesant, ultima strategie de securitate (iunie 2015) nu a mai prevăzut o astfel de definire. Spre deosebire de textul strategiilor precedente, care prevedea că securitatea națională ar reprezenta *o stare de fapt caracterizând națiunea*¹, comunitățile sociale, cetățenii și statul.

Această stare de fapt, pentru a constitui în conținutul ei starea de securitate, ar trebui să aibă ca fundament prosperitatea economică, legalitatea, o situație generală de echilibru (exprimat în toate domeniile vieții sociale și în viața indivizilor) dar și stabilitatea socială și politică. În ansamblu, dacă există, starea de fapt respectivă ar fi concret exprimată prin sintagma de „ordine de drept”, la a cărei menținere participă un ansamblu sistemic de acțiuni de natură diversă (politică, economică, militară, socială, juridică, imagologică, psihologică, informațională etc.), realizate toate acestea cu scopul final al asigurării unei exercitări neîngrădite a drepturilor și libertăților cetățenești, aceasta pe fondul unei manifestări complete a componentelor autodeterminării statului, prin exercitarea atributelor sale fundamentale, care derivă din calitatea statului de subiect de drept internațional și actor al scenei internaționale².

Evenimentele din ultimele două decenii ne arată o dinamică tot mai greu previzibilă și un comportament atipic al mediului intern și internațional, situație care deseori a condus la anularea paradigmei clasice, dar fără ca în mod concomitent cineva să aducă în locul paradigmei desuete vreo soluție înlocuitoare acceptabilă. O posibilă soluție ar fi revenirea la

¹ Președinția României, *Strategia de securitate națională a României*, București, 2007.

² Filofteia Repez, Gheorghe Deaconu, Cornel Dinco, *Securitate și insecuritate în era globalizării*, Editura Universității Naționale de Apărare Carol I, București, 2011, pp. 16-21.



modelul statului național și readucerea tradițiilor și tradiționalismului la importanța de odinioară, dar această soluție este aprig contestată de anumite cercuri, în special cercurile de natură financiară sau/și comercială, care au avut foarte mult de câștigat de pe urma procesului de globalizare. În mod evident, toate aceste aspecte anterior menționate nu vor putea decât să ne pună pe gânduri, atrăgând totodată atenția specialiștilor în științe militare asupra nevoii tot mai stringente de a se elabora noi teorii, de preferință cât mai realiste, privind securitatea națiunilor și modalitățile de realizare a ei.

Securitatea, ca nevoie permanentă a individului și colectivității

Dacă vom începe analiza noastră asupra conceptului de securitate printr-o abordare strict juridică, ținând cont de modalitățile concrete de realizare a ei, observăm următoarele:

- securitatea reprezintă indubitabil nevoia cea mai importantă, ocupând astfel poziția superioară în ierarhia drepturilor colective;
- nicio națiune adevărată (care nu reprezintă doar o adunare numeroasă de persoane aduse la un loc din variate cauze sau prin hazard) nu poate subzista decât prin realizarea acelei stări de fapt care se circumscrie stării de securitate;
- în mod concret, starea de fapt pe care se bazează securitatea este materializată sub forma unui ansamblu sistemic format din norme, acțiuni de diverse tipuri și măsuri menite să conducă la realizarea acelei stări de fapt;
- nu în ultimul rând, întotdeauna starea unei națiuni este condiționată de contextul geografic (geopolitic) și istoric, pe fondul dinamicii scenei internaționale, a structurii actorilor și relațiilor ce reprezintă și caracterizează această scenă³;
- ținând cont de cele arătate mai sus, rezultă că starea unei națiuni va deveni în primul rând caracterizată prin chiar elementele specifice securității naționale, aceasta neputând fi concepută decât sub forma unui sistem unitar și indivizibil; analiza elementelor acestui sistem ne oferă o imagine asupra configurației și stabilității unei națiuni, ori cel puțin indicatorii de bază ai stabilității unei societăți și trăinicieii statului format în jurul unei națiuni.

³ Filofteia Repez, Gheorghe Deaconu, Cornel Dinco, *Securitate și insecuritate în era globalizării*, Editura Universității Naționale de Apărare Carol I, București, 2011, pp. 34-51.



Potrivit acestor caracteristici, așa cum ele au fost expuse anterior, se poate afirma că securitatea națională ar putea fi caracterizată printr-o serie de aspecte esențiale, astfel:

➤ aceasta reprezintă permanent acel *cadru unificator* sau *integrator* pentru toate componentele sale, prin care securitatea ia ființă, pe care le menține încheigate într-o structură coerentă și, în mod normal, le și fortifică;

➤ în mod normal, securitatea reflectă în cea mai fidelă manieră ansamblul *ordinii constituționale* și, astfel, devine fundația ori structura de rezistență a înfăptuirii și menținerii națiunii și statului-națiune;

➤ în cadrul sistemului de drept, securitatea este un concept integrator dar și *un scop*, un reper central, apărând *sub forma unui drept inalienabil și imprescriptibil*, universal opozabil față de orice actor al scenei internaționale, față de orice forță internă, și care în mod normal trebuie să fie bazat pe sistemele tradiționale de valori;

➤ în mod practic, securitatea nu se poate realiza decât în contextul dat de securitatea regională și globală, fiind dependentă de acestea.

Potrivit acestor observații, rezultă foarte clar nevoia stringentă de obținere (și menținere) a stării de securitate (securitatea reală, nu doar cea percepută), printr-o continuă adaptare sau intervenție (atunci când este cazul) asupra dinamicii mediului geopolitic și în materia interacțiunilor cu alți actori ai scenei internaționale.

Componentele securității și ale securității naționale

Structural, securitatea reprezintă un sistem format din cinci componente aparent autonome: securitatea *economică*, *politică*, *militară*, *socială* și *de mediu*. Dar în chip particular, securitatea *națională* nu poate fi descrisă prin simpla analiză a componentelor sale ci și prin modurile de realizare practică. Analiza noastră acordă importanță acestui aspect, în special din cauza faptului că în ultimii ani s-a observat tot mai des apariția unor confuzii legate de înțelesul corect al termenului de „*securitate*” și respectiv „*apărare*”.

Venind parcă să sporească această neplăcută confuzie, în vara anului 2015 Președenția României elaborează documentul oficial cu titlul „Strategia națională de apărare a României”, în locul utilizării denumirii de „strategie de securitate”, dând astfel de înțeles că Președintele s-ar preocupa doar de anumite componente ale securității militare, dorind astfel ca în documentele



sale oficiale să se refere de o manieră strictă și limitativă la *apărare*, nu și la celelalte componente ale securității.

Trecând însă peste astfel de abordări oficiale cel puțin confuze dacă nu eronate, putem observa că securitatea (națională) are practic o serie de componente:

➤ **Apărarea națională**, despre care (pe baza definiției conținute în lege⁴) se afirmă că reprezintă un ansamblu sistemic *de acțiuni și măsuri desfășurate de autorități specializate ale statului, în scopul apărării și garantării suveranității naționale, a independenței și unității statale, integrității teritoriale și democrației constituționale*; din analiza acestui text se poate vedea că apărarea națională se referă doar la o componentă bine precizată a securității, neputând astfel îngloba câtuși de puțin securitatea în ansamblul său, ci constituind doar esența componentei militare a securității.

Legat de apărarea națională, nu putem să nu observăm cum în ultimii ani conținutul acesteia tinde să devină tot mai ambiguu, situație creată de tendința generală (provocată de globalizare dar și de alte procese sau fenomene contemporane⁵) a diminuării aspectelor legate de principiul autodeterminării, dintre care elementele cele mai importante sunt fără dar și poate, independența și suveranitatea. Momentul de față ne înfățișează o oarecare cădere în desuetudine ale acestor două valori care, tradițional, au reprezentat, încă din epoci vechi ale istoriei, valori supreme. După modelul vechilor imperii (Imperiul Roman, Imperiul Britanic, Imperiul Austro-Ungar etc.) în noile organizații internaționale (cum este cazul UE) tendința este ca statelor membre să le fie limitate tocmai acele atribute ale autodeterminării. Astfel de situații nu sunt deloc noi, fiind întâlnite în special dacă studiem împărțirea administrativă a marilor imperii din secolele trecute. În acele cazuri, fie unul, fie câteva state aveau într-adevăr rolul de leader și se bucurau de atributele autodeterminării, în vreme ce restul națiunilor aflate sub regim de ocupație, implicit nu aveau decât dreptul de a exista sub forma unor regiuni mai mult sau mai puțin autonome. Actualmente, în cadrul UE continuă să existe state care își mențin neștirbite

⁴ Potrivit Legii nr.45/01.07.1994 *Legea apărării naționale a României*, publicată în M.Of. nr. 172/07.07. 1994.

⁵ C. Moștoflei, P. Duțu, *Apărarea colectivă și apărarea națională*, Editura Universității Naționale de Apărare, 2004.



toate atributele autodeterminării, în vreme ce statele mai mici (de pildă, cele din estul Europei) au fost într-un fel sau altul silite aproape să renunțe tocmai la valorile supreme aparținând statului național: *independența și suveranitatea*.

➤ **Siguranța națională** reprezintă o altă componentă de bază a securității, această componentă fiind formată dintr-un ansamblu de norme, acțiuni și măsuri stabilite de lege⁶ și care sunt concret destinate garantării de către stat a ordinii constituționale, dar și a valorilor fundamentale ce sunt prevăzute de Constituție, în general a așa-numitelor valori democratice, a statului de drept și, nu în ultimul rând, a siguranței tuturor cetățenilor.

Se consideră că realizarea siguranței se face, practic, prin intermediul ansamblului acțiunilor (contra)informative și de securitate (aici în sensul de asigurare a pazei, a protecției) în privința unor anumite persoane sau/și obiective. Totodată, siguranța națională se va putea la fel de bine referi la garanțiile pe care statul le pune la dispoziția națiunii, din perspectiva realizării dar și conservării nevoilor și intereselor acesteia de securitate. Trebuie, de asemenea, precizat și faptul că siguranța se referă și la îndeplinirea acelei funcții specifice a securității, *de previziune*, producând efecte în materie de prevenire a surprinderilor de orice natură ar fi acestea, dar apte să prejudicieze securitatea.

Potrivit legii anterior citate, prin conceptul de siguranță națională se înțelege *starea de legalitate, de echilibru și de stabilitate socială, economică și politică necesară existenței și dezvoltării statului național român, ca stat suveran, unitar, independent și indivizibil, menținerii ordinii de drept, precum și climatului de exercitare neîngrădită a drepturilor, libertăților și îndatoririlor fundamentale ale cetățenilor, potrivit principiilor și normelor democratice statornicite prin Constituție*. Din textul acestei definiții date de lege, rezultă că starea de siguranță nu poate fi decât direct legată de starea de legalitate, dar și condiționată de existența unui echilibru la nivel social. Concomitent, legea mai prevede și faptul că siguranța națională *se realizează prin cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe*. Din această prevedere a legii nu putem decât să remarcăm *aspectele comune* de care se ocupă apărarea și siguranța națională.

⁶ *Legea nr. 51/1991 privind siguranța națională a României*, publicată în Monitorul Oficial nr. 163/07.08.1991, republicată în Monitorul Oficial nr. 190 din 18 martie 2014.



*

Revenind însă la afirmațiile anterioare, opinăm că actele oficiale (în special acelea care au putere normativă) ar trebui să identifice mai exact înțelesul noțiunilor de *apărare* și respectiv *securitate*, în sensul că ar trebui să stabilească mult mai precis domeniul de aplicare și, astfel, stabilirea într-un regim mult mai clar a conținutului activităților specifice și domeniului de aplicare în fiecare din cele două cazuri. Atâta vreme cât se va continua confuzia între securitate și apărare, asigurarea realizării acestora va fi cu neputință tocmai din pricina menținerii confuziei asupra a două domenii diferite în conținut.

➤ **Ordinea publică** reprezintă, potrivit dispozițiilor legii⁷, *un ansamblu de norme și măsuri de natură politică, economică și socială*, ce ar trebui să permită o funcționare de ansamblu normală a instituțiilor statului, nu în ultimul rând și menținerea liniștii publice, odată cu garantarea siguranței cotidiene a cetățenilor, dar și o respectare/protejare continuă a drepturilor indivizilor și comunităților.

Ținând seama de prezența celor cinci componente ale securității (politică, economică, militară, socială, de mediu) dar și de această dinamică deosebită a lumii moderne, pe fondul unei evoluții tehnologice foarte rapide, putem vedea că atât conceptul generic de securitate cât mai ales cel de securitate națională, au căpătat noi și noi înțelesuri și elemente componente. Un aspect important în reconsiderarea conceptului de securitate l-a reprezentat caracterul multidimensional al confruntării moderne⁸, situație care a adus noi și noi elemente în ecuația securității, cel mai adesea complicând neasemuit de mult această ecuație.

Toate aceste aspecte menționate aici au condus la situația momentului de față în care securitatea ne apare ca un domeniu din ce în ce mai complex, care depășește orice fel de tentative de previziune.

Concluzii

În urma scurtei noastre analize și ținând seama de aspectele critice invocate, putem concluziona următoarele:

⁷ Potrivit *Strategiei naționale de ordine și siguranță publică 2015-2020*, Ministerul Afacerilor Interne, București, 2015.

⁸ Lucian Stăncilă, *Acțiuni militare în câmpul de luptă modern*, Editura UNAP, București, 2004.



➤ încă nu există un act normativ centralizator privind securitatea, aceasta trebuind concomitent să fie prevăzută în cadrul unui document oficial cu putere de act normativ, sub toate formele și privind toate componentele sale;

➤ sistemul de securitate, așa cum este el conceput în momentul de față, este incapabil să răspundă acțiunilor neconvenționale (cu sau fără mijloace NBC) în forme asimetrice, hibride;

➤ actualmente, populația a fost complet scoasă în afara acțiunilor și măsurilor care privesc securitatea, nemaexistând nicio implicare activă a acesteia în cadrul activităților destinate securității.

Astfel de lucruri crează premisele unor mari disfuncții în cadrul sistemului de securitate și stârnesc temeri privind capabilitatea acestui sistem de a reacționa rapid și eficace în cazuri grave.

Bibliografie

1. *** *Strategia de securitate națională a României*, Președenția României, București, 2007
2. *** *Strategia națională de apărare a țării pentru perioada 2015-2020*, Președenția României, București, 2015.
3. *** *Strategia Națională de Ordine și Siguranță Publică 2015-2020*, Ministerul Afacerilor Interne, București, 2015.
4. *** *Concepția de înzestrare cu sisteme și echipamente majore a Armatei României în perioada 2006-2025*, Ministerul Apărării Naționale, București 2006.
5. *** Ordonanța de urgență a Guvernului nr. 1 din 21.01.1999 publicată în M.Of. nr. 22 din 21.01.1999 privind Regimul stării de asediu și al stării de urgență.
6. *** Ordonanța de urgență a Guvernului nr. 21 din 2004 privind *Sistemul Național de Management al Situațiilor de Urgență*
7. Moștoflei C.;
Duțu P. *Apărarea colectivă și apărarea națională*, Editura Universității Naționale de Apărare, 2004.
8. Repez, Filofteia;
Deaconu,
Gheorghe;
Dinco, Cornel *Securitate și insecuritate în era globalizării*, Editura Universității Naționale de Apărare Carol I, București, 2011.
9. Stăncilă, Lucian *Acțiuni militare în câmpul de luptă modern*, Editura UNAP, București, 2004.



**DE LA ATRIBUȚIE LA MISIUNE.
OPERAȚIONALIZAREA ATRIBUȚIILOR JANDARMERIEI (I)**

**FROM JOB DESCRIPTION TO MISSION. OPERATIONALIZING
THE TASKS OF THE GENDARMERIE (I)**

Prof. univ. dr. Țuțu PIȘLEAG
E-mail: tutu.pisleag@yahoo.com

Rezumat: *Articolul de față aduce în dezbatere relația dintre atribuție și misiune așa după cum sunt ele precizate în legea de organizare și funcționare a Jandarmeriei Române, deși nu se fac distincții clare între acestea și nu este dezvoltată o viziune asupra modului de operaționalizare a atribuției în raport cu circumstanțele situației în care sunt angajate structurile specializate de jandarmi. Totodată, specializarea impune o delimitare clară și asupra domeniului de acțiune, o definiție a standardelor de acțiune, a principiilor și tacticilor speciale. În același timp, o astfel de relație vizează și procesul de planificare, organizare, conducere și executare a unei acțiuni cu finalitate propriu-zisă în misiune (scop, obiectiv), modul cum este proiectat acest întreg proces dinamic și cum se încadrează misiunea în atribuție.*

Cuvinte cheie: *atribuție, misiune, formă de acțiune, procedură, forțe.*

Abstract: *The present article brings into discussion the relationship between the task and the mission as spelled out in the law on the organization and functioning of the Romanian gendarmerie, although there are clear distinctions between them and there is no vision on the organization of the task in relation to the circumstances of the cases in which the specialized structures of the police are employed. At the same time, specialization imposes a clear delimitation on the scope of action, and definition of action standards, principles and special tactics. Moreover, such a perspective also concerns the process of planning, organization, management and execution of an action with proper purpose in the mission (purpose, objective), how this whole dynamic process is designed and how the mission fits the legal vocation.*

Keywords: *assignment, mission, form of action, procedure, mission, forces.*

Articolul de față aduce în dezbatere aspectele legate de operaționalizarea atribuțiilor în raport cu situația de angajare a forțelor de jandarmi și, implicit, natura acestora. Din perspectivă teroretică dar și



practică, această relație implică un proces de planificare, organizare, conducere și executare a unei acțiuni, corelat cu domeniul atribuției dar și cu scopul acesteia. Deși este consacrat prin regulamente militare, acest proces trebuie adaptat la natura polițienească a atribuțiilor jandarmeriei, întrucât relaționarea este cu cetățeanul și nu cu un adversar într-o viziune conflictuală, militară. La nivel național nu este consacrat încă un model al ordinii publice care să opereze cu instrumente standardizate și autorizate privind cultura de aplicare a legii în domeniul de ordine publică. Este chiar imperios să se dezvolte o cultură în acest domeniu, întrucât acțiunile se pot planifica, organiza și desfășura într-o viziune mult mai flexibilă, echilibrată și chiar instinctuală.

Așa după cum se prevede în articolul 4 din lege¹, reies, printre altele, două caracteristici fundamentale ale jandarmeriei, cea de „instituție specializată a statului, cu statut militar”, și „organizarea pe principii militare ca sistem unitar de forțe și mijloace”. Problema majoră pentru dezbateră se centrează pe ideea de acceptare, recunoaștere și legitimare a jandarmeriei ca forță de poliție, pentru că potrivit acestor două caracteristici se manifestă tendința de a considera jandarmeria ca pe o forță intermediară între poliție și armată, bazată pe o cultură „războinică”, a cărei abordare este una autoritară, care poate afecta legitimitatea și încrederea cetățenilor, când, de fapt, acțiunile pe care le execută sunt în cea mai mare măsură polițienești,

¹ Art. 4, alin. (1) - Jandarmeria Română este organizată pe principii militare, ca sistem unitar de forțe și mijloace dispus conform organizării administrativ-teritoriale a țării, și are următoarea structură organizatorică:

- a) Inspectoratul General al Jandarmeriei Române, denumit în continuare Inspectoratul General;
 - b) Direcția Generală de Jandarmi a Municipiului București;
 - c) Brigada Specială de Intervenție a Jandarmeriei și grupările de jandarmi mobile;
 - d) inspectoratele de jandarmi județene;
 - e) instituțiile militare de învățământ pentru formarea și pregătirea continuă a personalului;
 - f) unitățile și subunitățile specializate, necesare pentru îndeplinirea atribuțiilor specifice Jandarmeriei Române, inclusiv de sprijin logistic și medical, înființate potrivit legii.
- (2) La propunerea inspectorului general al Jandarmeriei Române, ministrul administrației și internelor, în funcție de dinamica atribuțiilor și misiunilor jandarmeriei, poate înființa, desființa, disloca și redisloca unități, până la eșalonul brigadă exclusiv, în condițiile legii, servicii, secții, birouri, compartimente și subunități de jandarmi, în limita posturilor aprobate și a fondurilor bugetare alocate.



care au ca scop fundamental garantarea exprimării libertății de exprimare și asigurarea condițiilor optime a unui climat de siguranță. Însăși expresia de „restabilire a ordine publice” poate determina din start o atitudine de combatere a protestelor din perspectiva funcției de specializare, dar fără a lua în considerare comportamentul de mulțime ca fiind o variabilă extrem de complexă și că „emoția este o caracteristică de bază a condiției umane, cu consecințe”² de multe ori chiar imprevizibile. Din această perspectivă, pe fondul „creșterii continue a amenințărilor și a infracțiunilor cu care se confruntă societatea și al resurselor limitate disponibile pentru a face față acestora, se impune agențiilor de poliție să dezvolte programe axate pe măsuri preventive și pe identificarea amenințărilor emergente (...) prin identificarea proactivă a indicatorilor și luarea de măsuri bazate pe informații”³.

Având în vedere că în structura organizatorică a jandarmeriei există Direcția Generală de Jandarmi a Municipiului București, Brigada Specială de Intervenție a Jandarmeriei, Grupările de jandarmi mobile, Inspectoratele de jandarmi județene și Unitățile specializate, și că fiecare astfel de structură are în componere „structura de comandament”, inclusiv la nivelul Batalionului de jandarmi special, subordonat Brigăzii Speciale, se conturează astfel capacitatea de suport conceptual al acțiunilor. Ori, după treizeci de ani în care s-a executat o diversitate de acțiuni, indiferent de amploarea, intensitatea și densitatea acestora, rezultă că sunt suficiente argumente baza cărora să se pună bazele doctrinare ale unui manual de specialitate.

De asemenea, în conținutul legii se operează cu doi termeni, misiuni (specifice) și atribuții, care necesită câteva clarificări conceptuale, atâta vreme cât în textul de lege, la atribuții sunt enumerate misiunile prin corelare cu statutul militar al jandarmeriei, organizarea pe principii militare,

² Alexander J. Shackman, Richard J. Davidson, *The Nature of Emotion. Fundamental Questions*, Second Edition, Oxford University Press, 2018, p. 420.

³ Nate Huber, *Intelligence led policing for law enforcement managers*, in FBI Law Enforcement Bulletin, octomber 2019, <https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers>, accesat la 17 ianuarie 2020.



sistemul unitar de forțe și mijloace. Totodată, se mai utilizează și sintagma „îndeplinirea funcțiilor principale și de sprijin”⁴ în situații de urgență⁵.

Avem în vedere că tocmai formulările „execută misiuni de asigurare a ordinii publice”, „execută misiuni de restabilire a ordinii publice” creează confuzii la nivel conceptual, atâta vreme cât pentru astfel de acțiuni specifice adunărilor publice, acțiunile structurilor de jandarmi sunt concepute, planificate și organizate prin deliberare, iar la nivel european și nu numai, sunt alte abordări care se referă la managementul mulțimilor și controlul mulțimilor. În aceste condiții s-au consacrat modalitățile de abordare a evenimentelor de mulțime: escaladarea forței, managementul negociat, comanda, controlul și incapacitarea strategică, abordări care, de fapt, nu se exclud reciproc.

⁴ <http://www.jandarmeriaromana.ro>, accesat la 12 decembrie 2019.

⁵ Asigură măsurile de menținere, asigurare și restabilire a ordinii publice; asigură planificarea judicioasă a resurselor la dispoziție în vederea îndeplinirii misiunilor specifice; participă la planificarea și asigurarea capacităților operaționale necesare deblocării căilor de acces în zona afectată de o situație de urgență, în scopul salvării vieții omenești și facilitării accesului structurilor de urgență în locațiile afectate; participă la acțiuni de căutare și salvare a persoanelor; asigură măsurile de protecție a zonelor în care există pericolul iminent de producere a unor situații de urgență și în cele de evacuare a populației; asigură securizarea și supravegherea zonelor afectate/evacuate; participă, atunci când situația o impune, la transportul unor categorii de forțe și mijloace de intervenție, al persoanelor evacuate și al altor resurse, precum și la distribuirea apei și hranei pentru persoanele și animalele afectate sau evacuate; aplică măsurile de asigurare a ordinii publice și de protecție a zonelor în care s-au produs sau există pericolul iminent de producere a unor situații de urgență și restabilirea ordinii publice în zona afectată și în imediata vecinătate a acesteia; participă la asigurarea protecției transporturilor cu ajutoare umanitare și la distribuirea acestora; asigură paza pe timpul realizării misiunilor de evacuare a populației și a bunurilor materiale; asigură securitatea și paza perimetrului zonelor de intervenție/carantină; asigură securitatea și paza zonelor evacuate; sprijină acțiunea de evacuare a persoanelor, animalelor și bunurilor și realizarea taberelor/locurilor destinate evacuaților/sinistraților; participă, în sprijinul inspectoratelor pentru situații de urgență, cu forțe și mijloace la asigurarea reacției și înlăturarea efectelor produse de situația de urgență; asigură recunoașterea, cercetarea, evaluarea în teren și raportarea primară a consecințelor situațiilor de urgență; asigură monitorizarea pericolelor și riscurilor specifice; participă la stabilirea și pregătirea punctelor de îmbarcare a evacuaților din zonele afectate; asigură legături de comunicații și informatică pentru structurile proprii - <http://www.jandarmeriaromana.ro>, accesat la 12 decembrie 2019.



În baza procesului de planificare, organizare și desfășurare a unei astfel de acțiuni care se finalizează prin planul operațional, reiese nevoia de a identifica și defini acțiunea (operațiunea) tactică în toată complexitatea conținutului și fizionomiei sale. Opțiunea este de management iar ca document operativ avansăm propunerea de „Plan operațional pentru managementul adunării publice (evenimentului de mulțime)”. În ceea ce privește prevederea potrivit căreia „execută misiuni de restabilire a ordinii publice”, abordarea este una simplistă. Este tot mai dificil în contextul actual de a concepe din start restabilirea ordinii publice când protestele sunt tot mai profesionalizate, participanții cunosc foarte bine legislația în domeniul întrunirilor publice, cunosc foarte bine drepturile pe care le au, obligațiile și limitările forțelor de ordine. Este evident că protestele au evoluat, sunt noi tactici de intimidare a forțelor de ordine, de a le provoca în utilizarea forței, de a atrage atenția mass-media.

Opțiunea este pentru managementul și controlul mulțimii, de susținere a libertății de exprimare, de protejare a siguranței participanților, de facilitare a protestului și diferențiere în intervențiile punctuale de aplicare a legii pentru că, de fapt, „aplicarea legii ar trebui să fie o ultimă instanță, în urma unei game largi de eforturi preventive”⁶. În astfel de situații avem în vedere și faptul că „ordinea publică și libertățile publice sunt două concepte care sunt mai bine înțelese împreună decât separat. Dacă ne uităm la fiecare dintre ele, nu este ușor să le definim contururile”⁷, mai ales că „ordinea publică este un concept fundamental și ușor polisemantic”⁸.

Structurile de comandament sunt organizate pe servicii, compartimente, batalioane, detașamente/companii, secții, plutoane, posturi, grupe, structuri de suport logistic, medical sau de altă natură. Structura de comandament are responsabilitatea de planificare, organizare, conducere și

⁶ *Public sector achievement in 36 countries. A comparative assessment of inputs, outputs and outcomes*, The Netherlands Institute for Social Research, The Hague, December 2015, p. 133.

⁷ Bernard Stirn (Président de section au Conseil d'État), *Ordre public et libertés publiques*, Intervention du 17 septembre 2015 lors du colloque sur l'Ordre public, organisé par l'Association française de philosophie du droit les 17 et 18 septembre 2015, <https://www.conseil-etat.fr/actualites/discours-et-interventions/ordre-public-et-libertes-publiques>, accesat la 29 ianuarie 2020.

⁸ *Ibidem*.



coordonare a acțiunilor specifice pe care o structură de jandarmi le execută. Considerăm că întregul proces de planificare, organizare, conducere, coordonare și executare a acțiunilor trebuie regândit ca fiind specific unei forțe polițienești cu statut militar, de aplicare a legii în domeniul ordinii publice. Deși sunt prevăzute atribuții pe timpul stării de asediu, la mobilizare și în timp de război, în calitate și de componentă a forțelor armate, se pune problema dimensionării operative și proiectării capacității și capabilității combative pentru astfel de situații, cu precizarea că astfel de acțiuni au un caracter limitat în timp și spațiu. Astfel, se impune diferențierea pregătirii inițiale și continue a personalului în raport cu conceptele doctrinare în domeniu, dotării adecvate etc., mai ales că este dificil de definit concepte juridice fără ca aplicabilitatea acestora să poată fi verificată în teren.

Sistemul unitar de forțe reclamă „crearea unei înțelegeri comune a mediului operațional, a scopului acțiunilor, a problemelor și abordărilor de rezolvare ale acestora, ca o provocare pentru comandanți și personal”⁹. Analizând deopotrivă, misiunile și atribuțiile, așa după cum sunt ele prevăzute în lege, cu toate că nu există o delimitare clară a acestora și că nu este o prevedere explicită a statutului de forță de poliție a jandarmeriei, totuși, considerăm că angajarea structurilor de jandarmi în domeniul ordinii publice evidențiază natura polițienească a acțiunilor care presupun strategii operaționale specifice oricărei forțe de poliție care nu are statut militar, deși se observă o tendință de militarizare a acestora sub aspectul dotării. Poate tocmai acest sistem unitar de forțe impune o abordare modernă și unitară prin modalitatea de aplicare a legii în domeniul ordinii publice în raport cu evoluțiile specifice.

Din practică, se constată că cele mai frecvente acțiuni ale structurilor de jandarmi sunt în domeniul ordinii publice, fapt ce conduce la ideea că jandarmeria este o forță de poliție, de ordine publică. Observăm, de altfel, și caracterul militar al unei forțe de poliție – jandarmeria, prin organizare, statut, cultură, tradiții. Ori, din această perspectivă, „dezbaterea academică privind militarizarea poliției este concentrată și pe dezvoltarea democrațiilor care ridică întrebări cu privire la modul de democratizare/demilitarizare a

⁹ Nathan K. Finney, Jonathan P. Klug, *Mission Command in the 21st century: Empowering to Win in a Complex World*, Fort Leavenworth, Kansas, The Army Press, 2016, p. iii.



forțelor de poliție pentru a răspunde tuturor cerințelor unui stat constituțional modern¹⁰.

În tabelul de mai jos, avem în vedere o departajare a misiunilor și a atribuțiilor, deși în cadrul atribuțiilor regăsim unele misiuni care sunt considerate ca fiind atribuții. Astfel, este nevoie de o clarificare conceptuală a ceea ce reprezintă misiunea și atribuția. Potrivit dicționarului, prin misiune se înțelege „însărcinare dată cuiva de a face un anumit lucru”¹¹, „sarcină pe care o primește sau și-o asumă cineva”¹² sau „rol, rost, menire”¹³. Astfel, se poate aminti și alte sensuri ale misiunii, misiune diplomatică, misiunea școlii, misiunea bisericii, misiunea guvernului, misiune permanentă (ONU), misiune spațială, misiuni de consolidare a păcii etc.

Din perspectivă militară prin misiune se înțelege „sarcina, împreună cu scopul, care indică clar acțiunea care trebuie întreprinsă și motivul”¹⁴ iar prin referire la eșaloanele tactice mici „îndatorirea atribuită unei persoane sau unei unități; o sarcină”¹⁵. Atribuția reprezintă „sfera de autoritate, de competență, de activitate a cuiva; însărcinare dată cuiva pentru îndeplinire”¹⁶. Se poate deduce că toate aceste sarcini, îndatoriri au un anumit specific determinat de statutul militar al jandarmeriei, de natura polițienească a unora dintre aceste îndatoriri, de respectarea drepturilor omului, de respectarea unor standarde de aplicare a legii, de urgența îndeplinirii acestora, de respectarea unor principii în utilizarea forței, în utilizarea mijloacelor de protecție și intervenție în aplicarea legii etc. Dacă ne raportăm la conținutul art. 1 și 2 din lege¹⁷, se conturează domeniul de

¹⁰ Marleen Easton, *Military Policing*, The Sage Encyclopedia of War: Social Science Perspectives, Sage Publications; 2017, p. 1117.

¹¹ *Dicționar enciclopedic*, Editura Cartier, ediția a V-a, revizuită și actualizată, 2004, p. 541.

¹² *Ibidem*.

¹³ *Ibidem*.

¹⁴ Department of Defense, *Dictionary of Military and Associated Terms*, p. 144, <https://www.jcs.mil/Portals/0/Documents/Doctrine/pubs/dictionary>.

¹⁵ *Ibidem*.

¹⁶ *Dicționar enciclopedic*, Editura Cartier, Ediția a V-a, revizuită și actualizată, 2004, p. 71.

¹⁷ Art. 1, (1) Jandarmeria Română este instituția specializată a statului, cu statut militar, componentă a Ministerului Administrației și Internelor, care exercită, în condițiile legii, atribuțiile ce îi revin cu privire la apărarea ordinii și liniștii publice, a drepturilor și libertăților fundamentale ale cetățenilor, a proprietății publice și private, la prevenirea și descoperirea infracțiunilor și a altor încălcări ale legilor în vigoare, precum și la protecția



autoritate, de competență, ca fiind ordinea publică „percepută ca un anumit regim al societății iar menținerea acesteia predetermină securitatea și stabilitatea publică”¹⁸.

Misiuni	Modalitatea de executare	Atribuții	Modalitatea de executare
a) În condiții de normalitate (pe timp de pace), în calitate de instituție specializată, cu statut militar, ca forță de poliție, componentă a Ministerului Afacerilor Interne			
acțiuni, misiuni de menținere a păcii, art. 3, aln. (2)	participare, îndeplinire, art. 3, aln. (2)		
misiuni specifice în municipiul București – DJMB, art. 8, aln.(1)	planificare, organizare, conducere, executare	atribuții în municipiul București, DGJMB, art. 8, aln.(1)	îndeplinire
misiuni de asigurare și restabilire a ordinii publice, asigurare a protecției instituțiilor fundamentale ale statului și neutralizarea amenințărilor grave la adresa acestora, Bg.S.I.J.R., art. 9, aln. (1)	executare independent sau în cooperare, asigurare, neutralizare, Bg.S.I.J.R., art. 9, aln. (1)		
misiuni specifice , IJJ, art. 10, al. (1)	planificare, organizare, conducere, executare, IJJ, art. 10, al. (1)	atribuții , IJJ, art. 10, al. (1)	îndeplinire
misiuni de asigurare și restabilire a ordinii publice și de combatere	organizare, executare, G. Mb. J., art. 11, aln. (1)	atribuții , structuri specializate, art. 19, aln. (1), art. 20, aln.	apărare, executare misiuni , executare misiuni la solicitare,

instituțiilor fundamentale ale statului și combaterea actelor de terrorism. (2) Jandarmeria Română, prin atribuții, organizare, pregătire și dispunere teritorială, contribuie la garantarea suveranității, independenței, autorității, unității și securității statului, democrației constituționale pe întregul teritoriu național atât în timp de pace, cât și în situații de criză.

Art. 2. Jandarmeria Română își desfășoară activitatea în interesul cetățenilor, al comunității și în sprijinul instituțiilor statului, exclusiv pe baza și în executarea legii.

¹⁸ Vladas Tumulavičius, Jānis Ivančiks, Oleksandr Karpishchenko, *Issues of Society Security: Public Safety under Globalisation Conditions in Lithuania*, Journal of Security and Sustainability Issue, 2016 June Volume 5 Number 4, pp. 547 – 548.



Misiuni	Modalitatea de executare	Atribuții	Modalitatea de executare
a infracționalității, G. Mb. J., art. 11, aln. (1)		(1)	executare misiuni pe baza planurilor de cooperare, executare în cooperare, executare misiuni de intervenție antiteroristă, asigură paza sau protecția, participare în cooperare la misiuni , participare în cooperare, participare la misiuni în afara teritoriului statului român, asigurare măsuri de ordine și de protecție, efectuare acte necesare începerii urmăririi penale
misiuni specifice , B.J.S., art. 12, aln. (1)	executare, B.J.S., art. 12, aln. (1)		
misiuni de pază sau de protecție și apărare a unor obiective, bunuri, valori de importanță deosebită, alte misiuni pe un anumit domeniu de competență al jandarmeriei, U.S., art.14, aln. (1) .	executare, U.S., art.14, aln. (1)		
misiuni specifice , Dt, Cp., Pl., art. 13.	îndeplinire, independent ori în subordine, Dt, Cp., Pl., art. 13.		
b) Pe timpul stării de urgență – în calitate de instituție specializată, cu statut militar, componentă a Ministerului Afacerilor Interne			
misiuni specifice , stare de urgență, art. 21	îndeplinire, aplicare ordonanțe militare, art. 21		
c) Pe timpul stării de asediu, la mobilizare și în timp de război - în calitate și de componentă a forțelor armate			
		atribuțiile prevăzute la art. 19, atribuții în calitate de componentă a forțelor armate art. 22, aln. (1).	îndeplinire atribuții prevăzute la art. 19 - executare, participare, asigurare, executare în cooperare, executare orice alte misiuni

Tabelul nr. 1 Departajarea misiunilor și atribuțiilor structurilor specializate de jandarmi



Astăzi, tot mai mult, atât poliția cât și jandarmeria sunt „cele mai vizibile manifestări ale autorității guvernamentale responsabile de securitatea publicului (...) și trebuie să funcționeze în conformitate cu legile naționale și internaționale și să respecte drepturile omului în orice moment”¹⁹. Marea provocare pentru aproape toate forțele de ordine publică sunt protestele care iau o varietate de forme de exprimare prin caracterul de spontaneitate și nereglementare și care, „sub influența internetului și a rețelelor sociale sunt din ce în ce mai frecvente”²⁰, sunt „în mare parte mișcări fără conducere cu puțin atașament față de grupările sau ideologiile politice tradiționale”²¹. Multe proteste par „a fi alimentate de noua tehnologie de comunicare, îmbrățișează o viziune redusă asupra construirii instituțiilor dincolo de o respingere a elitelor existente și a structurilor de putere consacrate”²². Astfel de mobilizări civice impun forțelor de ordine publică adecvarea tacticilor de răspuns potrivit formelor de manifestare și obiectivelor protestelor. Reținem în același timp că „dat fiind că sunt rețele nemărginite deschise, care se reconfigurează mereu în funcție de nivelul de implicare a populației în general, această structură descentralizată deschide noi oportunități de a se alătura la mișcare și reduce, de asemenea, vulnerabilitatea mișcării la amenințarea cu represii, căci există puține ținte specifice care să fie reprimite, cu excepția locurilor ocupate”²³. În raport cu aceste elemente de noutate ale manifestării protestelor în spațiul public, se impune nevoia de revizuire și consolidare a aplicării legii privind problema libertăților civile pe timpul adunărilor publice, „aplicarea uniformă a standardelor de utilizare a forței, elaborarea de instrucțiuni clare cu privire la necesitatea autocontrolului, a muncii în echipă și respectării ordinelor”²⁴.

¹⁹ *Guidebook on Democratic Policing by the Senior Police Adviser to the OSCE Secretary General*, Vienna, May 2008, 2nd Edition, p. 6.

²⁰ *Facilitating Peaceful Protests*, Academy Briefing, No. 5, Geneva Academy of International Humanitarian Law and Human Rights, January 2014, p. 12.

²¹ Thomas Carothers and Richard Youngs, *The Complexities of Global Protest*, Carnegie Endowment for International Peace, 2015, p. 4.

²² *Ibidem*.

²³ Manuel Castells, *Comunicare și putere*, Editura Comunicare.ro, 2013, p. xxxix.

²⁴ Tony Narr, Jessica Toliver, Jerry Murphy, Malcolm McFarland, Joshua Ederheimer, *Police Management of Mass Demonstrations: Identifying Issues and Successful Approaches*, Police Executive Research Forum, 2006, p. 22.



Revenind la misiuni și atribuții, este nevoie de a aduce în atenție sintagma de forțe și mijloace întrebuintate pentru desfășurarea unei adunări publice în condiții de siguranță, prin care înțelegem „agregarea” personalului din structurile specializate, a mijloacelor de protecție și intervenție, a echipamentelor de suport, o combinare a acestora, care în final se configurează ca formă de acțiune tactică specifică, acțiune tactică de jandarmi (acțiune tactică polițienească, operațiune polițienească). Aceasta se exprimă și prin modul, poziția, atitudinea în care sunt sincronizate forțele și resursele la dispoziție în timp și spațiu, în raport cu scopul (văzut ca finalitate, rezultat, obiectiv, misiune), strategii și tactici, ca opțiuni, pentru a executa acțiuni simultane, succesive și secvențiale, dar care au în centru valorile democratice cu privire la respectarea drepturilor fundamentale ale omului într-o societate democratică.

Prin raportare la structurile forțelor armate, forma de acțiune evidențiază și atitudinea adoptată ca răspuns față de atitudinea adversarului, altfel spus, este nevoie de existența manifestării unui adversar care pune în pericol integritatea teritorială, independența și suveranitatea statului. Trebuie totuși, să precizăm că pentru forțele de jandarmi cu atribuții în domeniul ordinii publice, răspunsul exprimat ca atitudine este față de evenimentul de mulțime, de manifestarea acesteia în raport cu legea, și mai importantă este cerința de protecție și garantare a drepturilor constituționale. Considerăm că în cazul de față suntem mai degrabă în situația de management al mulțimii, de control al mulțimii, ca operațiune polițienească și nu în situația adoptării unei forme de acțiune. Ceea ce este comun constă în planificarea, organizarea și desfășurarea unor activități și măsuri în baza unui plan operațional prin care să se asigure siguranța participanților la o adunare și, implicit, a forțelor de ordine, protejarea unor bunuri etc. Intervine aici menținerea unui echilibru în raportul autoritate – libertate, astfel încât prin mijloacele și metodele prevăzute de lege să se apere „viața, integritatea corporală și libertatea persoanei, proprietatea publică și privată, interesele legitime ale cetățenilor, ale comunității și ale statului”²⁵.

²⁵Art. 19, alin (1), lit. a), Legea nr. 550 din 29 noiembrie 2004 privind organizarea și funcționarea Jandarmeriei Române, Monitorul Oficial al României nr. 1175 din 13 decembrie 2004, cu modificările ulterioare.



În situațiile în care se execută mai multe acțiuni tactice specifice, se configurează operațiunea tactică de jandarmi. În esență, forma de acțiune reprezintă un ansamblu de măsuri și activități concepute, planificate, organizate și desfășurate pentru îndeplinirea unei misiuni, pentru realizarea unui obiectiv specific. Pentru acțiunile specifice din domeniul ordinii publice, în procesul de planificare „planificatorii trebuie să stabilească misiunea de protejare a drepturilor constituționale ale tuturor participanților, oferind, în același timp, un mediu sigur și pașnic. Este esențial ca această viziune să fie împărtășită întregii echipe de planificare, întărită prin antrenament și monitorizare în timpul evenimentului”²⁶. Inexistența manifestării unui adversar din perspectiva conflictualității militare, în domeniul ordinii publice, în special pe timpul evenimentelor de mulțime, nu mai putem considera adoptarea și operaționalizarea unei forme de acțiune, ci mai degrabă managementul mulțimii centrat pe asigurarea protecției și siguranței participanților.

Intervine desigur și aici, nevoia unui plan de acțiune (plan operațional) proiectat și conceput pe trei etape, etapa pre-eveniment, etapa operațională (pe timpul evenimentului) și etapa post-eveniment, în care comunicarea tactică este esențială. Întregul proces de planificare are ca rezultat planul de acțiune (planul operațional) pe baza căruia se desfășoară acțiunea tactică sau operațiunea polițenească.

Pentru domeniul de ordine publică trebuie avut în vedere că „aplicarea legii răspunde la o gamă largă de incidente și operațiuni de securitate care sunt de obicei gestionate de o singură unitate sau departament”²⁷, de unde rezultă nevoia de elaborare a unui sistem de gestionare a incidentelor, cu precizarea că atributele de coordonare și conducere revin acelei forțe care are în competență domeniul, are cele mai multe forțe și are operaționalizate structuri de conducere. Față de toate cele prezentate și într-o perspectivă a actualizării legii de organizare și funcționare a jandarmeriei prin care să se delimiteze clar misiunile de atribuții și implicit de elaborare a unui manual al acțiunilor jandarmeriei, ca metodologie de aplicare a legii prin care să se definească tipologia formelor de acțiune, aducem în dezbatere față de prevederile legii actuale, răspunsul

²⁶ Bureau of Justice Assistance, *Managing Large-Scale Security Events: A Planning Primer for Local Law Enforcement Agencies*, May 2013, p. 18.

²⁷ *Ibidem*, p. 33.



ca formă de acțiune, excluzând reacția, cu particularizările și adaptările necesare, în situații de urgențe civile, altele decât cele din domeniul evenimentelor de mulțime.

Toate acestea au o contribuție substanțială în a redefini, adecva și moderniza știința tacticii de specialitate (de jandarmi), care în esență se referă la „capacități, tehnici și proceduri care pot fi măsurate, cuantificate și utilizate pentru îndeplinirea sarcinilor specifice”²⁸. Este deja recunoscut că „tactica necesită și adaptare la circumstanțele unice ale unei situații, în care tehnicile și procedurile adoptate, ca modele sau procese stabilite, pot conduce și la crearea de noi tehnici și proceduri”²⁹ ca pași standard, detaliați, care prescriu modul de îndeplinire a sarcinilor specifice.

În literatura de specialitate s-a consacrat și sintagma de procedeu de acțiune (luptă) care se poate defini ca modalitate de acțiune având o sferă de cuprindere mai limitată în timp și spațiu decât forma de acțiune. Este evident că forma de acțiune se exprimă prin tactici, procedee de acțiune, tehnici și proceduri care au ca finalitate misiunea și care la rândul acesteia le influențează, ceea ce face ca forma de acțiune să fie într-un proces de interrelaționare a acestor elemente și, totodată, de modernizare. Tehnicile sunt metode detaliate, utilizate de către forțe sau comandanți în îndeplinirea sarcinilor atribuite. Ele descriu elementele de bază în utilizarea echipamentelor și a personalului”³⁰. Procedurile se concretizează în „cel mai scăzut nivel de detalii al unui anumit curs sau mod de acțiune, descriu modul de a efectua o anumită sarcină”³¹. Toate aceste procedee, tehnici și proceduri, prin caracterul lor permanent includ „moduri de operare pentru arme și echipamente, acțiuni ale forțelor și coordonarea lor”³² și au ca finalitate „caracterul unitar al unei acțiuni, eficiența acesteia și completarea reciprocă a elementelor de dispozitiv”³³.

²⁸ *ADP 3-90 Offense and Defense*, Headquarters Department of the Army Washington, DC, 31 July 2019, pp. 1-3.

²⁹ *Ibidem*, p. 1-1.

³⁰ *Field Manual, FM 3-19.1 Military Police Operations*, Headquarters Department of the Army, Washington, DC, 22 March 2001, Appendix B Doctrine and Training Literature, 22 March 2001, p. 2 of 2.

³¹ *Ibidem*.

³² *Ibidem*.

³³ *Ibidem*.



Bibliografie

A. Documente oficiale

1. *** *Constituția României*, Monitorul Oficial al României, Partea I, nr. 233 din 21 noiembrie 1991, modificată și completată prin Legea de revizuire a Constituției României nr. 429/2003, Monitorul Oficial al României, Partea I, nr. 758 din 29 octombrie 2003.
2. *** *Legea nr. 550 din 29 noiembrie 2004 privind organizarea și funcționarea Jandarmeriei Române*, Monitorul Oficial al României nr. 1175 din 13 decembrie 2004, cu modificările ulterioare.
3. *** *Legea nr. 60 din 1991 privind organizarea și desfășurarea adunărilor publice*, Monitorul Oficial al României, Partea I, nr. 192 din 25 septembrie 1991, republicată.
4. *** *Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad*, Boletín Oficial del Estado núm. 63, de 14 de marzo de 1986, España.
5. *** *Guidebook on Democratic Policing* by the Senior Police Adviser to the OSCE Secretary General, Vienna, May 2008, 2nd Edition.
6. *** *The Anthology GODIAC – Good practice for dialogue and communication as strategic principles for policing political manifestations in Europe*, Polisen, With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission – Directorate – General Home Affairs and the Swedish National Police Board, HOME/2009/ISEC/AG/182, 2013.
7. *** *Instruction du 21 avril 2017 relative au maintien de l'ordre public par la police nationale*, Bulletin Officiel du Ministère de l'Intérieur.
8. *** *ADP 3-90 Offense and Defense*, Headquarters Department of the Army Washington, DC, 31 July 2019.
9. *** *Crowd Dynamics in Public Order Ops*, UN Peacekeeping PDT Standards for Formed Police Units, 1st edition, 2015.
10. *** *Field Manual, FM 3-19.1 Military Police Operations*, Headquarters Department of the Army, Washington, DC, 22 March 2001, Appendix B Doctrine and Training Literature, 22 March 2001.
11. *** *Facilitating Peaceful Protests*, Academy Briefing, No. 5, Geneva Academy of International Humanitarian Law and Human Rights, January 2014.
12. *** Bureau of Justice Assistance, *Managing Large-Scale Security Events: A Planning Primer for Local Law Enforcement Agencies*, May 2013.
13. *** Los Angeles Police Department, *Report to the Board of Police Commissioners, An Examination of May Day 2007*.
14. *** *Managing Major Events: Best Practices from the Field*, Police Executive Forum, Washington, 2011.
15. *** Department of Defense, *Dictionary of Military and Associated Terms*.
16. *** *Joint Concept Note 2/17, Future of Command and Control, Development*,



- Concepts and Doctrine Centre, 2017.
17. *** *Public sector achievement in 36 countries. A comparative assessment of inputs, outputs and outcomes*, The Netherlands Institute for Social Research, The Hague, December 2015.
18. *** World Economic Forum, *The Global Risks Report 2020*, 15th Edition, In partnership with Marsh & McLennan and Zurich Insurance Group.
19. *** *Dicționar enciclopedic*, Editura Cartier, ediția a V-a, revizuită și actualizată, 2004.
20. *** *FBI Law Enforcement Bulletin*, octomber 2019.

B. Lucrări de autori și surse web

1. Thomas, Carothers and Richard, Youngs *The Complexities of Global Protest*, Carnegie Endowment for International Peace, 2015.
2. Manuel Castells *Comunicare și putere*, Editura Comunicare.ro, 2013.
3. Cedric de Coning; Mateja, Peter *United Nations Peace Operations in a Changing Global Order*, Palgrave Macmillan, 2019.
4. John, Christian; Matthew, Lewis; Scott, Gerwehr; Russell W. Glenn, Barbara R. Pantich, Dionne, Barnes-Proby; Elizabeth, Williams; David, Brannan *Training the 21st Century Police Officer. Redefining police professionalism for the Los Angeles Police Department*, Public Safety and Justice RAND, 2003.
5. Marleen, Easton *Military Policing, The Sage Encyclopedia of War: Social Science Perspectives*, Sage Publications; 2017.
6. Trevor, Findlay *The Use of Force in UN Peace Operations*, Stockholm International Peace Research Institute, 2002.
7. Juan Carlos Montalvo Abiol *Concepto de orden público en las democracias contemporáneas*, Revista Jurídica Universidad Autónoma de Madrid, n° 22, 2010-II.
8. Nathan, K. Finney, Jonathan, P. Klug *Mission Command in the 21st century: Empowering to Win in a Complex World*, Fort Leavenworth, Kansas, The Army Press, 2016.
9. Nate, Huber *Intelligence led policing for law enforcement managers*, in *FBI Law Enforcement Bulletin*, octomber 2019.
10. Jaír van der Lijn; Ivan, Briscoe; Margriet, Drent; Kees, Homan; Frans-Paul van der Putten; Dick, Zandee *Peacekeeping operations in a changing world*, Netherlands Institute of International Relations Clingendael, 2015.



11. C. Martellaa; J. Li, C. Conradob; A. Vermeerenc *On Current Crowd Management Practices and the Need for Increased Situation Awareness, Prediction, and Intervention*, 2016.
12. Tony, Narr; Jessica, Toliver; Jerry, Murphy; Malcolm, McFarland; Joshua, Ederheimer *Police Management of Mass Demonstrations: Identifying Issues and Successful Approaches*, Police Executive Research Forum, 2006.
13. Stephen, Otter *Urban Safety Project, Urban Policing in Myanmar*, The Asia Foundation, October 2017.
14. Marco, Sassòli *Legislation and Maintenance of Public Order and Civil Life by Occupying Powers*, The European Journal of International Law, vol. 16 no.4, 2005, p. 665.
15. Alexander J. Shackman; Richard J. Davidson *The Nature of Emotion. Fundamental Questions*, Second Edition, Oxford University Press, 2018.
16. Bernard, Stirn *Ordre public et libertés publiques*, Intervention du 17 septembre 2015 lors du colloque sur l'Ordre public, organisé par l'Association française de philosophie du droit les 17 et 18 septembre 2015.
17. Vladas, Tumalavičius; Jānis, Ivančiks; Oleksandr, Karpishchenko *Issues of Society Security: Public Safety under Globalisation Conditions in Lithuania*, Journal of Security and Sustainability Issue, 2016 June Volume 5 Number 4.
18. *** <https://www.jcs.mil> > Portals > Documents > Doctrine > pubs > dictionary.
19. *** <https://www.few.vu.nl/~cma330/papers/SafetyScience.pdf>.
20. *** <https://www.statewatch.org/news/2010/nov/eu-policing-protests-godiak-project.pdf>.
21. *** <http://www.jandarmeriaromana.ro>.
22. *** <https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers>.
23. *** <https://www.conseil-etat.fr/actualites/discours-et-interventions/ordre-public-et-libertes-publiques>.
24. *** <https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers>.



BREXIT – ȘI VIITORUL POLITICII EXTERNE ȘI DE SECURITATE COMUNĂ A UNIUNII EUROPENE

BREXIT – AND THE FUTURE OF EXTERNAL AND COMMON SECURITY OF THE EUROPEAN UNION

Lt. col. lector univ.dr. Bogdan-Cezar CHIOSEAU

Academia Forțelor Aeriene „Henri Coandă”

E-mail: b.chioseau@gmail.com

Rezumat: Uniune, alianță, parteneriat, imperiu,... sunt termeni care din punct de vedere conceptual sunt diferiți, însă atunci când ne raportăm la etape istorice, în care au avut loc aceste „coaliții”, observăm că toate au urmărit în principal același lucru. Puterea.

Dominanță, supremație, deținerea controlului total, termeni ce pot fi asimilați ca și atribute ale puterii, analizați la nivel național tind spre o imagine a unei crude dictaturi, însă raportați la repere istorice, constatăm că, cel mai adesea acestea s-au instaurat prin violență și prin subminarea puterii celui mai slab. Unele forme moderne ale războiului (Războiul Hibrid) ne demonstrează faptul că, mai nou, violența poate fi înlocuită de înșelăciune și manipulare a maselor.

Cuvinte cheie: Brexit, securitate, alianță, uniune, referendum, Mare Putere.

Abstract: Union, alliance, partnership, empire,... all of them are terms that are different, conceptually speaking, but when we refer to historical stages, in which these "coalitions" took place, we notice that they all pursued mainly the same thing. The power.

Domination, supremacy, total control, terms that can be assimilated as attributes of power, analyzing them at national level they offer an image of a cruel dictatorship, but compared to historical landmarks, we find that, most often they were established by violence and by undermining the power of the weakest. Some modern forms of warfare (like Hybrid Warfare) recently show us that, violence can be replaced by deception and mass manipulation.

Keywords: Brexit, security, alliance, union, referendum, Great Power.

Introducere

În data de 31 ianuarie 2020, la miezul nopții, Marea Britanie părăsește marea familie europeană, după aproape o jumătate de secol de „conviețuire”.



Harta geopolitică a Europei se schimbă. Anglia, un actor important pe scena europolitică și un personaj principal atunci când se discută despre Politica Externă și de Securitate Comună (PESC), părăsește Uniunea Europeană (U.E.), însă cu promisiunea că nu va părăsi și Europa¹ și își va onora angajamentele față de securitatea și apărarea comună a Europei.

De ce s-a ajuns aici? A fost o surpriză referendumul din 23 iunie 2016? Reprezintă Brexitul o formă a războiului hibrid? Și, mai ales, ce efecte va propaga Brexit-ul asupra PESC a U.E.? Sunt întrebări care încă se mai aud pe holurile și în sălile de ședințe ale multora dintre cancelariile europene.

În încercarea de a găsi răspunsuri pertinente se simte nevoia unei scurte radiografii a ceea ce a fost U.E. înainte și, mai ales, după aderarea Regatului Unit al Marii Britanii.

Repere în timp

La 25 martie 1957, Belgia, Germania, Franța, Italia, Luxemburg, Olanda, membre ale Comunității Europene a Cărbunelui și Oțelului, pun bazele unei comunități economice, Comunitatea Economică Europeană (CEE), predecesoarea Uniunii Europene (U.E.) de astăzi, o structură, o „alianță” menită să își aducă aportul la integrarea și creșterea economică a statelor membre prin intermediul comerțului. Pentru a consolida această „alianță”, membrii ei fondatori lansează în 1950 și un proiect de constituire a unei Comunități Europene pentru Apărare, o armată europeană, inițiativă ce nu a avut însă succes, unul dintre motive fiind proaspăta înființată alianță, Organizația Tratatului Atlanticului de Nord (North Atlantic Treaty Organization - NATO, care venea cu misiunea de a asigura protecția statelor membre prin mijloace politice și militare.

Rând pe rând, în timp, se alătură CEE mare parte din statele europene. Astăzi U.E., continuatoarea CEE, are 27 de membri care, împreună, au dezvoltat vechea CEE și au construit o uniune politică și economică ce are la dispoziție o piață unică internă, cu un sistem de legi modern și standardizat.

¹ N.A. Interviu acordat de primul ministru britanic Theresa May publicației Bild în 20 ianuarie 2018 [<https://www.bild.de/politik/ausland/brexit/will-you-miss-us-mrs-may-54535638.bild.html>], accesat la 02.04.2020.



După 16 ani de la constituirea CEE, la 1 ianuarie 1973, Regatul Unit al Marii Britanii și al Irlandei de Nord, curtat de mai multe ori și cu câteva tentative eșuate de aderare, reușește cu scepticism și îndoială să se alăture Comunității Europene. Voalul de neîncredere care plutea pe continent referitor la incompatibilitatea economică a Regatului Unit precum și poziția rezervată a acestuia atunci când se discutau unele proiecte europene² nu s-a risipit total chiar dacă, referendumul din 1975, ne relevă faptul că peste 67% dintre britanici și-au manifestat intenția de a rămâne în Uniunea Europeană.

Astfel, Regatul Unit se alătură familiei europene chiar dacă, uneori, direcțiile impuse de la Strasbourg, Bruxelles și Luxemburg³ nu sunt tocmai pe placul britanicilor, o națiune obișnuită să fie tratată diferențiat, de pe poziția sa de mare putere economică și militară și pentru care normele și regulile europene, obligatorii pentru alte state membre, sunt adesea supuse unor discuții și dispute la Palatul Westminster⁴.

Londra acceptă din ce în ce mai greu poziția sa de „stat membru” în defavoarea statutului de „Mare Putere Mondială”, iar prioritățile acesteia sunt reprezentate de interesul național în păstrarea uniunii insulare (Anglia, Scoția și Țara Galilor) și preocuparea majoră privind îmbunătățirea relațiilor, deja privilegiate, pe care le are cu Statele Unite ale Americii în sectorul economic și mai ales militar. În plus, jocurile politice și confruntările dintre conservatori și laburiști⁵ au o nouă miză, rămânerea sau nu în Uniunea Europeană, iar peste toate acestea, criza migrației din perioada 2015-2016 și faptul că Regatul Unit, a doua mare economie europeană participă cu contribuții importante la bugetul european

² N.A. Guvernul britanic refuză implementarea Sistemului Monetar European. Primul ministru britanic, Margaret Thatcher, susține importanța menținerii suveranității Marii Britanii și își exprimă neîncrederea față de acest proiect european, [<https://www.margaretthatcher.org/document/107332>], accesat la 02.04.2020.

³ Strasbourg, Bruxelles și Luxemburg – Cele trei sedii ale Parlamentului European, [<https://www.europarl.europa.eu/sides/getDoc.do...>], accesat la 02.04.2020.

⁴ Locul unde se află cele două camere ale Parlamentului Regatului Unit al Marii Britanii și Irlandei de Nord: Camera Lorzilor și Camera Comunelor, [<https://www.parliament.uk/>], accesat la 02.04.2020.

⁵ N.A. Partidul Conservator – partid politic de centru dreapta, Partidul Laburist - partid politic de centru stânga, partide politice din Regatul Unit consacrate ca fiind rivale, [<https://www.openpolitics.ro/conservatorii-si-laburistii-lupta-pentru-brexite/>], accesat la 02.04.2020.



(aproximativ 9 miliarde de lire sterline anual, echivalentul a 0,5% din PIB-ul țării⁶), nu face altceva decât să contureze drumul Angliei în afara Uniunii Europene.

Așadar, la întrebarea, De ce s-a ajuns aici? deși nu este acceptabil din punct de vedere științific, putem răspunde cu o întrebare retorică și anume: Și-a dorit oare, cu adevărat, Marea Britanie apartenența la Uniunea Europeană?, iar la aceasta adăugând și aspectele prezentate, formulăm o concluzie pe care poate că ar fi trebuit să o anticipeze și decidenții de la Bruxelles: Regatul Unit și Uniunea Europeană sunt două entități ce nu pot fi compatibile întotdeauna, mai ales atunci când vine vorba despre interes național, influențe economice și financiare sau jocuri politice.

Brexitul și dorința britanicilor

Ideea „Brexitului” a apărut relativ repede, raportat la momentul aderării Regatului Unit la U.E., anul 1973, atunci când, printr-o procedură legislativă, propusă și susținută de guvernul conservator aflat la putere, Anglia devine stat membru al U.E. Metoda abordată de conservatori a fost vehement contestată de guvernul laburist care, un an mai târziu, după ce a preluat puterea, a considerat că nu este legală, iar pentru ca Marea Britanie să devină membră a Uniunii, trebuie consultați cetățenii britanici. Drept urmare, în 1975 se organizează primul referendum pe problema apartenenței Regatului Unit la U.E., laburiștii onorându-și astfel și promisiunile din campania electorală.

Este o perioadă marcată de schimbări și fluctuații ale raporturilor de putere. Majoritățile politice în Camerele Palatului Westminster se modifică ca urmare a rezultatelor alegerilor democratice, precedate de campanii electorale îndelung pregătite din care nu lipsesc discursurile populiste în care se preaslăvește măreția Imperiului Britanic și se critică faptul că deciziile Londrei au ajuns să fie monitorizate și analizate pe continent.

Cu toate acestea, prima tentativă de Brexit eșuează. Electoratul Regatului Unit decide cu 67,2% rămânerea în Uniunea Europeană arătând, pe deoparte, că este interesat de dezvoltarea și implicarea în proiectele comune cu partenerii europeni, iar pe de altă parte, încearcă să-și mențină

⁶ <https://business24.ro/international/ue/de-ce-vrea-marea-britanie-sa-iasa-din-ue-15649>, accesat la 02.04.2020.



prin această apartenență, o cale prin care poate influența și controla un mare centru de putere al lumii.

Uniunea Europeană este în ascensiune. Dezvoltarea ei pe toate palierele implică și implementarea unor direcții noi și comune de acțiune, măsuri de coordonare, monitorizare și control, toate acestea stând la baza elaborării unor pachete de legi și reglementări restrictive. Marea majoritate decide adoptarea unor principii și sisteme la care toate statele europene trebuie să se conecteze.

Marea Britanie este pusă în situația în care trebuie să accepte inițiativele Uniunii Europene, chiar dacă ele sunt propuse de Franța sau Germania.

Poziția conservatoare a Regatului Unit începe să fie una incomodă, nu se simte deloc confortabil atunci când se decide implementarea unui Sistem Monetar European, iar prin refuzul de a accepta implementarea acestuia, Anglia nu face alt ceva decât să confirme faptul că încă mai este tributară rivalității istorice franco-engleză, iar condițiile și deciziile „Bruxelles-ului”⁷ sunt din ce în ce mai greu digerabile.

Se conturează deja o nouă încercare de referendum. Noi partide politice apar pe scena Regatului Unit, născute din dorința vehementă de a realiza ruperea de U.E., dorință atât de puternică încât unul dintre partidele nou constituite poartă numele obiectivului lor principal „Partidul referendumului”. Acesta se autodizolvă în anul 1997, marea majoritate a membrilor săi întărind rândurile unui alt partid eurosceptic, Partidul Independenței Regatului Unit (UKIP).

Cu toate acestea, Marea Britanie „supraviețuiește” în continuare în cadrul Uniunii, însă odată cu numirea, la 10 mai 2010, a lui David Cameron în funcția de premier, lucrurile aveau să se schimbe.

Cameron primește misiunea de a forma prima coaliție guvernamentală liberal-democrată de după cel de-al Doilea Război Mondial, alianță politică pe care, cel mai tânăr prim-ministru al Angliei din ultimii 200 de ani trebuie să o conducă în mandatul proaspăt încredințat. Urmează o

⁷ Discursul primului ministru britanic Margaret Thatcher susținut la Bruges în 1988 conform [<https://www.margarethatcher.org/document/107332>], accesat la 02.04.2020.



perioadă agitată din mai multe puncte de vedere, atât pe plan intern cât și pe plan extern.

Astfel, pe plan intern, pentru a menține coeziunea în cadrul coaliției, liderul conservatorilor englezi lansează promisiuni și promovează idei și opinii despre care nici el nu este mereu convins. Deși susține ideea că Marea Britanie ar trebui să rămână în Uniunea Europeană, David Cameron propune guvernului pe care îl conduce organizarea referendumului, cedând astfel presiunilor UKIP, conduși de Nigel Farage, un vehement susținător al Brexitului.

Pe plan extern criza refugiaților pune presiune atât pe U.E. cât și pe Marea Britanie, iar la nivel european se gândesc direcții și măsuri ce prevăd chiar și stabilirea unor cote-parte de refugiați pentru fiecare stat în parte. Aceste acțiuni destabilizează piața muncii din Regatul Unit, motiv pentru care deciziile Bruxelles-ului sunt primite cu scepticism și reacții virulente la Londra, mai ales de către liderii pro-Brexit, care folosesc acest motiv pentru a atrage de partea lor pe cei care întâmpină dificultăți în găsirea unui loc de muncă.

În aceste condiții rezultatul referendumului nu mai rezintă o surpriză. Cu 51,9% pentru Brexit, 72% dintre cetățenii britanici decid ieșirea din U.E. a Regatului Unit și obligă guvernul de la Londra să își asume toate costurile și mai ales riscurile la care se expune Marea Britanie odată cu acceptarea și validarea rezultatului referendumului.

Pe scurt, Brexitul, privit din perspectivele expuse, a fost determinat de două cauze principale: lipsa de fermitate a guvernului Cameron și criza refugiaților suprapusă pe nemulțumirea clasei sociale de mijloc din Marea Britanie.

Brexit - o formă de război hibrid

Analizând cauzele prezentate anterior și modul cum au fost ele propagate și diseminate spre populația britanică cu drept de vot, putem observa faptul că o serie de trusturi de presă au abordat problema Brexitului atât de pe poziții pro-rămânere în U.E., cât și din perspective eurosceptice, împotriva continuării colaborării cu U.E., folosindu-se astfel puterea presei pentru a influența electoratul.

Continuând acest demers și analizând interesul mass-mediei pentru subiectul Brexit, nu putem omite un aspect ce poate fi considerat amenințare



la adresa sistemului național de securitate al Regatului Unit, și anume „bombardarea” spațiului public cu informații transmise prin intermediul presei, al rețelelor de socializare sau prin emisiuni la posturile de radio și televiziune unde, dezbaterile politice publice capătă aspect de „show de divertisment” unde se ironizează apartenența la Uniune și se prezintă aspectele pozitive ce pot rezulta în cazul rușiei de aceasta.

Un alt aspect extrem de cunoscut vânătorilor de paradisuri fiscale și în contradicție cu politica fiscală a U.E. îl reprezintă faptul că Marea Britanie este renumită ca fiind extrem de permisivă, neaplicând taxe pe veniturile produse/dobândite în afara Regatului Unit, fapt care a generat un exod al miliardarilor din toată lumea spre capitala britanică, cu investiții în domenii precum cel imobiliar, mass-media, sport etc.

De remarcat este și faptul că guvernul de la Londra și mai ales britanicii cu drept de vot, nu au părut deloc deranjați de prezența oligarhilor ruși, a magnaților din India sau a prinților miliardari din statele arabe care investesc masiv în proprietățile imobiliare, iar pentru a-și asigura conturile, cumpără publicații locale și naționale, acțiuni la cele mai importante platforme de socializare și sponsorizează campanii electorale.

Prezența lor în cele mai exclusiviste cluburi și achiziționarea unor reședințe în cele mai scumpe zone rezidențiale din Londra nu este privită la fel de îngrijorător precum este văzută și propunerea U.E. de a repartiza Regatul Unit⁸ o cotă de imigranți.

În sistemul bancar britanic sunt vărsate sume uriașe reprezentând infuziile de capital ale investitorilor imigranți, sume considerabile obținute nu în totalitatea lor și nu întotdeauna prin cele mai cinstitute și curate metode.

Un mare interes pentru investițiile din Marea Britanie îl manifestă „crema” miliardarilor ruși, iar dintre „personalitățile” acestei clase sociale, nu putem să nu amintim pe unele dintre cele mai interesante personaje, precum: miliardarul rus Alexander Lebedev - fost agent KGB, cel care cumpără publicațiile engleze „The Independent” și „Evening Standard”,

⁸ N.A. Londra, în toamna anului 2015 refuză cota de 17.000 de refugiați din totalul de aproximativ 160.000, [<https://www.ziare.com/invazie-imigranti/stiri-invazie-imigranti/presa-britanica-dezvaluie-planul-ue-romania-cota-de-7-000-de-imigranti-marea-britanie-nu-primeste-niciunul-infografic-1380816>], accesat la 02.04.2020.



Alișer Usmanov- membru important în conducerea Gazprom, cel care investește în acțiunile Facebook și în cele ale clubului londonez de fotbal Arsenal FC, bine-cunoscutul Roman Abramovici - cel care a investit în afaceri cu resurse naturale și care deține clubul londonez de fotbal Chelsea, Oleg Deripaska - regele rus al aluminiului, proprietar a unor imobile de lux în Belgrave Square și Surrey, care, de altfel, este un apropiat al președintelui Vladimir Putin și totodată bun prieten cu oameni politici puternici din Marea Britanie, iar lista ar putea continua...

Ceea ce însă este evident din afirmațiile anterioare este faptul că, sub o formă sau alta, prin coordonarea unor medii politice și prin influențarea populației în masă s-a reușit ruperea Regatului Unit de Uniunea Europeană. Motivele principale au fost șicanările politice și teama ca Marea Britanie să nu se scufunde sub valul de imigranți.

Motivele reale însă sunt de altă natură. Ele, chiar dacă par a fi desprinse dintr-o teorie a conspirației, sunt realități de necontestat. Faptul că o mare putere precum Rusia, își trimite spionii și oamenii de afaceri potenți într-o țară unde aceștia influențează clasa politică și electoratul prin sponsorizări dubioase și apariții spectaculoase în presa de scandal poate fi interpretat ca implicare în treburile interne ale Angliei.

Motivul?

Menținerea deschisă a unei principale rute comerciale și surse de venit ilicit pentru o mare putere aflată de o perioadă importantă de timp sub presiunea sancțiunilor internaționale și a unor măsuri restrictive.

Astfel, putem concluziona afirmând: Marea Britanie se află sub asediul și lovirile perfide ale unui război hibrid, o confruntare în care însă se complăce pentru aș acoperi golurile din visteria Regatului, goluri create urmare a deciziei influențate de a se rupe de U.E. Este o confruntare ce nu se va încheia curând, ultima speranță a Regatului Unit rămânând puternica sa legătură cu NATO și Statele Unite ale Americii.

Concluzii

Uniunea Europeană, împreună sau fără Marea Britanie, își continuă drumul. Una dintre principalele sale rute rămâne dezvoltarea unei gândiri strategice în domeniul Politicii Externe și de Securitate Comune (PESC) și în cel al Politicii de Securitate și Apărare Comună (PSAC).



Extinderea U.E. spre estul continentului, precum și aderarea mai multor state din Europa de Est la Alianța Nord-Atlantică, crează un sentiment de neliniște pentru Federația Rusă ale cărei reacții au fost de consolidare a poziției în bazinul Mării Negre, prin anexarea Crimeei și de impresionare a țărilor membre NATO și U.E., prin manevre militare navale în Marea Barents⁹ și Marea Baltică¹⁰ și prin raiduri aeriene¹¹, la limitele spațiilor aeriene naționale.

Ruperea Regatului Unit de Uniunea Europeană urmare și a acțiunilor specifice unei confruntări de tip război hibrid, nu reprezintă decât o bătălie câștigată în războiul Uniunii spre o alianță europeană modernă și puternică din punct de vedere economic și militar.

Structura PESC nu este altceva decât însumarea politicilor naționale de securitate ale statelor membre. Direcțiile de evoluție ale acestei structuri vizează implementarea unei strategii globale care are în vedere aspecte ce țin de securitate și apărare, în toate dimensiunile sale, de reziliență statală și societală în vecinătate, de abordarea integrată a crizelor și conflictelor externe, precum și de realizarea ordinii regionale într-o manieră cooperantă.

Cu toate că Marea Britanie a făcut pasul în afara Uniunii, ea nu a părăsit și Europa, motiv pentru care va participa în continuare la proiectele comune ale PESC, îndeplinindu-și angajamentele deja luate, iar pentru viitor, pe baza unor acorduri de cooperare și colaborare va rămâne un partener de încredere în flancul nord-vestic european, iar odată cu dezvoltarea relațiilor de colaborare cu siguranță va renaște dorința Regatului Unit de a fi iarăși împreună, într-o Europă mai bună și mai puternică

⁹ N.A. Exercițiul militar Zapad-2017 prin care s-a simulat un război conventional împotriva trupelor NATO din Europa, [<https://www.hotnews.ro/stiri-international-22188277-manevrelle-militare-zapad-...>], accesat la 05.04.2020.

¹⁰ N.A. Exercițiul militar naval Scutul Oceanic-2019, [<http://www.paginade-rusia.ro/marina-rusa-desfasoara-manevre-de-anvergura-in-marea-baltica/>], accesat la 05.04.2020.

¹¹ <https://moldova.europalibera.org/a/rusia-violeaz%C4%83-spa%C8%99Biul-aerian-nato-pe-fundalul-manevrelor-din-estonia/30181312.html>, accesat la 05.04.2020.



Bibliografie

1. Rudolf G. Adam *Brexit: Causes and Consequences*, Publisher: Springer, 2020.
2. Thomas Christiansen, Diane Fromage *Brexit and Democracy: The Role of Parliaments in the UK and the European Union*, Publisher: Springer International Publishing, 2019.
3. *** <https://www.bild.de/politik/ausland/brexit/will-you-miss-us-mrs-may-54535638.bild>.
4. *** <https://www.margarethatcher.org/document/107332>.
5. *** <https://www.europarl.europa.eu/sides/getDoc...>
6. *** <https://www.openpolitics.ro/conservatorii-si-laburistii-lupta-pentru-brexit>.
7. *** <https://business24.ro/international/ue/de-ce-vrea-marea-britanie-sa-iasa-din-ue>.
8. *** <https://www.ziare.com/invazie-imigranti/stiri-invazie-imigranti/presa-britanica...>
9. *** <https://www.hotnews.ro/stiri-international-22188277-manevrela-militare-...>



INFORMAȚIA PENTRU APĂRARE ÎN CONTEXTUL CONFRUNTĂRII INFORMAȚIONALE

DEFENSE INFORMATION IN THE CONTEXT OF INFORMATION WARFARE

Drd. Ion-Sorin MOLDOVAN

E-mail: moldovan.ion.sorin@gmail.com

Rezumat: Așa cum ne arată exemple relativ recente (cyber-atacul „OpIsrael” din 2013, atacurile cibernetice și informatice din același an din Singapore, agresiunile cibernetice din 2010, în Burma, Japonia și Coreea de Sud, cele din 2009, în SUA și Coreea de Sud etc.) în ultimii ani, operațiile militare menite să afecteze componenta militară a securității și care categorial se plasează în domeniul apărării, sunt desfășurate în multe cazuri prin utilizarea unor mijloace non-armate, cel puțin nu prin utilizarea armelor în înțelesul tradițional al termenului. Aceste schimbări sunt produse de mutațiile înregistrate de societatea modernă, în special din cauza evoluției tehnologice deosebite. Aceste evoluții au anulat de multe ori previziunile întocmite de mulți specialiști militari încă din perioada războiului rece, bazându-se pe concepțiile clasice. Autori precum Alvin Toffler¹ au sugerat totuși apropierea momentului în care se va dezvolta într-atât societatea informațională, încât însuși mediul de confruntare se va transfera de pe câmpul clasic de luptă în mediile virtuale ale câmpului informațional. Clipa în care informația a obținut o asemenea valoare, devenind totodată „scut” și „armă”, a condus la conexiunea logică dintre situația controlului asupra informației și deținerea puterii. Astfel încât, în cadrul confruntării moderne duse într-un spațiu multidimensional, dimensiunea informațională a căpătat o importanță aparte. Rămâne așadar de văzut din perspectiva informației pentru apărare, cum se modifică „regulile jocului”, în contextul generalizării confruntării informaționale.

Cuvinte cheie: informații, informații pentru apărare, mediu informatic, mediu virtual, rețele de calculatoare.

Abstract: As the relatively recent examples show us (“OpIsrael” cyber-attack of 2013, cyber-attacks of the same year in Singapore, cyber-attacks in 2010, in Burma, Japan and South Korea, in 2009, in the US and Korea South etc.), in recent years, military operations aimed at affecting the military component of security and being categorically

¹ Alvin Toffler, Heidi Toffler, *Război și antirăzboi. Supraviețuirea în zorii secolului XXI*, Editura Antet, București, 1995.



placed in the field of defense, are carried out in many cases with the use of non-armed means, or at least not with the use of weapons in the traditional sense of the term. These changes are caused by the changes of the modern society, especially due to the special technological evolution. These developments have often cancelled the forecasts made by many military specialists since the Cold War, based on the classical concepts. Authors such as Alvin Toffler suggested, however, that the information society would develop in such a way that the confrontation environment itself would be transferred from the classic battlefield to the virtual media of the information field. The moment when information gained such a value, becoming "shield" and "weapon", led to the logical connection between the state of control over information and the holding of power. Thus, in the context of the modern confrontation in a multidimensional space, the information dimension has acquired a particular importance. Therefore, it remains to be seen from the perspective of defense information, how the "rules of the game" change, in the context of generalizing the information confrontation.

Cuvinte cheie: information, information for defense, IT environment, virtual environment, computer networks.

Introducere

În contextul conflictului multidimensional modern², confruntarea a ajuns la un moment dat să se transfere din mediul material în dimensiunea informațională, acest fapt având influențele sale specifice asupra modului în care trebuie să fie gestionată, mai nou, informația pentru apărare. Conflictul purtat în era informațională vizează în mod predilect informația pentru apărare, iar în acest sens în „luptă” sunt trimise forțe specializate în acțiunile cibernetice și informatice, alături de acțiunile informaționale mai mult sau mai puțin tradiționale.

O astfel de confruntare neconvențională ne arată informația de apărare devenită scop și țintă, dar în situația în care poate fi folosită de o manieră ofensivă sau defensivă, sub forma unor acțiuni (contra)informative desfășurate fie independent, fie în cadrul unor operații mai vaste (desfășurate de obicei și în alte dimensiuni ale confruntării) care au drept scop nu doar aspecte legate de mediul informațional, ci la fel de bine, legate de mediul psihologic (psihosfera) și interacțiunea dintre personalul uman și aparatura de gestionare a informației. Noile tipuri de operații (implicând informațiile de apărare) se duc de așa manieră încât vizează și sfera mentală

² Gheorghe Arădăvoaice, Valentin Stancu, *Războaiele de azi și de mâine, agresivități nonconvenționale*, Editura Militară, București, 1999.



a adversarului, căutând pe cât posibil să evite recurgerea la mijloacele de luptă tradiționale și, în general, la activități purtate în mediul material, 3D. Lupta pentru apărarea sau atacarea informațiilor pentru apărare tinde să se poarte în mediul informațional și, în mod particular, în cel informatic sau cibernetic³.

Cum afectează confruntarea informațională mediul informațiilor pentru apărare

În momentul de față, acțiunile de confruntare informațională se desfășoară în diverse forme⁴, vizând cel mai adesea doar anumite categorii de informații, în special informațiile pentru apărare care, de regulă, sunt considerate foarte bine protejate. În condițiile conflictului multi-dimensional⁵, această protecție a informației pentru apărare devine tot mai dificilă, mai ales că noile forme de confruntare se pot prezenta:

➤ sub forma confruntărilor desfășurate la eșalonul de *comandă/control*, cel mai adesea, aceste acțiuni fiind însoțite și de forme tradiționale (clasice) de luptă, mai ales în ceea ce privește modalitățile de lovire a țintelor; acestea constituie o importantă componentă a confruntării desfășurate în mediul informațional, bazată cel mai adesea pe modalități de utilizare a informațiilor din domeniul militar, în special informațiile pentru apărare, atunci când acestea sunt gestionate la nivelul C2⁶;

➤ în cadrul confruntării *psihologice*, prin modificarea percepției corecte asupra realității a persoanelor care contribuie la obținerea sau prelucrarea datelor ce stau la baza formării informațiilor pentru apărare; prin influențarea stării psihice și morale a emitenților de informații pentru apărare, se poate influența forul decizional, astfel încât succesul unei operații militare survine fără recurgerea la violență;

➤ sub înfățișarea înșelătoare a unei acțiuni *virtuale*⁷, în mod uzual aflată în mediul informatic sau/și cibernetic, prin această acțiune spațiul

³ Stan Petrescu, *Arta și puterea informațiilor*, Editura Militara, București, 2003.

⁴ Abram Shulsky, Gary Schmitt, *Războiul tăcut*, Editura Polirom, Iași, 2008.

⁵ Constantin Moștofle, Gheorghe Văduva, *Tendențe în lupta armată*, Editura Universității Naționale de Apărare, București, 2004.

⁶ Mircea Mureșan, Gheorghe Văduva, *Războiul viitorului, viitorul războiului*, Editura Universității Naționale de Apărare, București, 2004.

⁷ Maxim Dobrinoiu, *Infracțiuni în domeniul informatic*, Editura C.H.Beck, București, 2006.



virtual este alterat și astfel se crează imagini false, aparatura cibernetică sau informatică aparținând adversarului, inducându-l pe acesta în eroare și, astfel, permițând prejudicierea informației pentru apărare sub o formă sau alta;

➤ sub forma unei acțiuni *propagandistice* și *imagologice*, acestea venind cel mai adesea împreună cu acțiunile psihologice, și având un efect de obicei indirect asupra informațiilor pentru apărare;

➤ în cadrul confruntării (radio)*electronice*⁸ menite, de obicei, să distrugă ori să altereze fluxurile de informații care sunt transmise prin câmpuri electromagnetice sau care sunt stocate în aparate influențate de acțiunea câmpului electromagnetic indus;

➤ sub forma acțiunilor de luptă purtate în mediul *cibernetice* și în cel *informatic*, vizate fiind rețelele adverse („*războiul în rețea*”), care sunt supuse unor agresiuni sub diverse forme, menite de obicei împiedicării proceselor de achiziționare, preluare, stocare și prelucrare a datelor și a informațiilor pentru apărare, de către rețelele militare adverse (ori asociate acestora);

➤ în cadrul confruntării *mediatice*, prin influențarea unor factori de decizie care au rol important în managementul informației pentru apărare, dar și prin crearea unor false percepții asupra realității, asemănător modului în care se acționează și în mediul propagandistic sau imagologic.

Apărarea națională constituie un domeniu al securității în care este de primă importanță ca datele și informațiile să fie corecte, utile și primite de factorii decidenți în timp real. Dezvoltarea tehnologică a ultimelor decenii a condus la situația în care aceste operații sunt cel mai adesea realizate prin intermediul mijloacelor informatice și cibernetice. Așa se face că operațiile purtate în aceste dimensiuni (cibernetice, informatică etc.) au ajuns să intereseze în mod direct informația pentru apărare.

Vizând tocmai informațiile pentru apărare, adversarul poate desfășura acțiuni de luptă sau chiar ansambluri de acțiuni (operații) cum ar fi:

⁸ Niculescu, Marian Mitea, Constantin Gh.Balaban, Gabriel Năstase, *Confruntările electronice și psihologice - vectori de succes în conflictele internaționale înalt tehnologizate*, Editura Victor, București, 2003.



✓ acțiuni destinate achiziționării de date/informații clasificate; mijloacele obișnuite de protecție a informațiilor pentru apărare se dovedesc de multe ori ineficiente în fața tehnologiilor moderne tot mai sofisticate;

✓ agresiuni destinate anihilării sau chiar distrugerii rețelelor adversarului⁹ sau aducerii acestuia în stare de neîntrebuințare și, astfel, zădărnisirea accesului la informațiile pentru apărare stocate acolo;

✓ acțiuni destinate împiedicării accesului la rețea în situația în care rețeaua propriu-zisă rămâne totuși intactă; astfel, emitenții de informații pentru apărare pot fi împiedicați să livreze în timp util informațiile solicitate de utilizatorii din cadrul sistemului de apărare sau, sistemul de senzori care transmite acest gen de informații, deși funcționează, nu mai este în măsură să le trimită către utilizatori, deoarece accesul acestora a fost împiedicat;

✓ acțiuni menite deturnării direcțiilor și sensurilor obișnuite de activitate ale rețelelor prin care informația de securitate este manageriată, astfel încât utilizatorii acestor rețele sunt trimiși (în mediul informatic/cibernetice) pe direcții greșite, fie în scopul de a se intoxica informațional, fie de a le produce întârzieri în activitate;

✓ unul dintre scopurile cel mai des întâlnite este spargerea de coduri ori parole de acces și, astfel, infiltrarea în rețeaua adversarului fără ca acesta să sesizeze acțiunea respectivă; bineînțeles, direct vizate sunt în special informațiile de apărare, dată fiind importanța lor în cadrul ecuației confruntării, indiferent sub ce formă ar fi purtată;

✓ agresiuni care nu vizează în mod direct rețeaua adversă și nici personalul advers unde activează emitenții de informații pentru apărare, ci chiar conținutul datelor și informațiilor care ajung la un moment dat să fie percepute de către adversar și sunt în măsură să contribuie la elaborarea informațiilor pentru apărare.

Viitorul informațiilor pentru apărare

Aspectele prezentate ne indică faptul că în contextul mediului multidimensional de confruntare informația capătă deopotrivă rolul de țintă și de armă¹⁰. Cum în mod special în domeniul apărării informațiile au un rol determinant, este de la sine înțeles că în cadrul mediului informațional (cu

⁹ Tudor Niculescu, *Războiul electronic*, Editura Militară, București, 1991.

¹⁰ Stan Petrescu, *Arta și puterea informațiilor*, Editura Militară, București, 2003.



toate componentele sale) se pot produce efecte dintre cele mai importante care să privească apărarea națională. Acțiunile de luptă specifice mediului informațional¹¹, tind să se extindă de la simpla afectare a informației, la afectarea mentalului celor care gestionează informațiile pentru apărare și influențarea proceselor de decizie ale acestora, de o manieră aptă să producă anumite consecințe asupra gestionării informației de apărare și eficacității acesteia.

Analiza situației existente în momentul de față ne indică faptul că în cadrul confruntării informaționale ce vizează în mod predilect informația pentru apărare, sunt implicate aproape toate dimensiunile confruntării moderne.

Astfel încât, *rețelele în care sunt gestionate informațiile pentru apărare*, în viitorul apropiat vor fi supuse unor *riscuri specifice* legate de tendințele dezvoltării tehnologice, așa cum o percepem în momentul de față. Astfel, am putea preconiza următoarea tendință de evoluție a situației în ceea ce privește *informația pentru securitate* în contextul confruntării moderne:

✓ mediul de confruntare devenind multidimensional, informația pentru apărare va trebui să se dezvolte după toate aceste coordonate, *căpătând forme specifice fiecăreia dintre dimensiuni*;

✓ în situația în care acțiunile de luptă se îndreaptă din ce în ce mai clar către forme hibride, neconvenționale (nu neapărat din categoria NBC) și asimetrice, efectele lor nu vor mai semăna cu acelea clasice, iar informația pentru apărare va trebui să se adapteze unor noi tipuri de utilizatori - *un personal combatant absolut atipic*, apt să elaboreze, prelucreze și utilizeze informația pentru apărare în moduri de neconceput pentru generațiile precedente de militari sau utilizatori ai acestui gen de informație;

✓ acțiunea contrainformativă vizând informațiile pentru apărare tinde să afecteze medii sau colectivități *care aparent nu au nicio legătură* cu emitenții și utilizatorii informațiilor pentru apărare; se va căuta tot mai mult realizarea unor acțiuni ce vizează psihologia maselor și

¹¹ Sorin Topor, *Războiul informațional*, Editura Universității Naționale de Apărare „Carol I”, București, 2006.



mentalul colectiv, influențarea informațiilor pentru apărare devenind *indirectă dar nu mai puțin eficace*;

✓ îndreptarea agresiunii nu atât asupra informației pentru apărare sau personalului care o gestionează, cât mai ales *asupra rețelei*, în scopul de a le deteriora și a le face să inducă în eroare decidenții adversarului.

Concluzii

Astfel de tendințe conduc la necesitatea reconceperii modului de organizare¹² a sistemelor menite gestionării sub orice formă a informațiilor pentru securitate și o schimbare a însuși managementului general al informațiilor pentru securitate, în sensul adaptării la noile condiții impuse de dezvoltarea tehnologică.

Altminteri, ne putem trezi în situația în care un potențial adversar ne învinge de la distanță, fără ca măcar să-i putem vedea chipul și fără¹³ utilizarea violenței în formele ei clasice.

Bibliografie

1. Arădăvoaice, Gheorghe; Stancu, Valentin, *Războaiele de azi și de mâine, agresiuni nonconvenționale*, Editura Militară, București, 1999.
2. Dobrinou, Maxim *Infracțiuni în domeniul informatic*, Editura C.H.Beck, București, 2006.
3. Marin, Ionel *Comunitatea de informații, soluția problemelor de securitate*, Editura ANI, București, 2004.
4. Moștoflei, Constantin; Văduva, Gheorghe *Tendențe în lupta armată*, Editura Universității Naționale de Apărare, București, 2004.
5. Mureșan, Mircea; Văduva, Gheorghe *Războiul viitorului, viitorul războiului*, Editura Universității Naționale de Apărare, București, 2004.

¹² Ionel Marin, *Comunitatea de informații, soluția problemelor de securitate*, Editura ANI, București, 2004.

¹³ Sun Tzu, *Arta războiului*, Editura Antet XX Press, București, 1993.



6. Niculescu, Tudor *Războiul electronic*, Editura Militară, București, 1991
7. Niculescu, Tudor;
Mitea, Marian;
Balaban,
Constantin Gh.;
Năstase, Gabriel
8. Shulsky, Abram;
Schmitt, Gary *Războiul tăcut*, Editura Polirom, Iași, 2008.
9. Petrescu, Stan *Arta și puterea informațiilor*, Editura Militara, București, 2003.
10. Sun Tzu *Arta războiului*, Editura Antet XX Press, București, 1993
11. Toffler, Alvin;
Heidi, Toffler, *Război și antirăzboi. Supraviețuirea în zorii secolului XXI*, Editura Antet, București, 1995.
12. Topor, Sorn *Războiul informațional*, Editura Universității Naționale de Apărare „Carol I”, București, 2006.

