Anul XIII nr. 4/2021

INFOSFERA

Revistă de studii de securitate şi informaţii pentru apărare

Revista este indexată în bazele de date internaţionale EBSCO şi CEEOL

Revistă cu prestigiu ştiinţific recunoscut de Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (CNATDCU)

Direcţia Generală de Informaţii a Apărării

CUPRINS

MESAJE ADRESATE

cu prilejul aniversării a cinci ani de la înființarea Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu”

DOCENDO DISCIMUS

MESAJUL MINISTRULUI APĂRĂRII NAȚIONALE, DOMNUL VASILE DÎNCU

Data de 1 ianuarie 2017 reprezintă o zi cu încărcătură deosebită în evoluţia educaţiei şi instruirii în domeniul informaţii pentru apărare, prin reproiectarea instituţională a Centrului de pregătire în domeniul informaţii pentru apărare „General Nicolae Condeescu”, ca structură componentă a Direcției generale de informații a apărării.

Profesionalismul, dăruirea şi perseverenţa manifestate de specialiştii Centrului de pregătire au contribuit semnificativ la atingerea unor deziderate importante pentru Direcţia generală de informaţii a apărării, precum şi la reprezentarea cu succes a Ministerului Apărării Naţionale pe plan internaţional, în contextul dezvoltării relaţiilor multilaterale și bilaterale cu parteneri externi.

Lărgirea spectrului de riscuri convenţionale, neconvenţionale și hibride, multe dintre acestea cu caracter transnaţional, diversificarea tipologiei ameninţărilor, precum şi numeroasele focare de criză şi conflict din apropierea frontierelor naţionale şi din zona de interes strategic a României generează provocări multiple la adresa instituţiilor de securitate, apărare naţională şi ordine publică. Din această perspectivă, complexitatea, volatilitatea şi impredictibilitatea mediului de securitate necesită o adaptare permanentă a structurilor de informaţii pentru apărare, cu implicaţii imediate şi profunde în zona pregătirii personalului, fapt ce impune materializarea dezvoltărilor organizaţionale multidirecţionale, bazate pe interoperabilitate educaţională, transformare adaptaţională, exploatarea oportunităţilor şi complementaritatea eforturilor.

Transformarea instituţională pe care aţi parcurs-o în aceşti ani evidențiază capacitatea dumneavoastră de a vă sincroniza în mod rapid cu cerințele de pregătire solicitate de structurile cu responsabilităţi şi atribuţii în domeniul informaţii pentru apărare, prin adoptarea şi implementarea de tehnici, tehnologii şi proceduri didactice şi de sprijin logistic ce oferă cadrul necesar succesului educaţional.

Manifest convingerea că la obţinerea tuturor acestor rezultate deosebite, evidenţiate atât de instituţiile beneficiare interne, cât şi de partenerii noştri externi, au participat structurile din compunerea Direcţiei generale de informaţii a apărării, Statului Major al Apărării şi Universităţii Naţionale de Apărare „Carol I”, sinergie ce reiese inclusiv din modul în care dumneavoastră aţi reuşit să gestionaţi provocările modernizării învăţământului militar, să preîntâmpinaţi materializarea riscurilor asociate implementării programelor de reformă necesare, reuşind astfel să asiguraţi înalta performanţă profesională.

Am onoarea şi bucuria ca, la ceas aniversar, să vă transmit întreaga apreciere pentru activitatea pe care o desfăşuraţi şi pentru contribuţia la dezvoltarea şi modernizarea continuă a procesului educaţional în domeniul informaţii pentru apărare.

Cu ocazia sărbătoririi acestui eveniment, vă urez multă sănătate, putere de muncă şi împliniri profesionale şi personale, dumneavoastră şi celor dragi.

La mulţi ani!

MESAJUL DIRECTORULUI GENERAL AL DIRECȚIEI GENERALE DE INFORMAȚII A APĂRĂRII, DOMNUL GENERAL MARIAN HĂPĂU

Centrul de pregătire în domeniul informații pentru apărare *„General Nicolae Condeescu”* aniversează cinci ani de efort didactic intens, emoţie şi provocare, atât din partea cadrelor cu atribuţii didactice, cursanților și a structurilor beneficiare, cât și din partea structurilor de sprijin, prilej ce îmi oferă deosebita plăcere de a adresa cuvinte de mulțumire acestora pentru modul în care s-au implicat în realizarea cu succes a procesului educaţional.

Recunoscut atât la nivelul intelligence-ului național, cât și de partenerii noștri externi ca o organizație de elită, centrul de pregătire acționează ca o structură modernă, flexibilă și eficientă.

Pentru dumneavoastră, cei care vă desfășurați activitatea în acest „câmp de confruntare intelectuală”, acesta este un moment important de reflecție asupra trecutului, prezentului și viitorului, asupra pașilor parcurși pe calea reformei învățământului militar în domeniul informații pentru apărare, dintotdeauna în strânsă legătură atât cu cea a structurilor Direcției generale de informații a apărării, cât și cu a întregii Armate Române. De experiența dumneavoastră și modul în care înţelegeţi să vă îndepliniţi misiunea beneficiem toți.

Reorganizarea şi dezvoltarea instituţională s-au realizat în baza lecțiilor identificate şi învățate, prin bune practici şi cooperare cu structurile de învățământ militar naționale, partenere și internaționale, context din care a reieșit foarte clar că transformarea nu este un proces în sine și, mai ales, că aceasta trebuie să vizeze organizația ca întreg.

Lumea în care evoluăm astăzi ne pune la dispoziție o altă logică de securitate, discutăm despre alte tipuri de amenințări, riscuri și vulnerabilități a căror dinamică trebuie anticipată în mod adecvat. În acest context, apreciez efortul centrului de pregătire de a încerca permanent să se transforme inovator, să devină o instituție flexibilă. Misiunea a fost adaptată continuu noilor provocări, iar aria de responsabilitate s-a extins. Acționând în noua logică de securitate, produsele de informaţii pe care ofițerii pregătiți în această instituţie le furnizează beneficiarilor sunt guvernate de principiul punerii la dispoziție a intelligence-ului acționabil care să ofere cunoaștere, nu doar informație.

Sunteți formatorii specialiștilor care gândesc și implementează reformele strategice. Fără componenta de educație nu putem aborda cu responsabilitate şi asumare alte componente strategice. Sistemul educațional pe care îl dezvoltaţi continuu urmărește pregătirea viitorilor lideri şi specialişti militari şi civili în domeniul informații pentru apărare prin promovarea competenței, concurenței și multidisciplinarității în cadrul procesului de instruire.

Dumneavoastră sunteți cei care contribuiţi la modernizarea ariei cercetării în intelligence și la coordonarea acesteia cu aria cercetării învățământului superior militar și non-militar, pentru a susține astfel dezvoltarea cunoașterii în cadrul forţelor armate.

În sălile de clasă şi laboratoarele centrului de pregătire s-a născut generația actuală de ofițeri ai Direcției generale de informații a apărării, care, prin efortul lor profesional, fac din instituția noastră un element esenţial în identificarea și contracararea amenințărilor la adresa securității naţionale, aliate şi a partenerilor.

În educație, puterea exemplului e determinantă pentru evoluție. Dumneavoastră sunteți un exemplu!

Apreciez şi mulțumesc pentru dăruirea profesională a ofițerilor, maiștrilor militari, subofițerilor și personalului civil care lucrează în cadrul Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” , urându-vă sănătate și împliniri pe toate planurile.

La mulţi ani!

MESAJUL ŞEFULUI DIRECȚIEI INFORMAȚII MILITARE, DOMNUL GENERAL-LOCOTENENT MARIAN SIMA

Instituțiile, ca și oamenii, trecând prin vreme, ajung la momente de aniversare și bilanț.

Aniversarea nu este doar un moment de sărbătoare, ci și unul de reflecție, de evaluare și proiecție personală sau instituțională. Edificarea unei instituții este un proces dificil, realizabil cu mari eforturi intelectuale, umane și materiale, pe durata mai multor ani, decenii și chiar secole. Este și cazul Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu".

Pe data de 01.01.2022, Centrul de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu" împlinește 5 ani de activitate, într-o perioadă complicată din punct de vedere sanitar la nivel global, cu provocări multiple și pentru munca de erudiție și profesionalizare interdisciplinară - multiculturală în domeniul informații pentru apărare.

Pentru cei care se gândesc la un viitor mai puțin complicat decât trecutul la care, inevitabil, ne raportăm, ne amintim că nici momentul în care generalul Nicolae Condeescu punea bazele modernizării și transformării serviciului de informații al Armatei României nu a fost unul prea fast, atunci când soarta țării și a armatei era critică în raport cu dinamica Primului Război Mondial.

În trecut, ca și în prezent, din dorința de a ține pasul sau chiar de a merge puțin înaintea vremurilor și a nevoilor Patriei, structurile de informații militare au rămas determinante pentru obținerea succesului în luptă.

Privind retrospectiv, observăm că dinamica mediului internațional și regional de securitate a condus la reconfigurarea instituțiilor sistemului național de apărare, inclusiv a Armatei României, atât la nivel structural, cât și doctrinar.

Creșterea capacității de reacție a sistemului militar se bazează pe asigurarea înzestrării și pregătirii performante a personalului din structura de forțe, precum și pe dezvoltarea capabilităților de înțelegere a mediului operațional, de anticipare și avertizare strategică.

Din aceste perspective, înființarea Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu" (01.01.2017), ca structură responsabilă pentru instruirea și educația personalului din Direcția generală de informații a apărării, s-a înscris în linia doctrinară de integrare și coerență a politicilor și strategiilor de securitate ale structurilor naționale de informații.

În plus, eforturile conducerii Direcției generale de informații a apărării pentru implementarea unei viziuni unitare privind modernizarea învățământului în domeniul informații pentru apărare, în acord cu Concepția de dezvoltare a învățământului militar elaborată la nivelul Ministerului apărării naționale, au permis crearea unei structuri care se adaptează continuu schimbărilor de paradigmă din sistemul educațional.

Centrul de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” și-a onorat menirea într-o manieră exemplară, devenind principalul centru de instruire și specializare, dezvoltare și implementare de tehnologii, proceduri capabile să asigure instrumentarul necesar îndeplinirii misiunilor în domeniul informații militare.

În această idee, este important ca programele de instruire și educație din cadrul Centrului să mențină aspectele sistemice din domeniul securității și apărării, structurate și adaptate cerințelor în dinamică pentru creșterea profesionalismului în domeniul informații pentru apărare.

În conformitate cu cerințele operaționale ale Direcției informații militare, una dintre marile provocări ale Centrului este diversificarea strategiilor didactico-pedagogice și asigurarea unui model de interconectare într-un spațiu adaptat permanent la cele mai moderne metode, tehnici și practici educaționale.

Un alt obiectiv major constă în asigurarea suportului tehnic-teoretic menit să confere structurilor de informații militare capacitatea de a desfășura acțiuni specifice în medii operaționale impredictibile și dinamice, o țintă de atins prin efortul comun al specialiștilor Direcției informații militare și Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu”.

În evoluția instituțională a Direcției informații militare, schimbarea generațiilor a fost și va fi posibilă și cu ajutorul specialiștilor Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu”!

Personalul Direcției informații militare educat și instruit în cadrul Centrului se regăsește azi pe toate palierele de conducere ierarhică, în toate profilurile specifice activității de informații militare. Practic, cunoștințele asimilate în cadrul Centrului de pregătire în domeniul informații pentru apărare sunt parte a efortului de intelligence depus în slujba securității României.

Evoluția domeniului informații militare a fost posibilă prin devotamentul, inteligența, perseverența și tenacitatea cu care acționează personalul Centrului. În egală măsură, este meritul conducerilor Direcției generale de informații a apărării și Centrului de pregătire în domeniul informații pentru apărare, care au cultivat sistemul de valori etice și morale specifice domeniului de activitate.

Aniversarea Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” este un prilej de a mulțumi atât conducerii unității, cât și personalului militar și civil pentru dăruirea cu care ne ajută să înțelegem mai bine misiunea noastră, ne învață cum putem să ne atingem obiectivele profesionale și cum să ne dezvoltăm continuu.

Vă felicit și vă urez succes în continuare!

La Mulți Ani!

MESAJUL ŞEFULUI DIRECȚIEI CONTRAINFORMAȚII ŞI SECURITATE MILITARĂ, DOMNUL GENERAL-MAIOR PETRU BĂICEANU

Dinamica şi impredictibilitatea mediului de securitate actual determină structurile de informaţii să acţioneze permanent în sensul adaptării rapide la coordonatele evoluţiei ameninţărilor interne şi externe, militare şi non-militare, de natură să afecteze securitatea naţională.

În această paradigmă, avem nevoie permanent de personal educat, pregătit şi instruit la standarde înalte, în măsură să acţioneze cu profesionalism şi determinare pentru îndeplinirea misiunilor încredinţate de conducerea Armatei României şi a Ţării, astfel încât să minimizăm riscurile şi să prevenim surprinderea strategică. Pentru îndeplinirea acestui deziderat beneficiem de sprijinul Centrului de pregătire în domeniul informaţii pentru apărare „General Nicolae Condeescu", atât pe zona de formare a viitorilor specialişti în activitatea de contrainformaţii şi securitate militară, cât şi pe latura de perfecţionare şi specializare a celor care deja activează în acest nobil domeniu.

Cooperarea intensă dintre specialiştii Direcţiei contrainformaţii şi securitate militară şi cei ai Centrului de pregătire a permis dezvoltarea unor programe de pregătire care să răspundă nevoilor actuale, iar platforma educaţională pusă la dispoziţie a asigurat permanent cadrul de inovaţie şi competitivitate necesar formării şi dezvoltării personalului propriu.

Pe de altă parte, programele educaţionale furnizate de Centru, în corelare cu nevoile prezente şi viitoare ale Direcţiei contrainformaţii şi securitate militară, au permis cursanţilor să abordeze problematici complexe, dinamice, adaptate realităţii, astfel încât să îşi poată îndeplini cu succes misiunile la cele mai înalte standarde de performanţă.

În concluzie, avem convingerea că obiectivul educaţiei în domeniile contrainformaţii şi securitate militară a fost, este şi va rămâne formarea şi dezvoltarea conştiinţei şi conduitei adecvate menţinerii şi consolidării climatului general de securitate, acesta reprezentând fundamentul desfăşurării oricărei activităţi în spectrul informaţii pentru apărare şi dezvoltării rezilienţei instituţionale.

Şi cu sprijinul Centrului de pregătire în domeniul informaţii pentru apărare „General Nicolae Condeescu", Direcţia contrainformaţii şi securitate militară continuă să ocupe avanposturile unui front nevăzut, sub deviza „*Nefas Est Nocere Patriae*". Pentru aceasta, vă mulţumesc şi vă doresc să rămâneți fideli preocupărilor dumneavoastră remarcabile, mult succes în misiunea dumneavoastră și împlinirea aspirațiilor personale și profesionale!

La mulţi ani!

MESAJUL COMANDANTULUI DETAŞAMENTULUI SPECIAL DE PROTECȚIE ŞI INTERVENȚIE, DOMNUL COLONEL ARTHUR-ROMEO ELISEI

Cu o tradiție de peste 23 de ani, într-un domeniu de pionierat în Armata României, prevenirea şi combaterea actelor de terorism şi a faptelor asimilate acestora îndreptate împotriva factorilor umani specifici, factorilor materiali şi activităţilor de importanță deosebită din cadrul Ministerului Apărării Naţionale (MApN), Detașamentul special de protecție și intervenție (DSPI) este structura din subordinea Direcției generale de informații a apărării (DGIA) specific organizată, instruită și înzestrată, abilitată prin lege pentru executarea de operații antiteroriste și contrateroriste de precizie, vizând asigurarea sau restabilirea securității principalelor categorii de factori umani și materiali din responsabilitatea MApN, care continuă să mențină la un nivel ridicat ștacheta performanței și profesionalismului în domeniul specific din responsabilitate.

Ca orice altă entitate tactică cu atribuții în domeniul prevenirii și combaterii terorismului, DSPI este supus provocării de a se adapta permanent mediului de securitate, în care rolul informației are caracter decisiv. Până în prezent, unitatea și-a creat premisele pentru identificarea instrumentelor prin care poate îndeplini interesele și obiectivele DGIA, proiectând principalii vectori de acțiune către creșterea performanțelor, dezvoltarea și protejarea capabilităților.

În proiectarea viitorului organizațional, DSPI urmărește dezvoltarea continuă și susținută a pregătirii profesionale a personalului propriu în cadrul Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu" (CPDIA), prin structura de pregătire în domeniul prevenirii și combaterii terorismului, în vederea obţinerii efectelor aşteptate pe linia nevoilor de instruire în domeniul specific de activitate și de evoluție în carieră.

DSPI dispune de o resursă umană matură şi bine antrenată, cu expertiză în domeniul de activitate şi experienţă într-o diversitate de discipline militare şi civile, precum şi de o dotare superioară cu armament, muniţii şi echipamente de înaltă tehnologie, ceea ce permite să valorifice într-o relație de parteneriat cu CPDIA experiența acumulată în anii de activitate, prin programe de formare profesională pe toate palierele educaționale, susținute de instructori specializați în centre și instituții internaționale de profil. În acest scop, generațiile viitoare de specialiști pot beneficia de un nivel înalt de pregătire pentru formarea deprinderilor necesare utilizării tehnicilor, tacticilor și procedurilor specifice, în concordanță cu capabilitățile operaționale esențiale.

Nivelul de performanță atins, precum și realizările obținute până în prezent, ne obligă și pe viitor la dezvoltarea standardului educațional și de instruire adaptat la un domeniu caracterizat de o continuă schimbare dinamică.

Ne bucurăm de o cooperare și coordonare exemplare cu CPDIA, iar acest moment aniversar ne oferă prilejul să le adresăm colegilor noștri cele mai alese urări în vederea îndeplinirii la standardele ridicate de performanță a misiunii și obiectivelor organizaționale asumate prin motto-ul „*Docendo Discimus*!"

La mulți ani !

MESAJUL COMANDANTULUI CENTRULUI DE PREGĂTIRE ÎN DOMENIUL INFORMAȚII PENTRU APĂRARE „GENERAL NICOLAE CONDEESCU“, DOMNUL COLONEL DR. DAN COLESNIUC

Centrul de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” (CPDIA) reprezintă instituția educațională de referință a Armatei României în domeniul informații pentru apărare (IAp)/defence intelligence.

CPDIA, componentă de elită a Direcției generale de informații a apărării, continuă tradiția formării de competențe inovatoare și atitudini valorice, proces inițiat odată cu organizarea armatei moderne și apariția primei entități de informații a Statului Major General, la data de 12 noiembrie 1859, prin Înaltul Ordin de zi nr. 83 al domnitorului Alexandru Ioan Cuza. Adaptabilitatea proactivă a pregătirii specifice a specialiștilor în domeniul IAp, pe fondul provocărilor mediului global de securitate, a determinat transformări structurale succesive, care au culminat cu reorganizarea actuală, începând cu data de 01.01.2017.

Centrul de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” este structură centrală a Ministerului Apărării Naționale, având în responsabilitate pregătirea specifică pe toate palierele educaționale: non-universitar, universitar, masteral, postuniversitar și studii doctorale.

Provocările mediului de securitate, caracterizat de volatilitate, incertitudine, complexitate și ambiguitate, dominat de ample transformări tehnologice și de tendințe polarizante la toate nivelurile societale, precum și cerințele de standardizare și interoperabilitate care decurg din statutul României de membru al Alianței Nord-Atlantice, al Uniunii Europene și al altor organisme internaționale, impun permanent nevoia de transformare și adaptare dinamică pentru eficientizarea pregătirii în domeniul IAp.

Procesele educaționale desfășurate în CPDIA au un caracter profund de transformare dinamică, prin: diversificarea metodelor didactico-pedagogice, de predare-învățare, pentru îmbunătățirea continuă a flexibilității gândirii și analizei critice; creșterea capabilităților de management și leadership la nivel tactic, operativ și strategic; identificarea, proiectarea, dezvoltarea și implementarea tehnologiilor emergente specifice erei informaționale, într-un mediu colaborativ, determinat de digitalizarea societății și a cibernetizării câmpului de luptă; realizarea influenței, efectului și consensului într-un mediu operațional întrunit și multinațional.

Capacitatea de proiecție curriculară flexibilă și sustenabilă pe termen mediu, lung și foarte lung, prin învățare și adaptare proactivă, reprezintă nucleul misiunii CPDIA în amplul proces de formare, specializare și perfecționare continuă a specialiștilor în domeniul IAp, la nivel tactic, operativ și strategic.

CPDIA dezvoltă gradual un model educațional integrat, personalizat și scalabil în funcție de cerințele operaționale, implementat inclusiv pe platformele IE-learning (Intelligence Electronic - Learning), ceea ce permite definirea clară și explicită a spațiului confruntării, crearea de conținuturi și elaborarea logică a argumentației în procesul de înțelegere holistică a evoluției unui eveniment sau fenomen.

Din această perspectivă, dezvoltarea continuă a activităților educaționale și de instruire non-universitare, universitare, masterale, postuniversitare, doctorale, de carieră și specializare, precum și extinderea activităților de cercetare științifică, se bazează pe o viziune sistemică, direcționată cu prioritate pe convergența următoarelor elemente determinante:

- Proiectarea programelor de formare și dezvoltare profesională pe baza standardelor naționale, europene și euroatlantice, pentru consolidarea continuă a culturii în domeniul IAp;
- Coordonarea operațională a pregătirii în domeniul IAp, organizată în instituții de învățământ non-universitar și universitar;
- Participarea personalităților reprezentative civile și militare la programele de pregătire, prin extinderea permanentă a colaborării cu instituții de prestigiu de la nivel național și internațional;
- Schimbul de experiență, specializarea și perfecționarea continuă prin asocierea cu parteneri locali, regionali și globali;
- Încheierea de acorduri internaționale și protocoale de cooperare națională cu instituții similare sau cu atribuții conexe domeniului IAp;
- Extinderea permanentă a parteneriatului profesional cu structurile beneficiare ale proceselor educaționale, naționale și internaționale, sub forme variate de asociere la nivel de specialiști;
- Abordarea provocărilor specifice domeniului IAp din punct de vedere conceptual și practic-aplicativ în contextul evoluțiilor tehnologiilor emergente și disruptive;
- Dezvoltarea laboratoarelor și platformelor de modelare-simulare în facilitățile proprii, instituții de învățământ superior și în cadrul altor organizații partenere;
- Participarea activă în cadrul grupurilor de lucru naționale și internaționale pentru standardizarea domeniului IAp;
- Participarea cu regularitate a specialiștilor instituției la forme de pregătire și misiuni naționale și internaționale;
- Investiții constante în infrastructura didactică pentru asigurarea pregătirii intradisciplinare și interdisciplinare;
- Inițierea de forumuri de dezbatere științifică prin organizarea de seminarii, mese rotunde, conferințe naționale și internaționale;
- Contribuția la dezvoltarea și implementarea noilor abordări conceptuale educaționale de la nivel NATO și UE, cum ar fi *NATO Intelligence Academy* și *Intelligence College in Europe*;
- Promovarea inovativă a tehnologiilor de vârf în identificarea de soluții la provocările spațiului cibernetic din perspectiva misiunilor specifice domeniului IAp;
- Extinderea rețelei cognitive în sectorul industriilor și al cercetării științifice, pentru crearea unui mediu colaborativ, interactiv și operativ la nivel de experți;
- Afilierea și contribuția la comunitățile de interese, create pe diferite platforme informaționale, referitoare la distribuirea de lecții învățate și bune practici, dezvoltarea doctrinară și organizațională, leadership și interoperabilitate educațională.

Centrul de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” va continua să fie o instituție inovatoare, care să asigure pregătirea la cele mai înalte standarde în domeniul IAp, pe toate palierele educaționale, la nivel tactic, operativ și strategic. În același timp, pregătirea personalului armatelor Alianței și din state partenere non-NATO în domeniul IAp reprezintă o premisă majoră pentru promovarea intereselor și imaginii Armatei României în mediul internațional și a extinderii conceptelor de securitate cooperativă, managementul crizelor și apărare colectivă dincolo de frontierele NATO și UE.

Promovarea conceptelor moderne de management și leadership, metode, tehnici și practici educaționale moderne, învățământ intradisciplinar, interdisciplinar și multicultural, reprezintă obiective operaționale prioritare ale CPDIA pentru dezvoltarea creativă a abilităților de comunicare și conștientizare situațională a specialiștilor în domeniul IAp.

Momentul festiv al Centrului de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu” îmi oferă deosebita bucurie și plăcere să mulțumesc conducerii Ministerului Apărării Naționale, Direcției generale de informații a apărării și structurilor din compunerea acesteia pentru contribuția decizională și sprijinul constant la dezvoltarea continuă a educației și instruirii în domeniul „informații pentru apărare”, ca premisă esențială a evoluției acestei structuri și a extinderii interoperabilității forțelor armate la nivel întrunit și multinațional.

Stimați și dragi colegi, cu ocazia acestui prilej aniversar al devenirii noastre instituționale, vă rog să primiți un gând de suflet, plin de respect pentru eforturile, devotamentul, valoarea și profesionalismul dumneavoastră, atitudini determinante în dobândirea prestigiului de care se bucură astăzi Centrul de pregătire în domeniul informații pentru apărare „General Nicolae Condeescu”, la nivel național și internațional.

Vă adresez tuturor felicitări, sănătate, împliniri în plan profesional și personal alături de cei dragi și să continuați cu demnitate îmbogățirea tradițiilor domeniului informații pentru apărare cu spiritul dumneavoastră creator.

DOCENDO DISCIMUS !

La Mulți Ani!

Direcția generală de informații a apărării

INFOSFERA, anul XIII, nr. 4, 2021

Revistă de studii de securitate şi informații pentru apărare

PROVOCĂRI PENTRU INTELLIGENCE ÎN EPOCA MAD 2.0

*Iuliana Adriana DUMITRACHE**

Abstract

The COVID pandemic – a game changer - came on top of the acceleration age, which is already abundant in massive acts of discontinuity. Therefore, approaching the security issues apart from the safety issues (which includes the civil, social, economic sphere) might be an inappropriate endeavor for these times we live. The article points out the effects the Intelligence Services has felt within the last months, directly or non-directly. Another topic is that Pandemic brought in new sensitive issues, therefore the intelligence institutions should re-direct their attention towards these new subjects of interest. Thus, due to a vast complexity of information, to an increasing, real-time acces to it, and also to the changing vectors, the analyst may feel the difficulty of the high incertainty and impredictibility of the situations. The Cynefin concept helps us be aware of their complexity. Further on, the plead for prospective, prediction analysis (both as products and as an ongoing form of thinking) is justified by the decision-makers` need of having on hand the most probable materials to support their decisions.

Keywords: *Massive Acts of Disruption, Cynefin, Pandemics, intelligence, HUMINT, analysis, forecast, resilience.*

În plină eră a MAD 2.0 – Massive Acts of Disruption

Harlan K. Ullman[1], în articolul *Noul MAD în vremuri de Westfalia II*[2], avansează un raționament potrivit căruia actuala conjunctură geopolitică este favorabilă unei alte accepțiuni a consacratului acronim MAD. Tradițional, acest acronim desemna termenul de *„Mutual Assured Destruction" (Distrugere Reciprocă Asigurată)* - o doctrină bazată pe Teoria Descurajării, conform căreia utilizarea pe scară largă a armelor de distrugere în masă ar rezulta în anihilarea completă, totală și irevocabilă atât a atacatorului, cât și a apărătorului, acest război terminându-se fără nicio victorie sau armistițiu, doar cu distrugere reciprocă.

Într-o accepție nouă, dar păstrând acronimul, *Distrugerea Reciprocă Asigurată* devine *Massive Acts of Disruption (Acte de Discontinuitate Masivă).* Într-o lume în care state relativ mici sau foarte mici, împreună cu actorii non-statali – inclusiv indivizii, exercită o influență considerabilă, uneori decisivă asupra cursului evenimentelor, pe măsură ce globalizarea și dispersarea puterii au sporit interdependența statelor, s-au creat neintenționat și multe vulnerabilități și fragilități. Aceste slăbiciuni pot fi exacerbate ca urmare a intervenției Actelor de Discontinuitate Masivă. Prin urmare, o determinare corectă a paradigmei de securitate globală sau națională nu se mai poate face fără a ține cont de Actele de Discontinuitate Masivă, care au în zilele noastre impactul cel mai profund asupra securității, stabilității și siguranței. Astfel, protejarea împotriva rupturilor sau discontinuităților devine una dintre cele mai importante prerogative ale guvernelor actuale și viitoare.

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

Actuala pandemie a demonstrat vulnerabilitatea și fragilitatea guvernelor în privința capacității de organizare, anticipare și răspuns la acest tip de criză disruptivă, căreia nu i se pot opune forțele miliare - forțe care în trecut au reprezentat fundamentul apărării statelor. Asta deoarece realitatea și însuși modul de viață se schimbă. Analistul Alexandru Georgescu (Fundația EURISC), în cadrul unui interviu în emisiunea *Sfere de Interes*[3], menționa imposibilitatea ca, în timpurile noastre, să se mai abordeze separat problemele de *securitate* față de cele de *siguranță* (care implică sfera civilă, socială, economică etc). Fenomenele generate de Actele de Discontinuitate Masivă sunt o fuziune de probleme de securitate, sociale, economice. Această schimbare de paradigmă și sintagmă ar trebui să ducă inclusiv la adaptarea pentru supraviețuire a comunităţilor/societăților, a instituțiilor și a relațiilor dintre ele.

Serviciile secrete sunt parte a acestei realități, o realitate mai puţin obişnuită, mai puţin transparentă, e drept, dar care în aceste zile este şi ea supusă schimbării. Între dezinformare, fake-uri, panică şi necesitatea asigurării securităţii cetăţenilor, deopotrivă cu a propriilor angajaţi, agenţiile de intelligence continuă să-şi îndeplinească misiunea[4].

Mutații cu impact în domeniul intelligence, în context pandemic

1. Efectele directe ale pandemiei în funcționarea serviciilor de intelligence

1.1. Este ușor de intuit că va fi greu pentru serviciile de informații să își desfășoare activitatea specifică în condiții pandemice. În opinia specialiștilor, această impresie are însă greutatea unei certitudini amare. Cel mai afectat palier este, așa cum ne așteptam, culegerea de informații din surse umane (HUMINT). De exemplu, în articolul „How Do You Spy When the World Is Shut Down?“[5], autorii afirmă că pandemia constituie cel mai mare obstacol pentru culegerea de informații din surse umane din istoria CIA. Fostul director al acestei instituții, Gina Haspel[6], declara că misiunile de tip HUMINT constituie specialitatea CIA în cadrul Comunității americane de Intelligence și că, „deși toate tipurile de culegere de informații sunt importante, o sursă umană bună este unică și poate furniza informații decisive privind secretele sau chiar intențiile adversarilor noștri“. Legăturile față-în-față și acțiunile pe teren rămân necesare, cu foarte rare excepții.

Prin suplimentarea mijloacelor tehnice de culegere se încearcă suplinirea, cel puțin temporară, a handicapului pe care HUMINT îl înregistrează în această perioadă, însă rezultatele, deși compensează într-o oarecare măsură, sunt totuși teribil afectate – neavând același grad de concretețe, de percepție și interpretare umană, de subtilitate. Articolul menționat mai sus precizează, tot referitor la CIA, că ofiţerii de informaţii se confruntă cu dificultăţi când trebuie să recruteze noi surse, iar tehnicile normale nu funcţionează în circumstanţele unice create de virus. Ofiţeri de caz din diverse zone ale lumii semnalează faptul că nu își pot desfăşura în siguranță activitatea în oraşe în care străzile sunt goale sau sub restricţii de carantină. În plus, este de aşteptat ca unii dintre lucrători să fie infectaţi de coronavirus.

Dacă vor continua multă vreme restricţiile legate de virus, impactul asupra operaţiilor va fi semnificativ, în special pentru că lucrul de acasă nu este o opţiune pentru mulţi angajaţi ai agenţiilor de *intelligence.* Atunci când acest fapt este posibil, ofițerii de informații beneficiază de un program flexibil, deși în unele secțiuni, precum centrele de operaţii, este necesar să existe personal în permanenţă. Multe agenţii abordează problema prin „trecerea la schimburi pentru a reduce numărul de persoane la birou la anumite ore” şi separarea personalului în „esenţial” şi „neesenţial”, dar aceste *disocieri* nu sunt riguros determinate și nici productive.

CIA a restricţionat accesul în clădirile sale, iar reuniunile cu alte agenţii guvernamentale au loc prin intermediul teleconferinţelor video. Activitatea de la distanţă este îngreunată de faptul că reţelele clasificate de comunicaţii digitale nu sunt operaţionale din locaţii îndepărtate. În plus, informaţiile *top secret* trebuie să rămână în spaţii fizice special desemnate.

1.2. Un alt factor menit să afecteze eficiența serviciilor de informații este că redirecționarea resurselor de personal operativ și a celor analitice către subiectul combaterii COVID-19 încetinește ritmul de lucru pe alte domenii ale securităţii naţionale. În acest moment, unele servicii de informații sunt implicate în limitarea răspândirii COVID-19 nu doar cu sprijinul informativ al decidenților, ci și sistemic.

Astfel, Shin Bet (Agenţia de securitate internă a Israelului - ISA) folosește tehnologia de combatere a terorismului pentru a stopa răspândirea coronavirusului (poate urmări telefoanele mobile ale persoanelor suspecte sau confirmate că au fost infectate cu virusul COVID-19). Shin Bet a răspuns la solicitarea Ministerului Sănătăţii „din responsabilitate şi înţelegând că are capacitatea de a salva viaţa cetăţenilor israelieni" (directorul agenţiei, Nadav Argaman)[7]. Astfel, Shin Bet preia numele persoanelor infectate de la Ministerul Sănătăţii şi apoi îşi foloseşte capacităţile de urmărire pentru a verifica, timp de 14 zile, şi a monitoriza persoanele infectate apropiate. Guvernul israelian a adoptat de urgenţă regulamente care autorizează ISA să utilizeze metadatele şi poliţia să utilizeze datele locaţiei pentru a gestiona focarele de coronavirus.

1.3. Pentru a cunoaște și contracara corect amenințările de natură pandemică se menține necesitatea întăririi segmentului MEDINT din cadrul serviciilor de informații naționale, cooptarea de specialiști de medicină militară sau, cel puțin în primă fază, a unora cu specializări militare din domenii conexe (NBC). O altă variantă ar consta în înființarea unor structuri aparte, dedicate acestor tipuri de amenințări, pe modelul celor CYBER sau după modelul american al Centrului Naţional pentru Informaţii Medicale (CNIM), parte a Agenţiei de Informaţii pentru Apărare (DIA), care folosește toate sursele de informaţii specifice unui serviciu de informații (interceptarea comunicaţiilor, imagini prin satelit, surse deschise, surse umane). Centrul dispune de o echipă multidisciplinară de experţi - virusologi, epidemiologi, toxicologi, medici, medici veterinari – și, deși are drept client principal armata americană (care folosește informaţiile pentru a monitoriza potenţialele ameninţări de sănătate pentru forţele sale din străinătate), analizele sale servesc acum mai mult decât oricând informării zilnice a oficialilor, aducând plus-valoare prin datele pe care nici Organizaţia Mondială a Sănătăţii sau Centrele pentru Controlul Bolilor nu le deţin[8]. Un fost director al CNIM[9] a descris misiunea ca fiind de „protejare a ţării de ameninţările cu care oamenii nici măcar nu vor şti că ne confruntăm"[10]. Încă din luna februarie a anului 2020, CNIM a estimat că focarul va atinge proporţiile unei pandemii.

2. Mutații în context pandemic cu impact indirect asupra activității de intelligence

2.1. Până de curând, agențiile de informații ale marilor puteri se concentrau asupra proliferării nucleare, asupra sistemelor de transport și lansare a armelor nucleare (nuclear-capable delivery systems) și dezvoltării tehnologiilor care ar spori capacitatea unor rachete, cum sunt cele hipersonice (împotriva cărora nu există nicio apărare până în acest moment).

Experții independenți (ex: Harlan Ullman) și actuali membri ai unor think-tank-uri consideră necesară, într-o primă fază foarte urgentă, re-orientarea tematică a activității serviciilor de informații în sensul concentrării pe acele implicații ale pandemiei care pot avea ulterior efecte disruptive la nivel macro și în domenii critice, cum ar fi:

- *Limitarea capacităților militare,* ca urmare: a constrângerilor bugetare/economice destinate luptei cu pandemia; a inevitabilei vulnerabilități a resursei umane; a regulilor de distanțare fizică; a dependenței unor sisteme și infrastructuri critice și a unor sisteme de armament de factorul uman; a percepției eronate conform căreia nu mai este nevoie de armată ca în trecut; a deciziilor politice care orientează fondurile către alte sectoare vitregite.
- *Restrângerea interacțiunii sociale firești:* îngreunează buna funcționare a tuturor domeniilor economice și sociale; duce la alienarea psiho-socială a persoanelor și a societăților; forțează desfășurarea unor

activități lucrative și decizionale în mediul online; afectează activitatea medicală, socio-administrativă, guvernamentală și în mediul aliat.

- *Amenințarea fluxurilor de aprovizionare critică:* sectoare întregi ale economiei sau părți din sistemul de sănătate depind de lanțuri prea lungi de aprovizionare sau de trasee care sunt controlate de actori geopolitici potrivnici; unele lanțuri de aprovizionare au furnizori cu monopol pentru produse critice.
- *Apariția unor probleme economice severe și diverse* - pierderea sau închiderea temporară a unor locuri de muncă sau sectoare de activitate, ceea ce poate cauza dezechilibre în lanț; dificultatea procurării materiilor prime sau întârzierea livrării lor pentru anumite industrii; lipsa lichidităților, deficite bugetare afectate.
- *Tulburări sociale* (amplificarea unor nemulțumiri, dezinformarea despre coronavirus, provocarea prin instigare sau dezinformare a unor categorii sociale împotriva altora, formarea de false tabere - pro și contra vaccinării, pro și contra teoriilor conspiraționiste, pro și contra programelor guvernamentale de gestionare a crizei).

2.2. Referitor la efectele psiho-sociale ale izolării și distanțării în context pandemic, se constată o escaladare a tacticilor de dezinformare, care iau în calcul activarea reacţiilor emoţionale, precum frica, la zvonurile care înconjoară o pandemie, mai ales atunci când este deficitar gestionată şi extrem de politizată. Tot ca o consecință a distanțării în context pandemic și a opririi practicilor economice curente s-a remarcat o creștere excepțională a dependenței de Internet și consum media. Creșterea nu a însemnat neapărat diversificare, ci doar o atenție mai mare acordată mediului de comunicare preferat. S-a constatat că cei care au încredere în mass-media mainstream (tv, radio, ziare) sunt mai puțin predispuși să creadă în teoriile conspirației și mai dispuși a avea încredere în instituții. Viceversa, cei care au încredere în rețelele de socializare au o predilecție, între anumite limite, predominant anti-sistem, anti-instituții, chiar anti-autoritate. Pe toate canalele de comunicare, fie mainstream, fie digitale, au fost mediatizate ipoteze conspiraționiste, ceea ce sensibilizează auditoriul la subiecte greu de combătut/dezinformare[11]: noul coronavirus a fost fabricat în SUA pentru a domina lumea; știri false despre coronavirus răspândite intenționat pentru a îmbolnăvi; noul coronavirus - destinat pentru a încetini îmbătrânirea populației; coronavirusul a fost propagat pentru a declanșa o criză economică mondială; noul coronavirus - fabricat de China pentru a domina lumea.

De asemenea, pe fondul iritării populației și a expunerii continue la știri alarmiste, manifestările sociale se contaminează reciproc, creând fenomene de tip „bulgăre de zăpadă", care înglobează, deopotrivă, pe lângă acuzațiile de limitare a libertăților în context pandemic, și acuzații de rasism, epurare etnică, care izvorăsc din proasta gestionare a unor evenimente și din izbucnirea unor tensiuni latente. Putem menționa aici fenomenele amestecate, care se potențează reciproc, care au animat și reverberează în Statele Unite: mișcările anti-măsuri COVID, acțiunile de tip *Cancel Culture*[12], protestele declanșate de moartea lui George Floyd, frustrarea și timorarea persoanelor care nu pactizează cu revoltele mișcării de extremă stânga comunistă Antifa (Anti-Fascist Action) și cu neo-iacobinismul *Black Lives Matter*. Fenomenul a fost amplificat în mod exagerat, fiind propagat și în alte state, culminând cu manifestații de stradă deosebit de violente, soldate ulterior cu dărâmarea unor statui ale unor personalități artistice și științifice sau cu scoaterea din programa de studiu a unor opere ale literaturii/muzicii universale considerate a avea tente discriminatorii sau ofensatoare (sau aparținînd unor astfel de personalități)[13].

Înțelegerea variabilelor din sistemele complexe – provocare deja prezentă pentru analiza de informații

Complexitatea crescândă a situațiilor care ne înconjoară în această epocă marcată de incertitudine pune la încercare, din ce în ce mai mult, însuși scopul existenței serviciilor

de informații - de a avertiza din timp cu privire la tendințele de manifestare ale unor riscuri și amenințări la adresa securității naționale/ internaționale, de a reduce efectul de surpriză/ incertitudine, în scopul sprijinirii fundamentării unor decizii, politici și strategii preventive. Se pare că va fi din ce în ce mai greu de realizat acest lucru, din două motive: multiplicarea în progresie geometrică a datelor și accesul tot mai mare și în timp real la informații, pe de o parte, precum și multitudinea de factori (izolați sau sinergic cu alții) care pot schimba evoluția situațiilor și despre care nu suntem conștienți că se pot manifesta. Aceste aspecte consolidează importanța analizei de intelligence în procesul de fundamentare a politicilor unui stat, respectiv de valorificare a oportunităților de realizare a unor interese de securitate națională. Cu alte cuvinte, va fi, simultan, din ce în ce mai greu pentru analiști și mai necesar pentru beneficiari ca serviciile de informații să sprijine cu estimări, dar mai ales cu predicții (tipuri de produse informative care, deși la prima vedere pot părea că nu au o însemnătate foarte mare, orientează nu doar procesul de planificare, ci și culegerea de informații), procesul decizional din domeniul securității naționale.

Mircea Mocanu[14], fost șef al structurii de analiză a informațiilor militare din cadrul NATO, aduce în discuție teoria Cynefin, când se pune problema provocărilor pentru analiza de informații în epoca actuală. Această teorie categorisește sistemele complexe în funcție de gradul lor de incertitudine. Expertul consideră mediul de securitate drept spațiu operațional sau ceea ce în știință este numit „sistem adaptiv complex", ale cărui vulnerabilități integrează în mod negativ interconexiuni complexe între componentele sale. Astfel, pentru a prevedea pe cât posibil pericolele, componentele mediului de securitate trebuie monitorizate integrat și în dinamica lor, pentru a pune în evidență evoluțiile ce pot duce la evenimente sau circumstanțe nedorite, dar și la oportunități de acțiune. În cazul unor medii de securitate cu entropie mare, cum este o criză politică internațională majoră sau spațiul operațional în cadrul unui conflict armat deschis, criticalitatea este intensă și multe cursuri de acțiune pot avea rezultate numeroase, cu probabilități apropiate. *„O situație care are o gamă largă de rezultate posibile are o mai mare volatilitate și, probabil, un risc mai mare decât o situație cu o gamă mai restrânsă de rezultate posibile*"[15].

Revenind la conceptul Cynefin, acesta conține o ierarhizare a gradului de incertitudine din sistemele complexe, o scară ierarhică în care sunt descrise situații generate de relațiile cauză-efect din cadrul sistemului: evidente, complicate, complexe, haotice și dezordine[16]. Acestea sunt situațiile/tipurile de probleme cu care se pot confrunta analiștii, dar și decidenții (managerii).

(1) Astfel, *situațiile simple* sunt caracterizate de:

- tipare recurente și evenimente structurate;
- relații clare cauză-efect, evidente pentru oricine;
- există răspunsuri corecte;
- informațiile sunt din categoria „cunoscute cunoscute";
- ciclul de răspuns e de tipul Percepție - Categorisire/Analiză - Răspuns.

În această situație analistul are toate datele, trebuie doar să aplice metoda de rezolvare care să conducă la rezultatul necesar. Acest tip de context este foarte util pentru învățământ, unde nu contează de fapt rezultatul, ci practicarea metodei.

(2) *Situațiile complicate* presupun următoarele caracteristici:

- este necesară diagnoza unor experți;
- relațiile cauză-efect pot fi identificate, dar nu sunt imediat vizibile oricui;
- sunt posibile mai multe răspunsuri, nu doar unul;
- informațiile sunt din categoria „necunoscute cunoscute";
- managementul se realizează pe bază de fapte concrete;
- același ciclu de răspuns: Percepție – Analiză - Răspuns[17].

Analiștii sunt experți care identifică relațiile cauză-efect și iau în considerare mai multe răspunsuri/cursuri de acțiune, sunt căutate informații acționabile, toate în cadrul ciclului

de intelligence (culegere, analiză - decizie și acțiune).

(3) *Situațiile complexe* implică:

- fluxuri de informații, energie și imprevizibilitate;
- nu există răspunsuri corecte și unice;
- se manifestă tipare emergente ca efect al adaptării;
- intervin „necunoscute necunoscute";
- apar multe idei concurente, antagonice, divergente; sunt necesare abordări creative, inovatoare;
- conducerea este concentrată pe tipare de evoluție;
- ciclu de răspuns cu secvența Testează – Percepe - Răspunde.

Fluxurile de informații și energie se desfășoară cu o dinamică ce determină imprevizibilitatea extinsă a comportamentului sistemului. Elementele relevante nu sunt cunoscute, categorisirea realităților nu mai are utilitate, analiștii fiind nevoiți să își imagineze comportamente, iar în acest caz apar multe scenarii posibile și idei diverse, toate legitim a fi luate în considerare. Leadershipul necesar trebuie să vizeze tot comportamente recurente sau emergente. În consecință, astfel de complexități reprezintă cele mai dificile provocări pentru analiștii de intelligence[18].

(4) *Situațiile haotice* sunt descrise ca având următoarele caracteristici:

- sistem cu turbulențe intense;
- nu se disting relații clare cauză - efect, deci nu are rost să se caute răspunsuri corecte;
- nu sunt cognoscibile elementele relevante pentru descrierea stării sistemului;
- trebuie luate multe decizii și nu este timp de a le gândi; tensiune intensă;
- leadership bazat pe tipare de comportament ale sistemului;
- ciclul de răspuns Acționează – Percepe - Răspunde.

Situația descrisă drept haotică este improprie analizei, răspunsul fiind mai degrabă instinctiv, ținând de talent și noroc, decât determinist, rațional.

(5)*Ultima situație, cea de dezordine,* cuprinde aspecte absolut aleatorii, unde răspunsul nu poate avea legături nici cu talentul nativ al unor factori de decizie, dar nici cu activitățile de analiză, care nu ar dispune de niciun element de abordare rațională a problemei.

Categoriile de sisteme enumerate mai sus pot fi identificate și în situațiile din mediul de securitate, însă spre deosebire de un flux de informații în condiții normale, deși aglomerat, care plasează majoritatea contextelor în modele de tipul 1, 2, mai rar 3 și rareori 4, condițiile dezvoltării accelerate continue a tehnologiilor, inflația de informații și fenomenele disruptive de tipul pandemiei aduc în discuție mult mai multe variabile sau necunoscute, ceea ce presupune mai multe situații de tipul 3 – complexe și 4 – aparent haotice sau haotice până la un punct. Aceste situații complexe, fiecare în particular, necesită un efort de analiză mult mai mare, mai multă atenție și timp acordat efortului de înțelegere, în condițiile în care structurile/instituțiile de analiză sunt structuri fixe, cu un număr limitat de analiști – structuri mai dificil de reconfigurat și redimensionat.

Reziliența – caracteristică imperios necesară, dar nu suficientă

Factorii de decizie (de nivel național, dar și aliat) sunt conștienți de complexitatea și dificultatea de a înțelege și de a face față epocii accelerației și propun reziliența la toate nivelurile drept măsură de adaptare. Pentru contracararea unor *Acte de Discontinuitate Masivă* (*Massive Acts of Disruption) s*e dorește generarea unor *Acte de Reziliență Masivă* (*Massive Acts of Resilience)***.** În actualele documente programatice NATO, UE, naționale ale României și ale altor state[19] termenul de reziliență apare foarte frecvent, fiind considerat deopotrivă un deziderat și o trasătură esențială a indivizilor, structurilor administrative, instituțiilor, structurilor de forță, pentru a reuși să își îndeplinească funcțiunea.

De fapt, reziliența este capacitatea unui individ, grup sau societate de a continua să se proiecteze, în viitor, în ciuda evenimentelor destabilizatoare, condițiilor de viață dificile, traume, uneori severe (Stefan Vanistendael, *Le*

resilience ou le realisme de l'esperance, Cahiers du BICE, 1996). Reziliența socială are trei proprietăți:

- rezistența — eforturile unei entități de a suporta o perturbare și consecințele acestora;
- recuperarea — timpul necesar pentru ca o entitate să se recupereze;
- creativitatea — adaptarea la noile circumstanțe și învățarea din experiența unor perturbări.

Reziliența nu este însă un element abstract, ușor de obținut, ci presupune experiență, o oarecare maturitate, know-how, anumite trăsături psihice în cazul persoanelor (rezistență la stress și frustrare, know-how – capacitatea de a învăta din propriile greșeli sau ale altora, capacitatea de revenire și auto-motivarea, un oarecare grad de desensibilizare) și mobilitate în cazul instituțiilor (leadership anticipativ și adaptativ, resurse financiare, flexibilitate și spirit inovativ pe durata și în timpul proceselor de producție sau de execuție în cadrul unităților interne și subordonate, management capabil să ia decizii din mers, procese interne constructive de analiză a deciziilor care nu culpabilizează, un foarte bun feedback sau capacitate de sondare a pieței). Nimeni nu are timp să învețe indivizii sau instituțiile cum să devină reziliente. Este un efort intrinsec asumat al acestora, uneori lipsit de succes. Prin urmare, introducerea și vehicularea, în documentele programatice, a unui atribut (rezilient) greu de cuantificat și internalizat/implementat nu este și suficientă pentru a-și produce efectele.

Pe de altă parte, acțiunea în scopul depășirii dificultăților, adaptarea din mers, sunt singurele atitudini care pot genera soluții. Absența disponibilității de a reflecta la ceea ce nu a funcționat, atitudinea contemplativă, pot mări blocajele, paraliza decizia și acțiunea eficientă. „O perioadă în care cei supuși tentației facilului indivizi, țări și alianțe de țări deopotrivă - vor avea dificultăți de adaptare și, copleșiți de complexitatea și magnitudinea schimbărilor, vor fi retrogradați la o poziție marginală: cea de spectator, audiență, public urlător, spațiu de manevră, piață de consum al produselor și ideilor”[20].

Concluzii

În opinia lui Harlan Ullman, este imperativ să se depună eforturi în anticiparea reprezentării unei lumi post-pandemie dominate de fenomene de tip MAD, precum și să se conștientizeze probabilitatea că vom dispune de mult mai puține resurse pentru apărare. Trebuie studiat dacă NATO ar putea deveni un catalizator pentru coalizarea țărilor care împărtășesc aceleași valori, astfel încât să poată face față discontinuităților și efectelor MAD prin numeroasele sale parteneriate și acorduri - Parteneriatul pentru Pace, Dialogul Mediteranean și chiar în cadrul partenerilor de coaliție (cum a fost cazul în Irak și Afganistan).

Un astfel de efort de imaginație a fost deja efectuat sub forma unui document elaborat de către un *grup de reflecție* desemnat de către Secretarul General al NATO. Documentul conține viziunea grupului de experți cu privire la rolul NATO în 2030, surprinde principalele fenomene și trenduri care vor influența NATO în actuala decadă și conține recomandări structurate tematic - recomandări care au fost dezbătute la întâlnirile NATO de nivel înalt din cursul anului 2021.

La nivel european, Sistemul de Strategie Europeană și de Analiză Politică (ESPAS) a elaborat un proiect menit să sprijine UE în identificarea de trenduri globale majore, a implicațiilor lor, precum și a opțiunilor de politici cu care se vor confrunta factorii de decizie. Printre factorii disruptivi cu cel mai mare efect se enumeră tehnologia informațională, digitalizarea, o criză financiară a statelor din sudul UE, dar și a statelor vecine de pe celălalt țărm al Mediteranei, un atac cibernetic pe scară largă, conflict inter-statal în Orientul Mijlociu sau Asia (ex: China - SUA în regiunea Asia - Pacific), o bătălie pe piața financiară între moneda chineză (renminbi) și dolarul SUA etc.

În planificările şi exerciţiile instituţiilor internaţionale, dar şi ale celor naţionale, de imaginare a viitorului, se acordă o atenţie deosebită şi tehnologiilor disruptive, ca acompaniind evenimentele de tip MAD ori neinterferând cu acestea. La Munchen sau Davos, în centrele marilor organizaţii internaţionale sau cu prilejul întâlnirilor în format G7 sau G20,

mesajele promovate converg către concluzia că, în anii ce vor urma, tehnologiile militare sau civile cu care vom coabita, dar care totuşi pot avea un potenţial disruptiv asupra securităţii internaţionale[21], sunt inteligenţa artificială, Big Data, sisteme noi de senzori, interfaţa om-maşină, robotică și sisteme de armament convențional avansate (lasere, arme hipersonice), sistemele autonome de armament, armele cu energie direcţionată, tehnologia cuantică (sisteme de calcul, comunicare şi criptare, sisteme de radar și senzori Quantum) şi biotehnologiile[22]. La acestea concură şi tehnologiile emergente, încă în dezvoltare: nanotehnologia, biotehnologia, ştiinţa cognitivă, psihotehnologia, robotica şi inteligenţa artificială[23].

Factorii de decizie de nivel înalt (șefi ai administrației locale și de nivel național, guvernamental) conștientizează că, pe viitor, va fi necesar să manifeste deschidere și încredere cu privire la avertizările privind posibila concretizare a altor factori puternic disruptivi, nu doar pandemii diverse, ci și diferite fenomene de tip „lebădă neagră" sau care pot schimba radical mersul lucrurilor (game changer). Acest lucru este transmis drept recomandare NATO pentru scenariile exercițiilor comune sau pot fi incluse ca subiecte de discuție în programele studiilor de leadership militar sau în cadrul Colegiului Național de Apărare.

Reziliența este studiată în mediul economic și financiar, evident sub o formă preventivă, cu denumirea de Total Loss Absorptive Capacity (TLAC - capacitatea de a absorbi șocuri), anticipând momentul intervenției băncilor centrale, a guvernelor, când industria financiară este în dificultate. Și în cazul economiei este esențială capacitatea de absorbție a șocului, fiind nevoie de un buget public solid, de rezerve (buffers), bănci centrale credibile, solidaritate, colaborare, parteneriate public-privat, coordonatori de acțiuni colective. Bionomics - credința că sistemele se echilibrează de la sine, fiindcă sunt complexe, nu convinge. Șocurile mari, non-liniaritățile, destabilizează ușor sistemele, mai cu seamă când se află în stări de echilibru precar[24].

Așteptările publicului occidental erau că pandemia nu va afecta Occidentul și Statele Unite, pentru că acolo există sisteme de infrastructură critică performante, clinici, institute de cercetare, sisteme sanitare faimoase și personal medical înalt calificat. Realitatea a fost că unele dintre cele mai bine pregătite țări au fost afectate serios, din cauza impactului leadeshipului autosuficient și neprofesionist: în multe țări obișnuite să fie mari puteri conducătorii au eșuat tocmai în obligația de a-și proteja cetățenii. Este posibil ca meritocrația să cunoască un reviriment în multe structuri administrative sau politice.

Semnale optimiste vin de la Forumul economic mondial, care a convocat lideri de afaceri și ai politicii de vârf, pe tema reclădirii societății și economiei într-o manieră mai sustenabilă în condițiile post-COVID, în cadrul celei de a 50-a reuniuni de la Davos, în iunie 2020. Astfel s-a născut proiectul Marii Resetări, care își propune crearea condițiilor pentru o economie a părților interesate (a stakeholder economy), construirea unui viitor pe baze mai reziliente, echitabile și sustenabile, care să incorporeze mai multe proiecte verzi de infrastructură publică, dar și folosirea inovațiilor generate de a patra revoluție industrială[25] pentru binele public, comun.

Rolul structurilor de analiză este și va fi foarte important în viitor, acestea urmând nu doar să evalueze ce se întâmplă deja (în măsura în care ne referim la operați/situații curente din zone de interes), ci să se concentreze foarte mult pe urmărirea unor evaluări foarte bine ancorate în realitate, pe abordări prospective, foarte apropiate de futurologie, pe generearea de scenarii alternative.

Demersul de a elabora avertizări și analize predictive este cu atât mai dificil cu cât dinamismul sistemelor din mediul de securitate se caracterizează prin non-linearitate, foarte propice situațiilor de tip *lebădă neagră*. Există fenomene nedetectate – aleatorii și altele separat sau simultan divergente - care nu sunt supuse legii cauzalității. Structurile de analiză vor avea probabil sarcina de a discerne, la nivel de specialiști, care sunt sursele incertitudinii în cunoașterea evoluțiilor sesizate, respectiv dacă incertitudinea se datorează lipsei de informații (information gap), dacă este incertitudine inerentă (nesiguranță determinată de probabilitatea

apariției unor fenomene non-determinate, aleatorii) sau, probabil, dacă incertitudinea este indusă de operații de manipulare și dezinformare inițiate de alte state/servicii de informații. Prin urmare, serviciile de intelligence tot vor aduce plus-valoare, deoarece produsele lor de prognoză sau previziune reprezintă evaluări probabile elaborate în mod științific privind evoluția cantitativă și calitativă a fenomenului cercetat.

Probabil că generarea de scenarii va fi o provocare permanentă, precum și un exercițiu continuu de imaginare a alternativelor, avându-se mereu în vedere cel mai probabil scenariu, alte scenarii alternative, cel mai rău scenariu, dar, de ce nu, și cel mai favorabil. În opinia lui Vasile Dîncu[26], ar trebui să se construiască scenarii și pentru activități non-militare, care pot contribui la binele societății - de tip economic, simulări de criză pe activități, evoluții economice, investiții, consum, capacitate de absorbție a forței de muncă excedentare, proiecte de redistribuire din partea statului, măsuri de stimulare economică etc. Metoda scenariilor este aproape singura posibilitate de explorare a viitorului marcat de incertitudine. Scenariile permit integrarea unor puncte de vedere diferite; de fapt, diversitatea punctelor de vedere este un plus evident care permite devoalarea unor elemente și structuri importante ale viitorului. Folosirea unor date parțiale sau lipsa de transparență pot afecta scenariile de analiză strategică.

Dincolo de teoria rezilienței, este bine de știut că sistemele sociale bine echilibrate pot absorbi o cantitate mare de factori perturbatori înainte de a se destabiliza. Totodată, pot exista situații de echilibru instabil și în care cauze minore pot duce la consecințe greu de imaginat („efectul fluture” din meteorologie – E. Lorenz).

Având în vedere că instrumentele de analiză cantitativă au o valoare limitată în domeniile caracterizate de existența elementelor intangibile (nemăsurabile) și în care factorul uman joacă un rol decisiv, trebuie acordată atenție, în pregătirea unui analist, dezvoltării abilităților acestuia de a utiliza în procesul de analiză atât elemente de „artă analitică” (gândire critică, intuiție - utilizată cu precauție, fler, capacitatea de a face conexiuni între elemente disparate), cât și de „știință” (cunoașterea metodelor analitice).

Bibliografie:

1. BORGE, Dan, *The Book of the Risk*, New York, Chichister, Weinheim, Brisbane, Singapore, Toronto: John Wiley and Sons, 2001;
2. FINLEY, Alex, Mendez, Jonna, Priess, David: „How Do You Spy When the World Is Shut Down“, 20.03.2020, lawfareblog.com. https://www.lawfareblog.com/how-do-you-spy-when-world-shut-down, accesat la 04.04.2021, ora 16.05;
3. FLORIDA, Richard: *Great Reset: How New Ways of Living and Working Drive Post-Crash Prosperity*, aprilie 2010, Harper Collins e-books, 2020;
4. *Global Trends to 2030: Can the EU meet the challenges ahead?,* European Strategy and Policy Analysis System (ESPAS), Luxembourg: Publications Office of the European Union, 2015, p 48, accesat la 02.04.2021, ora 22.09; https://espas.secure.europarl.europa.eu/orbis/sites/default/files/espas_files/about/espas-report-2015.pdf;
5. GEORGESCU, Alexandru, interviu privind documentul american Instrucțiuni Strategice Interimare privind Securitatea Națională în cadrul emisiunii *Sfere de interes*, Canal 33;
6. IANCU, Niculae: *Noul dicționar al apărării: tehnologiile disruptive*, pe blogul Monitorul Securității și Apărării, monitorulapărării.ro, accesat la 15.06.2021, ora 09.33;
7. IONIȚĂ, Liviu: *Serviciile de informații și COVID-19. Jurnal de pandemie*, Mediafax;
8. MOCANU, Mircea: *Analiza strategică în mediul de securitate contemporan*, Editura Universității Naționale de Apărare „Carol I”, București, 2018;
9. *On Cynefin as a Sensemaking Framework,* pe blogul *AII Life is Problemsolving*, la adresa KMCI.org//alllifeisproblemsolving/archives/on-cynefin-as-a-sensemaking-framework, accesată la 03.112018,
10. OMAND, Sir David: *Securing the State*, Hurst&Co, Londra, 2010;
11. *The Cynefin Framework. Using the Most Appropriate Problem-Solving Process*, la htpps://www.mindtools.com/pages/article/cynefin-framework.htm, accesată la 28.09.2018;
12. ULLMAN, HARLAN K.: Noul MAD în vremuri de Westfalia II, în *Lumea de mâine. Ce urmează după pandemie*, Curtea Veche Publishing, București, 2020.

[1]Harlan Ullman este consilier superior în cadrul fundației Consiliului Atlantic din Washington, susținător fervent al teoriei «porcupine defense» pentru Europa de Est, președintele companiei CNI Guard (în domeniul infrastructurii tehnologiilor de vârf) și partener al firmei de consultanță The Killowen Group.
[2]Harlan Ullman, K.: *Noul MAD în vremuri de Westfalia II,* în *Lumea de mâine. Ce urmează după pandemie.*
[3]Alexandru, Georgescu: *interviu privind documentul american „Instrucțiuni Strategice Interimare privind Securitatea Națională".*
[4]Liviu Ioniță: Serviciile de informaţii şi COVID-19. Jurnal de pandemie, Mediafax.
[5]Alex Finley; Mendez, Jonna; Priess, David: *How Do You Spy When the World Is Shut Down.*
[6]Gina Haspel a deținut conducerea CIA în intervalul 26.04.2018-19.03.2021.
[7]Liviu Ioniță: *Serviciile de informaţii şi COVID-19. Jurnal de pandemie,* Mediafax.
[8]Idem.
[9]Anthony Rizzo, profesor de biologie.
[10]Centrul a monitorizat începuturile epidemiei în Wuhan, iar în prezent *„strânge informaţii despre orice, de la tulpinile de viruşi din spitalele din Italia până la semne ale virusului în lagărele de refugiaţi din Siria"* (Jonathan Clemente, medic, citat în Ioniță, Liviu: Serviciile de informaţii şi COVID-19. Jurnal de pandemie, Mediafax).
[11]Alina Bârgăoanu în *Lumea de mâine. Ce urmează după pandemie?,* p 250.
[12]„Cancel Culture" reprezintă o campanie (manifestată preponderent în mediul digital, dar nu numai) care urmărește „anularea" sau distrugerea sistematică a carierei unei persoane publice care la un moment face o afirmație considerată controversată (posibil a fi etichetată, de exemplu, drept sexistă sau rasistă). „Cancel Culture" constituie una dintre cele mai agresive modalități de manifestare a „corectitudinii politice". Fenomenul a apărut inițial în Statele Unite, în lumea showbiz-ului și la Hollywood (Kanye West sau Scarlett Johansson au fost ostracizați de utilizatorii rețelelor de socializare, fiind literalmente umiliți public). În numele unei pretinse cauze de justiție socială, menționează *The Wall Street Journal* în 2019, „Cancel Culture" folosește tehnici de oprobriu, marginalizare și cenzură, similare celor din discursul public comunist axat pe „instituția dușmanului comun".
[13]De exemplu, în luna martie 2021, din cauza presiunilor pentru „decolonizarea" programelor școlare în urma protestelor *Black Lives Matter,* Universitatea Oxford a fost somată să scoată din programă studiul partiturilor muzicale, deoarece sunt considerate „colonialiste", „în complicitate cu supremația albă". Repertoriul clasic predat la Oxford, cuprinzând opere de Mozart sau Beethoven, se concentrează prea mult asupra „muzicii europene albe din perioada sclavilor". S-a propus și ca abilități muzicale cum ar fi cântatul la un instrument sau dirijatul orchestrei nu ar mai trebui să fie obligatorii din cauza repertoriilor „centrate structural pe muzica europeană albă", fapt care le-ar provoca „studenților de culoare o mare amărăciune", mai ales că „cea mai mare parte a profesorilor de tehnică (muzicală) sunt albi". Printre schimbările preconizate se numără înlocuirea studierii unor compozitori clasici cu teme precum „Africanii și muzica diasporei africane", „Muzici globale" și „Muzici populare".
[14]Mircea Mocanu, *Analiza strategică în mediul de securitate contemporan,* p.42-45.
[15]Dan Borge, *The Book of the Risk,* p.49.
[16]The Cynefin Framework. Using the Most Appropriate Problem-Solving Process, la htpps://www.mindtools.com/pages/article/cynefin-framework.htm, accesată la 28.09.2018.
[17]On Cynefin as a Sensemaking Framework, pe blogul AII Life is Problemsolving, la adresa KMCI.org//alllifeisproblemsolving/archives/on-cynefin-as-a-sensemaking-framework, accesată la 03.112018.
[18]Sir David Omand, *Securing the State,* p. 61.
[19]De exemplu, Strategia Națională de Apărare a României; Instrucțiuni Strategice Interimare privind Securitatea Națională a SUA.
[20]Igor Munteanu, în *Lumea de mâine. Ce urmează după pandemie?,* p.298.
[21]Niculae Iancu: *Noul dicţionar al apărării: tehnologiile disruptive,* pe blogul Monitorul Securităţii şi Apărării, monitorulapărării.ro, accesat la 15.06.2021.
[22]Richard Florida, *Great Reset: How New Ways of Living and Working Drive Post-Crash Prosperity.*
[23]Tehnologiile emergente sunt descrise drept în curs de implementare, parţial aplicate, dar încă nu deplin cunoscute şi întrebuinţate, radicale şi evoluând foarte rapid, cu potenţialul de a avea un impact considerabil asupra domeniului în care vor fi implementate. Impactul cel mai important urmează să vină, se află în viitor, şi, astfel, faza de apariţie este oarecum nesigură şi ambiguă.
[24]Daniel Dăianu în *Lumea de mâine. Ce urmează după pandemie?,* p 342.
[25]A patra revoluție industrială sau Industry 4.0 presupune automatizarea în curs de desfășurare a proceselor de producție tradiționale sau industriale, folosind tehnologii inteligente moderne. În această fază, comunicarea pe scară largă între mașini (machine-to-machine communication/M2M) și Internetul lucrurilor (Internet of things) este integrată pentru o automatizare sporită, comunicare și auto-monitorizare sporită.
[26]Vasile Dîncu, în *Lumea de mâine. Ce urmează după pandemie?,* p 398.

„DESECRETIZAREA" CONCEPTULUI DE SECURITATE. NOȚIUNI, COMPONENTE, DIMENSIUNI, DOMENII ŞI TIPURI DE SECURITATE

Laurențiu-Paul MÂNDRAȘ*

Abstract

Traditionally, security has been associated with the military, and the settlement of pursuing national interests, declaring war and peace have been the responsibility of the state, almost the sole actor of international relations. Since the middle of the twentieth century, security studies have extended the dimension of security from its intrinsic side, mainly state-military centered, to its extrinsic and exhaustive side, human and societal centered, related to the existence of threats to individuals and societies. Simultaneously, the effervescence of international relations specialists extended their study of security to other subjects or security actors besides states, namely the individual and human society. The state is no longer an exclusive subject of security and, in the context of theorizing societal security and human security, the state no longer has an exclusive role in international relations. Therefor, international and non-governmental organizations, multinational corporations, illicit organizations such as terrorists or organized crime organizations, and even the individual himself are playing increasingly important roles in the national, regional, and international security scene.

Keywords*: security, national security, societal security, human security.*

Este necesară o „desecretizare" a securității?

La momentul actual, termenul de *„securitate"* figurează de peste 6.98 miliarde[1] de ori în rezultatele digitale ale celui mai mare motor mondial de căutare a informațiilor pe Internet[2]. Comparativ cu populația mondială actuală, de aproximativ 7.8 miliarde de oameni, termenul are o incidență covârșitoare de 89.50%.

De ce este securitatea atât de importantă? În ce măsură avem cu toții aceeași înțelegere cu privire la securitate? Etimologic, cuvântul *securitate* a apărut pentru prima dată în limba latină, în perioada Imperiului Roman - 250 d.H., reprezentând numele zeiței protectoare a Romei, *Securitas*, cea care asigura securitatea în fața amenințării. Fiind format din alăturarea prepoziției *se-*, cu sensul de *fără*, și a substantivului *cura(ae)*, cu sensul de *grijă, anxietate*, cuvântul *securitas*, are sensul de *fără grijă* ori *lipsă de grijă*[3]. În aceste condiții, chiar dacă sensul predominant este legat de existența sau absența unui pericol, ne putem aștepta la o abordare unitară a domeniului de securitate în cadrul științelor sociale și politice și la acceptarea unei definiții și teorii unitare?

Cu toate că securitatea a fost dintotdeauna o preocupare majoră a omenirii, termenul în sine rămâne unul profund contestat, dar nu neapărat din perspectiva necesității sale, de existență a unei amenințări și de concepere și aplicare a unor măsuri de contracarare, ci mai ales din perspectiva *obiectului de referință* - cine și ce este securizat? - și din perspectiva asupra *amenințării* - cine și ce reprezintă o amenințare?[4] Față de aceste două, considerăm că o a treia perspectivă necesită atenția cuvenită, respectiv *care sunt actorii/ factorii de securitate - insecuritate*, cine răspunde de asigurarea securității și cine generează surse de insecuritate?

Problematica securității ridică un grad mare de complexitate, care presupune înțelegerea conceptelor utilizate, a definițiilor, dar și a contextului istoric ori social în care aceste

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

concepte au fost dezvoltate. Securitatea este înțeleasă diferit de locuitorii unui oraș bombardat în timpul unui război, ori de locuitorii unui oraș devastat de poluarea sistemului de aprovizionare cu apă, ori de locuitorii unui oraș afectat de șomaj în urma diminuării drastice a locurilor de muncă din cauza digitalizării și automatizării activităților economice derulate în regiunea respectivă; această diferență de înțelegere nu provine din faptul că amenințarea nu există, ci din amploarea, tipul și efectele acestei amenințări asupra vieții individuale, ori asupra societății și statului.

Într-o încercare de a lămuri problema securității, Edward A. Kolodziej se întreabă[5] ce ar trebui inclus și ce nu în studierea problemei securității și dacă afectarea oricărei valori și oricarui interes uman, dacă este percepută ca o amenințare, ar trebui transformată într-o problemă de securitate. Răspunsul nostru la dilema lui Kolodziej este acela că *obiectul securității* - amenințările - trebuie raportat la *subiectul securității* și la *actorii/ factorii de securitate* ori *insecuritate* responsabili. Doar așa perspectiva de abordare a securității este cât mai completă și pertinentă. De exemplu, este extrem de dificil, dacă nu chiar imposibil, să înțelegem insecuritatea SUA generată de protestele interne împotriva segregării rasiale de pe parcursul anului 2020, cunoscute în spațiul public drept proteste *Black Lives Matter*, dacă raportăm această insecuritate la mediul internațional și securitatea globală și nu la elementele specifice ale securității societale americane, precum cultura și identitatea.

Literatura de specialitate abundă de definiții ale securității, oferind perspective variate și uneori confuze și contradictorii, fără reliefarea unui numitor comun, iar unii autori[6] chiar argumentează imposibilitatea identificării unei definiții comune și unanim acceptate a securității. Achiesăm la această opinie tocmai datorită argumentelor expuse mai sus.

La momentul actual, termenul de *securitate* nu beneficiază de o definiție unanim acceptată, nici în domeniul științelor socio-umane, precum teoria relațiilor internaționale, studiile de securitate, domeniul psihologiei ori sociologiei, dar nici la nivelul statelor și organizațiilor regionale ori internaționale, ambiguitatea termenului și definițiilor fiind dată de *lipsa consensului privind subiectul, obiectul, actorii, componentele ori dimensiunile securității*.

Astfel, specialiștii domeniului au reprezentări despre securitate variate și, nu de puține ori, contradictorii, fiind identificate *15 tipuri de securitate*, conceptualizate în funcție de caracteristici diferențiate, precum*:*

- *obiectul de referință al securității* sau *subiectul securității*, care poate fi atât individul, comunitatea, societatea, statul, cât și sistemul regional și internațional de state, dacă securitatea este definită mai ales din perspectiva statală;
- *obiectul securității*, care este reprezentat de acțiuni care se constituie ori se pot constitui în *stări sau surse de insecuritate* - amenințări, vulnerabilități și pericole interne și externe la adresa securității, evident fiind distincte în funcție de *subiectul de securitate* avut în vedere;
- *actorii securității*, care pot fi grupați în cel puțin două categorii distincte, respectiv *actorii de securitate* - cine este chemat să asigure securitatea societății? - și *actorii sau factorii de insecuritate* - cine și ce generează amenințări și pericole la adresa securității?

Componente ale securității

Securitatea este multidimensională, iar caracterul său complex rezidă din faptul că aceasta este un fenomen psiho-social ce include cel puțin 3 componente principale[7] (a se vedea fig. nr. 1), respectiv: ***realitatea obiectivă, realitatea construită prin discurs*** și ***politicile și strategiile de securitate.***

În primul rând, ***securitatea este o realitate obiectivă/fiinţare*** exprimată prin prezenţa/ absenţa unor ameninţări și pericole în realitatea concretă în care omul acționează și interacționează cu alți semeni. Este ceea ce specific este înțeles ca *mediu de securitate,* adică însăşi existenţa şi funcţionarea grupurilor umane organizate

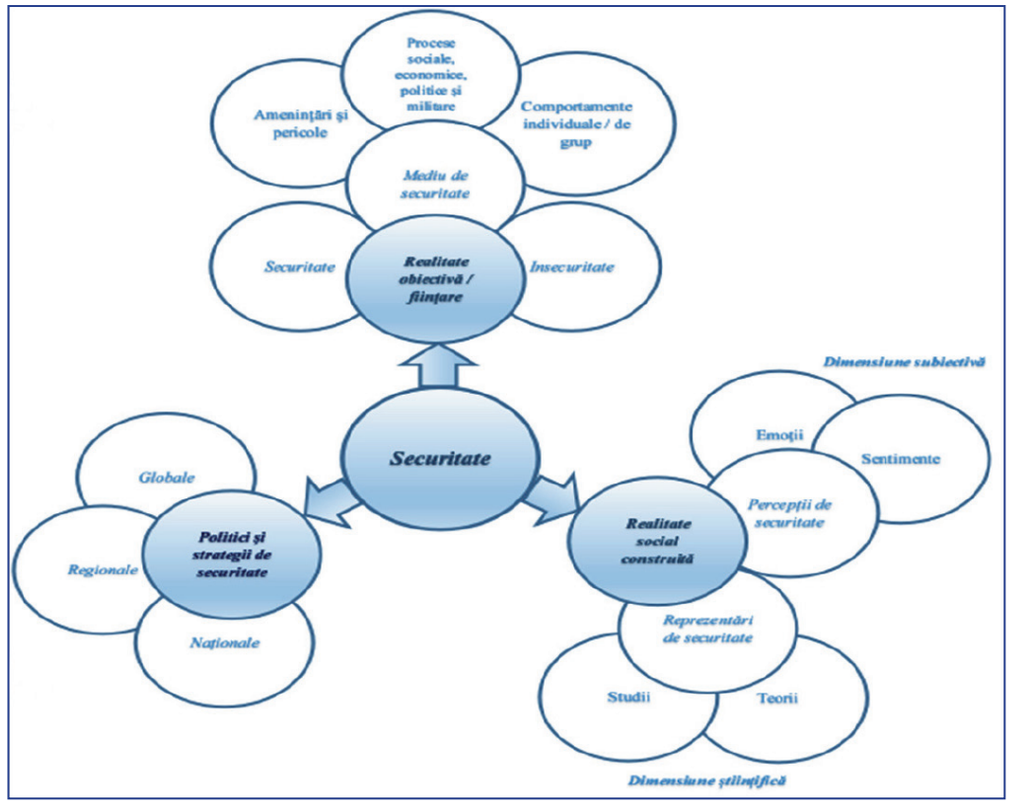


Figura nr. 1: Securitatea ca fenomen psihosocial

politic sau în alte moduri, dacă avem în vedere și actorii non-statali care furnizează sau creează probleme de securitate în zilele noastre, cum ar fi organizațiile private de securitate ori organizațiile teroriste. Securitatea este un tip special de realitate ce are o complexitate deosebită. Prin urmare, are şi modalităţi deosebite de manifestare care rezidă din diferența dintre setul de procese şi fenomene reale care pot apărea în mediul internaţional sau la nivelul unei societăţi oarecare, ca urmare a interacţiunii dintre diferite tipuri de actori, şi „imaginea" pe care oamenii şi-o construiesc prin reflectarea acestor procese şi fenomene[8].

Mediul de securitate este rezultatul desfăşurării unor procese sociale, economice, politico-militare şi comportamente individuale sau de grup, derulate în scopul prevenirii comportamentului în „grilă violentă" al altor actori[9]. Din această perspectivă, securitatea încorporează un set de atitudini şi acţiuni umane desfăşurate cu scop de apărare sau de înlăturare a sentimentului de teamă, angoasă etc., și se manifestă sub forma comportamentului uman la nivel individual sau colectiv. Pacea şi războiul au caracterizat relaţiile dintre state (sau alt tip de organizare politică a comunităţilor umane) din antichitatea clasică până astăzi[10]. Deşi toate popoarele au susţinut, aproape întotdeauna, că şi-au dorit cu ardoare pacea, istoria universală, pe perioada sa „lungă", ne arată că războiul a fost regula, iar pacea a reprezentat excepţia.

Evoluțiile internaționale din ultimele decenii evidențiază că războaiele şi conflictele în forma lor clasică de exprimare, cum a fost cea specifică secolului XX pentru o mare parte a lumii, au dispărut[11], dar au apărut alte elemente atât la nivelul societăţilor, cât şi în mediul internaţional, care pot genera atât amenințări și riscuri, cât și sentimente de frustrare, teamă şi angoasă. Atât percepţia, cât şi reacţia faţă de aceşti factori sunt diferite. Unele colectivităţi umane pot avea sentimentul că trăiesc în siguranţă, altele au o acută trăire a fricii şi angoaselor de toate felurile, de la cele existenţiale până la cele economice şi sociale. Frica şi liniştea, siguranţa și incertitudinea coexistă şi au grade diferite de manifestare. Prin urmare, credem că securitatea ca *realitate - ființare* se găseşte pe acelaşi continuum cu opusul ei – *insecuritatea*[12]. Societăţile umane nu s-au găsit niciodată în ipostaza de a putea să

realizeze o securitate absolută. Puteau să obțină o securitate politică și militară optimă, dar să aibă o insecuritate socială sau de mediu accentuată. Binomul *securitate - insecuritate* nu poate fi desfăcut decât în realitatea virtuală.

Din cea de-a doua perspectivă, ***securitatea este o realitate social construită***, fiind rezultatul observării, reflectării și analizei mediului de securitate, atât al celui intern/societal, cât și a celui internațional, de către un individ care poate fi un analist, teoretician sau om politic[13]. În urma acestor observații asupra mediului intern și/sau extern de securitate, această realitate rezultată se poate manifesta sub două aspecte, respectiv securitate subiectivă și securitate științifică.

Mai întîi, securitatea se poate exprima prin trăirile corespunzătoare – teamă, panică, liniște, pace, siguranță etc., resimțite de către individ la interacțiunea cu o amenințare directă sau potențială. Când procesul de reflectare are ca obiect securitatea ca realitate obiectivă/ființare avem de-a face, în fapt, cu dimensiunea subiectivă a securității, care ia forma unor trăiri exprimate prin sentimente de teamă, panică, angoasă etc.

Pe de altă parte, când observarea și cercetarea mediului intern și internațional se fac cu instrumente științifice de cercetare, se construiesc reprezentări/imagini ale securității materializate în studii și teorii ale domeniului[15], care de facto se constituie tot într-o dimensiune subiectiv științifică a securității. În acest tip de realitate există astăzi o foarte vie și complexă dispută științifică privind evoluția conceptului de securitate[17], dar și a formelor sale de manifestare.

Nu în ultimul rând, în cea de-a treia perspectivă, securitatea rezidă din acțiunea planificată a liderilor politici de a edifica o societate sigură și stabilă, dar și de a construi un mediu internațional fără amenințări și riscuri la adresa securității. Este ceea ce specialiștii au identificat a fi politicile și strategiile de securitate, care pot fi proiectate *la nivel național*[16], *regional* (complexe regionale de securitate) sau la nivel *global*.

Studiile privind securitatea societăților au câștigat o atenție tot mai mare în cercurile academice și guvernamentale de elaborare a politicilor de securitate, dar, la o privire mai atentă, se pare că există dezbateri puternice și dezacorduri între părțile interesate cu privire la ce înseamnă cu adevărat securitatea societăților[18]. Astfel, cel puțin la nivel național-statal, politicile de securitate sunt influențate[19] de *potențialul de putere*, înțeles ca putere militară, diplomatică, economică și simbolică, și *tipul de putere* manifestat în mediul internațional, *interesele* naționale promovate de stat, *ideologiile* politice și sistemul de *valori*, *tradițiile istorice*, *mentalitățile* specifice comunităților, de reacție în fața primejdiilor și amenințărilor de orice fel.

Problema diversificării surselor de securizare este, în primul rând, legată de modul de concepere al politicilor și strategiilor de securitate, iar dacă acestea sunt concepute ambiguu și neconcludent atunci sursele de insecuritate nu vor fi diminuate, ci, dimpotrivă, statele își ratează obiectivele de atingere a securității. De exemplu, cu referire la degradarea mediului înconjurător, Jessica Mathews remarca încă din 1989 faptul că statele se concentrează pe efecte și nu pe cauzele degradării, politicile fiind axate pe contracararea sărăciei și instabilității[20] și nu pe diminuarea activităților care degradează mediul.

Modul de concepere a politicilor și strategiilor de securitate a devenit important tocmai pentru țintirea tuturor posibilelor surse de conflict și „evadarea" din sfera strict militară

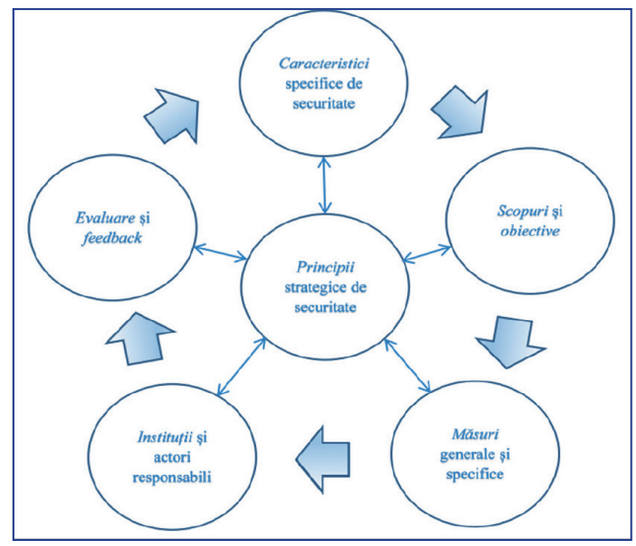


Figura nr. 2: Elemente componente minime ale unei strategii și politici de securitate

(a se vedea figura nr. 2). Dacă inegalitatea economică poate deveni sursă de conflict, atunci politicile de securitate trebuie să identifice soluții de diminuare a acesteia, căci, așa cum concluziona Richard Ullman încă de acum aproape 40 de ani, probabilitatea ca sursele non-militare de insecuritate să crească în intensitate este ridicată, iar neglijarea acestora este periculoasă[21].

Dimensiuni, domenii și tipuri de securitate

Luând în considerare principalele componente și trăsături ale securității, la care am făcut deja referire, precum *subiectul securității, obiectul securității, actorii de securitate/ insecuritate,* dar și *evoluția istorică a cercetării în domeniul securității,* considerăm că ***securitatea are patru dimensiuni principale*** *(vezi fig. nr. 3, Dimensiunile securității)*, cărora le corespund mai multe ***tipuri de securitate*** grupate pe ***domenii specifice***.

● În ceea ce privește **securitatea** în funcție de subiectul de securitate aceasta este clasificată în funcție de evoluția istorică a conceptelor de securitate și atenția acordată de către specialiști asupra subiecților de securitate, respectiv *stat, societate* și *individ*.

► ***Securitatea național-statală***

Istoric, statul s-a dovedit a fi regele neîncoronat al studiilor de securitate, subiectul principal de referință și obiect de securizat, motiv pentru care, pentru o lungă perioadă de timp, studiile de securitate s-au concentrat predominant asupra amenințărilor la adresa securității statului, în mod deosebit amenințările militare. Astfel, securitatea militară a statelor a dominat domeniul studiilor de securitate mai mult de prima jumătate a secolului XX.

Securitatea statului, adesea tratată sinonim cu ***securitatea națională***, caracterizează statele în principal în termeni de *putere - militară,*

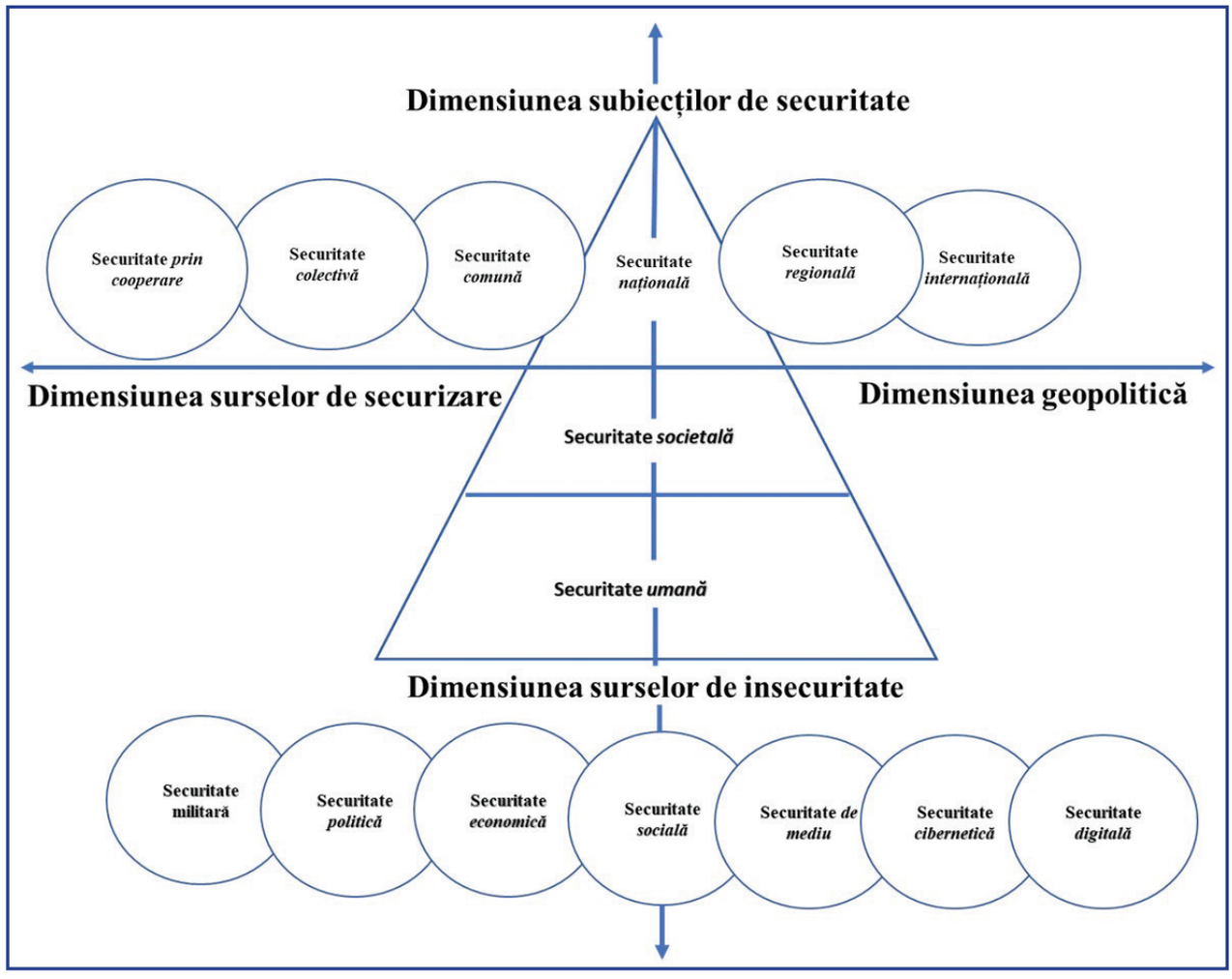


Figura nr. 3: Dimensiunile securității

politică, economică și informațională; cu referire la capacitatea lor de a-și utiliza această putere pentru atingerea *scopurilor* ori *intereselor,* prin *convingere*, *coerciție*, ori *război*, iar tocmai din această perspectivă, unii specialiști consideră că statele au scopuri limitate și interese pe termen lung de autoperpetuare, motiv pentru care războiul, ca formă de continuare a „politicii prin alte mijloace", este utilizat primordial prin raportare la analiza cost-beneficiu[22] pentru asigurarea securității proprii. Astfel, violența universală, anarhică și autoperpetuată nu este în interesul statului și, chiar dacă statele uzează de monopolul și dreptul de folosire a violenței, acesta nu este un scop în sine.

Pe cale de consecință, în mod tradițional, statul a avut un drept exclusiv de utilizare a violenței pe un teritoriu delimitat, iar securitatea sa depindea de amenințarea asupra acestui monopol de violență, fie prin invazie externă, fie prin rebeliune internă[23], motiv pentru care statul a depus și depune eforturi consistente pentru a-și păstra acest monopol de putere.

Începând cu perioada de final a Războiului Rece, literatura de specialitate a extins conceptul de securitate națională[24] și la alte domenii de securitate decât cel militar, iar, cel puțin în contextul geopolitic actual, securitatea național-statală nu mai include doar amenințări militare, reale sau percepute, ale altor actori similari, ci și amenințări non-militare – fenomene transfrontaliere precum imigrația, terorismul, evoluțiile de mediu, modificările tehnologice etc. Pe cale de consecință, scena de securitate începe să fie ocupată și de alte tipuri de actori decât cei tradiționali, respectiv actori non-statali, precum grupuri etnice, organizații neguvernamentale, naționale sau internaționale, organizații private de securitate, corporații multinaționale, agenții mass-media globale, companii digitale etc., care, încet și sigur, subminează rolul statului de principal actor și subiect de securitate, acesta fiind reclamat mult mai puțin să asigure integritatea teritorială a națiunii, ci mai mult să asigure nevoile cetățenilor săi – sociale, economice ori politice.

► **Securitatea societală**

„*Revoluția*" în domeniul studiilor de securitate și extinderea conceptului de securitate dincolo de domeniul statal a început în perioada marcată de șocul global al imploziei fostei Uniuni Sovietice, iar analiștii europeni au fost cei care au încercat să înțeleagă acest fenomen și, implicit, au extins în anii 1990 dimensiunea conceptului de securitate de la stat la societate și domeniile adiacente acesteia, Barry Buzan și Ole Waever fiind printre personalitățile marcante ale acestei „revoluții".

Inițial, în 1983, Barry Buzan a subliniat subdezvoltarea conceptului[25] cu privire la: *ambiguitatea definirii securității*; *suprapunerea conceptelor de putere și securitate*, în special definirea securității drept un derivat al puterii, în special a puterii militare; *incapacitatea de a explica revoltele religioase*; *subdezvoltarea studiilor de securitate* și, nu în ultimul rând, *ambiguitatea politică a securității*.

Pornind de la aceste critici, opt ani mai târziu, Buzan își revizuiește conceptele și extinde dimensiunea securității de la conotația sa statală la cea *societală*, considerând că societatea are un caracter distinct de cel al statului ori statelor în care este înglobată, sens pentru care introduce un nou tip de securitate, diferit de securitatea statală, respectiv ***securitatea societală***. Conceptul de securitate societală astfel dezvoltat pornește de la premisa că identitatea societății este principalul obiect de securizat, iar securitatea se divizează în cinci sectoare/domenii esențiale: *militar*, *politic*, *economic*, *societal* și de *mediu*[26], în cadrul cărora statul este actorul de referință pentru securitatea militară, politică, economică și de mediu, în timp ce societatea este actorul de referință pentru securitatea societală. Astfel, securitatea capătă o dublă conotație, a statului și a societății, primul fiind responsabil cu păstrarea suveranității, în timp ce cea din urmă are ca scop păstrarea propriei identități, iar supraviețuirea celor două entități, statul și societatea, este diferită și distinctă[27].

Securitatea societală face distincția dintre stat și societate inclusiv din perspectiva binomului securitate-insecuritate, în sensul în care nu este obligatoriu ca cele două să se potențeze reciproc. Starea de securitate a societății poate genera o insecuritate a statului și viceversa, mai ales în

cazul statelor multiculturale, cu o politică de omogenizare identitară forțată a societății, așa cum de exemplu s-a întâmplat în spațiul ex-sovietic. Chiar dacă URSS era putere militară mondială, domeniul economic și societal au condus la binemeritata sa prăbușire.

În fapt, granițele statale sunt fixe, în timp ce societatea nu este strict legată de spațiu geografic și granițe, iar din această perspectivă, securitatea societală se referă la identitatea indivizilor și la modul în care aceștia se identifică ca membri ai unei comunități[28]. Astfel, existența societății este dată de însăși apărarea identității proprii, din punct de vedere național, etnic și politic, identitatea națională fiind caracterizată prin afilierea la un teritoriu, atașament față de strămoși și identificarea ca actor în cadrul comunității internaționale care are dreptul de a înființa un stat național.

► ***Securitatea individuală/umană***

După cum îi este și denumirea, ***securitatea individuală/umană*** are rolul primordial de a fi un „*protector al individului ca exponent al speciei umane*”[29], iar acest tip de securitate a devenit primordial în concepția post-modernă a securității, atât din perspectiva securității statului, cât și din perspectiva securității internaționale, fiind lansate inclusiv programe internaționale centrate pe asigurarea securității individului și nu a statului.

Totuși, în cadrul securității individuale, relația individ-stat nu poate fi nici ignorată și nici abstractizată, fiind de acord cu Barry Buzan[30] că securitatea individuală este subordonată sistemului de organizare superior în care este înglobată, respectiv statul și sistemul de state internațional, iar relația stabilită de securitatea individuală cu aceste sisteme fiind bivalentă - individul este afectat - pozitiv sau negativ - de către securitatea statală și internațională, dar și securitatea statală și internațională este afectată de către individ, mai ales când aceste entități se află în opoziție.

Abordarea securității umane este centrată primordial pe două dimensiuni, o primă dimensiune aparținând programelor de securizare națională și internațională, axate pe asigurarea securității indivizilor, dar și a comunităților din care aceștia fac parte, din punctul de vedere al respectării drepturilor omului și al dezvoltării umane de către state, iar o a doua dimensiune fiind axată pe abordarea conceptuală a securității umane din perspectiva studiilor de securitate.

Inițial, *din perspectiva programelor de securizare*, la nivel internațional au fost stabilite o serie de ***drepturi umane***, în special civile și politice, în cadrul Convenției Europene a Drepturilor Omului, cunoscută și sub denumirea de Convenția pentru apărarea Drepturilor Omului și a Libertăților Fundamentale, elaborată de Consiliul Europei în 1950 și completată în 1952, 1963, 1983, 1984, 2000, 2002 și 2013[31].

Ulterior, *din perspectiva studiilor de securitate*, aproape concomitent cu abordarea școlii securității societale, la nivel internațional au fost inițiate dezbateri cu privire la ***securitatea umană***, drept o a treia perspectivă asupra securității, care provoacă domeniul securității prin permutarea accentului obiectului de studiu de la stat la individ. Potrivit acestei abordări, individul este obiectul securității, iar statul este doar mijlocul de obținere a acestei securități[32].

Un element important în problematica securității umane a fost prezentat în 1994 de United Nations Development Programme (UNDP) în cadrul *Human Development Report*. Din perspectiva UNDP, securitatea umană se bazează pe două componente esențiale: *siguranță* în fața amenințărilor cronice (foamete, îmbolnăvire și represiune) și *protecție* în fața amenințărilor zilnice, indiferent dacă acestea au loc în comunitate, la locul de muncă ori reședința. Pe baza acestor două componente, *securitatea umană* este divizată în 7 sub-componente[33]:

1. *securitatea individuală* - asigurarea siguranței personale împotriva violenței fizice și a criminalității;
2. *securitatea politică* - respectarea drepturilor politice individuale;
3. *securitatea comunității* - protejarea comunităților împotriva afectării valorilor tradiționale și violenței pe criterii de etnicitate;
4. *securitatea accesului la hrană* - garantarea accesului la hrană, inclusiv prin combaterea unui sistem defectuos de distribuție a alimentelor, fie prin combaterea lipsei puterii de cumpărare a hranei;

5. *securitatea de sănătate* - protecția vieții indivizilor împotriva bolilor;
6. *securitatea de mediu* - asigurarea protecției împotriva dezastrelor naturale și degradării mediului înconjurător;
7. *securitatea economică* - asigurarea venitului minim necesar, fie prin angajarea indivizilor în sistemul economic, fie prin protecția oferită de sistemele de asigurări sociale.

Chiar dacă perspectiva securității umane este destul de permisivă și cuprinzătoare, aceasta acoperă o gamă largă de amenințări contemporane la adresa securității. Secolul XXI găsește umanitatea confruntându-se cu o gamă diversificată de amenințări, în special neconvenționale, derivate din conflicte intra-statale, răspândirea bolilor, sărăcie ori contaminarea mediului, iar în acest cadru teoria securității umane nu infirmă rolul statului în asigurarea securității, însă evidențiază că însăși statele pot deveni amenințări la adresa securității indivizilor, mai ales când nu respectă drepturile omului.

De facto, dezbaterea asupra securității din perioada anilor 90 s-a concentrat pe regândirea dimensiunii militare a securității național-statale și lărgirea sensului și domeniilor conceptului, inclusiv la domeniile non-militare, sens pentru care considerăm că „maximul" extensiei securității a fost atins prin definirea *securității umane*. Dacă, inițial, acest efort de lărgire a sensului securității a pornit de la premisa că există domenii non-militare care se pot transforma în amenințări de securitate la adresa statului, dezbaterile s-au dezvoltat până la punctul în care au fost expuse argumente că anumite domenii non-militare se pot constitui ele însele în amenințări de securitate, atât la adresa statului, dar și la adresa individului ori societăților.

De exemplu, în 1995, J. Ann Tickner dezvoltă conceptul de „violență structurală", ca formă care include atât violența fizică, cât și violența indirectă asupra indivizilor, generată de structuri politice și economice inechitabile, care reduc speranța de viață prin lipsa accesului la nevoi materiale de bază[34], cu argumentul că *securitatea societății se obține prin eliminarea violenței structurale,* iar conceptul de securitate trebuie extins inclusiv la amenințările generate de diferențele ierarhice bazate pe sex, avere personală ori gradul de incluziune socială.

Corelarea conceptului de securitate umană cu cel de violență structurală și inechitate pare foarte ademenitor din perspectiva respectării drepturilor universale ale omului, însă principala dificultate practică din perspectiva teoriilor de securitate provine din găsirea unui consens în definirea securității din perspectiva inegalității, precum și din identificarea actorului chemat să securizeze securitatea, implicit să identifice inegalitatea și să pună în practică eliminarea acesteia și, per se, a violenței. Astfel, suntem de acord că o astfel de definiție a securității umane ridică probleme serioase în metodologia de identificare a acelor activități economice și politice injuste, căci „dacă toate activitățile economice injuste sunt inerent violente, atunci nicio societate inegală nu este sigură"[35], iar descrierea securității se poate realiza doar prin identificarea unui consens normativ și juridic pe care să se constituie un sistem politic și economic.

În concluzie, securitatea umană are două resorturi, de asigurare a libertății și dezvoltării individului, dar și de asigurare a siguranței sale în raport cu statul și lumea din care face parte, fiind bazată pe o serie de principii acceptate la nivel internațional[36]:

1. *Supremația drepturilor omului* - conflictele armate și intervențiile militare se realizează cu protejarea civililor. Derivat din acest principiu, scopul securității umane constă în evitarea uciderii indivizilor și fundamentarea juridică a intervenției militare.
2. *Legitimitatea autorității politice* - relațiile întreprinse la nivelul autorităților publice locale, statale, regionale ori internaționale se bazează pe stabilizarea situației și derularea unui proces politic pașnic și legitim, iar intervențiile externe asupra comunităților locale ori statale se realizează prin acorduri internaționale. Derivat din acest principiu, scopul

securității umane constă în siguranța indivizilor, legitimarea politică a autorităților și stabilirea unor zone umanitare în caz de criză ori conflict.

3. *Multilateralismul* - securitatea umană este globală, se bazează pe acțiunile comune ale statelor, care sunt recunoscute și asumate internațional în cadrul organizațiilor internaționale, precum ONU, NATO, OSCE, UE, FMI, etc. Derivat din acest principiu, scopul securității umane constă în crearea unor norme și reglementări internaționale de cooperare care să asigure respectarea unitară a regulilor, cu evitarea dublajelor și rivalităților.
4. *Parteneriatul și participarea asumată reciproc* - securitatea umană se fundamentează pe conlucrare și informarea directă a decidenților, mai ales în caz de conflict.
5. *Regionalizarea problemelor* - securitatea umană nu se poate asigura doar de către un stat ori grup de stat. Derivat din acest principiu, scopul securității umane constă în cooperarea regională ori globală, mai ales în cazul monitorizării zonelor cu potențial de conflict ori pentru asigurarea/stabilirea cooperării și dezvoltării economice.

● ***Dimensiunea securității în funcție de obiectul securității/sursele de insecuritate*** este clasificată în funcție de *domeniile din care provin principalele surse de insecuritate*, respectiv amenințările, riscurile și pericolele la adresa securității. Aceste surse de insecuritate pot afecta, în proporții variate, toți subiecții de securitate și, implicit, securitatea umană, societală sau statală, însă, primordial, literatura de specialitate se referă la sursele de insecuritate care afectează securitatea național-statală. Domeniile de referință ale securității cel mai des tratate sunt: *militar, politic, economic, social, de mediu,* și, nu în ultimul rând, domeniul *digital*, cu referire la *apărarea cibernetică* și *securitatea fluxurilor de date digitale.*

● ***Dimensiunea securității în funcție de modul de asigurare al surselor de securizare*** are relevanță, în principal, atunci când statul este subiectul de securitate și este clasificată în funcție de comportamentul și gradul de introvertism sau extravertism al statului în dezvoltarea capabilităților necesate pentru atingerea propriei securități naționale în cadrul relațiilor internaționale. Această dimensine este reprezentată de ***securitatea colectivă*** – coalizarea statelor împotriva unui agresor comun, realizată în cadrul unui organism care beneficiază de autoritate internațională, inclusiv printr-o renunțare parțială la suveranitate din partea statelor semnatare a unor acorduri internaționale specifice[37]; ***securitatea comună*** – atunci când preocupările de securitate ale unui grup de state sunt similare, securitatea națională a acestor state este considerată în comun; și ***securitatea prin cooperare*** – modalitate de asigurare a securității internaționale generată de diversificarea amenințărilor transfrontaliere, regionale și globale, la început de secol XXI.

● ***Dimensiunea securității în funcție de profunzimea geopolitică a mediului de securitate*** are relevanță atunci când subiecții și sursele de insecuritate sunt atât actori statali, cât și non-statali și este clasificată în funcție de *evoluția geopolitică a relațiilor internaționale stabilite de către actorii de securitate și implicarea acestora în combaterea surselor de insecuritate în cadrul mediului de securitate*, la nivel intern, regional și internațional. Acestă dimensine este reprezentată de ***securitatea regională*** – extinsă la aproape toate palierele din arealul securității; și ***securitatea internațională*** – analizată atât din perspectiva relațiilor stabilite între state, ca unici actori de securitate, pentru evitarea războiului și asigurarea păcii[38], cât și din perspectiva comportamentului statelor și tripla sa postură de actor, obiect de referință și sursă de insecuritate internațională pentru combaterea[39] unor noi tipuri de amenințări la adresa securității internaționale, transfrontaliere, care nu mai sunt însă generate exclusiv de către alte state, ci provin din noi domenii de securitate non-militară, precum ultranaționalismul anumitor grupuri etnice, crimă organizată, proastă guvernare a statelor, pandemii, terorism, sărăcie, management economic defectuos,

suprapopulare, state eșuate, migrație, poluare, distrugerea ecosistemului și biodiversității, asigurarea hranei etc.

În loc de concluzii

Securitatea este precum percepția umană. *Hic et nunc*. Aici și acum. Securitatea de ieri a unei entități de referință - individ, comunitate, stat - nu este aceeași cu securitatea de astăzi și va fi diferită de securitatea de mâine.

Tocmai din cauza complexității subiecților, obiectelor și actorilor de securitate, domeniul securității necesită o abordare multidisciplinară, interdisciplinară și transdisciplinară pentru reliefarea acelor componente care formează interacțiuni ce nu permit abordări unilaterale, cum ar fi tratarea securității militare în contextul securității economice a individului, societății și statului, așa cum securitatea statală nu poate fi abordată doar din perspectiva securității unei națiuni[40], căci astfel nu ar putea fi explicată securitatea regională ori internațională.

Concluzionând, subiectul securității este contestat, în principal, între individ, comunitate și stat, iar asigurarea securității variază între limita dintre securitatea individuală, cea societală și cea a statului, acestea funcționând pe principiul vaselor comunicante din domeniul științelor exacte.

Astfel, considerăm că perspectiva multi-subiect și multi-dimensiune de tratatre a securității este cea mai potrivită, căci doar o asemenea abordare complexă face distincția între individ, comunitate și stat, în sensul în care individul este unitatea de bază ireductibilă a societății, iar securitatea statului se bazează pe securitatea individului și a societății[41], chiar dacă pot exista situații, considerate a fi excepționale, când securitatea statului presupune insecuritatea anumitor cetățeni ori comunități.

Având în vedere aceste aspecte, chiar dacă domeniul securității este deja complex și indivizibil la modul real, putem concluziona că acesta poate beneficia de clarificări adiacente aduse de orice studiu multidisciplinar suplimentar asupra modului în care mecanismele de organizare și funcționare ale comportamentelor indivizilor, societăților și statelor se influențează reciproc și, separat ori cumulat, influențează securitatea în ansamblul său.

Bibliografie

1. *** Consiliul Europei, *Convenţia europeană a Drepturilor Omului*, accesibilă la https://www.echr.coe.int/documents/convention_ron.pdf, accesată în 20 februarie 2021;
2. *** United Nations Development Programme, *Human Development Report*, Oxford University Press, New York, 1994;
3. BOOTH, Ken, *Security and emancipation,* în *Review of International Studies,* nr. 17 (4), 1991;
4. BUȘE, Constantin; Hlihor, Constantin, *Security Between Classic and Modern*, în *Euro-Atlantic Studies***,** Issue No: 7, 2004;
5. BUZAN, Barry, *People, States and Fear. The National Security Problem in International Relations*, Wheatsheaf Books, Sussex, 1983;
6. BUZAN, Barry, Waever, Ole, Wilde, J., *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Londra, 1998;
7. BUZAN, Barry, *Regional Security Complex Theory in the Post-Cold War World*, în Söderbaum, Fredrik, Shaw, Timothy M., eds., *Theories of New Regionalism*, Palgrave Macmillan, New York, 2003;
8. BUZAN, Barry; Hansen, Lene, *The Evolution of International Security Studies*, Cambridge University Press, Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, 2009;
9. CHUTER, David, *From Threats to Tasks: Making and Implementing National Security Policy,* în *Journal of Security Sector Management,* vol. 5, no. 2 (October), 2007;
10. CULDA, Lucian, *Dependența securității omenirii de interpretarea dată globalizării,* în *Revista Geopolitica, nr. 1*, 2003;
11. DE SPIEGELEIRE, Stephan, *A Working Definition of Societal Security. Final Deliverable of Work Package 1.2 (Definition of Societal Security) of „European Security Trends and Threats In Society" (ETTIS), a European Union Seventh Framework Programme collaborative research project*, accesibil la https://www.

researchgate.net/publication/260061753_A_Working_Definition_of_Societal_Security_Final_Deliverable_of_Work_Package_12_Definition_of_Societal_Security_of_European_Security_Trends_and_Threats_In_Society_ETTIS_a_European_Union_Seventh_Framework, accesat în 23 februarie 2021;

12. FLURI, Phlilipp, Johnsson, Anders B., Born, Hans, *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices,* Geneva: Interparliamentary Union and Geneva Center for Democratic Control of Armed Forces, 2003;
13. GHERGHEȘ, Florin, *„Securitate" și sensul lui etimologic*, disponibil la „Securitate" și sensul lui etimologic | Cum se scrie? (cum-se-scrie.ro), accesat în 12.01.2021;
14. GUIEU, Jean-Michel, *Guaranteeing Peace through „Collective Security" in the 20th Century*, în Encyclopédie pour une histoire numérique de l'Europe, 22 iunie 2020, accesibil la https://ehne.fr/en/node/12329, accesat în 15 februarie 2021;
15. HEURLIN and Kristensen, Bertel, *International Security,* în Wiener, Jarrod, Schritte, Robert A, *International Relations, v*ol.II, EOLLS Publishers, Oxford, 2009;
16. HLIHOR, Constantin, *Politica de securitate în mediul internațional contemporan. Domeniul energetic*, Editura Institutului European, Iași, 2008;
17. HULA, Erich, *Fundamentals of Collective Security*, în *Social Research*, vol. 24, nr. 1, 1954, accesibil la www.jstor.org/stable/40969550, accesat în 15 februarie 2021;
18. KERR, Pauline, *Human Security*, în Alan Collins (coord), *Contemporary Security studies*, 3d. Edition, Oxford University Press, Oxford, 2013;
19. KISSINGER, Henry, *Mai are nevoie America de o politică externă*?, Editura Antet, f. a., București;
20. KOLODZIEJ, Edward A., Security and International Relations, Ed. Cambridge University Press, Cambridge, 2005;
21. LEPGOLD, Joseph, Nincic, Miroslav, *Beyond the Ivory Tower: International Relations Theory and the Issue of Policy Relevance*, Columbia University Press, New York, 2001;
22. MALIȚA, Mircea, *Între pace şi război,* Editura C.H. Beck, Bucureşti, 2007;
23. NYE, Joseph S. Jr și Lynn-Jones, Sean M., *International Security Studies: A Report of a Conference on the State of the Field,* în International Security, nr. 12, 1988;
24. SPIEGELEIRE, Stephan De, Jans, Karlijn, Sibbel, Mischa, Holynska, Khrystyna, Lassche, Deborah, *Implementing defence policy: a benchmark-"lite"*, în *Defense & Security Analysis*, nr. 35(1), 2019;
25. SACHS, Stephen E., *The Changing Definition of Security*, 2003, accesibil la http://www.stevesachs.com/papers/paper_security.html accesat în 23 februarie 2021;
26. SACHS, Stephen E., *The changing definition of Security*, 15 ianuarie 2004, accesibil la https://stephensachs.wordpress.com/2004/01/15/159/, accesat în 15 februarie 2021;
27. TUCHMAN Mathews, Jessica, *Redefining Security*, în *Foreign Affairs,* nr. 68(2), 1989;
28. ROBINSON, Paul, *Dicționar de securitate internațională*, Ed CA Publishing, 2010;
29. SIMONS, Hans, *Collective Security*, în *Social Research*, vol. 3, nr. 4, 1936, accesibil la www.jstor.org/stable/40981518, accesat în 15 februarie 2021;
30. VASILE-OZUNU, Mihail, *Securitate internațională și diplomație publică*, 2015, accesibil la http://europa2020.spiruharet.ro/wp-content/uploads/2015/04/Curs-SIDP.pdf, accesat în 15 februarie 2021;
31. WAEVER, Ole, Buzan, Barry, Kelstrup, Morten și Lemaitre, Pierre, *Identity, Migration and the New Security Agenda in Europe*, Londra, Pinter Publishers, 1993;
32. WILLIAMS, Paul D., eds., *Security studies. An introduction*, Routledge, New York, 2008.

[1] Căutarea a fost realizată în data de 15.02.2021, utilizând varianta în limba engleză a cuvântului *security*. Sursa: https://www.google.com/search?source=hp&ei=AUomYKapEOKkrgT5l4CADg&iflsig=AINFCbYAAAAAYCZYERliUv4L774b98rVXLzJXG89yFJ4&q=security&oq=security&gs_lcp=Cgdnd3Mtd2l6EAMyAggAMgIIADICCAAyAggAOggILhDHARCjAjoLCC4QxwEQowIQkwI6AgguOgsILhDHARCvARCTAlC3FVjiHGDKH2gAcAB4AIABtwKIAd8KkgEHMC42LjEuMZgBAKABAaoBB2d3cy13aXo&sclient=gws-wiz&ved=0ahUKEwjmref1g-TuAhViKosKHfkLAOAQ4dUDCAc&uact=5.

[2] Motorul de căutare *Google* este cel mai popular la ora actuală, cu o cotă de piață de 90%. Sursa: Top 8 Best Search Engines (of 2021) | RapidAPI.

[3] Florin Gherghes, *„Securitate" și sensul lui etimologic,* disponibil la „Securitate" și sensul lui etimologic| Cum se scrie? (cum-se-scrie.ro), accesat în 12.01.2021.

[4] Paul Robinson, *Dicționar de securitate internațională,* Ed CA Publishing, 2010, p. 6.

[5] Edward A. Kolodziej, *Security and International Relations,* Ed. Cambridge University Press, Cambridge, 2005, p. 2

[6] Barry Buzan, *People, States and Fear. The National Security Problem in International Relations,* Wheatsheaf Books, Sussex, 1983, p. 27.

[7] Constantin Hlihor, *Politica de securitate în mediul internațional contemporan. Domeniul energetic,* Editura Institutului European, Iași, 2008, p. 13.

[8] Joseph Lepgold, Miroslav Nincic, *Beyond the Ivory Tower: International Relations Theory and the Issue of Policy Relevance,* Columbia University Press, New York, 2001, pp. 3-4; apud Dacian Duna, *Politica securității europene la începutul secolului XXI. Uniunea Europeană şi noua geostrategie a Estului,* teză de doctorat, conducător ştiinţific prof. univ. dr. Vasile Puşcaş, Universitatea Babeş-Bolyai, Cluj-Napoca, 2007, p. 50, nota 102.

[9] Constantin Hlihor, *op.cit.,* p. 14.

[10] Mircea Maliţa, *Între pace şi război,* Editura C.H. Beck, Bucureşti, 2007, passim.

[11] Henry Kissinger, *Mai are nevoie America de o politică externă?,* Editura Antet, f. a., Bucureşti, p. 14.

[12] Constantin Hlihor, *op.cit.,* p. 16.

[13] Stephan De Spiegeleire, *A Working Definition of Societal Security. Final Deliverable of Work Package 1.2 (Definition of Societal Security) of „European Security Trends and Threats In Society" (ETTIS), a European Union Seventh Framework Programme,* accesibil la https://www.researchgate.net/publication/260061753_A_Working_Definition_of_Societal_Security_Final_Deliverable_of_Work_Package_12_Definition_of_Societal_Security_of_European_Security_Trends_and_Threats_In_Society_ETTIS_a_European_Union_Seventh_Framework, accesat în 23 februarie 2021.

[14] Constantin Hlihor, *op.cit.,* p. 16.

[15] A se vedea pe larg, Barry Buzan, Lene Hansen, *The Evolution of International Security Studies,* Cambridge University Press, Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, 2009; Constantin Buşe, Constantin Hlihor, Security Between Classic and Modern, în *Euro-Atlantic Studies,* Issue No: 7, 2004, pp. 117-122; Paul D. Williams, eds., *Security Studies. An introduction,* Routledge, New York, 2008.

[16] A se vedea David Chuter, *From Threats to Tasks: Making and Implementing National Security Policy,* in *Journal of Security Sector Management,* vol. 5, no. 2 (October), 2007, pp. 1–19; Phlilipp Fluri, Anders B. Johnsson, Hans Born, Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices, Geneva: Interparliamentary Union and Geneva Center for Democratic Control of Armed Forces, 2003.

[17] Barry Buzan, *Regional Security Complex Theory in the Post-Cold War World,* in Fredrik Söderbaum Timothy M. Shaw, eds., Theories of New Regionalism, Palgrave Macmillan, New York, 2003, pp 140-159.

[18] Stephan De Spiegeleire, Karlijn Jans, Mischa Sibbel, Khrystyna Holynska & Deborah Lassche, *Implementing defence policy: a benchmark-"lite",* în *Defense & Security Analysis,* nr. 35(1), 2019, pp.59-81.

[19] Constantin Buşe, Constantin Hlihor, Security Paradigm Between Classic and Modern, în *Euro-Atlantic Studies,* nr. 7, Editura Universității București, București, 2004, pp. 117-126.

[20] Jessica Tuchman Mathews, Redefining Security, în *Foreign Affairs,* nr. 68(2), 1989, p. 166.

[21] Richard Ullman, *op.cit.,* p. 53.

[22] Alan Collins (coord.), *Contemporary Security studies,* 3d. Edition, Oxford University Press, Oxford, 2013, pp. 37-38

[23] Stephen E. Sachs, *The Changing Definition of Security,* 2003, accesibil la http://www.stevesachs.com/papers/paper_security.html accesat în 23 februarie 2021.

[24] Ken Booth, Security and emancipation, în *Review of International studies,* nr. 17(4), 1991, pp. 313-326.

[25] Barry Buzan, *op.cit.,* 1983, p. 16.

[26] Barry Buzan, *op.cit.,* 1991, p. 19.

[27] Ole Waever, Barry Buzan, Morten Kelstrup și Pierre Lemaitre, *Identity, Migration and the New Security Agenda in Europe,* Londra: Editura Pinter Publishers, 1993, pp. 15-59.

[28] Buzan, B., Wæver O., Wilde, J., *Security: A New Framework for Analysis,* Lynne Rienner Publishers, Londra, 1998, pp. 119-121.

[29] Mihail Vasile-Ozunu, *Securitate internațională și diplomație publică,* 2015, p.9, accesibil la http://europa2020.spiruharet.ro/wp-content/uploads/2015/04/Curs-SIDP.pdf, accesat în 15 februarie 2021.

[30] Barry Buzan, *op.cit.,* 1991, p. 65.

[31]Consiliul Europei, *Convenţia europeană a Drepturilor Omului,* accesibilă la https://www.echr.coe.int/documents/convention_ron.pdf, accesată în 20 februarie 2021.
[32]Pauline Kerr, *Human Security,* în Alan Collins (coord.), op.cit., pp. 121–135.
[33]United Nations Development Programme, *Human Development Report,* Oxford University Press, New York, 1994.
[34]J.Ann Tickner, *op.cit.,* pp. 187-193.
[35]Stephen E. Sachs, *The changing definition of Security,* 15 ianuarie 2004, accesibil la https://stephensachs.wordpress.com/2004/01/15/159/, accesat în 15 februarie 2021.
[36]Mary Kaldor, *op.cit.,* pp. 217-223.
[37]Jean-Michel Guieu, *Guaranteeing Peace through „Collective Security" in the 20th Century,* în Encyclopédie pour une histoire numérique de l'Europe, 22 iunie 2020, accesibil la https://ehne.fr/en/node/12329, accesat în 15 februarie 2021. Vezi și Hans Simons, *Collective Security,* în Social Research, vol. 3, nr. 4, 1936, pp. 383–410, accesibil la www.jstor.org/stable/40981518, accesat în 15 februarie 2021; și Erich Hula, |*Fundamentals of Collective Security,* în Social Research, vol. 24, nr. 1, 1954, pp. 1-36, accesibil la www.jstor.org/stable/40969550, accesat în 15 februarie 2021.
[38]Joseph S. Jr Nye și Sean M. Lynn-Jones, „International Security Studies: A Report of a Conference on the State of the Field", în *International Security,* nr. 12, 1988, pp. 5-27.
[39]Bertel Heurlin and Kristensen, *International Security,* în Jarrod Wiener, Robert A . Schritte, International Relations, vol.II, EOLLS Publishers, Oxford, 2009, p. 173.
[40]Lucian Culda, Dependența securității omenirii de interpretarea dată globalizării, în *Revista Geopolitica,* nr. 1, 2003, p. 108.
[41]Barry Buzan, *op.cit.,* 1991, p. 46.

DIMENSIUNI MODERNE ALE CONFRUNTĂRILOR MILITARE

*Marian ȘTEFAN**

Abstract

In a future dynamic operational environment, characterized by the external influences of various public and private entities involved in scientific and technological development, research and development of advanced technologies, and due to politico-military and economic developments, modern armies will have to plan and conduct multi-field military operations. In order to adapt quickly and restore order in this already chaotically operational environment, military bodies need to turn potential challenges into opportunities through foresight, risk-taking and initiative. Forecasting through technological development forecasting, early experimentation with new technologies, scanning of the predictable horizon and analysis of evolutionary trends, will allow a modern army to overcome cost and innovation issues, project forces for rapid integration of new technology and develop new infrastructure. enabling forces to carry out missions in multi-field operations. Initiatives to explore relatively new military areas, such as cyberspace, as well as creating a connection between the military, industry and academia will provide insights into how emerging technologies can be integrated into military operations. In this way, the combined effort of the three areas of interest brings further knowledge of the risk that the military must manage in order to ensure success in the current operational environment.

***Key words**: operational environment, challenges, technology, hybrid threats.*

Caracteristici ale mediului operațional

În prezent, mediul operațional se confruntă cu o competiție globală acerbă pentru dezvoltarea inteligenței artificiale (AI) și a capacităților robotice. Actorii care câștigă cursa pentru supremație în aceste domenii au șansa de a obține avansul strategic față de adversarii lor. Complexitatea, democratizarea și avansarea rapidă a tehnologiei aduc o schimbare de paradigmă cu privire la abordarea tradițională a confruntărilor militare, în sensul în care mediul informațional și automatizarea proceselor de decizie și acțiune oferă spațiul de luptă preferat pentru unii actori statali și non-statali deoarece asigură atât anonimatul, cât și beneficiul neasumării directe a acțiunilor întreprinse. Acest mediu operațional care se schimbă constant între competiție și conflict, relevă o fereastră de oportunitate de scurtă durată care neexploatată la momentul oportun va permite potențialilor adversari integrarea proceselor tehnologice în moduri de operare a instrumentului militar în cadrul unor conflicte în care nu mai contează dotările numerice, ci doar instrumentarea elementelor surpriză, cele pentru care adversarul nu deține capabilități de reacție și răspuns adecvat.

În ciuda faptului că unele doctrine sau proiecte doctrinare descriu conceptual operațiunile multidomeniu, în realitate acestea reprezintă elemente ale strategiei militare[1]. Însă în condițiile actuale, în care amenințările capătă nuanțe din ce în ce mai complexe, strategia trebuie definită ca un proces complex de luare a deciziilor, care conectează scopurile (obiectivele) cu modalitățile și mijloacele de realizare a acestora. Strategia presupune planificare și implementare a unor

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

acțiuni asumate, calculate și conduse astfel încât să asigure atingerea scopurilor pentru care a fost proiectată. În prezent, orice strategie are nevoie de o evaluare continuă astfel încât să poată fi adaptată transformărilor variabilelor mediului operațional și în funcție de interesele naționale, politica, amenințările, capabilitățile și evoluția tehnologică. Ca urmare, strategiile au nevoie de modificări și reevaluări continue pentru a construi instrumentele necesare protejării unor valori și evitării surprinderii prin exploatarea vulnerabilităților.

Conflictele specifice secolului XXI relevă dimensiunile multiple în care se desfășoară acțiunile militare ce accesează toate domeniile mediului operațional – terestru, maritim, aerian, spațial, electromagnetic și cibernetic – prin orchestrarea eforturilor de angajare a componentelor militare naționale și aliate în scopul realizării unor efecte sinergice. Războiul modern necesită campanii comune, coordonate pe mai multe domenii și care presupun simultaneitate și susținere reciprocă. În timp ce pământul, marea, aerul, spațiul și mediul cibernetic au caracteristici unice și, uneori, fiecare pare a fi independent unul de celălalt, în realitate toate operațiunile și campaniile se bazează pe un aspect al sinergiei între domenii.

Studiul amenințărilor care exploatează vulnerabilitățile identificate în mediul operațional este important, mai ales pentru că, în plan internațional, se discută primordial despre conceptul de „război hibrid". Motivele probabile ale acestei apetențe pentru studiul conceptului de război hibrid ar putea fi globalizarea, care determină interconectarea tot mai profundă a statelor, precum și evoluția tehnologiei, care a provocat necesitatea alianțelor politico-militare ca răspuns la costul enorm pe care conflictul armat îl cere. De asemenea, elementul național al apărării determină o fragmentare a variabilelor mediului operațional, generată de specificitatea fiecărui stat în utilizarea instrumentelor de putere.

Evoluția relațiilor internaționale, turbulențele și accelerarea integrării și fragmentării ordinii mondiale au condus la forme și tipuri neașteptate și neconvenționale de amenințări la adresa securității naționale și internaționale. Unele dintre acestea provin din dezvoltarea tehnologică, altele din impactul tehnologiei asupra societății noastre, o parte din creșterea populismului și relevanței identităților și, ultimele, dar nu cele din urmă, de la propriile noastre minți și percepții care sunt influențate în mod dramatic de preconcepțiile noastre și de înclinația de a căuta căile cele mai ușoare în gândirea rațională. Toate acestea au un impact enorm asupra evaluării amenințărilor, asupra securității și apărării naționale. De aceea, acești factori trebuie explorați, cunoscuți și abordați într-o manieră științifică și comprehensivă pentru a preveni surpriza strategică, precum și apariția noilor tipuri de conflicte[2].

Această modalitate de abordare a securității într-o formă largă s-a extins, ulterior, cu un nou tip de componente, numite inițial *„amenințări ne-tradiționale"*, mai apoi *„amenințări de securitate emergente"*, pentru că NATO a privit aceste noi amenințări drept foarte importante, pătrunzând, astfel, cu mult curaj într-un teritoriu nou și incert. Această arie de amenințări include terorismul, proliferarea armelor de distrugere în masă, atacurile cibernetice, întreruperile de aprovizionare cu energie și produse energetice și chiar s-a extins la schimbările climatice și la migrație[3].

Identificarea elementelor comune, studierea și cunoașterea diferitelor teorii privind mediul operațional și natura conflictelor de tip hibrid, bazate pe exploatarea vulnerabilităților identificate în sistemele de securitate și apărare a unor state țintă, este utilă din cel puțin trei perspective. În primul rând, facilitează răspunsul la întrebarea de bază a unui decident politico-militar: *„De ce ne confruntăm cu această situație?"* În al doilea rând, promovează o analiză rațională a instrumentelor de putere de care un stat dispune și modul în care acestea pot fi întrebuințate pentru a face față unui nou tip de conflict sau pentru a răspunde unei noi amenințări. În al treilea rând, facilitează comunicarea științifică, prin stabilirea unui teren comun între specialiști cu viziuni diferite.

Perspective ale evoluției conflictelor militare

Evoluția conflictelor contemporane reflectă schimbări de paradigmă în abordarea amenințărilor și instrumentelor utilizate pentru pregătirea operațiilor militare clasice, care nu sunt necesare în obținerea supremației întotdeauna. În acest fel, am constatat că direcția principală de planificare este orientată către strategii de întrebuințare a elementelor de cunoaștere și control a situației prin dezinformare, influențare, punere în dependență economică, migrație controlată, controlul infrastructurilor critice și operații cibernetice anonime.

Statele membre UE şi NATO, regăsindu-se în același mediu de securitate complex, au stabilit o modalitate de cooperare comună, care a vizat într-o primă etapă amenințările hibride. În acest fel, UE şi NATO au stabilit să lupte împreună împotriva amenințărilor hibride[4]. Această strategie comună prevede faptul că primul responsabil şi respondent în cazul unui atac de natură hibridă este statul implicat, iar asistența UE şi NATO va fi oferită imediat pentru a sprijini țara vizată de atac și pentru contracararea amenințării în cauză. Această cooperare a fost concretizată atunci când o serie de state aliate din NATO şi membri ai Uniunii Europene au decis să stabilească formal, la Helsinki, pe 11 aprilie 2017, Centrul European de Excelență pentru Combaterea Amenințărilor Hibride[5].

În ciuda acestor dezvoltări, viteza de evoluție a societății noastre, a relațiilor internaționale şi securității a introdus noi categorii de amenințări neconvenționale. De această dată, amenințările externe sunt dublate de vulnerabilități interne transformate în amenințări. Acest lucru se întâmplă deoarece, în realitate, ele aparțin tipologiei de amenințări hibride[6] care au surse externe. Este cazul tuturor caracteristicilor democrației liberale, valorilor şi principiilor pe care le respectăm pentru că reprezintă modul nostru de viață, dar care sunt considerate vulnerabilități de către anumiți actori (în mod special de către Federația Rusă)[7], care au construit instrumente pentru a profita de aceste caracteristici ale societății liberal-democratice, privite ca vulnerabilități.

Aceste amenințări vin din specularea valorilor şi principiilor sistemului nostru democratic[8], profitând de lipsurile și neclaritățile identificate la nivelul acestor sisteme, provenind de la evoluția tehnologiei şi impactul ei asupra societății[9].

Platformele de socializare şi războiul informațional, inteligența artificială și utilizarea programelor de autoînvățare în mediul militar redefinesc mediul de securitate al viitorului și mediul de operare. Cele mai profunde schimbări provin din zona tehnologiilor avansate cu libertate de acțiune și posibilitate de decizie.

Mediul operațional la nivel global este caracterizat de existența a două fenomene principale: în primul rând, se manifestă din ce în ce mai acut fenomenul vidului de putere generat de state cu sisteme de conducere și guvernare fragile sau eșuate[10], care, prin vulnerabilitățile create, oferă oportunități pentru ascensiunea unor actori non-statali, care, la rândul lor, prin acțiuni asimetrice sau de natură hibridă, generează crize de securitate la nivel statal sau chiar regional. Creșterea numărului actorilor non-statali bine organizați, înarmați și finanțați creează la nivelul statelor slab guvernate amenințări la adresa securității și a suveranității. Aceste interferări ale actorilor non-statali în actul de guvernare se manifestă în două moduri: pe de o parte, aceștia se pot poziționa ca o posibilă alternativă la forma de guvernare tradițională bazată pe statul de drept și structuri statale recunoscute, dar eșuate din punct de vedere al măsurilor și politicilor promovate, iar pe de altă parte, aceștia pot contesta prin natura existenței și prezenței lor monopolul structurilor de forță ale statului gazdă[11].

Al doilea fenomen important care se manifestă în actualul mediu operațional este reprezentat de concurența strategică (lupta pentru diferite resurse, piețe, zone de influență, interese geopolitice și geoeconomice) între actori statali și non-statali cu interese contradictorii.

Cele două fenomene pot părea contradictorii la prima vedere, însă analizând detaliile și în special elementele comune se constată că, de fapt, există o legătură: în situațiile când instabilitatea duce la defalcarea elementelor de guvernare existente ale unui stat se creează breșe la nivelul structurilor de

comandă și conducere, așa-zise „porți deschise”, pe care puterile regionale sau globale, entitățile non-statale regionale sau transnaționale le pot exploata pentru a-și îmbunătăți pozițiile sau pentru a-și consolida influența[12].

Fragmentarea statelor a reprezentat principala preocupare în materie de securitate internațională în deceniile de după încheierea Războiului Rece. Spre deosebire de mediul de securitate internațional tensionat existent în perioada Războiului Rece[13], dar stabil din punct de vedere al politicilor externe ale celor două blocuri de putere, conflictele anilor 1990 și 2000 au fost percepute ca fiind „asimetrice”, cel puțin prin prisma instrumentării elementelor de tip neconvențional. Astfel, state cu o dotare tehnică militară inferioară și învechită, dar inovatoare și adaptate contextului mediului operațional, au devenit adversari redutabili pentru armatele unor state care cheltuiesc bugete însemnate pentru industria de apărare doar pentru simplul fapt că au cunoscut vulnerabilitățile adversarilor și au reușit să le exploateze cu succes. Deși acest fenomen persistă, asistăm acum la manifestarea conflictelor de tip hibrid, caracterizate de situații în care sunt utilizate atât amenințările clasice, cât și cele asimetrice, într-o manieră conjugată. Combinațiile inovatoare de utilizare a tehnologiilor convenționale și produsele noilor progrese tehnologice creează un tip de conflict dinamic și imprevizibil. „Câmpul de luptă” modern estompează distincția între zone de război și zone de pace, precum și între combatanții legitimi, adversarii neatribuiți și civili.

Tendințe și transformări ale mediului de securitate internațional

Analiștii economici și politici, prezenți la lucrările Forumului economic mondial de la Geneva, din anul 2016, încercând să previzioneze mediul de securitate pe termen scurt și mediu, au identificat șapte forțe cheie ale schimbării peisajului securității internaționale[14]. Aceste forțe sunt foarte interconectate, fiecare interacționând între ele și afectându-le pe celelalte. Cele șapte forțe cheie care conduc la schimbări ale mediului de securitate internațional sunt:

1. Inovația tehnologică: tehnologiile emergente creează provocări, dar și oportunități de rezolvare a acestora.
2. Resursele, managementul climei și securitatea: tensiunile între state cresc în intensitate din cauza concurenței în ceea ce privește accesul la resursele de bază (energie, apă și alimente).
3. Guvernarea eficientă: corupția și lipsa de transparență sau lipsa politicilor eficiente de stat de drept limitează progresul dezvoltării și destabilizează societățile.
4. Concurența geo-strategică: schimbarea balanței puterii economice și politice și slăbirea încrederii reciproce între superputerile statale conduc la concurența pentru sferele de influență.
5. Schimbările demografice: multe state se confruntă cu probleme demografice și cu fluxurile masive de migranți.
6. Coeziunea și încredere socială: alimentate de inegalitate, sentimente de excludere socială, neîncredere și marginalizare, părți însemnate ale societății amenință stabilitatea socială a statelor.
7. Amenințările hibride și asimetrice: într-o lume interconectată din punct de vedere al sistemelor de comunicare și al accesului la sursele de informare apar amenințări mai complexe ce presupun apariția adversarilor neatribuiți din punct de vedere statal și a „lebedelor negre”[15].

Dintre cele șapte, două justifică o atenție mai detaliată: (1) inovația tehnologică și (2) resursele naturale și managementul climei. Aceste două forțe cheie nu sunt doar importante în mod individual, ci devin și amplificatori ai celorlalte.

Puterea economică a unor state, schimbările și modificările demografice și avantajele tehnologiilor avansate reprezintă elemente care pot modela balanța puterii la nivel global. Rezultatul este un peisaj geopolitic în care statele exploatează din ce în ce mai mult oportunitățile și transformă provocările în căi prin care urmăresc utilizarea instrumentelor de putere pentru a atinge deziderate strategice.

Mediul operațional a fost întotdeauna gazda confruntărilor dintre state, națiuni și grupuri care au utilizat toate instrumentele puterii de stat pentru obținerea supremației. Pe măsură ce lumea se schimbă, la fel și capacitatea instrumentelor de putere ale statelor se adaptează pentru a face față acestor schimbări. Aceste schimbări reflectă modul în care instrumentele de putere statală sunt operate în funcție de natura conflictelor și de forma acestora. Conflictele de tip hibrid nu sunt o noutate pentru nici o armată din lume, însă evoluția societății, globalizarea, digitalizarea și hiperconectivitatea schimbă modul în care statele combină eficient instrumentele de putere DIMEFIL[16] de care dispun pentru a obține avantaje sau pentru a descuraja aceste amenințări hibride.

„DIME" (diplomatic, informațional, militar și economic) este un termen militar reintrodus în limbajul de specialitate pentru a le reaminti conducătorilor și factorilor de decizie să ia în considerare toate elementele puterii naționale, fără a se limita doar la puterea militară. Pentru a face față amenințărilor de tip hibrid au fost adăugate acestui concept DIME componentele ce trebuie instrumentate la nivelul capabilităților de răspuns adaptat: FIL – resurse din sfera financiară, de intelligence și de aplicare a legii pentru a fi aplicate la medii operaționale"[17].

Analizând acțiunile Rusiei și ale Grupării Statul Islamic (ISIS) pentru a evalua eficacitatea utilizării instrumentelor de putere DIMEFIL față de actorii statali și non-statali implicați în conflicte de tip hibrid, experții militari din cadrul Allied Command Transformation (ACT/NATO) au identificat următoarele tendințe[18]:

- tendința 1: în timp ce toate instrumentele DIMEFIL ale puterii naționale continuă să fie mijloace de influență viabile în cazul agresiunilor de tip hibrid față de statele naționale tradiționale, importanța instrumentelor non-militare a crescut în mod disproporționat, domeniul „Informațional" cunoscând cea mai mare importanță;
- tendința 2: în același timp, în timp ce instrumentele DIMEFIL continuă să fie viabile atunci când adversarul este o entitate statală, utilitatea lor în forma tradițională este semnificativ diminuată atunci când adversarul este un actor non-statal;
- tendința 3: în timp ce țările occidentale, alături de aliații și partenerii acestora, posedă capabilități logistice și au capacitățile necesare pentru a face față amenințărilor hibride, au existat situații în care aceștia au fost depășiți de situațiile inedite din cauza sincronizării inadecvate a instrumentelor DIMEFIL.

Schimbările de paradigmă privind modul de încadrare și definire a conflictelor au intervenit începând cu evenimentele din 11 septembrie 2001, moment din care sunt utilizați noi termeni pentru a descrie tipurile de confruntări militare în care SUA și aliații săi au devenit participanți. Unii dintre acești termeni provin din linia istorică de gândire militară și își au rădăcina în doctrinele militare ale diferitelor state, dar chiar și acele definiții consacrate pot să nu reflecte sensul dorit în procesul de planificare și decizie la nivel politic.

Conform teoriei militare, ținând cont de tipologia acțiunilor militare, conceptul de război hibrid este poziționat în spectrul conflictelor din generația a V-a: război puternic asimetric, nerestricționat, opus războiului limitat. Este un război de tip non-contact dus cu muniții și arme de precizie, UAV-uri, tehnici cibernetice ofensive și defensive, operații informaționale, utilizate pentru depășirea tehnicilor războiului de generația a IV-a, influențare psihologică și propagandă pe scară largă, tehnici de comunicare strategică ce fac apel la tehnologia informațională de ultimă generație, prevederi ale dreptului internațional care „sunt folosite în scopul susținerii legitimității acțiunilor proprii și ilegitimității acțiunilor adversarului"[19].

Acțiunile de tip hibrid au devenit o caracteristică frecventă a mediului de securitate contemporan și urmăresc exploatarea variabilelor mediului operațional identificate în plan politic, militar, economic, social, informațional și infrastructură. Din această perspectivă, construirea unei societăți reziliente, care să răspundă în mod

dinamic amenințărilor hibride, trebuie să fie văzută ca o oportunitate pentru a întrebuința în mod coerent și judicios instrumentele de putere ale statului în scopul unui răspuns adaptat la natura atacului.

Începutul acestui secol este caracterizat de o lume în care crizele şi conflictele sunt reale şi prezente în forme și dimensiuni diferite de tot ceea ce lumea a experimentat până în prezent. Asistăm la o polarizare ideologică şi religioasă, conflicte regionale în care amenințările Războiului Rece 2.0[20] devin din ce în ce mai evidente. Într-un astfel de mediu internaţional este evident faptul că schimbarea de paradigmă s-a produs, securitatea strategică centrată pe stat devenind primordială în raport cu securitatea umană (securitatea împotriva subdezvoltării, sărăciei etc.), ce a rămas în planul secund[21].

Realitatea geopolitică internațională schimbă modul în care trebuie să tratăm vechiul concept de război, aşa cum l-a definit Clausewitz (continuarea politicii cu alte mijloace) și să conștientizăm că mai multe tipuri de război (asimetric, cibernetic, informaţional, de agresiune etc.) pot fi folosite simultan de adversari flexibili şi sofisticaţi. În plus, ultimele două mari crize mondiale, cea economică și cea sanitară, au generat o presiune severă la adresa economiei globale, generând un sentiment sporit de vulnerabilitate economică, dar şi oportunităţi geopolitice, alimentând concurența pentru resurse și, uneori, chiar beligeranţa.

În acest fel, sintagma „război hibrid" a devenit alegerea potrivită pentru a descrie o strategie care combină războaiele convenţionale, războiul neregulat şi războiul cibernetic cu alte metode de influenţare (ştirile false, diplomaţia, ingerințele economice, intervenţiile electorale etc.).

Încercările creative ale strategilor militari moderni de a da o formă nouă diferitelor tipuri de conflicte și confruntări militare nu se regăsesc în paradigmele consacrate. Noile abordări conțin definiții care se suprapun sau au înțeles similar, însă acestea încearcă să ofere cadrul general și particular de încadrare a noilor tipuri de războaie și, de aceea, regăsim în noile doctrine militare următorii termeni: război asimetric, conflict neregulat, război compus, război combinat, război de distragere, război de a cincea generație, conflict de intensitate mică, război limitat, război fără restricții, război special, război neconvențional; de asemenea, identificăm și o serie de dimensiuni în care termenul „război" și rolul forței este departe de a fi evident: războiul cibernetic, războiul economic, războiul politic, războiul cultural și altele asemenea. Așadar, schimbarea de paradigmă derivă din încercările de a contextualiza situații noi, stări de fapt incerte, probleme ce nu au o motivație anume sau lucruri greu de înțeles în fața cărora, de regulă, încercăm să introducem o construcție negativă. „Folosim cuvinte *nu* pentru a descrie lucruri care credem profund că nu ar trebui să fie: actori non-statali, state eșuate, neregulate/neconvenționale/fără restricții/conflict asimetric"[22].

Introducerea în limbajul militar modern a noțiunii de război hibrid a condus la o actualizare a definițiilor existente, privite în contextul amenințărilor contemporane[23]. Unii strategi militari și analiști pe probleme de geopolitică, precum Colin Gray[24], sunt de părere că ar trebui să „uităm adjectivele consacrate care descriu aceste forme de război: războiul neregulat; război de gherilă; război nuclear; strategia navală; strategia contrainsurgentă. Numeroasele tipuri de război și instrumente de strategie nu au nici o importanță pentru natura războiului și a strategiei în sine. O teorie generală a războiului și a strategiei, precum cea oferită de Clausewitz și în diferite moduri, de asemenea, de Sun Tzu și Thucydides, este o teorie cu aplicabilitate universală"[25]. Gray afirmă că armata Statelor Unite este prea convențională pentru a se adapta la amenințările neregulate, amenințări dificil de explicat fără unele dintre acele „adjective care le descriu"[26]. O problemă apare atunci când adjectivul în sine este sursa de confuzie. În esență, războiul de tip „hibrid" presupune o combinație de cel puțin două amenințări întrebuințate în scopul producerii efectului dorit. Ambiguitatea acestui tip de conflict derivă din elementele care sunt instrumentate în modul cumulativ și de intensitatea cu care acestea se manifestă.

Din punct de vedere al abordării tradiționale, doctrinele militare ale armatei SUA extind lista

elementelor componente ale amenințărilor hibride pentru a include „două sau mai multe dintre următoarele: forțe militare, forțe paramilitare ale statului național (cum ar fi forțele de securitate interne, poliția sau polițiștii de frontieră), organizații insurgente (entități care se bazează în principal pe acțiuni subversive și violente pentru schimbarea stării de fapt), unități de gherilă (forțe indigene neregulate care operează pe teritoriul ocupat) și organizații criminale (cum ar fi bande, carteluri de droguri sau hackeri)”, punând un puternic accent pe utilizarea operațiilor informaționale și cibernetice[27]. Acest tablou asupra războiului hibrid, incluzând combinații de forțe convenționale și neregulate, oferă o percepție limitată doar la instrumentele militare de război, împreună cu elementele din sfera criminalității organizate și atacuri cibernetice. Pentru un studiu istoric al campaniilor militare, o astfel de abordare poate fi utilă, însă pentru a explica combinația instrumentelor de putere militare și non-militare întrebuințate pentru atingerea obiectivelor nu sunt de ajuns[28]. Această abordare pragmatică tradițională nu oferă cunoaștere și înțelegere asupra naturii actorilor generatori de amenințări și nici asupra circumstanțelor legate de contextul social sau economic al mediului operațional.

O altă școală de gândire a strategiilor militare oferă numeroase definiții pentru conceptul de război hibrid. Majoritatea acestor definiții care tratează caracterul hibrid al noului tip de conflict înglobează referințe cu privire la angajarea forțelor convenționale și neregulate, interpretează amenințările teroriste din punct de vedere operațional și includ o serie de abordări cu privire la utilizarea noilor tehnologii și instrumentarea tuturor resurselor pentru a contracara superioritatea militară a unui adversar[29]. O serie de analiști militari definesc „hibridul” ca reprezentând un mixt al mijloacelor și tehnicilor de luptă utilizate simultan cu războiul informațional pentru a câștiga influență asupra „populațiilor din zona de conflict și la nivelul comunității internaționale”[30].

Cele mai revoluționare tendințe de gândire strategică militară încearcă să înlocuiască războiul hibrid cu a altă sintagmă, „război fără restricții”. În acest sens, abordarea chineză a strategilor militari ai Armatei de Eliberare a Poporului, Qiao Liang și Wang Xiangsui, susține faptul că „noile principii ale războiului nu mai folosesc forța armată pentru a obliga un inamic să se supună voinței cuiva, așa cum trata Clausewitz problematica războiului, ci mai degrabă folosesc toate mijloacele, inclusiv forța militară și non-militară, letală și neletală, pentru a obliga un inamic să accepte interesele cuiva”[31]. Această teorie implică o abordare strategică pe termen lung elaborată în scopul atingerii obiectivelor și presupune faptul că, în cazul unui război hibrid, nivelul dotării unei armate cu tehnică de luptă modernă nu garantează succesul sau victoria, deoarece prin multitudinea de alte instrumente non-militare folosite eficacitatea armamentului clasic devine relativă din punct de vedere al efectului letal[32]. Domenii comune ale societății, precum economia, politica sau diplomația, cultura, mediul, fenomenul migrației „vor face ca oamenii obișnuiți și militarii să fie deopotrivă foarte uimiți de faptul că lucrurile obișnuite care le sunt aproape pot deveni și arme cu care să se angajeze în război”[33]. În rezumarea teoriei lui Liang și Xiangsui, un analist militar american, Nathan Freier, descrie în mod adecvat gama de război hibrid, enumerând utilizarea complementară a violenței selective, alături de „agitația politică, mobilizarea socială și agresiunea politică sau economică la nivel internațional, național și subnațional”[34].

Cunoscutul profesor american Joseph Nye oferă o viziune asupra utilizării instrumentelor de putere naționale denumite „soft power”, pe care le consideră elemente cheie pentru utilitatea studierii războiului hibrid în scopul identificării celor mai bune metode pentru a răspunde amenințărilor economice, diplomatice și informaționale[35]. În acest fel, Nye a descris elementele componente ale conceptului „soft power” ca reprezentând mecanisme ce pot fi instrumentate ca forțe de constrângere și care pot fi folosite în locul exercitării puterii militare sau în combinație cu capabilitățile militare. Instrumentele diplomatice, informaționale, economice, financiare, de informații și legale/

de aplicare a legii din modelul DIME-FIL al puterii naționale figurează, de asemenea, foarte proeminent în definiția războiului din a patra generație (4GW)[36]. 4GW presupune, totuși, că natura războiului nu s-ar schimba, numai antagoniștii și motivațiile lor ar fi diferite[37].

Războiul din cea de-a cincea generație se apropie, din punct de vedere conceptual, de ceea ce reprezintă utilizarea combinată a componentelor conflictului hibrid prin „utilizarea tuturor rețelelor societății - politice, economice, sociale și militare - pentru a continua lupta", fiind orientat spre perspectiva rezistenței și a insurgenței, având ca obiectiv principal „victoria militară imediată"[38].

În studiul războiului hibrid, Frank Hoffman tratează „războiul de tip nou", „războiul open source", „războiul modern", „conflictul polimorf", „conflictele combinate" și „războiul de generația a 4-a" ca școli de gândire care au reformat gândirea militară ce a condus la apariția termenului de război hibrid[39]. „Războiul hibrid este diferit, deoarece abordează „cum" intenționează să lupte adversarul"[40]. Hoffman consideră că noul caracter hibrid al conflictului - care prin definiție este un amestec de două sau mai multe amenințări materializate - trebuie să fie combinația de forțe convenționale, neregulate, terorism și criminalitate. Acest cadru ajută la conceptualizarea actorilor netradiționali (teroriști și criminali) și înțelegerea acestor entități ca instrumente ale statului care au capacitate unică de a fi instrumentate pe timp de pace. Însă, angajarea acestor entități în agresiuni la adresa unui stat, încălcând suveranitatea acestuia, se transformă în acte de război care presupun utilizarea unui spectru mai larg de alte instrumente de putere, cum ar fi constrângerile economice, instrumente politice și diplomatice și agresiuni informaționale. Prin urmare, caracterul hibrid al unui conflict trebuie privit deopotrivă pe timpul stărilor de război și pace, în măsura în care actorii implicați ies din zona gri, incertă, a agresiunilor nedeclarate și neasumate.

Chiar dacă noţiunea de „război hibrid" nu a întrunit consensul internaţional în planul teoriei militare, *„(...) toată lumea, inclusiv NATO şi Uniunea Europeană, este de acord că reprezintă o problemă (...), iar concluzia unanimă este că războiul hibrid implică utilizarea sincronizată a mijloacelor militare şi non-militare împotriva vulnerabilităţilor specifice pentru a crea efecte asupra adversarului"*[41].

Concluzii

În contextul strategiilor hibride sau al războiului neliniar[42], formele virtuale de interacțiune socială joacă un rol important în încercările de a influența percepția oamenilor asupra evenimentelor și a subiectelor de actualitate. Este puțin probabil ca în viitor conflictul să dispară din relațiile umane[43]. Spre deosebire de natura neschimbată a războiului, caracterul său, modul în care se desfășoară și mediul ales pentru ducerea acțiunilor de luptă se vor schimba continuu. Modul în care se desfășoară conflictele are la bază aspectele sociale, economice, politice și informaționale ale societăților și modalitatea în care aceste variabile interacționează la nivelul societăților implicate. Una dintre marile provocări actuale, care va rămâne primordială și în viitor, este de a anticipa caracterul în schimbare al războiului suficient de bine pentru a adapta cu rapiditate instrumentele utilizate atât pentru a oferi un răspuns adecvat, cât și pentru a identifica și remedia vulnerabilitățile proprii. Cea mai importantă schimbare a caracterului războiului de astăzi este proliferarea armelor inteligente, autonome, eficiente și ieftine. Acestea permit statelor mici și chiar actorilor non-statali să dobândească capabilități care anterior constituiau avantajul strategic al marilor puteri, precum sistemele spațiale, sistemele de înaltă precizie la distanță mare, armele autonome cu rază scurtă de acțiune.

În ciuda afirmațiilor politice contrare, confruntările militare nu dispar din peisajul contemporan. Doar că acestea capătă alte nuanțe, se manifestă în dimensiuni la care omenirea nu a avut acces până acum și tind să crească în frecvență și în durată. Conflictul armat rămâne astfel punctul central în relațiile dintre state sau dintre state și actori non-statali. Va rămâne

și în viitor, în acest fel, un concurs de voințe și interese, dominat de incertitudine, agravat de diferite conjuncturi și provocări generate de dezvoltarea tehnologiilor și a modalităților de instrumentare a noilor amenințări. Istoria ne oferă astfel de lecții de secole, liderii politici și militari angajându-se în războaie despre care „știau" că vor fi scurte și decisive, plătind ulterior prețul pentru ignorarea adevăratei naturi a războiului[44].

Bibliografie:

1. CHIFU Iulian, *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21*, în Gândirea militară românească, nr. 1, 2020.
2. CHIFU Iulian, „*Technology and Democracy. The Impact of the Evolution of Security and International Relations*", în Proceedings, 15-th International Scientific Conference „Strategies XXI" Strategic Changes and International Relations, 11-12 aprilie 2019, UNAp, București, pp. 11-23.
3. GRAY S. Colin. , *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2006), p. 4.
4. OPREA Ștefan, *Lumea sub efectele acțiunilor hibride*, 29 mai 2018, Monitorul apărării, https://monitorulapararii.ro/lumea-sub-efectele-actiunilor-hibride.
5. MCCUEN Jack, "*Strategy of Hybrid War*", în Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict, eds. Paul Brister, William H. Natter and Robert R. Tomes (New York, NY: Council for Emerging National Security Affairs, 2011), pp. 70–82.
6. FREIER P. Nathan, *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2007), p. 38.
7. NYE S. Joseph, *Soft Power: The Means to Success in World Politics* (New York, NY: Public Affairs, 2004).
8. HAMMES, Thomas X., "*Modern Warfare Evolves into a Fourth Generation*", în Unrestricted Warfare Symposium: Proceedings on Strategy, Analysis, and Technology, 14–15 March 2006, ed. Ronald R. Luman (Laurel, MD: Johns Hopkins University, Applied Physics Laboratory, 2006), pp. 65–88.
9. HOFFMAN, Frank "*The Hybrid Character of Modern Conflict*," în Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict, eds. Paul Brister, William H. Natter and Robert R. Tomes (New York, NY: Council for Emerging National Security Affairs, 2011), p. 38.

[1] U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, The U.S. Army in Multi-Domain Operations 2028 (Fort Eustis, VA: TRADOC, 6 December 2018), p. 5.

[2] Iulian CHIFU, *Amenințări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21*, în Gândirea militară românească, nr. 1, 2020.

[3] „*NATO's new division: A serious look at 'emerging security challenges' or an attempt at shoring up relevance and credibility*?", ISIS Europe Briefing Note, No. 51, September 2010, https:// www.natowatch.org/sites/default/files/NATOs_New_Division_0.pdf, accesat la 10.06.2020.

[4] Inițiativa de a stabili un cadru comun de cooperare a luat naștere din Comunicarea comună a Comisiei Europene și a Înaltului Reprezentant la Parlamentul European și Consiliu „Cadrul comun privind combaterea amenințărilor hibride - un răspuns al Uniunii Europene", decisă la Bruxelles la 6 aprilie 2016. Inițiativa a fost susținută în setul comun de propuneri pentru punerea în aplicare a Declarației comune UE - NATO, aprobată de Consiliul Uniunii Europene și Consiliul Atlanticului de Nord la 6 decembrie 2016.

[5] „*NATO welcomes opening of European Centre for Countering Hybrid Threats*", 11 aprilie 2017, https://www.nato.int/cps/en/natohq/news_143143.htm, accesat la 11.06.2020.

[6] Iulian Chifu, *Războiul hibrid şi reziliența societală. Planificarea apărării hibride*, Revista Infosfera, februarie 2018, pp. 23-30.

[7] Iulian Chifu, Simona Țuțuianu, *Torn Between East and West: Europe's Border States*, Routledge, London and New York, 2017, p. 270; Greg Simons, Iulian Chifu, *The Changing Face of Warfare in the 21st Century*, Routledge, London and New York, 2017, p. 278.

[8] Jan-Werner Muller, *Ce este populismul,* Editura Polirom, Iași, 2017, p. 179; Steve Richards, *The Rise of the Outsiders. How Mainstream Politics Lost its way*, Atlantic Books, London, 2017, p. 314.

[9] Iulian Chifu, „*Technology and Democracy. The Impact of the Evolution of Security and International Relations*", în Proceedings, 15-th International Scientific Conference „Strategies XXI". Strategic Changes and International Relations, 11-12 aprilie 2019, UNAp, București, pp. 11-23.

[10] https://www.globalpolicy.org/nations-a-states/failed-states.html, accesat la 11.06.2020, Statele eșuate nu mai pot îndeplini funcții de bază, cum ar fi educația, securitatea sau guvernarea, de obicei din cauza violenței sau a sărăciei extreme. În cadrul acestui vid de putere, oamenii cad victime ale facțiunilor și infracțiunilor concurente, iar uneori Națiunile Unite sau statele vecine intervin pentru a preveni un dezastru umanitar. Cu toate aceste măsuri de sprijin, unele state nu reușesc reabilitarea din cauza factorilor interni. De asemenea, guvernele străine pot destabiliza cu bună știință un stat alimentând războiul etnic sau sprijinind forțele rebele, determinând prăbușirea organismelor statale.

[11] P. Williams, "*Violent Non-State Actors and National and International Security*", 28 November 2008, International Relations and Security Network, Swiss Federal Institute of Technology, Zurich. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=93880, accesat la 12.06.2020.

[12] Marian Ștefan, *Modelling the operational environment through cyber attacks*, în Military Strategy Coordinates under the Circumstances of a Synergistic Approach to Resilience in the Security Field, Romanian Military Thinking Conference, pp. 348-359, București, 12-14.11.2020.

[13] http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf, accesat la 10.06.2020, *The Global Risks Report 2016,* 11th Edition.

[14] Ibid.

[15] Nassim Nicholas Taleb, (2010). *The Black Swan: the impact of the highly improbable* (2nd ed.). London: Penguin, 2010; teoria lebedei negre sau teoria evenimentelor lebede negre este o metaforă care descrie un eveniment care vine ca o surpriză, are un efect major și este adesea gestionat în mod necorespunzător.

[16] Thomas X. Hammes, "*Modern Warfare Evolves into a Fourth Generation*", în Unrestricted Warfare Symposium: Proceedings on Strategy, Analysis, and Technology, 14–15 March 2006, ed. Ronald R. Luman (Laurel, MD: Johns Hopkins University, Applied Physics Laboratory, 2006), pp. 65–88.

[17] Brett Daniel Shehadey, *Putting the "D" and "I" Back in DIME*, https://inhomelandsecurity.com/putting-the-d-and-i-back-in-dime/, accesat la 21.09.2020.

[18] The Effectiveness of DIMEFIL Instruments of Power, February 2017, https://inhomelandsecurity.com/putting-the-d-and-i-back-in-dime/ accesat la 10.06.2020.

[19] Colonel (r) prof. univ. dr. Eugen Siteanu, colonel (r.) Benoni Andronic, „*Războiul hibrid*", în Univers Strategic, nr. 2/2015, Bucureşti, p. 192.

[20.] Reizbucnirea și amplificarea unui nou Război Rece între SUA și Rusia, pe fondul creșterii amenințării terorismului în Orientul Mijlociu devastat de războaie civile, revoluții în nordul Africii și ascensiunea economică fulminantă a Chinei, generează noi și justificate neliniști privind redimensionarea galopantă a raporturilor de putere în lumea contemporană. https://ro.wikipedia.org/wiki/R%C4%83zboiul_Rece, accesat la 21.10.2020.

[21] Ștefan Oprea, *Lumea sub efectele acțiunilor hibride*, 29 mai 2018, Monitorul apărării, https://monitorulapararii.ro/lumea-sub-efectele-actiunilor-hibride, accesat la 22.09.2020.

[22] Montgomery McFate and Andrea V. Jackson, "*The Object Beyond War: Counterinsurgency and the Four Tools of Political Competition*," în Unrestricted Warfare Symposium: Proceedings on Strategy, Analysis, and Technology, 14–15 March 2006, ed. Ronald R. Luman (Laurel, MD: Johns Hopkins University, Applied Physics Laboratory, 2006), pp. 143–178.

[23] Davi M. D'Agostino, *Hybrid Warfare: GAO Report to Congress* (Washington, DC: U.S. Government Accountability Office, 2010.

[24] Colin S. Gray (29 decembrie 1943 - 27 februarie 2020) a fost profesor de Relații Internaționale și Studii Strategice la Universitatea Reading, îndeplinind și funcția de director al Centrului pentru Studii Strategice. A fost senior asociat la Institutul Național de Politici Publice, Washington D.C.

[25] Colin S. Gray, *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2006), p. 4.

[26] Ibid, p. 4.

[27] TRADOC G-2, "*Operational Environments to 2028: The Strategic Environment for Unified Land Operations*" (August, 2012), p. 5.

[28] Clausewitz, *On War*. Clausewitz descrie exclusivitatea forței militare pentru desfășurarea războiului ca urmare a incapacității oricărui alt instrument de putere existent la acel moment de a atrage forțele inamice sau de a ocupa teritoriul dorit.

[29] Timothy McCulloh and Richard Johnson, *Hybrid Warfare*, JSOU Report 13–4 (August, 2013); Nathan P. Freier, Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2007).

[30] Jack McCuen, "Strategy of Hybrid War", în *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict,* eds. Paul Brister, William H. Natter and Robert R. Tomes (New York, NY: Council for Emerging National Security Affairs, 2011), pp. 70–82.

[31] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Panama City: Pan American Publishing, 2002), pp. xxi-xxii.

[32] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford; New York: Oxford University Press, 2009), pp. 2–3. David Kilcullen descrie SUA ca fiind prinse într-un ciclu de gândire convențională, care este orbită de convingerea legată de propria putere de dominare. În timp ce America s-a concentrat asupra forței convenționale, alte națiuni s-au îndreptat spre reducerea semnificativă a rolului forțelor convenționale în desfășurarea războiului prin „armarea" altor dimensiuni ale arsenalelor lor strategice.

[33] Liang and Xiangsui, *Unrestricted Warfare*, pp. 16–17.

[34] Nathan P. Freier, *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2007), p. 38.

[35] Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York, NY: Public Affairs, 2004).

[36] Thomas X. Hammes, "Modern Warfare Evolves into a Fourth Generation", în Unrestricted Warfare Symposium: Proceedings on Strategy, Analysis, and Technology, 14–15 March 2006, ed. Ronald R. Luman (Laurel, MD: Johns Hopkins University, Applied Physics Laboratory, 2006), pp. 65–88.

[37] Frank Hoffman, "The Hybrid Character of Modern Conflict", în *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict,* eds. Paul Brister, William H. Natter and Robert R. Tomes (New York, NY: Council for Emerging National Security Affairs, 2011), p. 38.

[38] Hammes, *Modern Warfare Evolves into a Fourth Generation*, p. 65.

[39] Hoffman, *The Hybrid Character of Modern Conflict*, pp. 37–38.

[40] Ibid., p. 38. În mod interesant, Hoffman tratează noțiunea de „cum" intenționează să lupte adversarul sau „modul" în care vor fi folosite mijloacele, iar definițiile sale sunt, de obicei, menționate cu accent pe mijloace (convenționale, neregulate, teroriste și criminale) .

[41]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, accesat la 22.09.2020.

[42] T. Nissen, *Social Media's Role in 'Hybrid Strategies'*, NATO Strategic Communications Centre of Excellence, 2016, https://www.stratcomcoe.org/social-medias-role-hybrid-strategies-author-thomas-elkjer-nissen.

[43] Frank G. Hoffman and Ryan Neuhard, "No Wake for Ares," *Proceedings,* 141, no. 12 (December 2015), available at <www.usni.org/magazines/proceedings/2015-12/no-wake-ares>.

[44] T.X. Hammes, Chapter 2 The Future of Conflict, Charting a Course: Strategic Choices for a New Administration, Dec. 12, 2016.

REPERE CONCEPTUALE PRIVIND DEFINIREA DOCTRINEI OPERAȚIILOR NON-CINETICE

Alexandru-Dumitru PINTILI*

Abstract

There is a cliché that the armies of the world are always preparing for a final war. In fact, they are trying to win the next war. Today's conflicts are largely based on modern technological tools. Today's wars, based largely on non-kinetic operations, are emerging as a new type of conflict to which no one is prepared to respond adequately. Thus, a new philosophy of war appears due to the appearance of non-kinetic weapons. Currently, a weak opponent in the traditional sense of the conflict can prove to be a strong opponent by using informational, psychological, cyber or other non-kinetic fighting techniques.

War based on non-kinetic weapons is becoming increasingly independent, although at the initial stage it was only the support of classical military operations. Today, in most cases, we have in front of us a more powerful set of tools than classical military operations, because their use is possible in a larger number of situations.

The non-kinetic instruments dynamics development requires the understanding of the combat techniques used such as informational, psychological, cybernetic, economic, diplomatic, etc. The increasingly active spread of non-kinetic operations in the modern world must be acknowledged. Both their refinement and their focus not only on military but also on peaceful purposes are growing, which suddenly expands their scope.

Keywords: *non-kinetic operations; cyber operations; psychological weapons; information operations; modern conflict.*

Introducere

Evenimentele din ultimii ani – de exemplu, crizele ucraineană și siriană - au demonstrat în mod clar fragilitatea sistemului de relații internaționale. Asistăm la o transformare treptată a lumii, dintr-o lume monopolară într-o lume multipolară; această etapă se caracterizează printr-o creștere a tensiunilor internaționale, care se reflectă în expansiunea zonelor de influență, accentuarea migrației forțate, precum și creșterea amplorii activităților organizațiilor extremiste și radicale etc. Toate acestea ne fac să ne îndreptăm atenția spre problemele securității naționale, mai ales că astăzi, pe lângă tipurile obișnuite de războaie, auzim de conflicte informaționale, economice, financiare, cibernetice, iar una dintre noile modalități de confruntare între diverși actori devine, tot mai mult, așa-numitul „conflict non-cinetic".

În ultimul secol au fost prezentate, în repetate rânduri, în analizele experților, prognoze și opinii conform cărora războaiele, care timp de multe milenii au reprezentat o „normalitate" a omenirii, vor fi perimate mai devreme sau mai târziu. Din păcate, acest lucru nu a fost confirmat, iar astăzi amenințarea cu noi conflicte este încă foarte semnificativă. Aceste circumstanțe determină relevanța acestui articol, al cărui subiect este dat de tehnicile de război non-cinetic. Astfel, ne propunem să realizăm o scurtă analiză a istoriei dezvoltării principalelor componente ale acțiunilor non-cinetice în cadrul conflictelor internaționale, să luăm în considerare operațiile non-cinetice din prezent și să stabilim dacă aceste operații sunt într-adevăr o nouă abordare a desfășurării operațiunilor militare de tip hibrid. Noutatea științifică a cercetării constă în analizarea operațiilor de tip non-cinetic,

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

determinând dacă acestea sunt un „know-how" al războiului hibrid sau o continuare neagresivă a operațiilor militare utilizate anterior în istorie.

Operația non-cinetică – un „know-how" al războiului hibrid?

Însăși ideea că războiul nu este reprezentat doar de ostilități directe nu este nouă. Aceasta a fost exprimată chiar de Sun Tzu în tratatul „Arta războiului", scris în secolul al VI-lea î.Hr. Sun Tzu spunea în tratatul său că „Războiul este un mod de înșelăciune ... Cel mai bun război este să distrugi planurile inamicului. Următorul pas este să-l forțezi să-și rupă alianțele. Și cel mai rău lucru este dat de asedierea orașelor sale".[1] Prin urmare, putem presupune că o parte din etapele și componentele acțiunilor „non-cinetice" au fost descrise încă din secolul al VI-lea î.Hr.

O trecere în revistă a istoriei artei militare arată că principii similare de desfășurare a unor operații non-cinetice au fost folosite de nenumărate ori. Astfel, se poate observa cum utilizarea componentei informaționale și a celei psihologice au un impact semnificativ asupra grupului țintă. De exemplu, regele persan Xerxes I, înainte de a invada Grecia, a răspândit, prin agenții săi, zvonuri despre invincibilitatea armatei sale: „...dacă toți soldații persani trag cu arcul, săgețile vor eclipsa soarele", iar rezultatul dat de dezinformarea persană a funcționat foarte bine.[2] Genghis Khan și Hannibal, pentru a obține supunerea populației din teritoriile ocupate, s-au folosit de metode de teroare. Orice încercare de a rezista invadatorilor a fost suprimată cât mai sângeros și demonstrativ posibil. Cu ajutorul unor astfel de acțiuni frica a fost instalată în inimile populației, forțându-o să abandoneze lupta.

Odată cu apariția hârtiei tipărite și pătrunderea treptată a alfabetizării în masele largi, cuvântul tipărit a început să fie folosit din ce în ce mai mult în războiul informațional. Așa a început războiul informațional non-cinetic în mass-media. Pliantele au devenit un purtător tipic de propagandă și dezinformare, fiind livrate soldaților inamici sau populației în diferite moduri. Prima utilizare la o scară *industrială* a pliantelor de propagandă a fost în timpul Primului Război Mondial. În aceeași perioadă, principalii participanți la conflict au creat servicii speciale având ca obiect de lucru propaganda și dezinformarea. În prezent, tehnologia informațională modernă a adus războiul informațional și cel psihologic la un nivel complet nou (Fig.1). Tehnologiile au șters practic granițele dintre state, transformând planeta într-un singur câmp informațional.

Fig. 1[3]

Unul dintre obiectivele principale ale războiului informațional este obținerea unei dominații complete în spațiul informațional. Adversarul nu ar trebui, pur și simplu, să poată transmite un punct de vedere alternativ. Acest rezultat se obține prin diferite mijloace: control complet asupra mijloacelor de comunicare ce funcționează în zona de luptă sau prin metode militare.

Războaiele informaționale din lumea modernă sunt, de cele mai multe ori, purtate fără ostilități directe. Adesea, populația țării vizate de atacul informațional nici măcar nu știe despre asta. În acest caz, obiectivele războiului informațional sunt foarte simple: să ducă la o schimbare a regimului politic din țară sau să-l slăbească cât mai mult posibil. Războiul tradițional este foarte costisitor, iar metodele non-cinetice de influențare a deciziilor sunt o alternativă excelentă la acesta, destul de eficientă și care nu necesită victime. Omniprezența Internetului permite propagandiștilor să se infiltreze practic în fiecare casă.

Lovitura principală este acordată conducerii țării, activitatea organismelor de stat este discreditată și încrederea în autorități este subminată. Populației i se arată faptele de corupție (reale sau fictive) sau diferite infracțiuni ale liderilor politici ce pot conduce la o creștere a protestelor. Se creează o atmosferă de conflict și neîncredere în rândul cetățenilor statului vizat, iar opinia publică este manipulată activ. Mai mult decât atât, se poate încerca atragerea mass-media locale de partea agresorului, caz în care acestea devin „portavocea" mișcării de protest. De obicei, astfel de atacuri sunt însoțite de susținerea unei părți a elitei politice a țării vizate, care începe să coopereze cu agresorul. Apelurile la demonstrații, greve și alte acțiuni sunt difuzate prin mass-media și prin Internet, ceea ce subminează și mai mult situația. În același timp, acțiunile din stradă, din nou, sunt acoperite în mod corespunzător în mass-media, glorificându-i pe protestatari și arătând într-o lumină negativă forțele pro-guvernamentale și instituțiile responsabile cu aplicarea legii. Efectuarea unui astfel de complex de acțiuni (dacă are succes, desigur) duce la pierderea controlului în țară, la recesiune economică și, adesea, la război civil.

Există și un alt aspect mai profund aici. Mass-media moderne pot duce nu doar la haos în stat și la provocarea conflictelor civile. Astăzi, ele formează, practic, bazele societății moderne, transmițând anumite valori oamenilor și provocând reacții. Persoanei i se spune ce este corect și ce nu, ce ar trebui considerat normal și ce este anormal. Mai mult, toate acestea se fac într-o manieră atât de ușoară și discretă încât tehnicile de propagandă pur și simplu nu sunt vizibile.

Odată cu debutul erei postindustriale, operațiile informaționale au fost completate de acțiuni în spațiul cibernetic și de utilizarea tehnologiilor socio-politice distructive.[4] Acestea din urmă sunt acum atât de intens utilizate încât pot fi distinse ca o altă componentă a „operației non-cinetice". Mai mult, diversitatea lor permite chiar și o clasificare internă a unor astfel de acțiuni: de la simplul sprijin financiar și informațional al mișcărilor de opoziție și crearea unei „a cincea coloane" în statul adversar, până la introducerea agenților de influență care asigură așa-numita „ocupare ușoară" a țării și tranziția acesteia sub controlul extern. Metodele utilizate diferă în intensitate în funcție de puterea inamicului împotriva căruia sunt folosite. Exemple tipice de utilizare modernă a unor astfel de tehnologii sunt organizarea așa-numitelor „revoluții colorate" prin activitățile diferitelor organizații non-profit. Practica arată că astfel de acțiuni nu sunt doar mai eficiente, ci și semnificativ mai ieftine decât intervenția militară directă. Dar nici măcar nu este vorba de economisirea banilor: confruntarea militară directă este pur și simplu periculoasă pentru contracararea multor țări, iar „subminarea" sistemului lor de stat prin „implantarea democrației" este relativ sigură. Acum, în era globalizării și a revoluției informaționale, activitatea de confruntare a informațiilor și utilizarea tehnologiilor socio-politice distructive a devenit atât de extinsă încât experții au început să vorbească despre apariția așa-numitei ere a „post-adevărului".[5]

În istoria modernă, odată cu creșterea mobilității populației, astfel de acțiuni „pre-

hibride" pot fi implementate prin atribuirea cetățeniei pe teritoriul unui stat străin, legitimarea cetățenilor prin achiziționarea de terenuri sau imobile, migrație etc.; toate acestea sporesc pericolul și pot fi considerate unul dintre elementele care preced „războiul hibrid".

Cel mai important aspect al unei operații non-cinetice îl reprezintă componenta sa economică. În retrospectivă istorică, utilizarea acestei tehnici a început cu trecerea de la o economie de subzistență și economii naționale separate la un sistem economic mondial, asociat cu diviziunea interstatală a muncii și comerțului internațional. Istoria arată un număr mare de metode utilizate în cadrul acestei componente a confruntării; de exemplu, în timpul Războaielor Napoleoniene, Franța a falsificat bancnote englezești, austriece și rusești.

Odată cu debutul erei globalizării, componenta financiară a conflictelor non-cinetice a crescut semnificativ, atât în scara de aplicare, cât și în varietatea metodelor utilizate. Acestea din urmă variază de la blocarea directă a conturilor financiare ale unor persoane vizate și chiar a guvernelor statelor inamice, la metode indirecte bazate pe interdicții. Ca unul dintre primele exemple de război economic, putem cita „blocada continentală": un set de măsuri de blocare a comerțului Marii Britanii, efectuat de Franța între anii 1806-1814. În secolele XIX-XX, cel mai frecvent tip de război economic a fost tocmai „blocada navală". Înainte de începerea Primului Război Mondial, Turcia, Portugalia, Olanda, Columbia, Panama, Mexic, Argentina și El Salvador erau supuse blocadei. Inițiatorii blocadelor au fost: Marea Britanie, Franța, Italia, Germania, Austria, Rusia și Chile.[6] După al Doilea Război Mondial, sancțiunile economice au continuat să fie un instrument activ în politica internațională. În perioada 1971 - sfârșitul secolului al XX-lea, pot fi observate peste 120 de cazuri de sancțiuni, în primul rând în cadrul războiului economic dintre SUA și Rusia.

O altă componentă a confruntării economice, o reprezintă resursele. Această componentă a fost exploatată încă din cele mai vechi timpuri, sub forma asediului cetăților, prin blocarea accesului la alimente și apă. În prezent, odată cu dezvoltarea tehnologiilor și a diversității legăturilor economice, apar noi forme de confruntare pe tema resurselor, sub forma blocării transporturilor, a energiei, a resurselor petroliere și chiar a apei. Exemple tipice de astfel de acțiuni sunt date de încercările de a devia apele râului Iordan, care a servit drept unul dintre motivele „Războiului de șase zile" din 1967 sau blocada energiei și apei din Crimeea în 2014. Utilizarea potențială a armelor climatice poate fi considerată foarte apropiată de confruntarea resurselor în ceea ce privește caracteristicile. Informații confirmate despre folosirea acestui tip de armă nu există, doar anumite presupuneri cu privire la dezvoltarea sa de către unele țări.[7] Dar, dacă apare o astfel de armă, ea va deveni un mijloc ideal de a conduce o confruntare „non-cinetică".

Analizând istoria, putem concluziona că aceste conflicte non-cinetice moderne nu sunt un „know-how", ci doar o continuare a diferitelor forme de confruntare interstatală utilizate anterior, diferind prin:

- utilizarea complexă a diferitelor forme de confruntare non-militară și non-cinetică;
- creșterea semnificativă a capacităților tehnologice pentru implementarea anumitor forme de acțiune;
- impactul acțiunilor datorat globalizării lumii moderne.

Nevoia unei doctrine pentru operațiile non-cinetice

Sistemul internațional de securitate care a apărut ca urmare a celui de-al Doilea Război Mondial a influențat, în mare măsură, schimbarea abordărilor și a metodelor de conducere a puterii militare, economice, financiare, tehnologice etc. În acest sens, căutarea unui nou set de instrumente ce face posibilă dezvoltarea unei situații de criză benefice propriilor interese și, în același timp, crearea aspectului de imparțialitate, precum și ascunderea implicării directe în confruntările armate au căpătat o relevanță deosebită pentru unii actori puternici.

Trebuie subliniat că, în prezent, nu există un termen unic, pentru toți actorii, care să

reflecte utilizarea coordonată a instrumentelor politico-diplomatice, informațional-psihologice, economice și de altă natură pentru a atinge anumite obiective strategice. În general, în majoritatea structurilor guvernamentale și în comunitățile analitice ale statelor puternic dezvoltate, sunt utilizate la scară largă definiții precum „acțiune militară neliniară", „asimetrică", „neconvențională", „non-cinetică" și „hibridă". În majoritatea statelor, pentru a desemna o presupusă nouă formă de confruntare, se utilizează, de regulă, conceptul de „război hibrid". Acest concept s-a răspândit peste tot în lume, mai ales după evenimentele din Crimeea (2014) pentru a caracteriza „acțiunile agresive ascunse ale Rusiei care contravin dreptului internațional umanitar".

Potrivit experților NATO, „operațiile hibride" reprezintă un set de măsuri și acțiuni coordonate în termeni de obiective, loc și timp, desfășurate fără utilizarea directă și explicită a forței militare, menite să asigure impactul necesar asupra unui actor vizat.[8] O mare parte dintre aceste acțiuni au o caracteristică foarte importantă, aceea că sunt de natură non-cinetică. Aceste tehnici non-cinetice trebuie separate de operația hibridă modernă deoarece ele vizează „epuizarea" unui adversar fără utilizarea forțelor militare clasice, a celor paramilitare și implică acțiuni precum:[9]

- operații informaționale efectuate pentru influențarea conducerii și pentru obținerea unui control informațional al inamicului, pentru a-l induce în eroare, pentru a perturba schimbul de informații și pentru a-l provoca să ia decizii greșite;
- operații psihologice care vizează suprimarea stării morale și psihologice a populației și a spiritului de luptă al personalului armatei inamicului, crearea unei atmosfere de neîncredere în societate și formarea unei motivații necesare unor acțiuni distructive;
- atacuri cibernetice asupra infrastructurilor guvernamentale și comerciale cu scopul de a dezactiva sau împiedica funcționarea infrastructurii critice, precum și de a obține acces neautorizat la anumite tehnologii sau informații;
- embargoul economic și financiar, încetarea investițiilor, întreruperea aprovizionării cu energie, blocarea comerțului;
- acțiuni de protest ale mișcărilor de opoziție, acțiuni de influență în cadrul structurilor administrației locale, acțiuni de sabotaj efectuate de forțe separatiste, precum și a unor formațiuni paramilitare.[10]

Surpriza și *secretul* sunt considerate principiile de bază ale desfășurării „operațiilor non-cinetice". Faza inițială a acestui tip de operație o reprezintă destabilizarea deliberată a situației politice interne din statul vizat, susținută de o campanie de dezinformare, manipulare și propagandă. În condițiile agravării situației, unități speciale sunt transferate în zona de criză cu sarcina de a prelua controlul asupra obiectivelor cheie ale organelor de comandă și ale infrastructurii critice. Simultan cu aceasta, pentru descurajarea actorului vizat, în cadrul activităților de antrenament planificate se desfășoară o demonstrație a posibilității intervenției militare în zona respectivă.

În viitor, în zona de conflict, desfășurarea ostilităților se va baza, în special, pe acțiunea grupărilor locale de insurgenți și a celor paramilitare, în combinație cu o creștere semnificativă a acțiunilor de dezinformare, propagandă, manipulare și atacuri cibernetice. După preluarea controlului unei părți a teritoriului părții opuse, se vor lua măsuri pentru consolidarea legislativă a noului statut, schimbarea structurii politice și staționarea unităților forțelor armate în respectivul teritoriu. Principalul avantaj al „acțiunilor non-cinetice" constă în capacitatea părților beligerante de a-și nega implicarea în evenimente și de a-și atinge obiectivele fără pericolul unor represalii militare.

Există și o serie de neajunsuri și limitări caracteristice unor astfel de operații, precum: risc politic; destabilizarea economiei naționale; pericol pentru personalul civil; dificultate în organizarea interacțiunii dintre structurile publice și cele private. Esența și algoritmul operațiilor non-cinetice discutate mai sus sunt formulate în baza analizei experienței utilizării măsurilor militare și non-militare de către Rusia în peninsula Crimeea.

Cu toate acestea, în ciuda noutății relative a conceptului de operație non-cinetică, elaborarea problemelor cu impact complex asupra inamicului se realizează constant atât în cadrul alianțelor politico-militare, cât și la nivel individual. Statele puternic dezvoltate au introdus în practică metode de acțiune non-cinetice în ultimii douăzeci de ani pentru a-și atinge obiectivele politico-militare în diferite regiuni ale lumii. O discuție despre aceste noi concepte a avut loc și în cadrul Summit-ului NATO de la București (2008), la care a fost adoptat „Planul de implementare a unei abordări NATO cuprinzătoare în interesul contracarării amenințărilor moderne". În conformitate cu acest document, se preconiza că statele Alianței pot răspunde acestor tipuri de amenințări prin utilizarea coordonată, la toate nivelurile (de la tactic la strategic), a instrumentelor civile și militare de natură non-cinetică. [11]

NATO a observat că anumite acțiuni de tip non-cinetic au fost utilizate în aproape toate crizele și conflictele din ultimii douăzeci de ani care au avut loc pe continentul eurasiatic, Africa de Nord și Orientul Mijlociu. Rezultatele acestei analize sunt reflectate în doctrinele Alianței, unul dintre principalele documente din acest domeniu reprezentându-l „Manualul NATO de răspuns la criză".[12] Sistemul de răspuns la criză al NATO cuprinde un set de măsuri întreprinse de conducerea Alianței și de comandamentele sale, necesare pregătirii forțelor coaliției pentru demararea unor acțiuni de neutralizare și respingere a amenințărilor la adresa securității statelor membre.[13]

Experiența evenimentelor din Crimeea a arătat NATO că blocarea unui adversar ce folosește metode non-cinetice în cadrul unui conflict este destul de dificilă, aproape imposibilă, deoarece implicarea acestuia este greu de dovedit. Astfel că este necesară și urgentă dezvoltarea unor capacități non-cinetice de contracarare a unor amenințări de același tip, precum și redefinirea conceptelor de „atac" și „agresiune". Operațiile de tip non-cinetic, precum cele ale Rusiei împotriva Ucrainei, au demonstrat Alianței că acestea sunt o formă eficientă de atingere a obiectivelor strategice.

Când ne referim la conceptul de operație non-cinetică putem observa că aceasta se bazează pe „utilizarea instrumentelor militare și non-militare pentru a obține surpriza și pentru a obține un avantaj în fața actorului vizat folosind capacități diplomatice, economico-financiare, informaționale, electronice și cibernetice, combinate cu o campanie de manipulare și dezinformare, necesară în atragerea populației civile și în acoperirea și ascunderea intereselor."[14]

Analiza efectuată mai sus ne permite să tragem anumite concluzii referitoare la necesitatea unei doctrine a operațiilor de tip non-cinetic în cadrul unui conflict.

În primul rând, nu trebuie să considerăm operația non-cinetică ca fiind o metodă fundamental nouă de confruntare. Deși recunoaștem coerența acestei abordări, trebuie remarcat faptul că, deși toate componentele confruntării non-cinetice sunt utilizate în cadrul conflictelor hibride, nu există o proiecție inversă deoarece un conflict non-cinetic poate fi purtat fără a intra în faza confruntării militare directe.

În al doilea rând, varietatea acțiunilor non-cinetice arată că este imposibil să considerăm operația non-cinetică ca un fel de fenomen unic, omogen. Astfel de acțiuni diferă în scopuri și metode utilizate, ceea ce necesită o clarificare a clasificării lor.[15] Este necesar să se ia în considerare tendința de a muta accentul acțiunilor hibride de la desfășurarea războaielor de tip *proxy* la sfera confruntării non-militare și non-cinetice. Paradoxal, acest lucru nu face decât să crească nivelul pericolului lor. Utilizarea intensivă a metodelor non-cinetice de confruntare în sfera economică, socio-politică și a spațiului cibernetic în lumea globalizată are un efect mult mai distructiv decât conflictele clasice. Și nu au fost încă dezvoltate măsuri eficiente pentru a le contracara[16].

Acest pericol necesită clarificarea documentelor ce reglementează relațiile internaționale, introducerea de dispoziții cu privire la inadmisibilitatea aplicării sancțiunilor și desfășurarea operațiilor de informare fără aprobarea organizațiilor internaționale. Poate fi necesară clarificarea cu privire la aparatul

conceptual, de exemplu, introducerea în domeniul juridic a conceptelor deja utilizate de specialiști: „invazia informațională", „blocarea resurselor" etc. Documentele existente privind reglementarea componentei de putere a „războaielor hibride" necesită, de asemenea, clarificări. De exemplu, în ceea ce privește mutarea pedepsei pentru activitatea mercenară, de la persoane sau companii private la statele în care sunt înregistrate. În ceea ce privește componentele economice și informaționale, este necesară adoptarea unui cadru legislativ internațional, similar celui care reglementează componenta lor de putere.[17] După adoptarea actelor relevante, toate măsurile economice și informaționale care depășesc cadrul stabilit de dreptul internațional, pe baza documentelor revizuite, ar trebui să fie recunoscute ca o declarație de război a statului care le-a folosit.

În al treilea rând, forțele armate ale tuturor statelor trebuie să-și clarifice structura forțelor și a mijloacelor de aplicare a deciziilor militare, în ceea ce privește particularitățile operațiilor non-cinetice și frecvența apariției lor. Astfel, luând în considerare particularitățile tranziției confruntării non-cinetice în faza hibridă a acțiunilor, sunt necesare anumite clarificări deoarece în condițiile actuale acesta nu mai este un concept omogen, ci un set de opțiuni de acțiune, în care, în funcție de obiectiv, predomină o anumită componentă. Adesea, setul este dinamic, dezvoltându-se din acțiuni „pre-hibride" către o confruntare armată hibridă. Această soluție va contribui, pe termen lung, la creșterea securității lumii moderne, în timp ce întârzierea deciziei în acest sens va conduce la o creștere a riscurilor și amenințărilor.

La începutul lucrării am argumentat relevanța subiectului prin ideea că războiul nu este reprezentat doar de ostilități directe, așa cum a afirmat și Sun Tzu în tratatul său. Pe baza analizei definițiilor existente ale confruntărilor non-cinetice, a celor de tip hibrid și a punctelor de vedere ale specialiștilor din aceste domenii, se observă că „o componentă principală în cadrul unui conflict hibrid este reprezentată de implicarea unor grupuri militare sau non-militare pentru demararea unor operații non-cinetice ce pot aduce un câștig semnificativ și un avantaj decisiv fără a apela la acțiuni distructive." Teoria și practica desfășurării operațiilor non-cinetice nu sunt un „know-how" al confruntării hibride, ci un tip de confruntare mult folosită și dovedită, iar în condițiile moderne este utilizată cu o eficiență din ce în ce mai mare.

Bibliografie:

1. TZU, Sun *Arta războiului,* Ed. Libris, 2012, București;
2. LEONARD, Anya, "Thermopylae: Battle in the Shade", disponibil pe https://classicalwisdom.com/politics/wars/thermopylae-battle-in-the-shade/, accesat la 10.04.2021;
3. SHARP, Gene, *Power and Struggle (Politics of Nonviolent Action),* pg. 72, ebook, 1972;
4. PARMAR, Inderjeet, "US Presidential Election 2012: Post-Truth Politics", *Political Insight,* vol. 3, nr. 2, 2012, pg. 4-7;
5. KATASONOV, V., „Războaie economice și sancțiuni economice", disponibil pe https://topwar.ru/68238-ekonomic%20news-voyny-i-ekonomic%20news-sankcii.html, accesat la 10.04.2021;
6. BARKHAM, Patrick "Can the CIA weaponise the weather?", disponibil pe https://www.theguardian.com/us-news/shortcuts/2015/feb/16/can-the-cia-weaponise-the-weather-geoengineering, accesat la 10.04.2021;
7. "NATO's response to hybrid threats", disponibil pe https://www.nato.int/cps/en/natohq/topics_156338.htm, accesat la 28.03.2021;
8. PINTILI, A., Mitulețu, I., „Delimitări conceptuale privind operațiile informaționale, cibernetice, non-letale și non-cinetice", disponibil pe https://cssas.unap.ro/ro/pdf_publicatii/cs10-20.pdf, accesat la 29.03.2021;
9. "Hybrid threats as a concept", disponibil pe https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/, accesat la 28.03.2021;
10. *Bucharest Summit Declaration,* disponibil pe https://www.nato.int/cps/en/natolive/official_texts_8443.htm, accesat la 02.04.2021;
11. https://nato-crisis-response-system-manual-pdf.peatix.com/view/, accesat la 02.04.2021;
12. "NATO Crisis Management", disponibil pe https://www.cmdrcoe.org, accesat la 02.04.2021;

13. MARCUS, Jonathan, „Războiul hibrid al lui Putin este o durere de cap pentru NATO“, disponibil pe https://www.bbc.com/russian/international/2014/12/141106_nato_russian_strategy, accesat la 02.04.2021;
14. FADEEV A.S., V.I. Nichipor, “Military Conflicts of Today and Their Methods. Direct and Indirect Actions” in *Armed Conflicts of the 21st Century, Military Thought,* Nr. 9, 2019, pg. 36., disponibil pe https://dlib.eastview.com/browse/doc/57847373, accesat la 12.04.2021;
15. MACK Andrew, „De ce națiunile mari pierd războaie mici: politica conflictului asimetric“, *World Politics,* Vol. 27, nr. 2, pg. 175-200, 1975, disponibil pe https://web.stanford.edu/class/polisci211z/2.2/Mack%20WP%201975%20Asymm%20Conf.pdf, accesat la 12.04.2021;
16. Convenția internațională împotriva recrutării, utilizării, finanțării și instruirii mercenarilor. Adoptată prin Rezoluția Adunării Generale 44/34 din 4 decembrie 1989, disponibil pe https://undocs.org/en/A/RES/44/34, accesat la 12.04.2021.

[1] Sun Tzu, *Arta războiului,* Ed. Libris, 2012, București.
[2] Anya, L., Thermopylae: Battle in the Shade, disponibil pe https://classicalwisdom.com/politics/wars/thermopylae-battle-in-the-shade/, accesat la 10.04.2021.
[3] Ivyon, „Perspectivă - Puterea ochiului din spatele camerei“, disponibil pe https://ivymosquito.wordpress.com/tag/soldiers/, accesat la 10.04.2021.
[4] Gene Sharp, *Power and Struggle (Politics of Nonviolent Action),* pg. 72, ebook, 1972.
[5] Inderjeet Parmar, “US Presidential Election 2012: Post-Truth Politics”, *Political Insight,* vol. 3, nr. 2, 2012, pg. 4-7.
[6] Katasonov, V., „Războaie economice și sancțiuni economice“, disponibil pe https://topwar.ru/68238-ekonomic%20news-voyny-i-ekonomic%20news-sankcii.html, accesat la 10.04. 2021.
[7] Patrick Barkham, “Can the CIA weaponise the weather?”, disponibil pe https://www.theguardian.com/us-news/shortcuts/2015/feb/16/can-the-cia-weaponise-the-weather-geoengineering, accesat la 10.04.2021.
[8] NATO’s response to hybrid threats, disponibil pe https://www.nato.int/cps/en/natohq/topics_156338.htm, accesat la 28.03.2021.
[9] Pintili, A., Mitulețu, I., Delimitări conceptuale privind operațiile informaționale, cibernetice, non-letale și non-cinetice, disponibil pe https://cssas.unap.ro/ro/pdf_publicatii/cs10-20.pdf, accesat la 29.03.2021.
[10] “Hybrid threats as a concept”, disponibil pe https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/, accesat la 28.03.2021.
[11] *Bucharest Summit Declaration,* disponibil pe https://www.nato.int/cps/en/natolive/official_texts_8443.htm, accesat la 02.04.2021.
[12] https://nato-crisis-response-system-manual-pdf.peatix.com/view/, accesat la 02.04.2021.
[13] NATO Crisis Management, disponibil pe https://www.cmdrcoe.org, accesat la 02.04.2021.
[14] Marcus, J., „Războiul hibrid al lui Putin este o durere de cap pentru NATO“, disponibil pe https://www.bbc.com/russian/international/2014/12/141106_nato_russian_strategy, accesat la 02.04.2021.
[15] A.S. Fadeev, V.I. Nichipor, Military Conflicts of Today and Their Methods. Direct and Indirect Actions in Armed Conflicts of the 21st Century, Military Thought, Nr. 9, 2019, pg. 36., disponibil pe https://dlib.eastview.com/browse/doc/57847373, accesat la 12.04.2021.
[16] Mack A., „De ce națiunile mari pierd războaie mici: politica conflictului asimetric, Revista *World Politics,* Vol. 27, nr. 2, pg. 175-200, 1975, disponibil pe https://web.stanford.edu/class/polisci211z/2.2/Mack%20WP%201975%20Asymm%20Conf.pdf, accesat la 12.04.2021.
[17] Convenția internațională împotriva recrutării, utilizării, finanțării și instruirii mercenarilor. Adoptată prin Rezoluția Adunării Generale 44/34 din 4 decembrie 1989, disponibil pe https://undocs.org/en/A/RES/44/34, accesat la 12.04.2021.

ARTA DE A LUPTA DIN UMBRĂ. VALENȚE ALE INGINERIEI SOCIALE ÎN OPERAȚIILE INFORMAȚIONALE

Claudiu Marius IONESCU*

Abstract

Throughout history, industrial revolutions have led to major changes in areas such as economics, politics, justice, ecology, etc. and have generated technological innovations that have always been found in new approaches to military affairs. The industrial society as we know it for more than a century is gradually turning into an information society and will recursively generate changes in the thinking of military strategies.

In the current age of the Internet the truth can be killed at any time (if this is useful) because the trend of societies is shifting from an environment based on technological tools to an environment based on mass social engineering, extremely refined, subtle combinations between technology manipulation and dependence.

Keywords: *social engineering, International conflict, INFO-OPS, hybrid ware, strategic manipulation, propaganda.*

Introducere

Societatea industrială, așa cum o cunoaștem de mai bine de un secol, s-a transformat treptat într-o societate informațională, susținută de o tehnologie digitală, care va genera recursiv schimbări în gândirea și aplicarea strategiilor, inclusiv a celor militare. Se prefigurează ca, în viitor, confruntările militare să își modifice însăși esența lor, respectiv violența fizică, componentă care se atenuează tot mai mult. Au apărut o serie de noi doctrine și strategii militare, caracterizate prin lipsa regulilor cunoscute de angajare a unui război, ambiguitatea cunoașterii inamicului, lipsa dihotomiei dintre război și pace, precum și un alt mod de proiectare, organizare și desfășurare a conflictelor militare. Le putem numi războaie informaționale, operații non-kinetice cognitive sau acțiuni de intervenție socială în teritoriul inamic, dar indiferent de denumire ele sunt acțiuni de inginerie socială ce au la bază studii ale științelor sociale și neuroștiințelor, sprijinite de dezvoltarea fără precedent a tehnologiei informaționale.

Aceste tipuri de acțiuni se bazează preponderent pe echipamente non-militare, necesită mai puține resurse, pot avea remanență mare în timp și pot garanta succesul chiar și pentru state mici sau entități non-statale. Sunt atractive pentru că pot genera soluții pentru rezolvarea unor conflicte cu pierderi și distrugeri minime prin inițierea unor operații informaționale de la distanță, fără implicarea kinetică a forțelor proprii, în care efectele urmărite sunt *afectarea identității colective, polarizarea socială, subminarea convingerilor liderilor adversarului, încurajarea, renunțarea sau predarea, preluarea sau distrugerea sistemelor de comandă și control ale inamicului etc.*

Aceste tipuri de acțiuni sunt favorizate și de actuala perioadă de cultură, cunoscută și ca „*epoca post-adevăr*”, în care pseudo-educația și gândirea necritică primează, în care emoția are întâietate în fața rațiunii. În trecut doar organizațiile puternice aveau posibilitatea de a crea manipulare, însă în era social-media oricine are această posibilitate.

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

Conflictele din era informațională au nevoie de o colectare eficientă a informațiilor și acest demers se poate realiza doar prin structurile de intelligence, capabile să culeagă și să analizeze informațiile despre inamic din mediile sau zonele de interes la toate nivelurile (tactic, operativ și strategic). Structurile de intelligence pot fi, de asemenea, element de sprijin înaintat care poate acționa anterior desfășurării unei operații, în vederea obținerii unor informații necesare planificării.

Este nevoie, deci, ca învățământul militar din domeniul informații pentru apărare să fie adaptat la realitatea acestor vremuri, prin includerea unor teme referitoare la tipologia acțiunilor de inginerie socială, precum și la aplicațiile civile și militare ale acestora.

Este nevoie, de asemenea, de educație mediatică și de promovarea gândirii critice, condiții esențiale pentru formarea unor specialiști de intelligence bine ancorați în realitatea noilor paradigme ale conflictualității.

Ingineria socială

Sintagma de „inginerie socială", concept care provine din limba engleză (social engineering), desemnează un cumul de tehnici de influențare exercitate asupra oamenilor pentru a-i determina să întreprindă anumite acțiuni pe care, în mod normal, nu le-ar fi întreprins.

Apariția ingineriei sociale este strâns legată de evoluția științelor sociale. În cei aproximativ 150 de ani de la cele mai vechi referințe privind conceptul de *inginerie socială,* respectiv ale lui Charles Fourier, sociolog și economist francez adept al socialismului utopic, numit „*avocatul ingineriei sociale*"[1], care propunea ingineria socială ca instrument pentru crearea unei societăți ideale, sau ale inginerului francez Emile Cheysson[2] ce desemna o ramură a sociologiei aplicative care urmărea să prevină și să aplaneze conflictele sociale[3], *ingineria socială* a avut tendința să semene tot mai mult cu „*influența socială*", care este o acțiune orientată spre modificarea opțiunilor și manifestărilor fără constrângere, sub forma persuasiunii, manipulării sau îndoctrinării.

Începuturile aplicării științifice a ingineriei sociale în România au fost asociate cu educația, cu intervenția socială, încă din perioada interbelică. Astfel, Dimitrie Gusti (1880-1955), sociolog român, membru al Academiei Române (considerat creatorul sociologiei românești moderne), a teoretizat această știință denumind-o „*știință în slujba națiunii*", sub îndrumarea lui realizându-se un amplu program de reforme sociale, prin știință și cultura națională, într-o viziune numită de el „*inginerie socială*". Sociologul român încerca, astfel, să adere la un curent apărut în Statele Unite ale Americii de transformare a sociologiei sociale în inginerie socială[4].

Ideea creării unor metode de control al unor mari grupuri de oameni, în vederea modificării conduitei acestora într-un mod dorit, s-a cristalizat în secolul XIX, când statele europene au încercat să-și îmbunătățească colectarea de taxe şi înrolarea soldaților. În prezent, ne aflăm într-o fază a civilizației în care nici un domeniu al vieții sociale nu mai scapă posibilităților de manevrare a omului. Aceasta se realizează printr-o serie de „politici" (sociale sau științifice) diversificate, aplicate în domeniile economice, demografice, educaționale, culturale, de urbanism, de manipulare a opiniei publice, de marketing, într-un cuvânt „inginerie socială".

Ne aflăm într-o etapă în care, în scopul obținerii unor avantaje (politice, economice, militare), ingineria socială este îndreptată preponderent împotriva omului și nu în sprijinul acestuia. Este mult diferită de cea pe care au gândit-o „părinții" ei.

Conceptul de „inginerie socială" a evoluat mult în ultimii zeci de ani și datorită dezvoltării tehnologiei informației, identificându-se patru aplicații practice ale sale: în cadrul științelor **sociale,** în cadrul științelor **politice,** în cadrul **securității informatice** (cunoscută ca și „social engineering") și în **psihologie**.

În Franța, de exemplu, există două institute care oferă chiar diplome de stat în „*inginerie socială*": Universitatea Tolouse, prin Institutul regional de inginerie socială (*Institut régional d'ingénierie sociale*[5]*/IRIS*), respectiv Institutul regional de asistență socială (*Institut régional du travail social*[6]*).*

Ingineria socială modernă este și o știință ce are ca scop schimbarea socială și augmentează eficient neuroștiințele moderne cu științele clasice din domeniul social (psihologia, sociologia, antropologia), într-un mediu preponderent digital. Este utilizată în prezent cu succes în acțiunile militare, politice și economice. Poate fi utilizată în scopul dezvoltării unei societăți (prin implementarea unor politici publice) sau pentru a destabiliza un stat, ca acțiune precursoare unei intervenții militare.

În ultimul deceniu ingineria socială a devenit de notorietate și datorită utilizării ei în infracțiunile cibernetice, în scopul obținerii accesului la rețelele informatice, prin identificarea credențialelor de acces sau prin introducerea unor programe malware. Sunt cunoscute, astfel, o serie de metode de *social engineering,* precum: *phishing, catfishing, smishing, vishing, piggybacking, tailgating, impersonation, dumpster diving, pretexting computer tehnician, baiting* etc. Acestea sunt, în fapt, metode prin care se eludează tehnologia din domeniul securității informațiilor prin acțiuni direcționate spre cel mai vulnerabil element - omul. Astfel de acțiuni pot afecta infrastructura critică a unei țări prin distrugerea, blocarea sau preluarea controlului sistemelor informatice ale acestora.

Manipularea psihologică

Aplicațiile ingineriei sociale asupra grupurilor de oameni sau asupra indivizilor au randament ridicat deoarece omul poartă în el o mașinărie complexă care funcționează după reguli străvechi și, în cea mai mare parte a timpului, în mod automat, „inginerii sociali" cunoscând-o, dar nu și marea masă de oameni expusă.

Specialiștii arată[7] că ființa umană este în mod natural atentă și conștientă de pericolul unei amenințări exterioare fizice cu poluanți chimici, radiații, agenți biologici etc., amenințări pe care încearcă să le controleze conștient prin prevenție. Din păcate, nu a ajuns încă la un nivel de dezvoltare a instinctelor încât să poată fi conștientă de pericolul subtil al contaminării de ordin psihologic. Una dintre erorile majore pe care le facem ca specie este să nu fim conștienți de pericolul acestui tip de agresiune. Credem că dacă suntem expuși zonelor cu informație falsă nu este un pericol pentru că avem capacitatea de a distinge ușor între o informație adevărată și o informație falsă, că putem controla manipularea psihologică și, astfel, să controlăm manipularea mentală, respectiv efectele unei informații false și nerelevante.

Totuși, experimentele moderne de psihologie cognitivă au arătat că mintea umană nu este proiectată ca, în mod natural, să afle adevărul, ci doar pentru reproducerea speciei. Deci, căutarea adevărului (gândirea rațională) la om nu vine în mod natural, ci necesită un efort conștient. Neuroștiințele arată că procesarea și clasarea unei informații în creierul uman are două etape. Prima etapă este încărcarea informației pe hardul biologic, respectiv creierul. În mod natural, în această etapă orice informație pe care am înțeles-o este considerată de creier ca fiind adevărată dacă nu intervenim cu cea de-a doua etapă, respectiv analizarea informației în vederea clasificării (adevărată sau falsă).

În general, manipularea psihologică se bazează pe blocarea persoanelor expuse de a nu mai parcurge cea de-a doua etapă, pentru a nu avea posibilitatea analizării veridicității informației la care sunt expuse. Aceasta se poate face prin mai multe moduri:. prin transmiterea informației în mod subliminal (sub pragul senzorial, de exemplu prezentată cu o intensitate auditivă sau luminoasă scăzută); când suntem „bombardați" cu o cantitate mare de informație ce nu poate fi analizată critic, ca urmare a resurselor limitate pe care le avem ca specie umană (atenție, memorie); când ne aflăm într-o stare de oboseală avansată sau distrași, implicați în alte sarcini, astfel încât resursele de memorie și atenție sunt focalizate în altă direcție decât cea a informațiilor asimilate în prima etapă; când informația vine dintr-o sursă pe care o considerăm credibilă și hotărâm, în mod conștient, să suspendăm analiza din etapa a doua.

Și totuși, chiar dacă realizăm în etapa a doua că o informație este falsă, aceasta ne poate contamina mental, influențându-ne inconștient hotărârile. O bună practică pentru a nu fi manipulați este să verificăm permanent și să controlăm în

mod conștient dacă deciziile luate sunt chiar ale noastre. Specialiștii consideră că odată expuși la o informație falsă (și dacă suntem conștienți de asta), chiar dacă avem impresia că noi controlăm situația, că i-am blocat astfel efectele asupra emoțiilor, cogniților și comportamentelor noastre, putem fi deja contaminați psihologic. Soluția este să ne selectăm cu atenție sursele de informare.

Ingineria socială - instrument în cadrul războiului informațional

Așa cum am apreciat anterior, paradigma conflictelor militare se schimbă. În prezent, un stat democratic poate fi implicat într-un război chiar dacă starea aparentă este de pace. Acesta poate fi un război nimicitor, iar statul țintă să nu aprecieze corect dimensiunea atacurilor și să fie copleșit chiar și înainte de a realiza că este implicat într-un război. Și toate acestea fără a se utiliza forța kinetică (prezență obligatorie până acum în conflictele armate), ci doar prin diverse instrumente ale ingineriei sociale: prin manipulare strategică, prin influențarea populației și a conducătorilor și prin acțiuni cyber.

Autorul acestor tipuri de operațiuni poate fi o entitate de orice fel: un stat inamic, o țară neutră sau un stat aliat sau chiar o entitate non-statală, care are avantajul de a se exprima preponderent în spațiul virtual, sub anonimat, mediu unde este dificil de identificat sursa generatoare a agresiunii. Este un tip de război care favorizează atacatorul pentru că acesta se poate eschiva sub pragul de percepție al reacției unor state în alianță (ex. NATO) sau al unor organizații internaționale (ONU, OSCE), iar motivele agresiunii pot fi diverse: de a determina, de a controla sau de a altera decizia strategică sau politica internă și externă a statului țintă.

Astfel, analizând scopurile principale ale unui război (interese financiare, etnice, economice, politice, geostrategice) putem concluziona că pentru a exploata resursele unui stat, pentru a-l transforma în „piață de desfacere", pentru a-i impune un interes politic, există în prezent o serie de posibilități rafinate, cum ar fi recurgerea la acțiuni de inginerie socială în zona sau mediul de interes (intervenții sociale la nivel de individ sau grup), care sunt mult mai puțin costisitoare decât cucerirea teritoriului prin intermediul forței și mult mai eficiente din punct de vedere al remanenței efectelor.

Acest tip de acțiune este înlesnit și de tehnologia informațională de astăzi, care are posibilitatea eludării granițelor fizice și facilitează accesul unei entități agresoare, fie ea statală sau non-statală, la cetățenii statului țintă, cât și la instituțiile și serviciile acestora. Societatea digitizată de astăzi extinde și îmbunătățește posibilitatea achizițiilor de date și dă posibilitatea atât a apărării acestora, cât și a perturbării celor inamice. Viteza de comunicare mare, costul redus al acțiunilor de inginerie socială (dezinformare, influențare, manipulare strategică) și eficiența demonstrată în conflictele moderne generează o tendință de utilizare la scară tot mai mare a metodelor de atac „*cyber-cognitive*" și de „piratare a creierului", termen utilizat de autorul francez Lucien Cerise în cartea sa „Neuropirații"[8]. În aceste tipuri de conflicte, platformele social media și Big Data joacă un rol definitoriu, fiind o imensă sursă de informații pentru algoritmii care creează profile personale sau de grup în zonele sau mediile de interes.

Aplicațiile ingineriei sociale în conflictele militare nu trebuie asociate strict cu războiul informațional sau cu operațiile informaționale. Ingineria socială reprezintă esența unor conflicte de tip non-kinetic, din care fac parte și cele informaționale.

Prin utilizarea ingineriei sociale se pot crea realități alternative false, favorizate de libertățile specifice statelor democratice (libertatea cuvântului, comunicarea liberă a ideilor) și de tehnologia existentă. Se pot perverti realitatea și adevărul răstălmăcindu-le prin combinații care utilizează simultan acțiuni fizice și cognitive (PSYOPS, propagandă, dezinformare). În final, realitatea alternativă conduce la perceperea de către populația vizată a unui model predefinit.

În prezent, s-a generat un nou tip de conflict, preponderent informațional, sprijinit și de o dezvoltare fără precedent a tehnologiei informației și a științelor sociale. Se mai numește și Războiul 2.0[9]. (Afrem, 2019), denumire dată de caracterul digital al tehnologiei militare actuale,

și se sprijină pe teoria că războaiele nu se mai câștigă doar în tranșee, ci și în fața calculatorului prin intermediul tehnologiei informației și al „bătăliei creierelor". Acest lucru presupune folosirea ingineriilor sociale cum ar fi diversiunea, manipularea, dezinformarea, folosirea distorsiunii cognitive (erori de logică) și a deformării realității, precum și tehnici consacrate cum este „Fereastra Overton"[10] (un complex de manipulare socială în șase pași, dezvoltat de Joseph P. Overton, prin care o idee imposibil de acceptat într-o societate poate deveni lege personalizată). În acest fel, realitatea de zi cu zi poate fi „alterată" prin schimbarea opiniilor oamenilor cu ajutorul ingineriei sociale și a tehnologiei informației.

Conflictele de tip informațional sunt o formă de conflict specifică secolului al XXI-lea, un instrument eficient de descurajare de nivel strategic ce poate fi utilizat atât pe plan global, cât și în conflicte zonale în diferite zone de operații. Deși este un tip de conflict modern, problematica acestuia nu este nouă. De mii de ani sunt cunoscute efectele slăbirii puterii și a demoralizării instituțiilor de forță dintr-un stat; *„nu este nevoie să distrugi fizic inamicul, ci este suficient să îi distrugi voința de a lupta"* spunea Sun Tzu[11]. Războiul informațional este total diferit de cel clasic, el se desfășoară în cea mai mare parte prin acțiuni subversive, cu scopul slăbirii puterii prin demoralizarea populației și a personalului structurilor implicate în securitatea națională, prin distrugerea încrederii populației în acestea. Tehnicile înglobează în mod sinergic ingineria socială cu puterea și forțele armate disponibile. Odată cu revoluția tehnologică din domeniul comunicațiilor, din ultimul secol, războiul informațional a ajuns să fie considerat de gânditorii militari ca un tip de război distinct, la fel de important ca celelalte cunoscute de-a lungul Istoriei (terestru, aerian, maritim, spațial).

Măsuri de limitare a efectelor

În general, într-un război informațional măsurile ce se pot lua împotriva ingineriilor sociale sunt reduse. Societățile deschise au multe vulnerabilități, nu au o linie a frontului și limite în ceea ce privește regulile de angajare. În acest scop, este nevoie de un sistem funcțional de avertizare strategică care să-i permită statului să evite o astfel de situație și să cunoască din timp acțiunile ostile, în vederea reducerii efectelor.

Avertizarea strategică reprezintă una dintre cele mai eficiente măsuri pentru diminuarea sau stoparea efectului unor operațiuni din gama ingineriilor sociale de masă (manipulare strategică, influență, sabotaj, spionaj) care vizează distrugerea statului și, în același timp, reprezintă răspunsul optim pentru diminuarea sau stoparea efectului operațiilor mai sus enunțate. Aceasta se poate realiza numai în urma unei analize complexe, numită de specialiști „intelligence strategic"[12].

Războiul informațional este un tip de război care implică toate mediile sociale. Este nevoie, deci, ca pe lângă factorii decizionali populația să fie una dintre beneficiarele avertizării strategice. Aceasta trebuie să genereze o implicare activă a cetățenilor pentru sesizarea riscurilor și semnalarea acestora către autoritățile competente în vederea inițierii unor măsuri de contracarare a evoluției. În acest fel se va preveni degenerarea conflictelor într-o formă agravantă.

O altă măsură pe care un stat o poate lua constă în dezvoltarea unei culturi de securitate în societate. Cea mai eficientă apărare împotriva ingineriilor sociale dezvoltate într-un război informațional este conștientizarea implicațiilor sociale ale unei acțiuni ostile. Astfel, trebuie ajuns la nivelul în care o masă critică a populației unui stat să fie conștientă de riscurile și implicațiile la adresa sa și a societății din care face parte. Aceasta se poate realiza, în mod eficient, prin crearea unor seturi de norme și valori (popularizate în rândul cetățenilor) ce vor trebui să fie protejate și respectate, elaborate la nivel central prin politici publice.

Creșterea exponențială a fluxului informațional a pus problema identificării unor soluții pentru contracararea ingineriilor sociale promovate prin media, precum propaganda, dezinformarea și manipularea în masă a opiniei publice. În acest sens, la începutul secolului al XXI-lea a apărut noțiunea de *media literacy*[13] sau educație mediatică. Conform Institutului de

Leadership „Aspen Media", educația mediatică constă în formarea capacității de a accesa, analiza, evalua și crea media într-o varietate de forme. Cultura mediatică permite oamenilor să fie creatori și producători de mesaje mediatice, să înțeleagă fiecare tip de produs media, să permită dezvoltarea unei media independente. Cultura media este o extensie a culturii generale. Educația mediatică constituie una dintre soluțiile de contracarare a propagandei, a manipulării și a dezinformării pe termen lung. Ea trebuie să fie studiată în școli încă din clasele primare pentru ca fiecare dintre noi să ne putem transforma dintr-un consumator de mesaje media într-o persoană cu un simț critic ridicat, conștientă de potențialul de manipulare la care suntem expuși permanent prin diverse reclame. Deși educația mediatică este intens promovată în țările Uniunii Europene pentru importanța ei deosebită în educația tinerilor, în România ea nu este prezentă încă în programa școlară.

Ca măsură împotriva ingineriilor sociale desfășurate în cadrul unui război informațional poate fi și dezvoltarea gândirii critice în rândul populației României, prin introducerea acestui tip de gândire în educație la toate nivelurile (în state ca SUA a fost introdusă încă din anii '60). Și în acest sens România are de făcut pași importanți. În mod tradițional, în societatea românească de tip paternalist sunt utilizate în mod curent *gândirea dezideravă* (cu funcții psihologice, dar fără funcții de cunoaștere) sau *gândirea inautentică* de tip manipulativ-speculativ, „*adevărul este la mijloc*" fiind o expresie reprezentativă pentru societatea românească.

În cadrul unui conflict non-kinetic ca războiul informațional, câmpul de luptă poate fi reprezentat de platformele social media. Bazele militare pot fi considerate fabricile de troli și roboți (sau boți), componente automatizate de tip cyber ale ingineriei sociale, extrem de eficiente datorită ariei de răspândire nelimitată și a posibilităților de automatizare a acțiunilor.

Prin intermediul mass-media actuale și, implicit, a platformelor social-media specializate, în care predomină gândirea necritică, se pot manipula opiniile unui grup social (dar și ale indivizilor) și se pot genera confuzie, frustrări, derută, nesiguranță, comportamente impulsive sau chiar violente, manifestări specifice noii tipologii a războiului.

Prin diverse acțiuni de inginerie socială de masă, precum manipularea strategică, sabotaj, dezinformare sau propagandă, se poate realiza un bombardament informațional la nivel strategic cu scopul agresării identității colective (ce menține coeziunea la nivelul societății), cu efecte devastatoare, pe termen lung, pentru un stat. Ele generează, în plan ofensiv, multiple avantaje în raport cu soluțiile clasice militare, deoarece se evită pierderile materiale și de vieți omenești sau victimele colaterale. Statele democratice sunt vulnerabile la agresiunile (bombardamentele) informaționale în condițiile în care libertatea de exprimare dintr-o societate deschisă permite direcționarea cu ușurință a fluxurilor de mesaje către populație.

Prin aplicarea ingineriilor sociale de masă se poate diviza o societate prin afectarea identității, prin polarizare socială, prin falsificarea tradițiilor și a istoriei, cultura putând fi așadar o armă (în NATO existând deja conceptul de *culture intelligence* - CQ)[14].

Principalele instrumentele de sprijin înaintat ale manipulării strategice pot fi structurile de intelligence, care pot acționa anterior în vederea obținerii unor elementele de cunoaștere a statului țintă, necesare planificării operațiilor de influență. La polul opus, statul agresat, aflat în poziție defensivă, va încerca să se apere de astfel de agresiuni, dar va avea un consum mare de resurse doar pentru a limita efectele unor astfel de atacuri.

Încercările de influențare în masă ale unora față de alții au fost dintotdeauna o tendință a oamenilor. Aceste încercări se vor menține în continuare, iar în viitorul imediat vor avea un trend ascendent, atât în lumea civilă, cât și militară, deoarece oamenii politici, comercianții, militarii, managerii și alte categorii implicate în influențarea în masă caută permanent metode și soluții cât mai eficiente pentru a-și rezolva problemele mai bine, mai repede și cu costuri cât mai mici. Din această perspectivă, putem

concluziona că viitorul este al ingineriei sociale, capabile de a realiza aceste scopuri prin acțiuni cu remanență pe termen lung sau definitiv, prin manipulare, propagandă și influențare.

Uneori, pentru rezolvarea unor probleme se pot folosi aceleași premise care le-au generat sau, cum se mai spune, „*cui pe cui se scoate*". Astfel, agresiunile generate prin intermediul ingineriilor sociale se pot combate tot prin inginerie socială. În acest sens, pentru a proteja cetățenii împotriva agresiunii psihologice (propagandă, manipulare), pentru a crea o reziliență societală ridicată, statul trebuie să intervină cu elemente educaționale (ca introducerea gândirii critice în programele de învățământ) și psihologice bine gândite. De asemenea, o atitudine decisă în domeniile de expertiză ale fiecăruia, precum și identificarea și cultivarea valorilor sociale (respectul față de instituțiile statului, familie) scad posibilitatea de a fi manipulați.

Concluzii:

Este puțin probabil ca în viitorul apropiat marile puteri să își piardă supremația militară din punct de vedere al capabilităților kinetice, însă ele vor fi rămâne vulnerabile față de unele amenințări non-kinetice (prin poluare psihologică), cum ar fi cele de tipul ingineriilor sociale. În timp ce acțiunile militare clasice, de tip kinetic, vor continua să influențeze, în mare măsură, capabilitățile inamicului, acțiunile militare non-kinetice bazate pe inginerii sociale vor influența mult mai eficient comportamentul actorilor, respectiv opiniile și starea populației, ale liderilor politici și militari dintr-o zonă de interes.

Decidenții politico-militari ar trebui, prin urmare, să se concentreze nu numai pe contracararea acțiunilor de tip kinetic, dar și pe elaborarea unor strategii care să genereze sau să le contracareze și pe cele non-kinetice pentru că în acest secol, în orice tip de conflict militar modern, „bombardamentul artileriei" de la începutul bătăliei este desfășurat prin intermediul ingineriilor sociale de masă, implementate prin intermediul tehnologiei digitale a informațiilor.

În prezent, ingineria socială - domeniu multidisciplinar – nu se studiază în mod special în România, deși este unul dintre vectorii generatori ai schimbării sociale în toate mediile. Iată de ce este important să introducem în cadrul tuturor formelor de învățământ militare cursuri de dezvoltare a gândirii critice și de educație mediatică în rândul elevilor și al studenților, în vederea reducerii vulnerabilității cadrelor militare în fața poluării psihologice desfășurate prin intermediul tehnologiei digitale.

În cazul învățământului în domeniul informații pentru apărare, cunoașterea și aprofundarea complexului ingineriei sociale, a aplicațiilor sociale ale acesteia, sunt necesare pentru dezvoltarea personală a viitorilor specialiști din domeniul intelligence care vor acționa în medii operaționale diverse (fizice și virtuale), unde adaptabilitatea și reziliența sunt calități specifice domeniului. Este necesar, de asemenea, ca viitorii specialiști și lideri din acest domeniu să cunoască specificul acțiunilor de inginerie socială în scopul identificării și contracarării unor acțiuni ostile ce utilizează un astfel de vector purtător.

Toate acestea se pot realiza prin proiectarea unei curricule care să cuprindă noi unități de curs cu referire la ingineria socială, precum și la domenii conexe precum sociologia și psihologia aplicată, științele cognitive, neuroștiințele sau neuromarketing-ul.

Bibliografie:

1. ROSTÁS, Zoltán (2000), *Monografia ca utopie. Interviuri cu Henri H. Stahl (1985-1987)*, Editura Paideia.
2. KENT, Sherman (1949), *Strategic Intelligence for American Policy*, Princeton Legacy Library.
3. DAVID, Daniel (2015), *Psihologia poporului român. Profilul psihologic al românilor într-o monografie cognitiv-experimentală*, București, Editura Polirom.
4. LE BON, Gustave (2002), *Psihologia mulțimii*. București: Editura Antet.
5. CIALDINI, Robert (1993), *6 Weapons of influence*, București: Editura RAO.
6. HENTEA, Cătălin (2008), *Noile haine ale propagandei.* București, Editura Paralela 45.
7. ZAMFIR, Cătălin, Vlăsceanu Lazăr (1998), *Dicționar de sociologie*, București, Editura Babel.

8. SHERR, James (2015), *The New East-West Discord. Russian Objectives, Western Interests,* Clingedael Report, Netherlands Institute of International Relations.
9. PELTIER Thomas R. (2006), *Social Engineering: Concepts and Solutions.*
10. AFREM, Alina Virginia (13 martie 2019). Războiul 2.0., Revista Intelligence.
11. DAVID, Daniel (2017), *Contaminarea psiho-logică: Manipularea și contaminarea mentală*, Revista Sinteza.
12. CERISE, Lucien (2018), *Neuro-pirații, reflecții despre ingineria socială*, București, Editura Mica Valahie.
13. SUN TZU (2012), *Arta războiului*, București: Editura Libris.
14. HOBBS, Renee (2010), *Digital and Media Literacy: A Plan of Action ,* Aspen Institute.
15. CLINE, E. Lawrence. (2017), *From Cultural Intelligence to Cultural Understanding: A Modest Proposal*, Small Wars Journal.
16. https://intelligence.sri.ro/
17. http://copainsdavant.linternaute.com/e/iris-institut-regional-d-ingenierie-sociale-339808
18. https://irtshdf.fr/irts/
19. https://smallwarsjournal.com/jrnl/art/from-cultural-intelligence-to-cultural-understanding-a-modest-proposal
20. https://www.revistasinteza.ro/contaminarea-psihologica-manipulare-si-contaminare-mentala
21. https://www.mackinac.org/OvertonWindow

[1]Lafon, Patrick, *Virtue in Political Life:Yves Simon's Political Philosophy for Our Times,* 2017.
[2]Emile Cheysson (1836-1910), inginer francez, promotor al ingineriei sociale în politicile publice.
[3] Zamfir, Cătălin, Vlăsceanu Lazăr (1998), Dicționar de sociologie, București, Editura Babel.
[4]Zoltán Rostás, *Monografia ca utopie. Interviuri cu Henri H. Stahl (1985-1987)*, Editura Paideia (2000).
[5]http://copainsdavant.linternaute.com/e/iris-institut-regional-d-ingenierie-sociale-339808 - accesat la 20.07.2021.
[6]https://irtshdf.fr/irts/ - accesat la 20.07.2021.
[7]David Daniel, „Contaminarea psihologică: Manipulare și contaminare mentală", *Revista Sinteza*, 2017, disponibil la URL: https://www.revistasinteza.ro/contaminarea-psihologica-manipulare-si-contaminare-mentala - accesat la 20.07.2021.
[8]Lucien Cerise, *Neuro-pirații, reflecții despre ingineria socială,* 2018.
[9]Alina Virginia Afrem, „Războiul 2.0.", *Revista Intelligence*,13 martie 2019.
[10]Mackinac Center for Public Policy, disponibil la URL: https://www.mackinac.org/OvertonWindow - accesat la 23.07.2021.
[11]Sun Tzu, *Arta războiului,* Ed. Libris, 2012, București, p.2.
[12]Termenul de „intelligence strategic" a fost lansat de Sherman Kent în lucrarea *Strategic Intelligence for American Policy* – 1949, fiind definit drept „cunoașterea pe care decidenții politici și militari trebuie să o posede pentru a asigura bunăstarea națională".
[13]Renee Hobbs, *Digital and Media Literacy: A Plan of Action ,* Aspen Institute*,* 2010*,* disponibil la URL: http://aspeninstitute.org - accesat la 19.07.2021.
[14]Lawrence E. Cline, „From Cultural Intelligence to Cultural Understanding: A Modest Proposal*"*, *Small Wars Journal*, diponibil la URL: https://smallwarsjournal.com/jrnl/art/from-cultural-intelligence-to-cultural-understanding-a-modest-proposal - accesat la 23.07.2021.

ASIGURAREA SECURITĂȚII JURIDICE ÎN CONTEXTUL EVOLUȚIEI AMENINȚĂRILOR CIBERNETICE

Sorina Ana MANEA*

Abstract

Providing judicial security, key condition in the rule of law, is presently enhanced by the dynamics and complexity of the cyberspace impact. When talking about cyber threats, even though the issue is generally approached from the perspective of attacks upon network systems and IT&C systems, complex cyber threats may also be generated by the law system. Capture and processing of personal data are carried out through a process called Big data, that provides conversion of the daily life into a data flow. The outcome is a new way of social life, based on continuous tracking and which offers unprecedented opportunities for social discrimination and behavioral influence. Through the following paper, we endeavour submitting to a debate ways of providing a stable environment created according to the law system, in the context of the current cyber threats.

Keywords*: judicial security; cyber security; national defence and security.*

Supremația legii este consacrată prin articolul 1, alineatul 5 din Constituție. Însemnătatea acestui concept fundamental în practică este că, pe lângă respectarea legii de către întreaga populație, instituțiile Statului au, de asemenea, obligația respectării legii, iar dintre toate instituțiile statului autoritatea legiuitoare este cea căreia îi incumbă cel mai stringent necesitatea îndeplinirii acestei obligații, în sensul că activitatea de legiferare trebuie să se realizeze în limitele și în conformitate cu legea fundamentală.

Parlamentul fiind unica autoritate deținătoare a competenței de legiferare, ca rezultat al îndeplinirii puterii legislative, are și o obligație suplimentară și anume să asigure calitatea legii, întrucât aceasta trebuie cunoscută și înțeleasă de subiecții săi. Necesitatea cunoașterii și înțelegerii legii, ca urmare a formulării acesteia de o manieră clară, precisă și previzibilă, reprezintă modalitatea de respectare a principiului securității juridice din perspectiva destinatarilor ei.

Securitatea juridică, ca principiu, este consacrată la nivelul jurisprudenței și presupune obligativitatea ca legea să asigure destinatarilor ei abilitatea de a-și adapta comportamentul cu certitudine și, de asemenea, să protejeze subiecții de drept împotriva folosirii arbitrare a puterii statului.

Principiul securităţii juridice exprimă faptul că cetăţenii trebuie protejaţi împotriva incertitudinii și nesiguranței generate de normele juridice și interpretarea neunitară a acestora *„contra unui pericol care vine chiar din partea dreptului, contra unei insecurităţi pe care a creat-o dreptul sau pe care acesta riscă s-o creeze"*[1].

Curtea Europeană a Drepturilor Omului a subliniat importanţa asigurării accesibilităţii şi previzibilităţii legii, statuând că *„nu poate fi considerată «lege» decât o normă enunţată cu suficientă precizie, pentru a permite individului să-şi regleze conduita. Individul trebuie să fie în măsură să prevadă consecinţele ce pot*

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

decurge dintr-un act determinat"[2]; *„o normă este previzibilă numai atunci când este redactată cu suficientă precizie, în aşa fel încât să permită oricărei persoane – care, la nevoie poate apela la consultanţă de specialitate – să îşi corecteze conduita"*[3]; *„în special, o normă este previzibilă atunci când oferă o anume garanţie contra atingerilor arbitrare ale puterii publice"*[4].

Ca urmare a consacrării principiului accesibilității și previzibilității în dreptul comunitar, și implicit în temeiul art. 11 din Constituție, a fost dezvoltat şi principiul încrederii legitime. Potrivit jurisprudenţei Curţii de Justiţie a Uniunii Europene[5], principiul încrederii legitime impune ca legislaţia să fie clară şi previzibilă, unitară şi coerentă și impune limitarea posibilităţilor de modificare a normelor juridice[6].

Printre altele, principiul securității juridice este strâns legat de asigurarea interpretării unitare a legii. În acest sens, în cauza Păduraru împotriva României 2005, Curtea Europeană a Drepturilor Omului a statuat că „în lipsa unui mecanism care să asigure coerenţa practicii instanţelor naţionale, asemenea divergenţe profunde de jurisprudenţă, ce persistă în timp şi ţin de un domeniu ce prezintă un mare interes social, sunt de natură să dea naştere unei incertitudini permanente (mutatis mutandis, Sovtransavto Holding, citată mai sus, § 97) şi să diminueze încrederea publicului în sistemul judiciar, care reprezintă una dintre componentele fundamentale ale statului de drept"[7].

Menținerea securității juridice și a încrederii destinatarilor legii în sistemul de drept se realizează și prin instituirea de garanții contra atingerilor provocate de folosirea arbitrară a puterii publice, o astfel de garanție fiind controlul democratic asupra autorității executive exercitate de Parlament.

Relevanța principiului securității juridice, precum și a principiilor corelative devine și mai evidentă în contextul în care domeniul cibernetic este astăzi o componentă vitală a societății. Până în prezent, România nu dispune de o legislație sistematică în domeniul cibernetic, care să fie corelată corespunzător cu legislația în domeniul apărării țării și securității naționale, deși Curtea Constituțională a României a reținut că securitatea cibernetică este intrinsec legată de apărarea țării și securitatea națională[8].

Cu toate că în prezent, din perspectiva protecției infrastructurii sistemelor informatice, precum și a instituțiilor de drept public sau privat competente să implementeze politici de securitate, în sensul protocoalelor informatice de menținere a securității rețelelor și sistemelor informatice, sunt aplicabile prevederile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, care transpune în totalitate Directiva (UE) 2016/1.148[9], garanțiile oferite cetățenilor împotriva folosirii arbitrare a puterii statului sunt greu de identificat. Astfel, controlul activității autorității naționale în domeniul securității rețelelor și sistemelor informatice, CERT-RO este realizat de Consiliul Suprem de Apărare a Țării[10], în calitatea sa de organizator și coordonator al activităților care privesc apărarea țării și securitatea națională.

Însă, având în vedere natura constituțională a domeniului securității naționale, precum și impactul pe care un eventual eșec în asigurarea securității cibernetice îl poate avea asupra securității naționale, eventualitatea controlului democratic prin puterea legislativă pare mai adecvată. În același sens și Curtea Constituțională a României[11] a reținut că Parlamentul European a precizat în Amendamentul 10 a) că „*având în vedere diferențele dintre structurile naționale de guvernanță și pentru a menține mecanismele sectoriale deja existente sau organismele de supraveghere și de reglementare ale Uniunii și a evita suprapunerile, statele membre ar trebui să dispună de competența de a desemna mai multe autorități naționale competente responsabile cu îndeplinirea atribuțiilor legate de securitatea rețelelor și a sistemelor informatice ale operatorilor de piață vizați de prezenta directivă. Cu toate acestea, pentru a asigura o bună cooperare și comunicare transfrontalieră, este necesar ca fiecare stat membru să desemneze un singur punct unic de contact responsabil pentru cooperarea transfrontalieră la nivelul Uniunii, fără a aduce atingere mecanismelor*

de reglementare sectoriale. În cazul în care structura sa constituțională sau alte prevederi o impun, un stat membru ar trebui să fie în măsură să desemneze o singură autoritate care să îndeplinească atribuțiile autorității competente și ale punctului unic de contact. Autoritățile competente și punctele unice de contact ar trebui să fie organisme civile, care să funcționeze integral pe baza controlului democratic, și nu ar trebui să desfășoare activități în domeniul informațiilor, al aplicării legii sau al apărării și nici să fie legate organizațional în vreun fel de organismele active în aceste domenii."[12].

Observațiile Parlamentului European referitoare la separarea autorităților competente în domeniul securității cibernetice și cele din domeniul informațiilor, al aplicării legii sau al apărării sunt semnificative mai ales în contextul actual al dezbaterii privind afectarea libertăților fundamentale prin măsuri restrictive dispuse în temeiul unor norme legale echivoce. În acest sens se constată că, în ultimii ani, Curtea Constituțională a dezvoltat o bogată jurisprudență în materia accesului, prelucrării și stocării de către structurile de forță ale statului de date și informații protejate prin art. 26 și 53 din Constituția României. Acest intens proces de control constituțional a generat modificări semnificative în legislația din domeniul apărării țării și securității naționale, ceea ce denotă că legiuitorul nu a acordat atenția cuvenită calității actelor normative și, prin urmare, putem spune că a generat inconsecvențe în respectarea principiului securității juridice și, mai ales, a principiului încrederii legitime.

De asemenea, de respectarea principiului securității legitime sunt legate și aspectele referitoare la prelucrarea și stocarea datelor de trafic referitoare la abonați și la utilizatori de către furnizorul unei rețele publice de comunicații electronice sau de către furnizorul unui serviciu de comunicații electronice destinat publicului. Astfel, în 6 octombrie 2020, Curtea de Justiție a Uniunii Europene (CJUE) s-a pronunțat asupra faptului că Directiva privind confidențialitatea electronică[13] nu permite statelor membre UE să adopte legislație menită să restrângă domeniul de aplicare a obligațiilor sale de confidențialitate, cu excepția cazului în care sunt respectate principiile generale ale dreptului UE, în special principiul proporționalității, precum și drepturile fundamentale prevăzute de Carta drepturilor fundamentale a Uniunii Europene. Cauzele deduse judecății privesc Regatul Unit, Franța și Belgia, state a căror legislație prevedea obligativitatea pentru furnizorii de servicii de comunicații electronice să transmită autorităților publice datele despre trafic și locație ale persoanelor fizice sau să păstreze aceste date într-un mod general și nediscriminatoriu, precum și stocarea acestor date pentru diferite intervale de timp. Motivul pentru o asemenea prevedere în legislația statelor menționate îl constituia asigurarea securității naționale. CJUE a stabilit, însă, că astfel de legi intră în domeniul de aplicare al directivei sus-menționate, reținând că *„deși revine statelor membre să își definească interesele esențiale de securitate și să adopte măsuri adecvate pentru a le asigura interne și externe securitatea națională, simplul fapt că a fost luată o măsură națională în scopul protejării securității naționale nu poate face ca legislația UE să nu fie aplicabilă și să scutească statele membre de obligația lor de a respecta această lege"*[14].

CJUE a stabilit limitări în ceea ce privește capacitatea statelor membre de a restrânge domeniul de aplicare a directivei, precizând*: „trebuie avut în vedere faptul că protecția dreptului fundamental la viață privată impune […] ca derogările și limitările privind protecția datelor cu caracter personal trebuie să fie aplicate numai în măsura în care sunt strict necesare",* directiva excluzând dispozițiile naționale care impun furnizorilor să păstreze date generale și nediscriminatorii privind traficul și localizarea ca măsură preventivă pentru protejarea securității naționale și combaterea criminalității.

Cu toate acestea, CJUE a prevăzut, de asemenea, mai multe situații în care statele membre pot deroga de la cerințele generale de confidențialitate ale directivei în scopul protejării securității naționale, combaterii criminalității grave și prevenirii amenințărilor grave împotriva

securității publice, cu îndeplinirea următoarelor condiții: să prevadă aceste derogări clar și precis; să fie implementate cerințe materiale și procedurale; și persoanele în cauză au garanții efective împotriva oricărui abuz. În special, CJUE a autorizat ordinele care impun furnizorilor să întrețină păstrarea generală și nediscriminatorie a datelor privind traficul și localizarea, precum și stocarea țintită în cazul în care un stat membru se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește a fi autentică, prezentă sau previzibilă, atâta timp cât măsura este supusă controlului efectiv al unei instanțe sau organism administrativ independent și dispusă pentru o perioadă de timp considerată strict necesară.

În România, legea prevede că datele de trafic referitoare la abonați și la utilizatori stocate de către furnizorul unei rețele publice de comunicații electronice sau de către furnizorul unui serviciu de comunicații electronice destinat publicului, trebuie să fie șterse ori transformate în date anonime, atunci când nu mai sunt necesare la transmiterea unei comunicări, dar nu mai târziu de 3 ani de la data efectuării comunicării[15].

Prin urmare, elementele pe care se bazează principiul securității juridice sunt certitudinea şi predictibilitatea legii. Acestea sunt necesare pentru a menține încrederea legitimă a cetățenilor în sistemul de drept și, în subsidiar, în autoritățile statului, fie ele reprezentante ale puterii legislative, executive sau judecătorești. Se poate spune deci, că securitatea juridică este parte intrinsecă a securităţii sociale, care denotă raporturile dinamice și constitutive dintre cetăţean şi puterile statului[16].

Apreciem că respectarea principiului securității juridice este o cerință pentru protejarea securității sociale, componentă a securității naționale.

Bibliografie:

1. CONSTANTINESCU, Mihai; Iorgovan, Antonie; Muraru, Ioan; Tănăsescu, E.S., *Constituția României revizuită - comentarii și explicații,* București, 2004, Editura All Beck;
2. DIMA, B., *Conflictul între palate. Raporturile de putere dintre Parlament, Guvern și Președinte în România post-comunistă,* București, 2014, Editura Hamangiu;
3. DUȚU, P., Sarcinschi, A., Bogzeanu, A., *Apărarea Națională, între viziune și realitate, la început de mileniu,* București, 2013, Editura Universității Naționale de Apărare „Carol I";
4. IORGOVAN, A., *Tratat de drept administrativ*, vol. 2, București, 1996, Editura Nemira;
5. MÂȚĂ, D. C., *Securitatea națională - concept, reglementare, mijloace de ocrotire,* București, 2016, Editura Hamangiu;
6. MOȚIU, E. I., *Autoritățile administrative autonome din domeniul siguranței naționale și al mediatizării informațiilor,* București, 2010, Editura C.H. Beck;
7. MURARU, I, *Drept Constituțional și Instituții Politice,* București, 1998, Editura Actami;
8. PANC, D., *Securitatea cibernetică la nivel național și internațional. Instrumente normative și instituționale,* București, 2017, Editura Hamangiu;
9. PREDESCU, I., & Safta, M., *Principiul securității juridice, fundament al statului de drept. Repere jurisprudențiale*. Disponibil la https://www.ccr.ro/wp-content/uploads/2021/01/predescu.pdf.

[1]Artin Sarchizian, Principiul securității juridice, 14.04.2019, disponibil la http://www.drepturile-omului.eu/jurnalul/jurnalul-drepturilor-omului-nr-12019/params/post/1768664/principiul-securitatii-juridice, ultima accesare la 31.01.2021.

[2] Hotărârea CEDO Sunday Times împotriva Regatul Unit al Marii Britanii şi Irlandei de Nord, 1979.

[3] Hotărârea CEDO Rotaru împotriva României, 2000.

[4] Hotărârea CEDO Damman împotriva Elveţiei, 2005.

[5] Hotărârea Curții de Justiție a Uniunii Europene în cauza Faccini Dori v Recreb Srl, 1994, paragraful 21 și urm., disponibil la https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:61992CJ0091&from=EN#Footnote*, ultima accesare 02.02.2021; Foto-Frost v Hauptzollant Lübeck.Ost, 198722, paragraful 9, disponbil la https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:61985CJ0314&from=EN, ultima accesare la 02.02.2021.

[6] Hotărârea Curții de Justiție a Uniunii Europene din 24.03.2011, ISD Polska și alții împotriva Comisiei Europene, Cauza C-369/09 P. „orice particular are dreptul să se prevaleze de principiul protecției încrederii legitime în cazul în care se află într-o situație din care reiese că administrația comunitară, prin furnizarea unor asigurări precise, l-a

determinat să nutrească speranțe întemeiate (Hotărârea din 16 decembrie 1987, Delauche/Comisia, 111/86, Rec., p.5345, punctul 24, Hotărârea din 25 mai 2000, Kögler/Curtea de Justiție, C82/98 P, Rec., p.I-3855, punctul 33, precum și Hotărârea din 22 iunie 2006, Belgia și Forum 187/Comisia, C-182/03 și C-217/03, Rec., p.I5479, punctul 147). În plus, asigurările date trebuie să fie conforme cu normele aplicabile (a se vedea în acest sens Hotărârea din 20 iunie 1985, Pauvert/Curtea de Conturi, 228/84, Rec., p.1969, punctele 14 și 15, precum și Hotărârea din 6 februarie 1986, Vlachou/Curtea de Conturi, 162/84, Rec., p.481, punctul 6)", disponibil la https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62009CJ0369, ultima accesare 01.02.2021.

[7] Hotărârea CEDO Păduraru împotriva României 2005, paragraful 99 și urm.

[8] Decizia Curții Constituționale nr. 455/2018 referitoare la admiterea obiecției de neconstituționalitate a dispozițiilor Legii privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și Decizia Curții Constituționale nr. 17/2015 asupra admiterii obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României.

[9] Directiva Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, publicată în Jurnalul Oficial al Uniunii Europene, seria L, nr. 194 din 19 iulie 2016.

[10] Hotărârea Guvernului nr. 494 din 11 mai 2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.

[11] Decizia Curții Constituționale nr. 17/2015 asupra admiterii obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României.

[12] Raportul PE 514.882v02-00 din 12.02.2014 referitor la propunerea de directivă a Parlamentului European și a Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune (COM(2013)0048 - C7-0035/2013 - 2013/0027(COD) disponibil la https://www.europarl.europa.eu/doceo/document/A-7-2014-0103_RO.html?redirect, ultima accesare 02.02.2021.

[13]Articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009.

[14]Disponibilă la http://curia.europa.eu/juris/document/document_print.jsf?docid=232084&text=&dir=&doclang=RO&part=1&occ=first&mode=DOC&pageIndex=0&cid=5875047#Footnote*, ultima accesare 03.02.2021.

[15]Art. 5 din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

[16]S. Frolu, „Securitatea juridică în paradigma securităţii naţionale. Consideraţii şi determinări conceptuale", în *Echilibrul de putere şi mediul de securitate,* Sesiunea anuală de comunicări ştiinţifice cu participare internaţională, din 17-18 noiembrie 2011, Bucureşti, Ed. Universităţii Naţionale de Apărare „Carol I", 2011, pp. 185-198.

IMPLICAȚIILE TEHNOLOGIILOR CUANTICE ÎN SECURIZAREA INFORMAȚIILOR

Bogdan-Silviu FĂLTICEANU*

Abstract

Quantum computer technology and quantum key distribution are two disruptive technologies in their first stages of research and development. Their impact on information security in general and cryptography in special is still to be evaluated depending on the speed of development, new breakthrough in algorithmic, protocols and quantum processing technology. From Cesar's code to Enigma and Quantum Key Distribution humanity always tried to gather and share information in a secure way, without being decrypted or intercepted. In this incipient phase of quantum era it may seem this is the best solution so far, but as always history will tell.

Keywords*: quantum computing, encryption, quantum key distribution, qubit.*

Introducere

În ultimele decenii ale secolului al XX-lea oamenii de știință au căutat combinarea a două teorii extrem de influente și revoluționare: teoria informației și mecanica cuantică. Succesul lor a dus la o nouă viziune asupra calculului și informației. Această nouă viziune, teoria informației cuantice, a schimbat pentru totdeauna modul în care s-au gândit calculele, informațiile și conexiunile lor cu fizica și a inspirat noi aplicații, inclusiv algoritmi și protocoale extrem de diferite.

Până de curând, științele informației au fost ferm înrădăcinate în mecanica clasică. De exemplu, mașina Turing este un model mecanic care se comportă conform principiilor mecanice pur clasice. Mecanica cuantică însă a jucat un rol din ce în ce mai mare în dezvoltarea de dispozitive de calcul noi și mai eficiente. Până în anii 90, influența mecanicii cuantice în domeniul teoriei informaţiei a rămas scăzută, manifestându-se preponderent la nivel teoretic in diferite lucrări ştiinţifice. În două decade de la crearea primului calculator cuantic, în anul 1998, la Oxford, care avea o putere de procesare de doar 2 qubits, puterea de procesare a crescut de 38 de ori, ajungând la 76 de qubits[1] în decembrie 2020. Conform declaraţiei directorului de cercetare de la IBM, până în anul 2023 compania va crea un calculator cuantic de 1000 de qbiti, iar planul pe 10 ani de cercetare al companiei Google include crearea unui sistem de 1 milion de qubits[2]. Craig Gidney şi Martin Eker demonstrează că unui sistem cuantic de 20 de milioane de qubiti i-ar trebui doar 8 ore de calcul pentru a decripta o cheie RSA de 2048 biti[3]. Considerând plaja largă de utilizare a acestei metode de criptare, de la identitatea digitală, semnătura electronică şi până la criptarea datelor 3DSecure în domeniul eCommerce[4], precum şi creşterea exponenţială a puterii de calcul în domeniul tehnologiilor cuantice, putem argumenta tendinţe cu impact asupra securităţii informaţiei.

Maşina Turing - o tehnologie disruptivă în 1936

În cel de-al Doilea Război Mondial, forțele naziste știau că transmiterea comunicărilor secrete fără posibilitatea de decriptare era cheia dominării lumii. Tehnologia lor premiată a fost mașina Enigma, un dispozitiv electromecanic de criptare care a permis diviziilor de tancuri

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

germane, ambasadelor și chiar submarinelor să trimită mesaje radio criptate. Ei au crezut că sistemul lor este nedecriptabil. Enigma avea o cheie de 67 de biti sau 2^{67} posibilităţi de configurare.

Cantitatea enormă de posibilităţi de configurare părea imposibil de decriptat, până când un tânăr matematician britanic, numit Alan Turing, a creat maşina Turing. Profitând de anumite greşeli ale forțelor naziste, precum transmiterea vremii la o oră fixă, începerea transmisiei cu acelaşi cuvânt şi de faptul că literele folosite pentru setarea rotoarelor maşinii nu puteau fi criptate, Marea Britanie a reuşit decriptarea codurilor secrete ale Germaniei, fapt care a reprezentat un factor crucial în victoria Aliaților în cel de-al Doilea război Mondial.

Privind către timpurile actuale, în anul 2017 o echipă de cercetători de la compania de dezvoltare a inteligenței artificiale „Enigma Pattern" a reușit să decripteze comunicările mașinii Enigma în doar 10 minute, folosind 2000 de servere în cloud, bazându-se pe analiza lexicologică a limbii germane și folosirea unui atac de tip dicţionar[5].

De-a lungul istoriei recente a tehnologiei informației, au existat numeroşi algoritmi precum SHA-1, DES, RSA 512 etc., care, la fel ca maşina Enigma, au fost consideraţi la momentul creării a fi aproape imposibil de decriptat, însă de multe ori au apărut noi metode de calcul, tehnologii, sau tehnici care au reuşit „imposibilul".

Evoluţia puterii de procesare clasice versus evoluţia puterii de procesare cuantică

Având în vedere procesualitatea transformărilor din domeniile emergente şi disruptive, vom realiza o scurtă analiză comparativă între evoluţia primilor 24 de ani a puterii de procesare a sistemelor informatice clasice și evoluţia tehnologiilor de calcul cuantic.

Precizia aparent de neclintit a legii lui Moore - care afirmă că viteza computerelor, măsurată prin numărul de tranzistoare care pot fi plasate pe un singur cip, se va dubla în fiecare an sau doi - a fost creditată ca fiind motorul revoluției electronice și este considerată primul exemplu de traiectorie tehnologică auto-împlinită. Putem vorbi de efectul acestei legi abia după primele două-trei decade de la inventarea tranzistorului şi a fost posibilă datorită inovaţiilor apărute, precum circuitul integrat, semiconductoarele metal-oxid etc. Echivalentul acestei legi în domeniul tehnologiei calculatoarelor cuantice nu există, deocamdată, din cauza perioadei relativ recente de creare a primului qubit (1998), însă putem afirma că odată cu descoperirea de noi inovaţii critice şi găsirea unor utilizări pe scară largă va urma o creştere accelerată a acestui domeniu.

În anul 1947, William Shockley, John Bardeen și Walter Brattain, de la Laboratoarele Bell, inventează tranzistorul. Cei trei cercetători au descoperit cum să producă un întrerupător electric cu materiale solide și fără a fi nevoie de vid. După 11 de ani de la inventarea tehnologiei de bază - tranzistorul, Jack Kilby și Robert Noyce dezvăluie în anul 1958 circuitul integrat, cunoscut sub numele de cip, iar domeniul tehnologiei informaţiei încă nu ajunsese la nivel de utilizator casnic. Abia peste 16 ani de la inventarea cipului şi la peste 27 de ani de la inventarea tranzistorului, Douglas Engelbart prezintă un prototip al computerului modern, cu un mouse și o interfață grafică cu utilizatorul (GUI). Aceasta marchează evoluția computerului de la o mașină specializată pentru oamenii de știință și matematicieni la o tehnologie mai accesibilă publicului larg.

Echivalentul inventării tranzistorului la nivel de domeniu cuantic - qubit-ul a avut loc în anul 1995 la Institutul Național de Standarde și Tehnologie și Institutul de Tehnologie din California, iar crearea propriu-zisă, în condiţii de laborator, realizându-se în 1998. Pentru următorii 20 de ani domeniul a reprezentat interes doar la nivel de cercetare, puterea de procesare a calculatoarelor cuantice crescând de 36 de ori, ajungând în anul 2020 la 76 de qubits[6].

Similar cu evoluția sistemelor de calcul bazate pe tehnologia fizicii clasice, la 25 de ani de la apariția tehnologiei a fost creat şi primul computer cuantic destinat publicului larg. SpinQ Gemini este un computer cuantic de birou comercial conceput și fabricat de SpinQ Technology. Produsul de primă generație cu doi qubits a fost lansat în ianuarie 2020. Hardware-

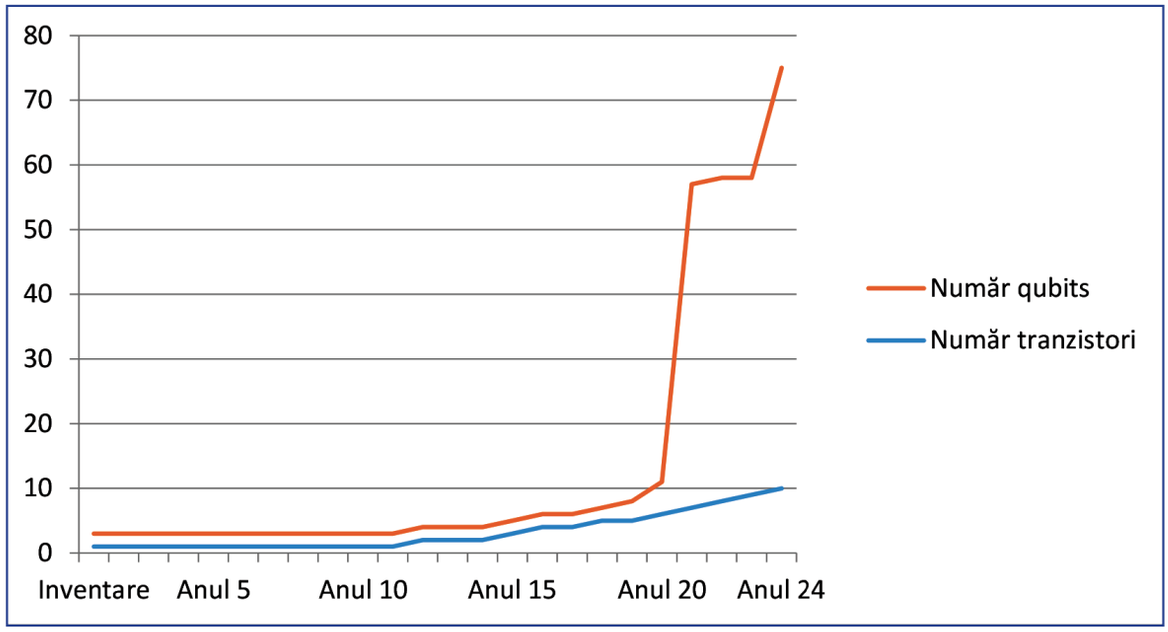


Fig 1. Analiza comparativă a evoluţiei puterii de procesare în primii 24 de ani de la crearea elementelor de bază a celor două tehnologii: qubit vs tranzistor.

ul se bazează pe spectrometru RMN, cu magneți permanenți care furnizează câmp magnetic de 1 T[7]. La nici un an diferenţă se anunţă lansarea celei de-a doua versiuni, cu o putere dublă, în al doilea trimestru al anului 2021.

Putem observa o similaritate între evoluția în timp a celor două tehnologii. Dacă în sistemele clasice primii 24 de ani de cercetare dezvoltare au reuşit să producă o densitate de 10 tranzistori per chip, în sistemele cuantice evoluţia puterii de procesare pare a avea un ritm mai accelerat de atât, ajungând la 76 qubiti în acelaşi interval de timp de la crearea elementului de bază al tehnologiei. Ca în orice domeniu disruptiv, previziunile evoluţiei sunt extrem de greu de anticipat ca urmare a avansului tehnologic sau apariției unei „lebede negre" în domeniul cercetării, care poate stagna sau dimpotrivă accelera rapid dezvoltarea.

După cum putem observa, în contextul evoluțiilor din primii 24 de ani de la apariția tranzistorului, nu se putea preconiza explozia ce avea să urmeze datorită dezvoltării unei noi tehnologii a microcipurilor IBM. Probabil discursul în jurul acestei problematici era la fel de scăzut precum discursul de astăzi în jurul tehnologiilor cuantice. Datele pe care le avem până în acest moment despre evoluţia cercetării în domeniul calculatoarelor cuantice demonstrează clar o curbă accelerată de dezvoltare, mult mai rapidă decât cea a revoluţiei tehnologiei calculatoarelor clasice. Menţinerea, accelerarea sau stagnarea acestui trend depinde, în mare măsură, de rezultatele activităţilor de cercetare-dezvoltare şi de interesul organizaţiilor sau naţiunilor în finanțarea acestui domeniu.

Considerații asupra celor mai utilizate metode de criptare a informațiilor

Principalii algoritmi de criptare a informațiilor existenți astăzi, sunt: Advanced Encryption Standard (AES), Triple Data Encryption Standard (Triple DES), Rivest-Shamir-Adleman (RSA)[8].

Advanced Encryption Standard (AES) este algoritmul standard utilizat de guvernul Statelor Unite, precum și de multe alte organizații. Deși extrem de eficient în forma de 128 de biți, AES folosește și chei de 192 și 256 de biți în scopuri de criptare foarte solicitante. AES este considerat, pe scară largă, invulnerabil la toate atacurile, cu excepția forței brute. Mulți experți în securitatea Internetului consideră că AES va fi, în cele din urmă, considerat standardul de bază pentru criptarea datelor din sectorul privat.

Triple DES este succesorul algoritmului original Data Encryption Standard (DES), creat ca răspuns la hackerii care au aflat cum să decripteze DES. Bazat pe o criptare simetrică, a fost cel mai utilizat algoritm simetric din industrie, deși este

treptat eliminat. TripleDES aplică algoritmul DES de trei ori la fiecare bloc de date și este utilizat, în mod obișnuit, pentru a cripta parolele UNIX și PIN-urile ATM.

Rivest-Shamir-Adleman (RSA) este un algoritm de criptare asimetrică care elimină factorizarea produsului a două numere prime mari. Numai un utilizator cu cunoștințe despre aceste două numere poate decoda mesajul cu succes. Semnăturile digitale utilizează de obicei RSA, dar algoritmul încetinește atunci când criptează volume mari de date.

Algoritmii simetrici de cheie publică utilizați astăzi se bazează pe două probleme matematice, factorizarea mai sus menționată a numerelor mari (de exemplu, RSA) și calculul logaritmic discret. Ambele au o structură matematică similară și pot fi sparte cu algoritmul lui Shor[9]. Algoritmi recenți, pe baza curbelor eliptice (cum ar fi ECDSA), folosesc o modificare de problemă logaritmică discretă care îi face la fel de slabi împotriva computerelor cuantice. Kirsch și Chow[10] menționează că un algoritm Shor modificat poate fi folosit pentru a decripta date criptate cu ECC. În plus, au subliniat că spațiul cheie relativ mic al ECC, în comparație cu RSA, îl face mai ușor de spart de computerele cuantice. În plus, Proos și Zalka[11] au explicat cum o criptare ECC de 160 de biți ar putea fi decriptată de un computer cuantic de 1000 qubit.

Algoritmul lui Grover reprezintă o amenințare pentru unele scheme criptografice simetrice, însă cercetările arată că Advanced Encryption Standard-AES de peste 128 biți este rezistent deocamdată la computerele cuantice[12]. Algoritmul menționat mai sus slăbește criptarea simetrică, fiind necesar doar un număr egal cu rădăcina pătrată de qubiti raportat la biții clasici. De exemplu, pentru un sistem de cifrare simetric de n biți, un calculator cuantic operează cu formula $\sqrt{2n} = 2^{n/2}$, adică o cheie AES de 128 biti va fi echivalentă uneia de 64 biți într-un calculator cuantic. Un alt indicator al securității AES în era post-cuantică este că NSA (Agenția Națională de Securitate a SUA) permite cifrului AES să securizeze (protejeze) informațiile clasificate pentru niveluri de securitate SECRET și TOP SECRET, dar numai cu dimensiuni ale cheii de 192 și 256 biți[13].

Rețele de distribuire a cheilor cuantice QKD (Quantum Key Distribution)

Traficul din rețelele clasice poate fi interceptat, supus atacurilor de tip „man in the middle" etc., în timp ce cu ajutorul rețelelor cuantice visul unei comunicări perfect sigure este real. Acestea ar putea sprijini lumea să elimine frauda online și furtul de identitate, atacurile de hacking și ascultarea electronică. Pe de altă parte, ar putea permite teroriștilor și infractorilor să comunice în secret absolut - iar guvernele să-și ascundă secretele fără ca nimeni să afle vreodată. Într-o lume a criptării impenetrabile, toate comunicațiile electronice umane ar putea deveni complet private - cu consecințe uluitoare, atât bune, cât și rele, pentru securitatea cibernetică.

Pe 29 septembrie 2017 acest deziderat s-a apropiat semnificativ de realitate. O echipă de criptografi și fizicieni de la Academia Chineză de Științe au susținut un apel video de jumătate de oră cu omologii lor din Viena, folosind criptarea cuantică, o tehnologie care face imposibilă piratarea sau ascultarea comunicațiilor. Apelul Beijing-Viena a fost efectuat printr-o conexiune de Internet convențională de tip Skype, dar ceea ce a fost revoluționar a fost o cheie de criptare sigură generată de un dispozitiv cuantic montat într-un satelit chinezesc. Și, în mod crucial, fizica cuantică care a creat cheia înseamnă că orice încercare de a sparge codul poate fi detectată imediat[4].

În momentul actual există numeroase programe de cercetare, iar majoritatea actorilor statali implementează tehnologia QKD:

✓ în România există inițiativa Institutului naţional de cercetare dezvoltare pentru tehnologii izotopice şi moleculare, care își propune construirea, în termen de 10 ani, a unei reţele QKD care va conecta Clujul de Bucureşti.

✓ la nivel european a fost aprobat programul Quantum Technologies Flagship (lansat în anul 2018 la Bucureşti, împreună cu reprezentanţi din alte şase state europene, cu un buget de un miliard de euro), care își propune cercetarea şi dezvoltarea tehnologiilor cuantice în următorii 10 ani. Programul urmărește construirea unei reţele pentru integrarea tehnologiilor cuantice în sistemele de comunicaţii tradiţionale pentru a securiza comunicaţiile infrastructurilor critice, ale instituţiilor bancare, ale reţelelor de energie etc.

✓ pe plan global, cea mai mare reţea cuantică (QKD/*quantum key distribution*) care permite securizarea datelor este deţinută de către Republica Populară Chineză; aceasta permite transmiterea datelor prin fibră optică şi fluxuri satelitare fără a exista posibilitatea de interceptare şi conectează 150 de utilizatori de pe teritoriul chinez; reţeaua se întinde pe o lungime de 4600 km.

Concluzii

Securizarea informaţiilor a fost şi este o preocupare continuă a organizaţiilor şi entităţilor statale. Metodele de asigurare a confidenţialităţii, integrităţii şi autenticităţii informaţiei au variat de-a lungul timpului şi au crescut în complexitate exponenţial. Tehnologia calculatoarelor cuantice este încă în fază incipientă de dezvoltare, însă trendul crescător arată că există un progres semnificativ şi un interes la nivel internaţional din partea actorilor statali şi a organizaţiilor din domeniul tehnologiei.

Odată cu creşterea puterii de procesare a calculatoarelor cuantice şi, în consecinţă, scăderea eficienţei metodelor actuale de securizare a informaţiilor, va evolua şi tehnologia de securizare cuantică a cheilor de criptare - *quantum key distribution*. Integrarea în tehnologiile existente, precum 5G, fluxuri de date satelitare etc., a tehnologiei QKD ar oferi raportul maxim de viteză de transmisie concomitent cu asigurarea totală a confidenţialităţii, integrităţii şi autenticităţii informaţiilor.

Bibliografie:

1. CHEN L., Jordan S., Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *"NIST: Report on Post-Quantum Cryptography*," NIST, Tech. Rep., 2016;
2. GIDNEY Craig and Eker Martin, *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,* Quantum 5, Vol. 433, 2021;
3. HOU Shi-Yao, Guanru Feng, Zipeng Wu, Hongyang Zou, Wei Shi, Jinfeng Zeng, Chenfeng Cao, Sheng Yu, Zikai Sheng, Xin Rao, Bing Ren, Dawei Lu, Junting Zou, Guoxing Miao, Jingen Xiang, Bei Zeng, *SpinQ Gemini: a desktop quantum computer for education and research*, Editura Quant-ph, 2021;
4. LIAO Sheng-Kai et al., *Satellite-Relayed Intercontinental Quantum Network*, Phys. Rev. Lett. 120, 030501, 2018;
5. KIRSCH Z., *Quantum Computing: The Risk to Existing Encryption Methods* Ph.D. dissertation, Tufts University, Massachusetts, 2015;
6. National Security Agency, "*National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information"*, NSA, Tech. Rep., 2003;
7. PROOS J. and Zalka C., "Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves", *Quantum Info. Comput*., vol. 3, no. 4, 2003;
8. YHONG Han-Sen, Wang Hui, *Quantum computational advantage using photones*, Editura Science, 2020;
9. https://www.nature.com/articles/d41586-020-03434-7;
10. https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023;
11. https://www.rsa.com/en-us/products;
12. https://www.techradar.com/news/we-watched-an-ai-crack-the-enigma-code-in-just-over-ten-minutes;
13. https://www.simplilearn.com/data-encryption-methods-article.

[1] https://www.nature.com/articles/d41586-020-03434-7 accesat la data de 27.07.2021.

[2] https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023 accesat la data de 27.07.2021.

[3] Craig Gidney and Martin Eker, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum 5,Vol 433, 2021, pp. 3-7.

[4] https://www.rsa.com/en-us/products accesat la data de 27.07.2021.

[5] https://www.techradar.com/news/we-watched-an-ai-crack-the-enigma-code-in-just-over-ten-minutes accesat la data de 27.07.2021.

[6] Han-Sen Yhong Hui Wang, Quantum computational advantage using photones, Editura Science , 2020.
[7] Shi-Yao Hou, Guanru Feng, Zipeng Wu, Hongyang Zou, Wei Shi, Jinfeng Zeng, Chenfeng Cao, Sheng Yu, Zikai Sheng, Xin Rao, Bing Ren, Dawei Lu, Junting Zou, Guoxing Miao, Jingen Xiang, Bei Zeng, SpinQ Gemini: a desktop quantum computer for education and research , Editura Quant-ph, 2021.
[8] https://www.simplilearn.com/data-encryption-methods-article accesat la data de 27.07.2021
[9] Craig Gidney and Martin Eker, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum 5,Vol 433, 2021.
[10] Z. Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods," Ph.D. dissertation , Tufts University, Massachusetts, 2015.
[11] J. Proos and C. Zalka, "Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves,", Quantum Info. Comput., vol. 3, no. 4, 2003, pp. 317–344.
[12] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NIST: Report on Post-Quantum Cryptography," NIST, Tech. Rep., 2016.
[13] National Security Agency, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information," NSA, Tech. Rep., 2003.
[14] Sheng-Kai Liao *et al.,* Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. 120, 030501, 2018

„SOLUȚIONISMUL TEHNOLOGIC” – ASPECTE PRO ŞI CONTRA ÎN ANALIZA DE INTELLIGENCE

Raluca-Mihaela STĂNESCU*

Abstract

The world is constantly evolving in the so-called VUCA environments (V – volatility, U - uncertainty, C – complexity and A – ambiguity). If adopting a PESTLE analytical model (which includes political, economic, social, technological, legal and environmental factors), we will notice that new technologies represent "the factors upon which the game's changes take place". This concept, usually considered in the predictive analysis and the projective studies, may be defined as a new element dramatically changing the situation or the current status. This technological factor changes the way we live, think, interact, communicate or access services in a more and more digitalized society.

Keywords: *technology, intelligence analysis, knowledge, training.*

Introducere

Pornind de la afirmația lui Mark Lowenthal[1] potrivit căreia serviciul tradițional de informații se află într-un proces permanent de *„oboseală a reformei”*, în cele ce urmează ne propunem să identificăm modul în care tehnologia informației și comunicațiilor (TIC) afectează așa-numitul „ciclu informațional”, oferă noi oportunități de culegere, evaluare și integrare a surselor vechi și noi de informații, generează noi riscuri corporative și personale pentru analiștii de informații, în special în spațiul cibernetic, introduce noi prejudecăți în raționamentul analitic, modifică abilitățile clasice dezvoltate de analiștii de informații, oferă noi instrumente pentru a sprijini activitatea zilnică a analiștilor (de tipul „big data”, sisteme predictive, analize semantice) sau schimbă modul în care produsele informative sunt diseminate (într-un format care adaugă mai mult conținut vizual: hărți, infografii și diagrame).

Tehnologii care grevează „ciclul informațional”

Procesul accelerat de inovare afectează, în egală măsură, acțiunile și fenomenele infracționale. EUROPOL a elaborat în anul 2017 un Raport intitulat *„Criminalitatea în era tehnologică”,* în care se afirma că *„pentru aproape toate tipurile de crimă organizată, infractorii implementează și adaptează tehnologia cu abilități din ce în ce mai mari și cu un efect tot mai vizibil. Probabil aceasta este acum cea mai mare provocare cu care se confruntă autoritățile de aplicare a legii din întreaga lume, inclusiv în UE”*[2]. Într-una din secțiunile raportului, *„Explorarea crimei organizate de mâine”*, EUROPOL identifică opt factori cheie ai schimbării, în strânsă legătură cu tehnologiile informaționale și alte tehnologii conexe domeniului: Internet și deep web, social media, big data, *cloud computing*, aplicații mobile, nanotehnologie și orașe inteligente.

Având în vedere că tehnologiile sunt un factor cheie în noile tendințe penale, agențiile de

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

aplicare a legii trebuie să își consolideze eforturile pentru eficientizarea capabilităților în domeniul *intelligence*. În acest context, experții din forțele de poliție și/sau serviciile de informații au nevoie de instruire continuă, îmbunătățită și specializată pentru a contracara noile tipuri de amenințări și pentru a profita de noile oportunități.

Noile tehnologii sunt, simultan, parte a problemei actuale de securitate, dar și parte a soluției. După atacurile de la 11 septembrie 2001 din SUA, a existat permanent un efort de îmbunătățire a abilităților analiștilor de informații. Pe de altă parte, Comunitatea de informații a suportat blamul unanim al opiniei publice după ce au avut loc incidente sau atacuri, pe de o parte pentru că analiza se poate realiza obiectiv post-factum, iar pe de altă parte pentru că disponibilitatea informațiilor este mult sporită. De cele mai multe ori, o astfel de situație generează o dezbatere intensă în media, care se soldează cu întrebări referitoare la utilitatea existenței unui aparat informativ supra-dimensionat.

Alternative la schemele tradiționale

Ciclul informațional este prezentat în multe manuale, articole și cursuri de specialitate ca fiind „placa turnantă" a întregii discipline informative. Acest ciclu este, în fapt, o construcție pur teoretică prin care este tradusă o imagine oarecum ireală a muncii informative și care creează impresia unei diagrame statice, secvențiale și ciclice. Mai mult decât atât, unele modele acreditate exclud etape cheie precum feedback-ul sau evaluarea.

Articolul de față își propune să abordeze modul în care instrumentele TIC și nivelul actual de dezvoltare tehnologică modifică întregul proces informativ, așa cum era cunoscut până de curând.

Noile tehnologii permit includerea de noi sarcini în faza de culegere, inclusiv anumite misiuni care au fost considerate întotdeauna parte a etapelor ulterioare. De exemplu, sistemele de gestionare a surselor deschise permit extragerea entităților și sunt capabile să efectueze imediat integrări de informații pe baza acestora. Noile tehnologii sunt capabile, cu un grad sporit de succes, să sintetizeze texte și să traducă informații în hărți și în alte aplicații de geo-localizare. De asemenea, încercări recente ale specialiștilor vizează automatizarea evaluării informațiilor, de exemplu, prin validarea informațiilor din surse multiple.

Monitorizarea informațiilor devine ea însăși o specializare distinctă. În prezent, anumite sisteme reprezintă o sursă de alimentare continuă pentru alte sisteme de informații de bază și actuale.

Mai multe tipuri de tehnologii sunt puse acum în sprijinul sarcinilor de analiză: metoda

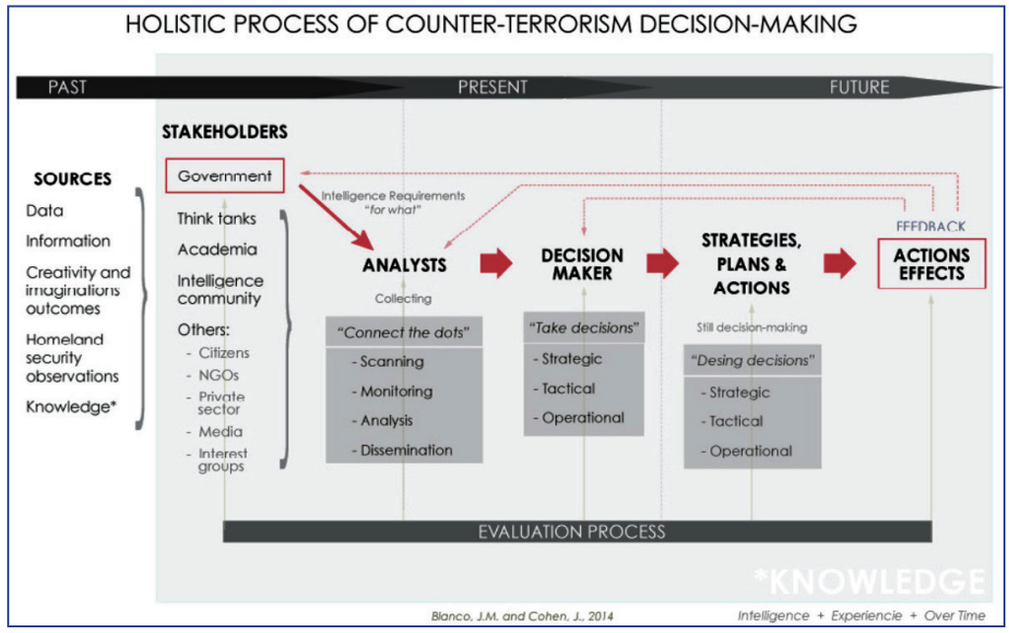


Figura 1 - Procesul complet de luare a deciziei în domeniul combaterii terorismului[4]

Analizei Ipotezelor Concurente, sisteme de suport decizional, pachete statistice sau platforme integrate (IBM i2).

Tehnologiile modifică, de asemenea, modul în care sunt prezentate informațiile, încorporând din ce în ce mai mult în rapoartele informative elemente vizuale și multimedia, în detrimentul textului, ceea ce face ca munca analiștilor și a factorilor de decizie să fie mai facilă, mai accesibilă și mai economică din punct de vedere al timpului alocat.

Tehnologiile pot fi utile și în formarea analiștilor de informații, îmbunătățindu-le abilitățile prin așa-numitele *„jocuri serioase”* (*„serious games”*), simulări sau studii de caz.

Din aceste motive, propunem un concept mai larg, cum ar fi procesul informativ, care poate fi definit ca „setul de activități dezvoltate de către analiști într-o organizație și care vizează obținerea de informații și analize care să sprijine adoptarea unor decizii oportune”[3].

„Soluționismul tehnologic” – o opțiune care trebuie evitată?

Societatea actuală se caracterizează prin utilizarea intensivă a tehnologiilor, în special în domeniul TIC. Contribuția fundamentală a acestora în furnizarea de noi servicii și aplicații create în sprijinul cetățenilor, care pot interacționa în orice moment și loc, a generat în egală măsură noi riscuri și amenințări, devenind, astfel, elementul cheie de „modificare a jocurilor” actuale.

Printre opiniile cheie care încearcă să avertizeze asupra efectelor negative ale tehnologiilor, putem evidenția lucrările lui Evgheni Morozov. În 2013, Morozov a criticat ceea ce fusese numit drept „soluționism tehnologic”, adică ideea potrivit căreia tehnologia reprezintă un obiectiv, în loc să fie un mijloc de a obține obiective multiple și variate. Pentru Morozov, fiecare problemă are o soluție tehnologică.

Există chiar și soluții tehnologice menite să facă față unor probleme care nu există. În domeniul analizei de informații, este posibil să se găsească avertismente tehnologice, precum cele subliniate de Lowenthal, referitor la Big Data.[5] O abordare corectă a problemei ar fi să te bazezi pe beneficiile tehnologiilor, menținând o „conștientizare situațională” față de acestea. Noile tehnologii sunt sursa unor noi amenințări și riscuri, dar, în același timp, fac parte din soluție. O posibilă dezbatere privind tehnologiile în relație cu analiza de informații presupune existența a două scenarii posibile: automatizarea tehnologică a analizei versus sprijinul tehnologic al analizei (sau stimularea analizei prin intermediul tehnologiei). Analiza de informații este un proces bazat pe resursa umană, fiind, în același timp, compatibilă cu tehnologia.

În domeniul inovației europene, Comisia Europeană a finanțat unele proiecte, cum ar fi RECOBIA, care au evidențiat dificultățile cu care se confruntă organizațiile în identificarea instrumentelor care răspund nevoilor analitice. Aplicațiile patentate sunt scumpe și necesită timp pentru a fi dezvoltate, iar evoluția comercială prezintă riscuri suplimentare, cum ar fi prețurile ridicate datorate ciclului scurt de viață al inovației tehnologice, riscuri în securitatea informațiilor și a datelor sau propuneri tehnologice care nu pot fi considerate încă mature. O astfel de situație conduce la o paralizie tehnologică.

În opinia comunității de analiști, instrumentele de analiză a informațiilor nu sunt eficiente pentru separarea „semnalului de zgomot”[6] sau pentru reducerea incertitudinii. Există un decalaj evident între platformele bazate tehnologic și așteptările analiștilor.

Experții în domeniu au avertizat asupra faptului că „incertitudinea, complexitatea și ambiguitatea în care analistul operează pentru a ajunge la raționamente cu privire la evenimentele și acțiunile viitoare vor fi menținute o vreme, în ciuda îmbunătățirii instrumentelor software”[7].

Cu toate acestea, există un grad ridicat de consens cu privire la suportul tehnologic oferit în domeniul analizei de informații, ca modalitate de:

- gestionare a complexității;
- limitare a prejudecăților cognitive, avertizând asupra acestora și asupra impactului produs de acestea;
- gestionare a volumului, volatilității și varietății informațiilor, mai ales în

Externe	Mediul VUCA	Identificarea tendințelor *„Wild Cards”*	Provocare prospectivă
	Informații	Infoxicare	Provocare cantitativă
		Gradul de încredere al sursei și credibilitatea informației	Provocare calitativă
Interne	Organizație	Leadership Gestionarea schimbării Digitalizare	Provocare organizațională
	Analiști	Prejudecăți cognitive Impactul tehnologic asupra abilităților cognitive Perimarea cunoștințelor și abilităților Preocupări privind securitatea cibernetică	Provocare cognitivă

Figura 2 - Provocări tehnologice în analiza de informații[8]

formă nestructurată (text, imagine, videoclip etc.);
- depășire a limitării umane de a procesa și interpreta cantități mari de date și informații;
- suport al sarcinilor analitice;
- optimizare a aspectului produselor informative, cu precădere prin intermediul instrumentelor de vizualizare;
- instruire și dezvoltare a noilor abilități analitice cu ajutorul platformelor de simulare și a jocurilor serioase.

Provocările tehnologice în analiza de informații ar putea fi împărțite în două mari categorii: externe (mediul și caracteristicile informaționale specifice actuale) și interne (organizații și analiști).

Provocări generate de noile tehnologii

Într-un mediu VUCA, există două provocări principale pentru analiști. Pe de o parte, aceștia trebuie să detecteze tendințele tehnologice care afectează fie obiectul analizei, fie propria lor funcție de analist, dintr-o perspectivă dual în ambele cazuri: noi amenințări și noi oportunități. Pe de altă parte, este recomandabilă dezvoltarea unui exercițiu prospectiv care să permită anticiparea unor *wild cards* tehnologice, fapte cu probabilitate redusă și impact ridicat, care să adapteze strategiile actuale.[9]

Analistul de intelligence se poate afla, la un moment dat, într-o stare de *infoxicare*, *infobezitate* sau supraîncărcare cu informații, în situația în care dispune de prea multe informații pentru a urmări un subiect sau pentru a sprijini procesul de luare a deciziilor. Generarea necontenită de conținut („supraîncărcarea cu informații”) ar putea fi explicată printr-o relație scăzută între semnal (informații valide), zgomot (informații disponibile) și ignoranța cetățeanului obișnuit cu privire la modul de gestionare a informațiilor, contribuind la generarea unui efect de redundanță informativă. Sintagma provine din limba engleză și a fost utilizată inițial de către Alvin Toffler, în 1970, în cartea sa *Șocul viitorului*, deși fusese menționată anterior de Bertram Gross[1].

Lumea actuală, în care conceptul de post-adevăr a fost recent introdus, ne arată cum apelul la emoții este deasupra faptelor. Minciunile, propaganda, dezinformarea și înșelăciunea găsesc adesea sprijin în noile tehnologii, atât ca element facilitator, cât și ca potențial[11]. În urmă cu un deceniu, marea provocare era reprezentată de gestionarea volumului de informații. În prezent, ne confruntăm cu o altă provocare dificilă: evaluarea întregului volum de informații atunci când, din ce în ce mai mult, o parte din acesta sau în totalitate, este fals, fabricat sau manipulat.

Pe plan intern, noul mediu afectează atât serviciile de informații, cât și pe analiști. Organizațiile, ca parte a societății actuale, trebuie

să dezvolte o monitorizare continuă a dorințelor și așteptărilor oamenilor pe care îi deservesc. Din nou, componenta tehnologică este un factor cheie, care duce la dezvoltarea unor strategii și planuri ambițioase de transformare digitală.

Organizațiile trebuie să promoveze și să gestioneze schimbarea. Cu siguranță, succesul va fi în mâinile acelor organizații care reușesc să schimbe regulile jocului și nu al celor care știu doar să se adapteze. Transformarea digitală din interiorul organizațiilor presupune o dimensiune externă (față de beneficiar), dar și una internă, luând decalajul digital al angajaților săi drept una dintre cele mai mari provocări cu care trebuie să se confrunte.

Prejudecățile sunt erori mentale inconștiente rezultate din tendința instinctivă de a simplifica luarea deciziilor, ducând la comenzi rapide sau devieri ale raționamentului. Acestea se bazează, de regulă, pe memorie, experiență, educație, bagaj cultural sau ideologii. Biasurile sunt o consecință a provocărilor cantitative și calitative prezentate de informații. Daniel Kahneman argumenta, într-un studiu realizat în anul 2012, că există două tipuri de gândire: una rapidă și intuitivă, iar alta lentă și logică.[12] Prima este utilă pentru a aborda mediile cunoscute și familiare, fiind un gând care este întotdeauna activat și nu generează oboseală. Problema este de a răspunde într-un mod cât mai rapid la probleme complexe. În acest scop, trebuie să activăm gândirea lentă, care este epuizantă, necesită resurse cognitive ridicate și nu poate fi menținută activă în mod continuu. În acest context, existența unor prejudecăți ar trebui să-i determine pe analiști să fie precauți.

De exemplu, unele prejudecăți induse de tehnologie sunt generate de modul în care sunt utilizate motoarele de căutare. Mai exact, referitor la acest tip de prejudecăți, Eli Pariser descrie *bula de filtrare* prin care algoritmii ghicesc ce tipuri de informații ar dori să vadă un utilizator pe baza știrilor sau site-urilor accesate anterior sau în funcție de locație și istoricul căutărilor.[13] Utilizatorii sunt izolați de informațiile care sunt în dizarmonie cu punctele lor de vedere, menținându-i într-o buclă. Tehnologiile ar putea consolida și alte prejudecăți clasice, cum ar fi: informațiile proxime (la îndemână), confirmarea, finalizarea, ancorarea sau euristica[14].

În același mod, tehnologiile pot afecta unele dintre abilitățile cognitive ale analiștilor, cu efecte evidențiate recent de studiile în domeniu, ca de exemplu:

- *„Efectul Google”*: Folosim motorul de căutare Google și Internetul, în general, ca memorie suplimentară, reducând astfel cerințele personale de memorare și având încredere că putem recupera cu ușurință informații de pe net.
- *„Efectul Shallows”*: Nicholas George Carr dezvoltă un argument potrivit căruia Internetul poate avea efecte dăunătoare asupra gândirii, afectând capacitatea de concentrare și contemplare și determinând un deficit în capacitatea de stocare a memoriei și în procesarea informațiilor. Citirea unor articole și cărți lungi a devenit o sarcină dificilă. În acest caz, multi-taskingul, un obicei al vremurilor noastre, ar fi o posibilă cauză[15].
- *„Focus effect”*: Daniel Goleman evidențiază dificultățile de concentrare asupra unei singure sarcini, situație în care marea conectare umană la tehnologie *(„tehnificare”*, cum o numește el) și dependența de o multitudine de input-uri informaționale influențează, în mare măsură, capacitățile cognitive. Soluția propusă de acesta este meditația, pentru că, în opinia sa, multitasking-ul nu există și nu este specific omului[16].
- *„Efectul de dependență”*: Dopamina ne cere să primim continuu informații noi, ceea ce conduce la o limitare a capacităților de analiză profundă.

Aceste observații, parțial controversate, dar totuși intens vehiculate, necesită identificarea unor zone de convergență și a unor puncte de consens. Tehnologiile afectează creierul, dar poate fi observat că nu există pierderi de abilități mentale, ci mai degrabă o adaptare care, în plus, are loc pe termen lung. Plasticitatea creierului determină un proces adaptativ.

Aceste aspecte capătă o serie de particularități în cazul procesului informativ:

Sarcini	Provocări
Planificare și direcționare	Supraveghere tehnologică Cerințe tehnologice Identificarea cerințelor utilizatorului final Opțiune: dezvoltare proprie sau produs comercial Analiză cost-beneficiu Preocupări legate de securitate
Culegere, monitorizare și prelucrare	Instrumente de culegere. Extragerea datelor entității. Nouă solicitare a serviciilor de informații: instrumente de verificare Instruire pentru utilizarea instrumentelor OSINT Preocupări legate de securitate
Analiză	Acord anterior: analiză condusă de om și analiză bazată pe tehnologie Instruire folosind instrumente analitice. Complexă, deoarece implică cunoștințe în diferite domenii (data mining, statistică etc.) Dezvoltarea suportului computerizat pentru tehnici de analiză structurate și avansate (de exemplu metoda de Analiză a Ipotezelor Concurente, cu suportul tehnicii statistice elaborate de Bayes)
Diseminare	Dezvoltarea instrumentelor de vizualizare, integrate cu capabilități analitice Complexitate prin instruire

Figura 3: Provocări tehnologice în procesul informativ[17]

Factorul tehnologic – noi valențe în analiza de informații

În anii ’90, Armata SUA a propus un nou program de instruire militară. Parametrii acestuia au fost stabiliți urmărind un obiectiv clar, acela de a dezvolta capacitatea membrilor de a acționa în contexte extrem de complexe. Nevoia de schimbare a apărut ca urmare a identificării principalelor caracteristici care să determine scenariile viitoare în diferite medii. Așa a apărut termenul de VUCA (acronim utilizat pentru „volatilitate, incertitudine, complexitate și ambiguitate“). Ca urmare a acestei inițiative, în 2004 au fost publicate primele rezultate ale unui nou program cunoscut sub numele de *Metoda de pregătire a gândirii* și *Gândește ca un comandant* (TLAC). Concluziile au fost enunțate încă de la primele rânduri ale documentului: „Succesul operațiunilor viitoare va depinde de capacitatea liderilor și soldaților de a gândi creativ, de a decide rapid, de a profita de tehnologia disponibilă, de a se adapta cu ușurință și de a acționa ca o echipă”.

Acest scenariu nu este o opțiune, ci o realitate și reprezintă o adevărată provocare pentru analiști, cu un plus de complexitate care derivă din faptul că analiștii nu sunt instruiți pentru un astfel de context.

Volatility/ Volatilitate	Schimbările sunt rapide, aproape imprevizibile, ceea ce face dificilă identificarea tendințelor sau tiparelor și reducerea stabilității proceselor. Tipul, magnitudinea, volumul și viteza cu care acestea apar îngreunează sarcinile de analiză.
Uncertainty/ Incertitudine	Multe dintre schimbările care au loc sunt perturbatoare, dovedind că trecutul nu trebuie să fie un indicator al viitorului și împiedicând pregătirea în fața scenariilor viitoare.
Complexity/ Compexitate	Fiecare eveniment este condiționat de o multitudine de cauze și factori, fiecare dintre aceștia fiind, la rândul lor, corelați cu un al treilea eveniment. Această situație generează un nivel ridicat de confuzie, care împiedică crearea unei viziuni clare asupra situațiilor cu care ne confruntăm.
Ambiguity/ Ambiguitate	Răspunsul la întrebări cheie (cine, unde, de ce, când etc.) este greu de stabilit. Erorile de interpretare și pluralitatea de sensuri reprezintă o cauză care are ca efect confuzia, și, în consecință, imprecizia datelor.

Figura 4: Elemente VUCA[18]

Este imposibil ca următoarele generații de analiști să fie bine pregătite dacă ignorăm mediul VUCA. În mod similar, vom eșua și în procesele de recrutare dacă nu elaborăm un *Profil corespunzător pentru analiști* și continuăm să ne concentrăm exclusiv pe sarcinile pe care aceștia trebuie să le îndeplinească. Prin urmare, este necesar să luăm în considerare nu numai limitările și condițiile impuse de prezent, ci trebuie să ne raportăm la viitor, prin înțelegerea provocărilor și oportunităților pe care acesta ni le dezvăluie, identificând, în egală măsură, abilitățile necesare de pregătire pentru ca analistul să nu fie copleșit de mediul complex pe care îl va avea de gestionat.

Pentru a răspunde acestor limitări, a apărut un al doilea termen corelat cu VUCA, ca un antonim al celui dintâi, denumit *„VUCA Prime"* (*vision* - viziune, *understanding* - înțelegere, *clarity* - claritate, *agility* - agilitate), care se axează pe perspectiva din care trebuie înțelese aceste medii. Este configurat ca un set de abilități necesare atât pentru prezentul, cât și pentru viitorul societății noastre.[19]

Luând în considerare definițiile anterioare despre modul în care se poate concretiza viitorul, din experiența noastră de zi cu zi ca analiști, dar și ca manageri ai departamentelor de analiză și profesioniști ai noilor tehnologii, subliniem necesitatea de a folosi noi principii pentru formarea viitorilor analiști: utilizarea jocurilor serioase, concentrarea pe crearea de abilități (nu numai pe cunoștințe), schimbarea abordării de predare prin favorizarea învățării (prin responsabilizarea și autorizarea elevilor) și necesitatea de a considera orice organizație ca un centru de învățare continuă, fără a transfera această responsabilitate exclusiv către sectorul educațional.

Viziune versus Volatilitate	Gândire de tip proiectiv, transformată în obicei. Imaginație creativă a unor scenarii și o analiză a acestora într-un proces de back-casting pentru a detecta indicatori, pentru a evita riscuri și amenințări viitoare. Obiectivul și metodologia aplicate trebuie să fie clar definite. Trebuie să putem integra rapid cantități mari de informații, în afara procesului sau instrumentelor, dar cu o precizie și o viteză mai reduse.
Înțelegere versus Incertitudine	Fenomenul supus analizei trebuie să fie pe deplin înțeles. Răspunsul ar trebui să depășească propria experiență și cunoștințele anterioare. Trebuie construite rețele de cunoștințe, cu încredere și credibilitate, care să uzeze de noi tehnologii pentru a consolida întregul proces și a îmbunătăți progresiv abilitățile de raționament.
Claritate versus Complexitate	Chiar și haosul poate avea sens. Generarea de hărți mentale. Urmărirea analizelor existente în dinamică pentru a detecta noi dovezi (monitorizare). Înțelegerea fiecărui fenomen din interior și din perspectiva globală simultan. Evitarea explicațiilor simpliste, mono-cauzale sau a unor întâmplări banale; încercări de a răspunde la toate întrebările posibile. Una dintre marile provocări este cunoașterea și știința utilizării informațiilor în continuă schimbare, provenite din surse disparate.
Agilitate versus Ambiguitate	Maximizarea capacității de învățare, de învățare prin eșuare, de comunicare, de reacție și de adaptare. Presupune rezolvarea rapidă a problemelor și luarea constantă a deciziilor. Atitudine proactivă și concentrare asupra problemei pentru a anticipa efectele chiar înainte de a formula răspunsul. Tehnologiile utilizate ca suport trebuie să fie adaptabile atât utilizatorilor, cât și nevoilor, generând soluții generaliste.

Figura 5: Elemente VUCA Prime

Jocul – modalitate de dobândire a unor abilități transversale

Când ne referim la joc, avem în vedere atât necesitatea existenței sale în procesele de antrenament (*jocuri serioase*), cât și valoarea acestuia în ceea ce privește atitudinea, pe care o vom numi „minte ludică".

Antrenamentul în care jocul este permis depășește conținutul teoretic, facilitând analiștilor punerea în practică, atât individual, cât și în echipă, a abilităților necesare înainte de o anumită întrebare sau sarcină de lucru, fără însă a fi expuși riscului, așa cum s-ar întâmpla dacă lucrurile ar avea loc într-un context real. Este un proces de *învățare bazată pe experiență,* care facilitează obținerea imediată a feedback-ului și care antrenează, de asemenea, agilitatea răspunsului, permițând analistului să fie expus la dileme care se schimbă rapid. Aceste cerințe sunt strâns corelate cu cererea tot mai mare de descoperire, colectare, evaluare, integrare și sinteză a datelor obținute prin utilizarea noilor tehnologii.

În cadrul acestui tip de activități, nivelul didactic este maximizat, deoarece nu doar conținutul teoretic este prezentat, ci și dezvoltarea și utilizarea acestuia, analiștii fiind nevoiți să se ocupe, într-un mod simulat, de problemele pe care le-ar genera realitatea.

Această problemă este evidentă încă de la vârste fragede când metodologia de predare anacronică din centrele educaționale actuale minimizează importanța acestei componente, cel mai probabil din rațiuni de încadrare în timp sau chiar din necunoașterea modului de vizualizare a ei în afara mediului copiilor.

Deși este adevărat că agenții precum CIA folosesc jocurile de ani de zile ca instrument de instruire pentru agenții lor, utilizarea acestor tehnici nu este răspândită pe scară largă.

Cu toate acestea, jocul nu numai că facilitează procesele evidențiate, dar poate funcționa ca sursă de idei, generator de improvizație și potențial de creativitate. De asemenea, poate facilita căutarea alternativelor, luarea deciziilor, contribuind în același timp la îmbunătățirea abilităților sociale și la obținerea unui control mai bun asupra prejudecăților. Toate acestea sunt domenii relevante pentru orice analist de informații.

Evidențierea acestor beneficii include ingeniozitatea umană, experiența și creativitatea ca factori relevanți în analiza de informații, dar și nevoia de a lucra cu mașini și de a fi diferiți de acestea. Dacă responsabilizarea oamenilor care este astăzi permisă prin utilizarea noilor tehnologii beneficiază de o mai mare creativitate, nu numai la nivel individual, ci și la nivel organizațional, adoptarea unor decizii mai inteligente sau rezolvarea unor probleme mai complexe ar putea fi cu atât mai facilă.

Complexitatea factorului uman – cunoștințe, abilități, competențe

În 1970, Alvin Toffler descria simptomele produse de *șocul viitorului*. Viteza cu care se produce schimbarea ajunge să genereze implicații mai mari decât direcția în care aceasta se materializează. Evenimentele se întâmplă atât de repede încât trebuie să putem vorbi simultan despre trecut și viitor. Gestionarea complexității, sublinia Toffler, ar fi problema majoră pentru societăți în viitor. Un context care, prin pură definiție este dăunător acelor persoane și organizații care manifestă rezistență și au dificultăți de adaptare la schimbări vertiginoase, produce un impact major asupra unui element esențial: cunoașterea. Crearea, transmiterea și asimilarea cunoștințelor avansează și se modifică în același mod ca societatea, știința, tehnologia sau comunicațiile. În acest sens, Toffler însuși a afirmat că „analfabeții secolului XXI nu vor fi cei care nu pot citi și scrie, ci cei care nu pot învăța, dezvăța și reînvăța"[20].

Toffler preluase cuvintele psihologului Herbert Gerjuoy, care activa în cadrul Organizației de Cercetare în domeniul Resurselor Umane, și care afirma că „noua educație trebuie să învețe individul cum să clasifice și să reclasifice informațiile, cum să evalueze veridicitatea acestora, cum să schimbe categoriile atunci când este necesar, cum să treacă de la concret la abstract și înapoi, cum să privească problemele dintr-o nouă perspectivă - cum să se învețe pe sine. Analfabetul de mâine nu va fi omul care nu poate

citi; el va fi omul care nu a învățat cum să învețe". Toffler a adăugat că instruirea persoanelor nu se va baza pe cunoștințe fixe pe care le stocăm în minte, ci în funcție de abilitățile necesare, vor fi adaptate fiecărui moment în parte.

Mulți ani mai târziu, în cadrul Conferinței „Noile frontiere ale analizei de informații: amenințări comune, perspective diverse, noi comunități" (Roma, Italia, 31 martie - 2 aprilie 2004), s-a arătat că, după căderea Cortinei de Fier, cerințele s-au schimbat complet. Nu a fost o transformare bruscă, dar a fost o provocare în ceea ce privește pregătirea analiștilor, care au fost determinați să acorde atenție altor medii până în acel moment neglijate, cum ar fi scenariile globale, care necesită o înțelegere atât pe termen scurt, cât și pe termen lung, cu multiple conotații culturale noi și diferențe lingvistice.

Folosirea imaginației și a intuiției, ascultarea, experimentarea, greșirea, crearea și distrugerea creativă sunt abilități cheie pentru a trăi în viitor. ***Cunoașterea va deveni un set de abilități*****,** nu de cunoștințe imobile, și utilizarea acesteia, în raport de oportunitățile oferite de noile tehnologii, va fi un factor cheie pentru obținerea succesului. Obiectivul va fi acela de a crea valoare diferențială printr-o abilitate specifică la un moment dat. După cum afirma Toffler, învățând elevii cum să învețe, să se dezvețe și să reînvețe pot fi încorporate în educație noi dimensiuni.

Schimbarea paradigmei de învățare

Scopul educației este învățarea, nu predarea. Cartea publicată sub semnătura autorilor Ackoff și Greenberg, în 2008, și intitulată *Turning Learning Right Side Up: Putting Education Back on Track* pune accentul tocmai pe încercarea de a răspunde la întrebarea de ce tindem în continuare să învățăm oamenii să fie mașini, în loc să-și îmbunătățească abilitățile ca oameni, așa cum arătam anterior. Memorarea este confundată cu învățarea și asta ne condiționează, astfel încât cu greu ne vom aminti în viața noastră adultă ceea ce am învățat în perioada copilăriei. Totuși, obiceiurile și deprinderile dobândite (vorbitul, mersul, îmbrăcatul) vor rămâne, în general, în amprenta noastră într-un mod peren.

Este vorba despre generarea aceluiași dinamici care declanșează învățarea înainte de un nou loc de muncă. În acest proces, predarea, dacă există, este minimă. Cu toate acestea, învățarea apare prin observare, imitare, necesitate, explicarea exemplelor de referință și nu prin simpla comunicare (transmiterea unui mesaj vorbit).

Învățarea excede formatelor standardizate și standardizează acele formate care permit adultului să acționeze și să evolueze în cadrul societății.

Înveți încercând, eșuând, interacționând informal pentru a obține răspunsuri și împărtășind ceea ce ai interiorizat.

Învățarea prin explicare este un alt pilon al acestui proces. „Explicatorul" are nevoie de un efort suplimentar în care profesorul nu este necesar, și anume de a se pune în mintea celuilalt pentru a putea răspunde la întrebarea lui. O practică care implică dezvoltarea „culturii de mediu", nu doar predarea pe baza a ceea ce este cunoscut, ci explicarea pe baza dificultăților pe care le pune un terț. Înveți să „înveți de la alții". În acest context, este necesar să se utilizeze analiști experimentați, ca mentori pentru cei aflați la început de carieră, împărtășind, astfel, experiență, instruire și abilități.

Procesul de învățare în comunitățile analitice

Urmând scenariul anterior și ținând cont de faptul că noile tehnologii ne permit o mai mare difuzare zilnică între mediile fizic și digital, este posibil, de asemenea, să vorbim despre nevoile de învățare din cadrul organizațiilor.

Viziunea lui Peter Senge despre o organizație de învățare, ca grup de oameni care își îmbunătățește continuu capacitățile creative, ar putea avea aplicabilitate în echipele de analiză de intelligence. Potrivit lui Peter Senge, organizațiile de învățare sunt „...organizații în care oamenii își multiplică în mod continuu capacitatea de a crea rezultatele pe care le doresc cu adevărat, unde se alimentează modele noi și expansive de gândire, unde aspirația colectivă este eliberată și unde oamenii învață continuu să vadă întregul împreună[21].

Claritate versus Complexitate	Gândire adaptativă Gândire laterală Managementul cunoștințelor Managementul supraîncărcării cu sarcini Managementul diversității Curiozitate intelectuală Tehnici de creativitate Managementul prejudecăților cognitive Analiza datelor Tehnici de operare cu estimări Abordări generale/holistice, precum și viziune tehnică Alfabetizarea informațională mediatică Explicații prin observare
Agilitate versus Ambiguitate	Gândire critică Experimentare Lecții învățate Învațarea prin scepticism Respingerea informațiilor redundante Învățare autonomă Managementul presiunii sociale Proactivitate Inginerie decizională Abilitatea luării deciziilor în echipă Adaptarea metodologiilor la obiectivul studiului Găsirea de soluții Dezvoltarea procesului de analiză a informațiilor Managementul crizelor Managementul timpului și priorităților Tehnici de *„jocuri serioase”* (*„serious gaming”*) Managementul talentelor Scrierea critică Rezoluție/luarea deciziilor
Viziune versus Volatilitate	Învață să înveți Să știi cum să înveți Antrenament continuu Antifragilitate Creativitate Agilitate Motivație Modestie Adaptabilitate cognitivă Inteligență colaborativă Managementul cunoștințelor bazat pe echipă Diagnoza barierelor de colaborare Utilizarea autodidactă a noilor tehnologii Jocul meu Viziune evaluativă Capacitatea de relaționare în rețelele sociale

Înțelegere versus Incertitudine	Transparență Încredere Gestionarea excesului de încredere (sinceritate introspectivă) Colaborare/lucru în echipă Conștientizare tehnologică Crearea de scenarii/simulări Generarea de idei Validarea cunoștințelor dobândite Abilități interpersonale Inteligența maselor Leadership în echipe virtuale și transculturale Tehnici de vizualizare a informațiilor Dezvoltarea echipei de înaltă performanță Managementul echipelor virtuale

Figura 6: Abilități necesare pentru gestionarea mediilor VUCA[23]

Pentru ca acest lucru să se întâmple, se afirmă că organizațiile trebuie să „descopere cum să valorifice angajamentul și capacitatea oamenilor de a învăța la toate nivelurile”[22].

Senge evidențiază diferite moduri de învățare. „Învățarea supraviețuirii” sau „învățarea adaptativă” este importantă și necesară, dar nu este suficientă, iar organizațiile trebuie să dezvolte o „învățare generativă” care sporește capacitățile organizaționale. Acesta este motivul pentru care un serviciu de informații trebuie să identifice continuu modul în care poate îmbunătăți cunoștințele și, în special, dezvolta noi abilități.

Acest concept are mai multe legături cu noile abilități necesare supraviețuirii în mediile VUCA. În acest scop, organizațiile ar trebui să cultive cinci domenii/capacități:

1. Gândirea sistemică: abilitatea de a înțelege și de a aborda întregul și de a examina relația dintre părți;
2. Expertiza personală: organizațiile învață numai prin intermediul persoanelor care învață;
3. Modelul mental: învățarea de a dezvălui proiecțiile noastre interne despre lume, de a le scoate la suprafață și de a le ține riguros sub observație/analiză;
4. Construirea unei viziuni comune: împărtășirea *„imaginilor despre viitor”*, care încurajează angajamentul real mai degrabă decât conformitatea;
5. Învățarea în echipă: alinierea și dezvoltarea capacităților unei echipe de a atinge obiectivele pe care membrii ei și le-au propus.

Toate acestea reprezintă elemente cheie pentru analiza de intelligence, în care este nevoie de abordări holistice pentru a obține *„imaginea de ansamblu”* despre fenomenele de securitate și o filozofie puternică a gândirii critice, capabilă să conteste judecățile anterioare sau intuitive. Învățarea individuală și în echipă trebuie să fie echilibrată, ținând cont de faptul că analiza de informații este o activitate de echipă.

Pentru a facilita luarea deciziilor, această învățare trebuie să fie ghidată de viziunea comună despre misiunea echipei și de obiectivul îmbunătățirii procesului de informații și a produsului final informativ. La acest demers trebuie să contribuie nu numai guvernele sau instituțiile, ci și profesorii, personalul din departamentele de resurse umane, managerii și analiștii.

Viitorul, oricât de perturbator sau de îndepărtat ar părea, nu este imposibil de anticipat și de controlat. În calitate de organizații, analiști sau cetățeni, cu toții avem capacitatea, dacă nu responsabilitatea, de a interveni în evoluția viitorului prin deciziile pe care le luăm. A dobândi și a uza de abilitățile noastre pentru a anticipa cât mai exact evenimentele și acțiunile reprezintă doar începutul, devenind, treptat, o condiție *sine qua non* pentru viitorul nostru.

Concluzii

Articolul a încercat să identifice modul în care tehnologiile afectează așa-numitul ciclu informațional. Noile tehnologii oferă noi oportunități de a culege, evalua și integra surse vechi și noi de informații, de a analiza datele și de a elabora produsul finit într-un mod cât mai profesionist.

Pe de altă parte, noile tehnologii generează riscuri corporative și personale pentru serviciile și analiștii de informații, în special în spațiul cibernetic, introducând, totodată, tendințe noi. Putem concluziona că analiza de informații este supusă în prezent unei serii de provocări tehnologice specifice. Unele dintre acestea sunt de natură externă: mediul tehnologic în continuă evoluție și caracteristicile informației (infoxicare și dificultăți tot mai mari de asimilare a informațiilor și de evaluare a surselor). Altele aduc în prim plan provocări interne, atât pentru organizații, cât și pentru analiști: transformarea digitală, noua conducere, prejudecățile cognitive, perimarea rapidă a cunoștințelor și abilităților sau noile preocupări de securitate.

Acest articol propune o agendă pentru îmbunătățirea învățării analizei de *intelligence*, bazată pe trei piloni principali: în primul rând, concentrarea pe învățare, în loc de predare; în al doilea rând, concentrarea pe învățarea organizațională; și în al treilea rând, concentrarea pe învățarea prin jocuri și acțiuni. Admițând că tehnologiile reprezintă un factor cheie în noile tendințe la nivel global, serviciile de informații și instituțiile de aplicare a legii trebuie să își consolideze eforturile pentru a-și îmbunătăți capacitățile de culegere a datelor. În acest scop, un cadru VUCA adaptativ poate contribui la analizarea și interpretarea corectă a informațiilor, permițând, totodată, identificarea de noi cunoștințe și abilități necesare pentru abordarea tuturor tipurilor de riscuri și amenințări.

Nu în ultimul rând, pe fondul unei posibile expuneri în mediul virtual din care își obțin informațiile, analiștii sunt cei care se confruntă cu noi preocupări și tot ei sunt cei care trebuie să dezvolte noi abilități de lucru, adaptate realității digitale dinamice în care operează.

Scenariul actual de lucru, determinat de VUCA, a impus o nouă abordare a leadership-ului serviciilor de informații din întreaga lume în raport de emoții, deprinderi, succesul echipei sau performanța angajaților, într-un context în care valorile și principiile organizaționale tind să se coaguleze în jurul inteligenței emoționale, gândirii flexibile, soluționării problemelor și adoptării deciziilor într-o manieră creativă, atuuri atât de necesare pentru inovare, obținerea unor rezultate de excepție și atingerea obiectivelor instituționale.

Bibliografie:

1. BADALAMANTE, R. V. & Greitzer, F. L., *Top Ten Needs for Intelligence Analysis Tool Development. Proceedings of the First Annual Conference on Intelligence Analysis Methods and Tools,* Richland, Pacific Northwest National Laboratory, 2005, disponibil la URL: https://www.pnnl.gov/coginformatics/media/pdf/topten_paper.pdf, accesat la 5 noiembrie 2020.
2. BLANCO, J. M. & Cohen, J., *The future of counter-terrorism in Europe. The need to be lost in the correct direction*, European Journal of Future Research, 2014, Vol. 2, Nr. 1, disponibil la URL: https://link.springer.com/article/10.1007%2Fs40309-014-0050-9, accesat la data de 4 noiembrie 2020.
3. BLANCO, J.M. & Cohen, J., *Knowledge, the great challenge to deal with terrorism*, Revista de Estudios en Seguridad Internacional, RESI, 2016, disponibil la URL: http://www.seguridadinternacional.es/revista/?q=content/knowledge-great-challenge-deal-terrorism, accesat la data de 4 noiembrie 2020.
4. BLANCO, José María, Cohen, Jéssica, Rubio, Yaiza, Brezo, Félix, *The T-Factor – New Technologies and Intelligence Analysis Learning*, European Law Enforcement Research Bulletin - Innovations in Law Enforcement, 2017.
5. CARR, N., *The Shallows: What the Internet Is Doing to Our Brains*, 2010, W. W. Norton & Company.
6. COOK, Maia; SMALLMAN, Harvey S., "Human Factors Of The Confirmation Bias In Intelligence Analysis: Decision Support From Graphical Evidence Landscapes", *Human Factors The Journal of the Human Factors and Ergonomics Society,* 2008, 50(5).

7. EUROPOL, *SOCTA Report: Crime in the Age of Technology – Europol's Serious And Organised Crime Threat Assessment 2017*, disponibil la URL: https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017, accesat în data de 4 noiembrie 2020.
8. GOLEMAN, D., *Focus: The Hidden Driver of Excellence*, 2013, Harper Collins US Brand Code.
9. GROSS, B., *The Managing of Organizations: The Administrative Struggle*, 1964, The Free Press of Glencoe.
10. KAHNEMAN, D., *Thinking Fast and Slow*, 2012, New York: Farrar, Straus and Giroux.
11. LOWENTHAL, M. M., *A Disputation on Intelligence Reform and Analysis: My 18 Theses*. International Journal of Intelligence and Counterintelligence, 2013, Vol. 26.
12. LOWENTHAL, M. M. & Marks, R. A., *Intelligence Analysis: Is It As Good As It Gets?*, International Journal of Intelligence and CounterIntelligence, 2015, 28:4.
13. PARISER, E., *The Filter Bubble: What The Internet Is Hiding From You*, 2012, Penguin.
14. PETERSEN, J., *Out of the Blue How to Anticipate Big Future Surprises*, The Arlington Institute, 1997, 2nd ed. Lanham: Madison Books.
15. SENGE, P., *The Fifth Discipline: The Art and Practice of the Learning Organization*, 1990, Currency.
16. SILVER, N., *The Signal and the Noise: Why So Many Predictions Fail - but Some Don't*, 2015, Penguin Books.
17. TOFFLER, A., *Future Shock*, 1970, Editura Random.
18. VINER, K., "How technology disrupted the truth", *The Guardian,* 12.07.2016, disponibil la URL: https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth, accesat la 5 noiembrie 2020.

[1] M. M. Lowenthal, „A Disputation on Intelligence Reform and Analysis: My 18 Theses", *International Journal of Intelligence and Counterintelligence,* 2013, Vol. 26, pp. 31-37; Lowenthal, M.M. & Marks, R.A., Intelligence Analysis: Is It As Good As It Gets?, *International Journal of Intelligence and CounterIntelligence,* 2015, 28:4, pp. 662-665.

[2] EUROPOL, SOCTA Report: Crime in the Age of Technology – Europol's Serious And Organised Crime Threat Assessment 2017, disponibil la URL: https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017, accesat în data de 4 noiembrie 2020.

[3] Blanco, J. M. & Cohen, J, The future of counter-terrorism in Europe. The need to be lost in the correct direction, European Journal of Future Research, 2014, Vol. 2, Nr. 1, disponibil la URL: https://link.springer.com/article/10.1007%2Fs40309-014-0050-9, accesat la data de 4 noiembrie 2020; și Blanco, J.M. & Cohen, J., Knowledge, the great challenge to deal with terrorism, *Revista de Estudios en Seguridad Internacional,* RESI, 2016, disponibil la URL: http://www.seguridadinternacional.es/revista/?q=content/knowledge-great-challenge-deal-terrorism, accesat la data de 4 noiembrie 2020.

[4] Ibidem.

[5] Lowenthal, M. M., A Disputation on Intelligence Reform and Analysis: My 18 Theses, International Journal of Intelligence and Counterintelligence, 2013, Vol. 26, pp. 31-37.

[6] Silver, N., *The Signal and the Noise: Why So Many Predictions Fail-but Some Don't,* 2015, Penguin Books.

[7] Badalamante, R. V. & Greitzer, F. L., Top Ten Needs for Intelligence Analysis Tool Development. Proceedings of the First Annual Conference on Intelligence Analysis Methods and Tools, Richland, Pacific Northwest National Laboratory, 2005, disponibil la URL: https://www.pnnl.gov/coginformatics/media/pdf/topten_paper.pdf, accesat la 5 noiembrie 2020.

[8] Blanco, José María, Cohen, Jéssica, Rubio, Yaiza, Brezo, Félix, The T-Factor – New Technologies and Intelligence Analysis Learning, European Law Enforcement Research Bulletin - Innovations in Law Enforcement, 2017, p. 4.

[9] Petersen, J., Out of the Blue How to Anticipate Big Future Surprises, The Arlington Institute, 1997, 2nd ed. Lanham: Madison Books.

[10] Gross, B., The Managing of Organizations: The Administrative Struggle, 1964, The Free Press of Glencoe.

[11] Viner, K., (2016) How technology disrupted the truth, *The Guardian,* 12.07.2016, disponibil la URL: https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth, accesat la 5 noiembrie 2020.

[12] Kahneman, D., Thinking Fast and Slow, 2012, New York: Farrar, Straus and Giroux.

[13] Pariser, E., The Filter Bubble: What The Internet Is Hiding From You, 2012, Penguin.

[14] Cook, M.B. & Smallman, H.S., Human Factors Of The Confirmation Bias In Intelligence Analysis: Decision Support From Graphical Evidence Landscapes, Human Factors, 2008, 50(5): pp. 745-754.

[15] Carr, N., *The Shallows: What the Internet Is Doing to Our Brains,* 2010, W. W. Norton & Company.
[16] Goleman, D., Focus: The Hidden Driver of Excellence, 2013, Harper Collins US Brand Code.
[17] Blanco, J. M. & Cohen, J., The future of Counter-Terrorism in Europe. The Need To Be Lost In The Correct Direction, *European Journal of Future Research,* 2014, Vol. 2, Nr. 1, disponibil la URL: https://link.springer.com/article/10.1007%2Fs40309-014-0050-9, accesat la data de 8 noiembrie 2020.
[18] Blanco, José María, Cohen, Jéssica, Rubio, Yaiza, Brezo, Félix, *The T-Factor – New Technologies and Intelligence Analysis Learning,* European Law Enforcement Research Bulletin - Innovations in Law Enforcement, 2017, p. 6.
[19] Ibidem, p. 7.
[20] Toffler, A., *Future Shock,* 1970, Random House, p. 414.
[21] Senge, P., *The Fifth Discipline: The Art and Practice of the Learning Organization,* 1990, Currency, p. 3.
[22] Ibidem, p. 4.
[23] Blanco, José María, Cohen, Jéssica, Rubio, Yaiza, Brezo, Félix, op.cit.p. 10.

PENINSULA CRIMEEA: REDUTA FEDERAȚIEI RUSE PE DIRECȚIA MAREA NEAGRĂ – MAREA MEDITERANĂ

Gheorghe MATEI*

Abstract

In order to reaffirm itself as an uncontested global actor, the Russian Federation aspires to „new horizons" where the „Putinist" ideology could be easily adopted by authoritarian/dictatorial elites and moves the effort's centre of gravity towards projecting the doctrine away from Europe and into Africa, the Middle East and Asia-Pacific.

In this context, the EU and NATO enlargement process in Eastern and South-Eastern Europe and the resilience consolidation of the states in the respective areas have determined the Russian Federation to reconsider their effort on the Western Strategic Direction (defence consolidation, harassment and interests promoting through third parties) and to capture the initiative on the South-Western Strategic Direction.

The newly created and consolidated outpost (the Crimean Peninsula) was quickly transformed from a territory that was conquered, estranged, leased and then reclaimed into a stronghold on the South-Western Strategic Direction and use as a natural extension of the territorially -expansionist foreign policy of the Russian Federation

Crimean Peninsula's return to the „motherland" was followed by ample programmes meant to easily connect the Peninsula to the Russian continental land from economic, transport infrastructure and especially military standpoints. The latter was carried through overcrowding the newly acquired land with personnel and equipment.

Keywords*: the Crimean Peninsula, the South-Western Strategic Direction, security, defense, A2/AD system.*

1. Mixul favorabil: taurisci - ucraineni - *„omuleți verzi"* - ruși

Locuită în Antichitate de taurisci, cucerită și stăpânită de greci, romani, goți, khazari, tătari și otomani, Peninsula este ocupată de ruși în anul 1783[1] și cedată RSS Ucrainene în 1954[2] de către liderul sovietic Nikita Hrușciov, ca gest de complezență la aniversarea a 300 de ani de la *„unificarea"* Ucrainei cu Rusia.

Parte componentă a Ucrainei după destrămarea URSS[3] (1991), Peninsula este ulterior parțial concesionată de către Federația Rusă (pentru circa 2 miliarde dolari anual, pe o perioadă de 20 de ani, Moscova putând folosi facilități portuare atât în portul Sevastopol, cât și în alte porturi din Crimeea). De asemenea, *Acordul referitor la flota Mării Negre* (1997) stipula că F.Rusă poate cumpăra o parte dintre cele mai moderne nave ce urmau să revină Ucrainei în urma împărțirii Flotei după implozia URSS.

În anul 2010 (cu șapte ani[4] înainte să expire), acordul a fost prelungit de către Viktor Ianukovici[5] până în 2042, prin *Acordul de la Harkov*, prin intermediul căruia F.Rusă își asuma, la rândul său, obligația de a furniza Ucrainei gaz natural

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

la preț preferențial (conform *doctrinei Falin-Kvitsinsky*[6]). Acordul trebuia înțeles de către semnatari și *„spectatori”* ca fiind încă un mesaj privind blocarea oricărei tentative de evadare necontrolată a Ucrainei din zona de control - proxy a Federației Ruse.

Himera europenizării exacerbate, înfiripată în rândul unei mari părți a populației ucrainene, și continuarea negocierilor cu Uniunea Europeană au alimentat și mai mult dorința Federației Ruse de readucere a Crimeii în componența *„patriei-mamă”*. Momentul favorabil a apărut odată cu refuzul conducerii Ucrainei, în frunte cu președintele pro-rus, Victor Ianukovici, de a semna la Vilnius (30 noiembrie 2013) Acordul de Asociere cu UE. Evenimentul a generat în Ucraina fenomenul numit *Maidan*, prin ieșirea în stradă a unei mari mulțimi de persoane, nemulțumită de situația social-politică din țară.

Surprinzătoarea implicare „marțiană”, prin apariția unor *„omuleți verzi”*, „humanoizi” nerecunoscuți de nimeni, a arătat, încă o dată, dacă mai era necesar, importanța deosebită pe care o are peninsula în marele joc geostrategic „inter/intragalactic”. De teama „străzii” și, poate, a „omuleților verzi”, Ianukovici fuge în „bârlogul ursului” la Moscova, iar Kremlinul, sub pretextul necesității de a proteja cetățenii ruși, ordonă ocuparea Peninsulei Crimeea (martie 2014). În noua configurație „marțiano-ucraineano-tătaro-rusă[7]” a fost organizat un referendum (16 martie 2014 - *93% pentru*) și Moscova este „obligată”, două zile mai târziu, să admită „cererea” noilor entități de a fi incluse în Federația Rusă, ca doi subiecți federali: Republica Crimeea și orașul federal Sevastopol[8].

De-a lungul istoriei, poziția geografică a peninsulei a suscitat interesul marilor imperii/puteri aflate în expansiune în zona Mării Negre, oferind avantajul strategic necesar pentru controlul acesteia. Avanpost militar și economic la M.Neagră, Crimeea a reprezentat și continuă să reprezinte o necesitate vitală pentru realizarea visului extinderii F.Ruse pe direcțiile strategice V și SV.

Din secolul al XVIII-lea și până în prezent, indiferent de situația geopolitică din zona M.Negre, F.Rusă a reușit să mențină un anumit grad de control asupra Crimeii. Deținerea supremației M.Negre, controlul asupra gurilor Dunării și influența în Balcani au fost deziderate importante aflate la masa negocierilor marilor actori internaționali prezenți în Regiunea Extinsă a Mării Negre, de la „Războiul Crimeii”

(1853-1856), finalizat cu Tratatul de Pace de la Paris (1856)[9], la Revoluția bolșevică din 1917, la implozia URSS („cea mai mare catastrofă geopolitică a secolului XX”[10]), la anexarea din 2014 și până în prezent.

2. De la *„ghimpe”* în coasta F.Ruse la *„cal troian”* în securitatea Mării Negre

Exponențialitatea importanței Pen.Crimeea a ajuns în zona critică cu mult timp înainte de anexarea din 2014. Tranziția de la agonia, sub conducerea lui Boris Elțin, la stabilizarea economică internă, sub conducerea lui Vladimir Putin în primele două mandate (2000-2008), a renăscut speranța reafirmării Federației Ruse ca actor global, iar un obiectiv important al politicii externe ruse a fost/este recâștigarea fizică a unei părți din teritoriile pierdute și controlul celeilalte părți de la distanță, conform *doctrinei Putin*.

Recâștigarea și/sau controlul rapid cel puțin al teritoriilor din vecinătatea F.Ruse pe direcțiile V (spre vestul Europei) și SV (prin M.Neagră spre M.Mediterană) nu mai puteau fi amânate, mai ales în condițiile în care state din Europa de Est și Sud-Est aderaseră la NATO[11] și UE[12]. Întreținerea unor conflicte înghețate (Transnistria/R.Moldova, Abhazia și Osetia de Sud/Georgia și Nagorno-Karabah/Azerbaidjan) devenise insuficientă, în contextul în care toate aceste state urmăreau alinierea la standarde democratice și/sau o cooperare tot mai apropiată cu Occidentul. Erau necesare măsuri concrete, vizibile și radicale în teren, pentru a transmite un mesaj clar „concurenței” (Occidentului) privind determinarea F.Ruse în ceea ce privește controlul zonei *proxy* acesteia.

Primul pas - precedentul **Georgia 2008**[13] a evidențiat foarte clar două aspecte:

- F.Rusă este decisă să treacă, *pe față* (fără a se obosi să-și mascheze acțiunile), la fapte pentru a menține ceea ce a mai rămas din *zona tampon,* din perioada Războiului Rece, dintre cei doi poli de putere (de la Vest: Republica Democrată Germană – Cehoslovacia – Ungaria – Iugoslavia - Albania, până la Est: Estonia – Letonia

– Belarus – Ucraina – Georgia – Armenia – Azerbaidjan). În prezent, zona tampon este ajustată la doar câteva sute de km, pe linia Belarus (stat într-o uniune statală[14]) - Ucraina (amputată în anul 2014[15] și cu potențial de scindare în est[16]) - R.Moldova (cu Transnistria[17] și Găgăuzia[18]) - Georgia (cu cele două republici autonome Abhazia[19]și Osetia de Sud[20]) – Armenia – Azerbaidjan (Nagorno-Karabah[21], Nakhchivan[22] și Karki[23]);

- determinarea timidă a Occidentului în a sancționa intervențiile F.Ruse în proximitatea acesteia, chiar dacă aceasta încalcă legislația internațională și acordurile semnate, căutându-se mai degrabă evitarea confruntării directe dintre Est și Vest.

Mesajul transmis cu acea ocazie (Georgia 2008) nu a temperat entuziasmul extinderii spre Est a NATO și UE, iar revitalizarea economică a F.Ruse (2000-2008) a readus încrederea la Kremlin că se poate și mai mult în ceea ce privește politica externă proxy.

Pasul al doilea pe lista de priorități era *ghimpele Crimeea*. Ghimpe în coasta F.Ruse pentru că, deși „în inimile și mințile oamenilor, Crimeea a fost întotdeauna o parte inseparabilă a Rusiei. Această convingere fermă este bazată pe adevăr și dreptate și a fost transmisă din generație în generație, peste timp în orice împrejurări, în ciuda tuturor schimbărilor dramatice prin care țara noastră a trecut de-a lungul întregului secol al XX-lea[24]", Moscova era nevoită să plătească sume importante de bani anual (2 mld. USD) și să acorde diverse alte facilități Ucrainei (ex.: gaz la preț preferențial) pentru a folosi facilități în Pen.Crimeea.

Similar Georgiei, care sub conducerea președintelui de atunci, Mihail Saakașvili (2004-2013), încerca o cooperare/coordonare apropiată cu Occidentul și Turcia pentru a contracara influența F.Ruse în zona Caucazului de Sud (proiectul Saakașvili - „Caucazul Unit"), Ucraina „cocheta" cu ideea de a adera la UE[25] (ca prim pas către integrarea, în viitor, în NATO).

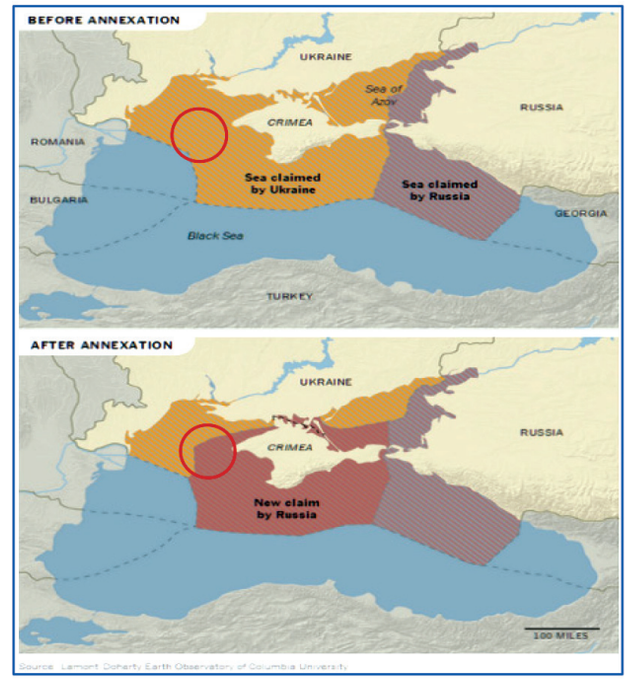
Situația, oricum de-a dreptul iritant - sfidătoare (așa cum o percepea conducerea de la Moscova), nu mai putea continua în acest mod și s-a decis trecerea la pasul doi: anexarea Pen. Crimeea, cu aplicarea tuturor fațetelor războiului contemporan (propagandă, dezinformare, cumpărarea bunăvoinței conducerilor politico-militare centrale și locale, amplificarea dependenței companiilor importante de sprijinul primit din F.Rusă și alte acțiuni hibride, culminând cu acțiunea militară).

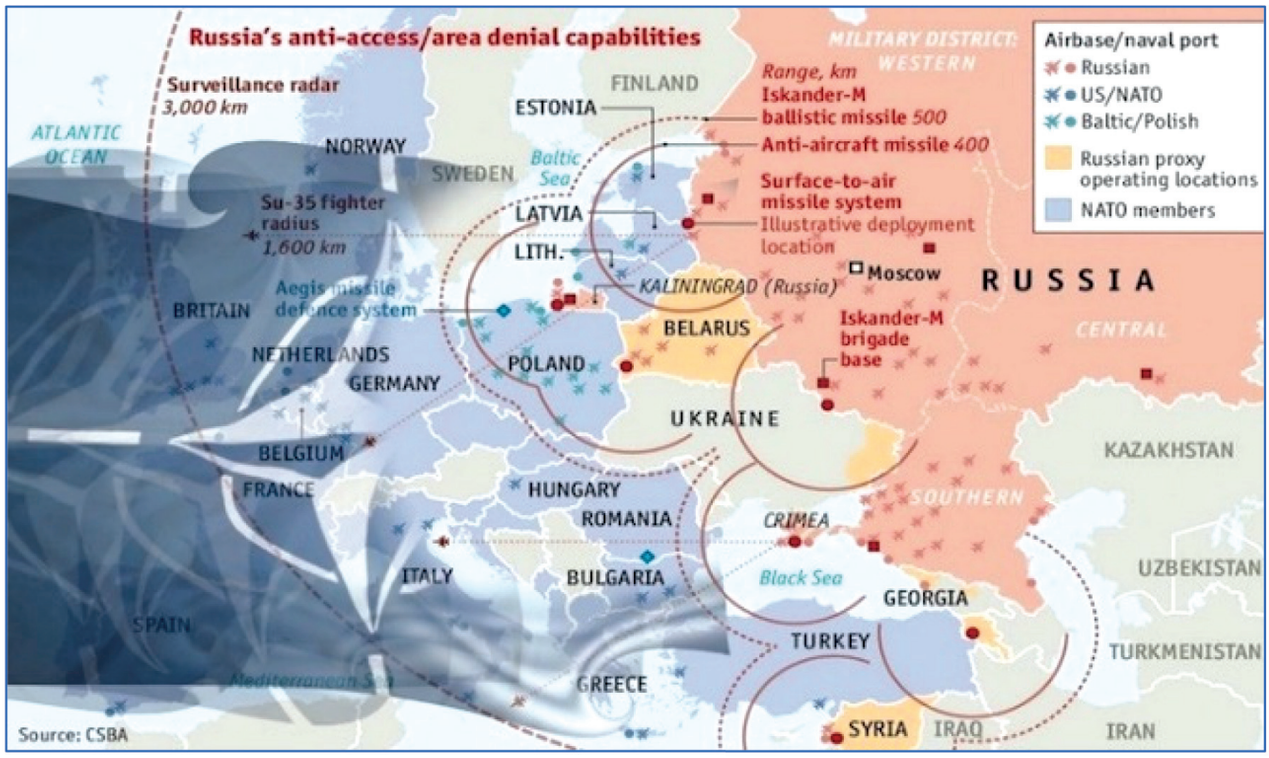
Preluarea, din nou, a controlului total asupra peninsulei și transformările operate ulterior la nivelul acesteia au determinat tranziția de la statutul de *ghimpe* în coasta F.Ruse la cel de *cal troian* în ceea ce privește securitatea în regiune, prin aceasta sperând a fi controlată atât M.Neagră, cât și zone situate dincolo de aceasta (gurile Dunării și Balcani și, prin M.Mediterană, Orientul Mijlociu și Nordul Africii).

3. Dinamica resuscitării „redutei" Pen.Crimeea

Revenirea Crimeii și Sevastopolului în componența patriei-mamă a fost urmată de ample programe de conexare facilă a peninsulei cu zona continentală a F.Ruse, din punct de vedere economic, al infrastructurii de transport și, mai ales, militar.

Din punct de vedere *economic*, Zona Economică Exclusivă (ZEE) a F.Ruse s-a dublat





ca suprafață și a devenit resursă importantă de energie, mai ales că cea mai mare parte a resurselor exploatate (sub pază militară) sunt situate în nord-vestul M.Negre.

De asemenea, au fost implementate proiecte importante de investiții în infrastructura de transport (podul Kerci, autostrada Tavrida, aeroportul internațional Simferopol), de alimentare cu energie electrică (centralele termoelectrice Sevastopol și Simferopol) și de racordare la gaze (conducta Kuban - Crimeea) și la apă (deficitară în urma stopării alimentării cu apă din Ucraina - canalul Crimeii de Nord).

Din punct de vedere *militar*, vârful de lance a tot ceea ce înseamnă capabilități militare dislocate în Crimeea este Flota rusă a M.Negre (FRMN), componentă de nivel operativ-strategic a Flotei Maritime Militare a F.Ruse, alături de celelalte trei flote (Flota de Nord, Flota din Oceanul Pacific și Flota din M.Baltică) și de Flotila din M.Caspică[26].

FRMN îndeplinește misiuni pentru asigurarea securității naționale și promovarea intereselor ruse de politică externă și de securitate, în principal în M.Neagră (inclusiv M.Azov) și M.Mediterană. Pentru îndeplinirea misiunilor încredințate, FRMN are în înzestrare capabilități navale considerabile: nave de suprafață, nave antisubmarin, nave purtătoare de rachete și de sprijin, submarine, o componentă aeriană (Aviația FRMN) și Trupe de Apărare de Coastă.

Deși anterior anexării peninsulei (2014), componenta militară rusă dislocată în Crimeea era limitată cantitativ și calitativ, FRMN a fost întrebuințată activ, cu succes, în conflictele din Georgia (2008), respectiv Ucraina (2014).

După anexare, F.Rusă a început să investească masiv în programe de modernizare a forțelor armate dislocate în Peninsulă, în principal prin dotarea cu tehnică și armament modern necesare dezvoltării *mediului A2/AD (Anti Access/ Area Denial)* în M.Neagră.

Supraaglomerarea cu tehnică și personal a Pen.Crimeea, în perioada 2014-2021, a generat o creștere exponențială a numărului de militari ruși (de la *12.500* în 2014 la *43.000* planificați pentru anul 2025, militari ruși și ucraineni din peninsulă care s-au înrolat în structurile armatei ruse), precum și a capabilităților disponibile pentru îndeplinirea noilor misiuni.

În continuare vom prezenta, pe componente, doar o parte dintre modificările organizatorice ale structurilor dislocate în Peninsulă și capabilitățile noi intrate în dotarea acestora, după 2014:

♦ *Componenta navală* (anterior, dotarea FRMN includea capabilități învechite, preponderent nave produse cu 30-40 de ani în urmă):

◊ introducerea în înzestrarea FRMN a unor platforme navale noi, printre care:

- 3 fregate clasa Amiral Grigorovici (proiect 11356): Amiral Grigorovici (2016), Amiral Essen (2016) și Amiral Makarov (2017), dotate cu complexe moderne de rachete Kalibr[27]-NK[28] (cu rază de acțiune de până la 2.500 km[29]);
- 6 submarine[30] clasa Kilo+ (proiect 636.3): Novorossiysk (2014), Rostov pe Don (2014), Staryy Oskol (2015), Krasnodar (2015), Velikiy Novgorod (2016) și Kolpino (2016), înzestrate cu complexul modern de rachete Kalibr-PL;
- 7 nave purtătoare de rachete: clasa Vasily Bykov (proiect 22160) - Vasily Bykov (2018), Dmitriy Rogachev (2019) și Pavel Derzhavin (noiembrie 2020); clasa Buyan-M (proiect 21631): - Vyshny Volochek (2018), Orekhovo-Zuevo (2018), Ingușetia (2019), Grayvoron (ianuarie 2021), de asemenea, dotate cu sisteme de rachete Kalibr.

◊ revitalizarea crucișătorului Moskva (nava amiral a FRMN-operațională din 1983) din cadrul Diviziei 30 Nave de Suprafață - Sevastopol, care deși a fost introdus la reparații în 2016, în Șantierul Naval Sevastopol, și părea că va fi casat, fiind o navă veche, a fost modernizat și începând cu anul 2020 îndeplinește, din nou, misiuni în Marea Neagră;

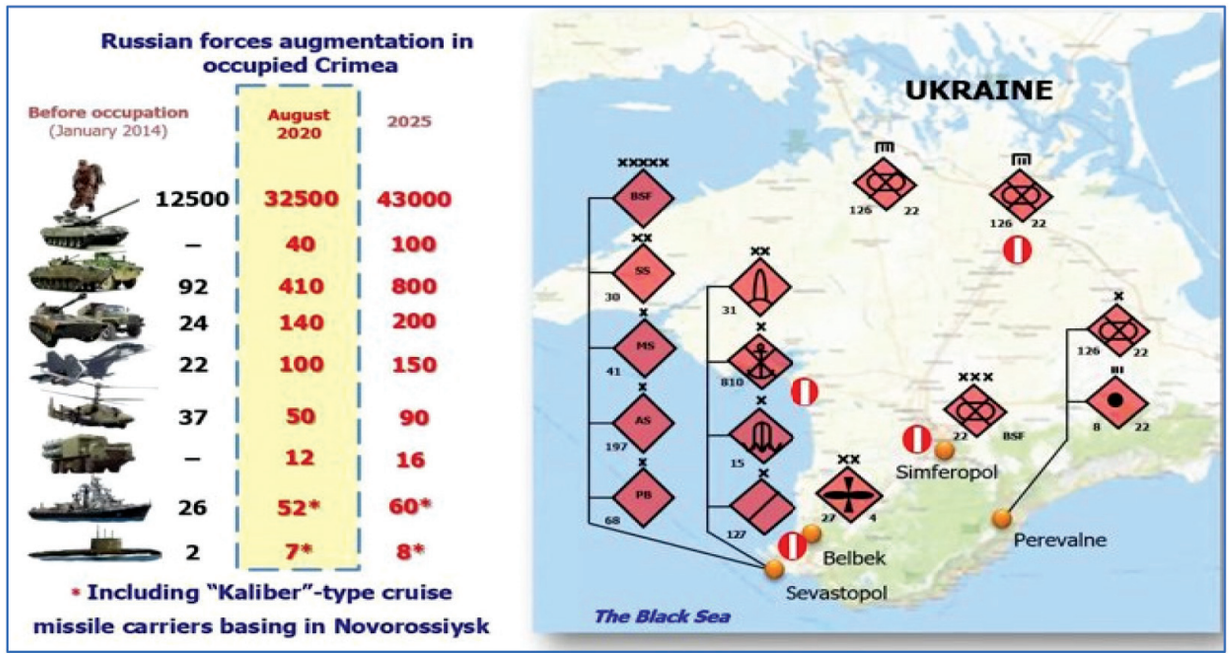
◊ modernizarea navelor vechi, proces în care sunt angrenate mai ales nave de sprijin;

◊ constituirea unor detașamente speciale dotate cu vedete rapide antidiversiune Grachonok și Rapter pentru combaterea misiunilor de sabotaj/ diversiune.

Noile tipuri de nave au fost dotate cu tehnică utilizând noul *Concept modular pentru armament*, lucru care va permite adaptarea rapidă a acestora la noi capabilități dezvoltate ulterior (ex.: racheta hipersonică Zircon, aflată în faza finală de testare).

♦ *Componenta aeriană* (cu o evoluție de la aprox. 50 de aeronave relativ învechite la aprox. 150 de avioane și elicoptere noi sau modernizate și 5 divizioane de rachete de tipul S-400 Triumf):

◊ constituirea (2014) Diviziei 27 Aviație Mixtă - Belbek, în subordinea Armatei 4 Forțe Aeriene și Apărare Antiaeriană - Rostov pe Don, prin redislocarea unor structuri din zona continentală, organizată pe trei regimente[31],



dotate cu aprox. 60 de aeronave de tipurile Su-30M2, Su-27, Su-24M, Su-24MR, Su-25SM și Su-25UB și aprox. 40 de elicoptere de tipurile Ka-52, Mi-35, Mi-28N, Mi-8AMTȘ și Mi-26 (majoritatea tehnicii de aviație enumerată a fost fabricată și introdusă în înzestrare în perioada 2012-2016);

◊ modernizarea înzestrării celor două regimente de aviație din organica FRMN[32]:

- Regimentul 43 a primit 12 avioane multirol de tipul Su-30SM, iar cele 12 aeronave de bombardament/cercetare-recunoaștere de tipurile Su-24, respectiv Su-24MR ale Escadrilei 2 Aviație ale aceluiași regiment au fost modernizate;
- aeronavele aflate în dotarea Regimentului 318 (13 aeronave de tipurile Be-12 și An-26 și 20 elicoptere de tipurile Ka-27, Mi-8, Ka-29 și Ka-31R[33]) au fost dotate cu aparatură de bord modernă;

◊ modernizarea înzestrării sistemului de apărare antiaeriană[34] dotat cu sisteme de rachete antiaeriene S-400 Triumf (cinci divizioane), S-300, Buk-M2/3 și Pantsir-S/S1.

♦ *Componenta de apărare de coastă* (înființată/modernizată aproape de la zero):

◊ înființarea (2016) Corpului 22 Armată - Simferopol din cadrul Trupelor de Apărare de Coastă, care include aproape toate structurile terestre dislocate în Pen.Crimeea[35] (majoritatea structurilor corpului au fost constituite după anexarea din 2014[36], fiind înființate de la zero sau pe baza unor unități militare care anterior aparțineau Forțelor Armate ucrainene);

◊ întărirea sistemului de apărare de coastă cu sisteme de rachete de coastă Bal, Bastion și Utes;

◊ dotarea cu tehnică modernă: transportoarele blindate de tip BTR-80[37] au fost înlocuite cu cele moderne de tip BTR-82AM, iar dronele au intrat în înzestrarea majorității structurilor militare.

♦ *Componenta aeropurtată*[38] (înființată de la zero):

◊ înființarea (2017) Batalionului 171 Desant-Asalt - Feodosia din cadrul Diviziei 7 Desant-Asalt - Novorossiysk și reorganizarea acestuia (în curs de desfășurare) în Regimentul 97 Desant-Asalt – Feodosia.

Suplimentar, la toate categoriile de forțe și genuri de armă au fost făcute investiții masive în *infrastructură:* modernizarea bazelor de dislocare permanentă (terestre, aeriene și navale), baze de antrenamente, poligoane de instrucție (inclusiv Opuk), aerodromuri, piste de decolare/aterizare (poate cea mai importantă care ar trebui menționată este cea de la Belbek, modernizată pentru a putea ateriza inclusiv aeronave ale Aviației Strategice, în special, bombardiere cu rază lungă de acțiune de tipul Tu-22M3).

♦ *Perspectiva apropiată*:

◊ alte 12 nave purtătoare de rachete, dotate cu sisteme Kalibr, sunt planificate a fi introduse în înzestrarea FRMN în perioada următoare:

- clasa Vasili Bykov, proiect 22160: Sergey Kotov (2021), Viktor Velikiy (2022), Nikolay Sipyagin (2023);
- clasa Buyan-M, proiect 21631: Naro-Fominsk (2022), Stavropol (2023);
- clasa Karakurt[39], proiect 22800: Kozelsk (2020-în teste), Tsiklon (2021), Okhotsk (2020-în teste), Askold (2021), Amur (2021) și Vikhr (2021).

◊ corveta Merkury, proiect 20386 (2022);

◊ navele mici purtătoare de rachete Burya, Tucha și Taifun (proiect 22800), probabil, vor intra (2022-2023) în dotarea FRMN. (În funcție de evoluțiile mediului de securitate și redirecționarea efortului pentru apărarea intereselor strategice există posibilitatea ca o parte din navele planificate a intra în dotarea FRMN să fie redirecționate către Flota rusă din Marea Baltică).

◊ la Sevastopol va fi instalată (începând din anul 2021) noua stație de radiolocație de tip Yakhroma, care „lucrează în patru game de unde: metrice, centimetrice, decimetrice și milimetrice și are o deschidere de 270 de grade”[40], ca parte a componentei terestre a sistemului rusesc de avertizare timpurie asupra unui atac cu rachete (conform planurilor anterioare, era planificat a fi

instalat un radar de tipul Voronej-SM, cu rază de acțiune aprox. 6.000 km, capabil să urmărească până la 500 de ținte simultan);

◊ probabil vor fi dislocate în Pen.Crimeea sisteme de rachete Iskander, după finalizarea procesului de modernizare aflat în curs de derulare;

◊ sistemele de apărare antiaeriană S-300 vor fi înlocuite, probabil, cu noile sisteme S-350 Vityaz;

◊ în înzestrarea FRMN există posibilitatea de a mai fi introduse încă un submarin și una dintre fregatele Proiect 22350, similară cu fregata Amiral Gorșkov;

◊ posibilitatea redislocării unor bombardiere cu rază lungă de acțiune de tipul Tu-22M3 în Pen. Crimeea.

Prin măsurile întreprinse ulterior anexării, avanpostul nou-creat și consolidat a fost rapid transformat dintr-un teritoriu *cucerit, cedat, concesionat* și *revendicat* într-o **redută pe direcția strategică Sud-Vest** și este folosit ca o continuare firească a politicii externe expansioniste teritoriale sau, dacă nu pentru moment teritorială, de promovare/apărare a intereselor Federației Ruse în regiune.

4. Pen.Crimeea - avanpost geostrategic pe direcția strategică Sud-Vest: M.Neagră – M.Mediterană

Extinderea NATO și UE în estul și sud-estul Europei și consolidarea rezilienței statelor din respectivele zone au determinat Moscova să-și focuseze efortul strategic pentru:

◊ consolidarea apărării, hărțuire și promovarea intereselor prin interpuși în state satelit/client pe direcția strategică Vest;

◊ preluarea inițiativei/ofensivă pe direcția strategică Sud-Vest (F.Rusă – M.Neagră – M.Mediterană - Orientul Mijlociu - Nordul Africii și mai departe în continentul african).

Pași concreți pe direcția strategică Sud-Vest au fost demarați de mult și au presupus:

- dezvoltarea celor două baze militare din Siria (Baza Navală Tartus și Baza Aeriană Hmeymim) și susținerea președintelui sirian Bashar al-Assad la conducerea statului;
- cooperare cu Turcia (stat membru NATO), în anumite domenii: vânzarea de sisteme de rachete de tipul S-400 Triumf, construcția unei centrale nucleare, misiuni de luptă în comun în nord-estul Siriei, etc.;
- cooperarea apropiată cu Egiptul, inclusiv prin exerciții navale în comun în Marea Mediterană[41] și Marea Neagră[42];
- implicarea activă în conflictul din Libia, prin susținerea mareșalului Khalifa Haftar în conflictul cu Guvernul de Uniune Națională pentru a prelua conducerea Libiei (deși pe tabere opuse cu partenerul turc);
- comerț cu armament cu Algeria (al treilea importator de armament rusesc);
- reașezarea relațiilor cu state din Peninsula Arabică (ex.: vizita președintelui Vladimir Putin în Pen. Arabică - octombrie 2019 și încheierea unor parteneriate de cooperare multi-domeniu cu state din regiune);
- îndeplinirea unor misiuni antipiraterie în Golful Aden și Marea Arabiei (F.Rusă dislocă, pe principiul rotației, nave în zonă pentru securizarea intereselor);
- înființarea unei baze navale la Marea Roșie, în Sudan[43], ca punct de asigurare

tehnico-materială a forțelor navale ruse, în sprijinul navelor care îndeplinesc misiuni anti-piraterie în Marea Roșie și Cornul Africii, precum și pentru navele care participă la exerciții navale în Oceanul Indian;

- cooperarea militară intensificată cu Africa de Sud (exercițiul naval ruso-sino-sud-african cu numele de cod *Mosi* - noiembrie 2019 și misiuni de zbor ale Aviației Strategice ruse spre/dinspre Africa de Sud cu bombardiere strategice de tipul Tu-160 în luna octombrie 2019);
- cooperarea militară cu Insulele Capului Verde și Guineea Ecuatorială (escale ale Forțelor Navale în porturile acestor state);
- susținerea unor regimuri dictatorial-autoritare din alte state africane, mai ales prin brațul înarmat reprezentat de armata privată Wagner (ex.: R.Centrafricană).

Politica externă promovată de autoritățile ruse, care doresc să creeze percepția aparentă a caracterului defensiv al acesteia, se fundamentează pe doi piloni care au definit/ vor defini următorii pași ai F.Ruse în politica sa expansionistă: (1) dreptul F.Ruse *de a proteja viața și demnitatea cetățenilor noștri, indiferent unde s-ar afla* și (2) dreptul la *regiuni unde are interese privilegiate,* unde se află țări cu care a avut *tradițional relații cordiale și prietenești, legături istorice speciale.*

Venirea generalului Serghei Șoigu la conducerea Ministerului rus al Apărării (noiembrie 2012) și schimbarea filosofiei anterioare de organizare și întrebuințare a Forțelor Armate au condus la reorganizarea și repoziționarea în regiunile militare Vest și Sud (inclusiv Crimeea) a unui număr important de structuri militare, înzestrate cu armament modern, cu statutul *gata de luptă permanent.*

Cu state de organizare a forțelor armate similare pe timp de pace și pe timp de război, organizate pe șase armate de arme întrunite în regiunile militare Vest și Sud (câte trei armate în fiecare regiune militară) și un corp de armată în Crimeea, cu câteva divizii și brigăzi de desant aerian, cu capabilitățile de transport ale Aviației Militare de Transport (în principal, aeronave de tipurile An-124-100 și Il-76MD), cu mijloacele aeriene ale Aviației Strategice (bombardiere strategice de tipurile Tu-160 și Tu-95MS și bombardiere cu rază lungă de acțiune de tipul Tu-22M3), cu două Flote (Flota rusă din M.Neagră și Flota rusă din M.Baltică) și cu o Flotilă (Flotila rusă din Marea Caspică), cu triada hipersonică (Avangard[44] - Kinzhal[45] - Zircon[46]), cu tangaje între legislația internațională și dreptul rus de a-și apăra interesele, F.Rusă încearcă să răspundă extinderii NATO spre Est și să-și promoveze interesele de politică externă și în Orientul Mijlociu și Africa.

Concluzii

Dacă în urmă cu șapte ani F.Rusă dispunea de capabilități reduse în Peninsula Crimeea, acum militarizarea accelerată a Peninsulei a făcut din aceasta o adevărată *redută* pentru apărarea intereselor rusești în M.Neagră și un *avanpost* al politicii externe proxy în Regiunea Extinsă a M.Negre, dar și pe direcția strategică Sud-Vest (din M.Neagră până în Orientul Mijlociu și Africa).

Strategia rusă în M.Neagră, urmărită de secole de conducătorii ruși, începând cu Petru cel Mare, presupune atingerea a cel puțin două obiective majore: *controlul regiunii* (inclusiv acces la gurile Dunării) și *asigurarea libertății de mișcare spre/dinspre strâmtorile turcești*, pentru a susține eforturile de proiecție a forței în M.Mediterană, Orientul Mijlociu și Africa.

Politica agresivă promovată de către Kremlin, trecând, fără ezitare, peste barierele legislației internaționale, pe principiul *interesul primează,* coroborată cu capacitatea de redirecționare rapidă a efortului strategic de pe o direcție pe alta *(Vest, Sud-Vest, Asia-Pacific, Arctica)* trebuie să crească dinamismul eforturilor de consolidare a potențialului de descurajare multi-domeniu al statelor aflate pe direcțiile de interes strategic ale Federației Ruse.

Regândirea politicilor de securitate în Marea Neagră, unde interesele geostrategice globale se ciocnesc, unde, încă o dată, se refac *jocurile*, unde se retrasează granițe și unde se încearcă resetarea ordinii mondiale, necesită *fermitate strategică*, *flexibilitate tactică* și *efort concertat* din partea unor lideri competenți și patrioți, în cadru aliat.

Bibliografie

1. *The future of the Russian military/Russia's ground combat capabilities and implications for US-Russia competition*, RAND Corporation;
2. *Trends in international arms transfers 2019*, SIPRI, March 2020;
3. *United Nations Conflict Analysis Practice Note*, Version: 13 May 2016;
4. *Russian Octopus in action - case Ukraine*, Centre for Global Studies Strategy XXI, 2020;
5. GRANT, Thomas D., „Frozen Conflicts and International Law", *Cornell International Law Journal*: Vol.50: No. 3, Article 1, 2017;
6. KUIMOVA, Alexandra; Siemon T. WEZEMAN, Ru*ssia and Black Sea Security*, SIPRI, Dec 2018, https://www.sipri.org/publications/2018/sipri-background-papers/russia-and-black-sea-security;
7. HILL, William H., *More than a Frozen Conflict: Russian Foreign Policy Toward Moldova*, Atlantic Council, Eurasia Center, August 2018, https://www.atlanticcouncil.org/wp-content/uploads/2018/08/More_Than_A_Frozen_Conflict_web_final.pdf;
8. *Armaments, Disarmament and International Security*, SIPRI, 2019;
9. „Resolving Frozen Conflicts, The Challenges of Reconciliation", in *Per Concordiam*, nr.2, 2010, https://www.marshallcenter.org/en/publications/concordiam/resolving-frozen-conflicts-challenges-reconciliation;
10. https://geostrategy.org.ua/Black Sea Security Analytical journal 2 (38) 2020;
11. https://defenseromania.ro;
12. https://remnmilitaryblog.com;
13. https://bsmap.ro;
14. https://monitorulapararii.ro;
15. https://csba.org;
16. https://agerpres.ro/politica-externa;
17. https://risap.ro;
18. https://newstrategycenter.ro
19. https://geopolitics.ro;
20. https://stratcomcoe.org;
21. https://blacknews.ro;
22. https://adevarul.ro/international;
23. https://larics.ro;
24. https://dw.com;
25. https://behorizon.org;
26. https://rand.org.

[1] În urma războiului ruso-turc (1768-1774). Meritul a revenit Feldmareșalului Grigori Potemkin, sfetnicul împărătesei Ekaterina a II-a, cea care, practic, a finalizat faimosul *Testament al lui Petru I cel Mare*, respectiv ieșirea la *„mările calde"*.

[2] Hatmanul Ucrainei, Bogdan Hmelnițki, de teama polonilor, a hotărât, în urma unei decizii a Parlamentului de atunci, unificarea cu Rusia, condusă de țarul Aleksei Mihailovici (tatăl viitorului țar Petru I, supranumit cel Mare).

[3] Uniunea Republicilor Sovietice Socialiste.

[4] De ce cu șapte ani înainte? Conducerea politică de la Kiev începuse să cocheteze cu ideea de asociere la UE.

[5] Atunci, președinte al Ucrainei.

[6] O strategie a Moscovei de înlocuire a influenței militare cu presiunea economică prin preț la gaze corectat ca „bonus de ascultare" și cu amenințarea întreruperii tuturor furnizărilor de gaze.

[7] Peninsula este locuită de aproximativ 2,3 milioane de persoane (67,9% ruși, 15,6% ucraineni, 10,5% tătari crimeeni și 6% alte etnii) potrivit recensământului din 2014.

[8] Orașul-bază militară Sevastopol este atât de important încât, rapid, i-a fost oferit rangul de oraș federal, alături de Moscova și Sankt Petersburg, deși are mai puțin de 400.000 de locuitori și în condițiile în care în Federația Rusă există multe orașe care depășesc fiecare un milion de locuitori.

[9] 30 martie 1856 - Rusia pierde inițiativa pe direcțiile strategice V și SV (în zone aflate sub stăpânirea Imperiului Otoman), controlul asupra gurilor Dunării și o parte din influența asupra Principatelor Române și Serbiei (art.7) și este obligată la un regim restrictiv la Marea Neagră (inclusiv dezafectarea fortăreței Sevastopol - ulterior cea mai importantă bază navală sovietică/rusă la Marea Neagră) - art. 11 și 13.

[10] Declarația președintelui rus Vladimir Putin.

[11] Ungaria, Polonia, Cehia (1999), Bulgaria, Slovacia, Slovenia, Estonia, Lituania, Letonia, România (2004), Croația, Albania (2009).

[12] Cehia, Estonia, Letonia, Lituania, Slovacia, Polonia și Ungaria (2004), Bulgaria și România (2007), Croația (2013).

[13] Războiul ruso-georgian din august 2008.

[14] Uniunea Statală Rusia-Belarus, inițial înființată la 2 aprilie 1996 și apoi consolidată prin semnarea a două tratate: Tratatul Uniunii Bielorusia și Rusia (2 aprilie 1997, Minsk) și Tratatul Uniunii Slave (8 decembrie 1999, Moscova).

[15] În anul 2014, Peninsula Crimeea a intrat în componența Federației Ruse.

[16] În prezent, în regiunile Donețk și Lugansk este în desfășurare un conflict armat pentru separarea celor două regiuni de Ucraina.

[17] Denumită oficial Republica Moldovenească Nistreană, teritoriu îngust la granița dintre Ucraina și R.Moldova, Transnistria și-a autoproclamat independența în septembrie 1990, fără recunoaștere internațională.

[18] Unitatea Teritorială Autonomă Găgăuzia - unitate autonomă în sudul R.Moldova.

[19] Republica Autonomă Abhazia - regiune în nord-vestul Georgiei, la granița cu Federația Rusă, autoproclamată independentă – a doua oară, în august 2008, în urma conflictului ruso-georgian.

[20] Republica Autonomă Osetia de Sud - regiune aflată la granița de nord a Georgiei cu F.Rusă, autoproclamată independentă în august 2008.

[21] Nagorno-Karabakh - regiune autonomă situată în zona central-vestică a Azerbaidjanului, revendicată de Armenia.

[22] Republica Autonomă Nakhchivan - exclavă a Azerbaidjanului, care se învecinează cu Armenia la est şi nord, cu Turcia la nord-vest şi cu Iran la sud-vest, dorită îndelung de către Armenia.

[23] Karki - sat, exclavă a Republicii Autonome Nakhchivan/Azerbaidjan, în interiorul teritoriului armean, ocupat de Armenia.

[24] Declarația președintelui Vladimir Putin în anul 2014, după anexare.

[25] Negocierile au avansat până în noiembrie 2013.

[26] Pentru îndeplinirea de misiuni în Marea Neagră și/sau Marea Mediterană, atunci când situația o impune, au fost/pot fi folosite nave ale Flotilei din Marea Caspică, care prin căi navigabile interne sunt rapid redislocate în sprijinul celor din cadrul FRMN.

[27] Complexele de rachete Kalibr pot întrebuința trei tipuri de rachete: 3M54 - rachetă antinavă, 3M14 - rachetă de croazieră și 91R1 - rachetă-torpilă, dezvoltate în mai multe versiuni. Rachetele 3M14T și 3M14K pot fi dotate cu ogive convenționale (rază de acțiune: aprox. 1.500 km) sau cu ogive nucleare (rază de acțiune: aprox. 2.600 km).

[28] Complexele de rachete Kalibr-NK dispun de instalații de lansare 3S14 capabile să utilizeze rachete Kalibr, racheta antinavă Onyks, racheta antinavă BrahMos și, în perspectivă, racheta antinavă hipersonică Zircon.

[29] În prezent, se află în faza de cercetare-dezvoltare noua rachetă Kalibr cu rază de până la 4.500 km.

[30] Submarinele sunt utilizate începând cu anul 2015 și în estul Mării Mediterane pentru misiuni de luptă în cadrul conflictului din Siria (în permanență două dintre acestea sunt dislocate în Marea Mediterană). Suplimentar față de cele nou-introduse în înzestrare, FRMN mai are în dotare și submarinul Alrosa (clasa Kilo, operațional începând cu anul 1990), aflat în prezent în proces de reparații-modernizare.

[31] Regimentul 37 Aviație Mixtă - Gvardeiskoe, Regimentul 38 Aviație Vânătoare - Belbek și Regimentul 39 Elicoptere - Djankoi.

[32] Regimentul 43 Aviație Asalt - Saki și Regimentul 318 Aviație Mixtă – Kacia. Cele două regimente au existat și înainte de 2014, dar cu o dotare mult inferioară.

[33] Elicopter de avertizare timpurie, introdus în înzestrare în anul 2020.

[34] Divizia 31 Apărare Antiaeriană - Sevastopol din cadrul Armatei 4.

[35] Brigada 810 Infanterie Marină - Sevastopol, Brigada 126 Apărare de Coastă - Perevalnoe, Brigada 127 Cercetare - Pargolovo, Brigada 11 Rachete și Artilerie de Coastă - Anapa, Brigada 15 Rachete și Artilerie de Coastă - Sevastopol, Regimentul 8 Artilerie - Simferopol, Regimentul 1096 Rachete Antiaeriene - Sevastopol, Regimentul 68 Geniu - Evpatoria și Centrul 744 Transmisiuni – Sevastopol.

[36] Anterior anului 2014, în forma actuală existau Brigada 11 și Regimentul 1096. Brigada 810 și Centrul 744 au fost formate prin reorganizarea unor structuri existente (regimentul de infanterie marină al FRMN și Centrul 529 Transmisiuni - Sevastopol).

[37] Aflate în înzestrarea Brigăzii 810 Infanterie Marină.

[38] Categorie independentă de forțe ale armatei - Trupele de Desant Aerian.

[39] Este planificată intrarea în dotare a 8 nave purtătoare de rachete clasa Karakurt până în anul 2024.

[40] Potrivit agenției de presă rusă Tass, care citează o sursă din cadrul Complexului Militar Industrial Rus.

[41] Componenta navală rusă dislocată în estul Mării Mediterane desfășoară periodic exerciții navale în comun cu Forțele Navale egiptene în raioane din partea sud - sud-estică a Mării Mediterane.

[42] Ex.: Podul Prieteniei-2020, 17-24 noiembrie 2020, în zona Novorossiysk.

[43] Acord parafat între Federația Rusă și Sudan în noiembrie 2020.

[44] Avangard - vector planor hipersonic cu lansare de pe platforme terestre, care poate fi echipat cu încărcături convenționale sau nucleare și poate evolua cu viteze maxime de 27 Mach.

[45] Kh-47M2 Kinzhal - rachetă balistică hipersonică cu lansare de pe platforme aeriene, cu rază de acțiune de peste 2.000 km, cu viteză de 10-12 Mach și cu capacitate de a efectua manevre evazive pe timpul zborului către țintă.

[46] 3M22 Zircon - rachetă de croazieră antinavă, hipersonică, cu lansare de pe platforme navale capabilă să lovească ținte aflate la aprox. 1.000 km, cu o viteză de 8-9 Mach.

REGIMUL TALIBAN – DE LA STRUCTURI TERORISTE LA ACTE DE GUVERNARE

Marian ȘTEFAN*

Abstract

Twenty years after the most devastating terrorist attacks, the US withdrawal from Afghanistan and the immediate takeover of the country by the Taliban represent the greatest strategic success for Al-Qaeda and the global jihadist movement since 9/11.

Understanding how to implement a military strategy in Afghanistan has a number of key features. First, the nature of irregular warfare makes it extremely difficult to assess the effectiveness of a strategy, leading coalition forces to rely on partial, incomplete, or misleading tactical and operational data to measure strategic progress. Without obvious strategic values, neither civilians nor military leaders can gain a clear understanding of strategic progress in an operational environment characterized by obscurity and societal fragmentation. Second, the military's attempts to provide decision-makers with the justification for tactical actions taken and the strategic value of operational control of territories, constantly providing positive assessments of tactical and operational progress, led to a picture of the surreal operational environment, which strengthened the approach. strictly military of the second phase of the joint mission in the theater of operations Afghanistan.

Keywords: *terrorism; Al-Qaeda; the Taliban; operational environment.*

Începuturi ale manevrelor de forțe

Atacurile din 11 septembrie 2001 au catapultat Al-Qaeda de la o relativă obscuritate la un nume de „uz casnic“ în Statele Unite. Pe măsură ce World Trade Center și o parte a Pentagonului s-au prăbușit, a devenit clar că SUA au subestimat amenințarea reprezentată de grupul extremist islamist, condus de un proscris saudit din Afganistan care visa să unească musulmanii și să distrugă „mitul invincibilității americane”.

Fondată în 1988 de Osama bin Laden, Al-Qaeda a apărut din legăturile structurilor tribale afgane insurgente aflate în linia întâi pe câmpul de luptă împotriva Uniunii Sovietice, redirecționate, treptat, spre lupta împotriva Occidentului, prin recrutarea rapidă a diferiților adepți mujahedini dezamăgiți de sprijinul administrațiilor americane pentru Israel și dictaturile din Orientul Mijlociu. Când regimul taliban a preluat puterea în Afganistan, în 1996, i-a oferit organizației Al-Qaeda sanctuarul care i-a permis să organizeze tabere de antrenament și baze de planificare a atentatelor teroriste, inclusiv cele din 9/11.

Evenimentele din 11 septembrie 2001 au constituit și încă reprezintă o puternică inspirație și motivație pentru o generație revoltă a extremiștilor islamiști. Însă, aceste evenimente au provocat, de asemenea, o reacție de care se temeau unii lideri talibani și Al-Qaeda, care, potrivit unor declarații ulterioare actelor teroriste, se pare că s-au opus atacului asupra Statelor Unite. Majoritatea musulmanilor din întreaga

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

lume au fost dezgustați de uciderea în masă a civililor în numele religiei lor. Efectul scontat de strategul operațiunilor teroriste, bin Laden, acela de a reuși să provoace la nivelul opiniei publice americane o poziție fermă de dezacord și nesusținere a deciziilor guvernului de a continua intervențiile armatei SUA în afacerile interne ale altor state, în spații și zone aflate la mare depărtare de granițele statului, a provocat exact contrariul și anume faptul că opinia publică s-a coalizat unanim pentru a susține răspunsul ferm sugerat de președintele Bush, fapt ce s-a transformat în cel mai lung război al Americii.

Al-Qaeda „a reușit prea bine cu 11 septembrie", a declarat Barak Mendelsohn, profesor de științe politice la Haverford College, pentru Today's WorldView. „A depășit așteptările lor și apoi le-a fost imposibil să repete efectiv un eveniment la scara celui din 9/11".

După intervenția din Afganistan, condusă de SUA în 2001, liderii Al-Qaeda au fugit în Pakistan sau Iran, mulți fiind uciși sau capturați. Bin Laden a dispărut din peisajul zonei de conflict câțiva ani și atunci când a reapărut pe canalele mediatice internaționale, dornic să repete atacurile din 11 septembrie, a fost informat de către liderii grupului că, în configurația redusă și descentralizată a organizației Al-Qaeda, o astfel de operațiune era de neconceput.

În urma intervenției în forță a structurilor coaliției în teatrul de operațiuni Afganistan, lumea occidentală a considerat, în scurt timp, învinsă gruparea teroristă, însă Al-Qaeda a demonstrat o rezistență remarcabilă, chiar și după două decenii. Intervenția susținută de administrația președintelui George W. Bush în Irak în 2003 s-a dovedit a fi un avantaj pentru grup, alimentând apariția unui nou și puternic afiliat grup Al-Qaeda, condus de Abu Musab al-Zarqawi, un extremist iordanian cu tendințe de violență nediscriminată. Grupurile islamiste din Somalia, Yemen și Africa de Nord au consolidat, de asemenea, legăturile cu Al-Qaeda, ceea ce a catalizat transformarea organizației dintr-un grup strâns concentrat în Afganistan și Pakistan într-o rețea extinsă de francize în Africa, Asia și Orientul Mijlociu, coalizate ideologic și descentralizate organizațional, particularitate ce oferă o mare mobilitate de acțiune și un eficient management organizațional dovedit de acțiunile instrumentate în ultimii ani. Uciderea lui Bin Laden de către US Navy SEAL în Pakistan, în 2011, a dat o lovitură puternică grupării Al-Qaeda, dar revoltele din „Primăvara arabă" din acel an au oferit noi oportunități organizației de a-și extinde influența în zone slab guvernate sau în care transformările politice și sociale au produs haos, stimulând promisiunile de loialitate din partea grupărilor islamiste implicate în războaie civile în Siria, Libia și în alte părți ale lumii. Când Statul Islamic s-a desprins din afiliatul irakian Al-Qaeda, a încercat să se poziționeze ca o alternativă mult mai radicală. Declarațiile organizației Statul Islamic, cu pretenții teritoriale de califat în Irak și Siria, i-au oferit popularitate și susținere la nivelul islamiștilor radicali din întreaga lume, care au călătorit în regiune pentru a se alătura grupului, ce reușise, exploatând vidul de putere și slăbiciunile administrative, să construiască un „stat" și o mașină de propagandă diferită de orice altceva cunoscut până la acel moment.

Chiar și în condițiile de transformări și rebranduiri, Al-Qaeda a reușit să se mențină prin filialele sale, iar disponibilitatea organizației de a se integra în mișcările locale i-a asigurat supraviețuirea. Însă, la rândul său, organizația teroristă, divizată de probleme și conflicte locale, a produs un paradox: chiar dacă reputația pe care a câștigat-o în urma evenimentelor din 11 septembrie a ajutat-o să-și extindă dramatic amprenta internațională, filialele sale sunt acum mai preocupate de luptele locale decât de purtarea unui război împotriva Occidentului. În aceste condiții, mediul operațional actual la nivel geostrategic se confruntă cu problema existenței unei organizații teroriste mai slab coalizată, dar cu o prezență mai numeroasă în anumite zone neguvernate sau slab guvernate.

Revenirea la putere a regimului taliban

Victoriile rapide ale talibanilor în Afganistan au făcut ca sărbătorirea aniversării a 20 de ani de la evenimentele din 11 septembrie să aducă un plus de încredere în rândul membrilor comunității

jihadiste Al-Qaeda, care, împreună cu susținătorii săi și grupurile media afiliate, au injectat rețelele de socializare cu pachete de conținut bine pregătite: discursuri din partea conducerii, postere, hashtag-uri desemnate și canale întregi dedicate succesului acțiunilor teroriste din 11 septembrie 2001. Acum, atenția lumii s-a îndreptat către talibani, noii conducători ai Afganistanului ce continuă să mențină legăturile cu Al-Qaeda.

Al-Qaeda și afiliații săi prezenți pe grupurile de socializare și-au exprimat exaltarea și au împărtășit sentimentul de victorie al recuceririi teritoriilor afgane de către noul regim taliban. Al-Qaeda din Peninsula Arabică a numit cucerirea talibanilor „începutul unei transformări esențiale", sucursalele din Africa de Nord și Sahel ale Al-Qaeda au considerat-o, împreună, ca o dovadă că jihadul militant este singura „cale spre glorie", ecouri ce au generat apariția a zeci de noi grupuri de social media dedicate exclusiv acestor evoluții. Între timp, teroriștii din întreaga lume meditează la o nouă migrație (hijra) jihadi în Afganistan, afirmând că țara va fi acum, fără îndoială, „centrul jihadului global".

Au trecut două decenii de conflicte continue de când regimul taliban al anilor 2000 a refuzat să-l predea pe Osama bin Laden Statelor Unite, iar în data de 29 februarie 2020 liderii talibani au fost de acord cu condițiile stabilite prin Acordul de la Doha, semnând un document ce presupune interzicerea atacurilor Al-Qaeda împotriva SUA pe teritoriul afgan până la data retragerii trupelor. Aceste aspecte ridică o întrebare: ar risca noul regim taliban să pună în pericol noua putere câștigată, găzduind și susținând o grupare teroristă din cauza căreia au pierdut puterea în urmă cu 20 de ani? Răspunsul este că talibanii nu sunt la fel ca în anul 2001. Noul regim și membrii săi sunt mult mai puternici din punct de vedere militar, având beneficiul elementelor de logistică și capabilitățile americane abandonate ca urmare a retragerii trupelor din Afganistan, iar la nivel diplomatic au inițiat deja stabilirea unor relații diplomatice cu lideri regionali, precum Rusia și China, îndreptându-se cu solicitările de recunoaștere guvernamentală spre comunitatea internațională. În contrast cu modalitatea în care au acționat pentru reocuparea administrativă în forță a teritoriilor și recâștigarea puterii de stat prin acte violente, noul regim taliban a desfășurat o campanie globală de PR, elaborată cu meticulozitate: conferințe de presă, promisiuni civice, o prezență online extinsă și articole care promit printre altele un bun tratament al femeilor musulmane.

Cu toate aceste acțiuni, regimul taliban actual a arătat mai multe fețe. Există în maniera acestora de pseudo-guvernare o latură civilă pe care o arată cosmetizat comunității internaționale, o latură socială pentru unicul public care contează - jihadiștii afiliați și susținătorii islamici radicali și o față reală dură și radicală pentru marea masă a populației afgane, aspecte relevate odată cu începerea retragerii trupelor coaliției, moment de care talibanii au profitat din plin, reușind, uneori prin luptă, alteori prin trădare și intimidare, să reocupe teritorii pe care le pierduseră în anii de conflict.

Pe 31 august 2021, în ultimele ore ale retragerii SUA, talibanii au lansat un nou număr al publicației lor în limba arabă, *al-Somood*. În cadrul acestuia au contracarat acuzațiile ridicate de gruparea Stat Islamic și anume că noul regim taliban a devenit un agent al Statelor Unite din cauza Acordului de la Doha, asigurând comunitatea musulmană și radicalii jihadiști că „talibanii de astăzi nu sunt diferiți de talibanii de ieri, au aceeași ideologie exact de când au preluat conducerea în 1996 și cine spune altceva sau îl prezintă într-o imagine diferită, fie ignoră ideologia talibană față de începuturi, fie are o gândire și o dorință de abatere de la adevărata credință sau de schimbare a acesteia".

Este recunoscut faptul că organizația Al-Qaeda, prin conducătorii și membrii săi, a promis loialitate față de talibani. Acest angajament, numit *bay'ah*, reprezintă mai mult decât un simplu gest de alianță, fiind considerat în lumea musulmană o relație sacră, sfântă, care rareori poate fi anulată. Osama bin Laden a jurat loialitate față de liderul taliban de atunci, Mullah Omar în anii 1990, și urmând acest model fiecare lider și luptător Al-Qaeda au procedat la fel. În 2016, după uciderea conducătorului talibanilor, Mullah

Mansour, Al-Qaeda a publicat un videoclip de 14 minute cu actualul său lider Ayman al-Zawahiri, pledând din nou loialitate talibanilor, în fața noului lider, Haibatullah Akhundzada. Vorbind în numele întregii organizații Al-Qaeda și a afiliaților săi din Somalia, Yemen, Africa de Nord și nu numai, Zawahiri a declarat: „Eu, ca emir (al Al-Qaeda), îți dau angajamentul nostru de credință, reînnoind jurământul șeicului Osama (Allah are milă de el), chemând lumea musulmană să sprijine (talibanii) și să-i promită loialitate. Promitem loialitate pentru a stabili un califat prin metoda profetului. Suntem soldații și susținătorii tăi și o brigadă printre brigăzile tale.”, adresându-i-se lui Akhundzada cu apelativul „emirul credincioșilor”.

Această relație dintre membrii grupării teroriste Al-Qaeda și regimul politic taliban a evoluat odată cu transformările și războaiele pe care afganii le-au purtat de-a lungul timpului, devenind mai profundă și mai indisolubilă prin angajamentele fiecărui lider nou al grupării, așa cum s-a întâmplat și în cazul lui Jalaluddin Haqqani, liderul rețelei Haqqani, aripa radicală a talibanilor. Haqqani a devenit comandantul militar al talibanilor la doar o lună după atacurile de la 11 septembrie, transformându-se în una dintre cele mai influente figuri. După moartea lui Jalaluddin Haqqani în 2018, talibanii i-au publicat prin intermediul revistei al-Somood testamentul, în care acesta își exprima venerația față de personalități proeminente din Al-Qaeda, precum bin Laden și Abu Musab al-Zarqawi, cerându-le musulmanilor să le urmeze calea.

Legăturile solide dintre liderii comunității musulmane oferă garanții organizației teroriste Al-Qaeda pentru ca nici un acord sau presiune geopolitică să nu îi separe vreodată de regimul politic al talibanilor. Rădăcinile relației talibanilor cu Al-Qaeda au devenit de-a lungul istoriei, marcată de războaie cu marile puteri și de luptele interne, prea adânci pentru a fi rupte.

În urma eforturilor comune ale forțelor coaliției de a anihila gruparea teroristă, prin identificarea și arestarea membrilor și susținătorilor și prin neutralizarea celulelor active, Al-Qaeda nu mai reprezintă aceeași forță de luptă față de începutul conflictului din Afganistan în 2001. După ani de lupte, fragmentări și numeroase încercări de recoagulare în Afganistan și în regiunile învecinate, aceasta încă nu are valoarea strategică din urmă cu 20 de ani. Nici subdiviziunea Al-Qaeda din subcontinentul indian, care a efectuat câteva atacuri teroriste izolate, nici Ansar Ghazwat ul Hind, grupul afiliat Al-Qaeda din Kashmir, nu s-au dovedit suficient de puternice până acum astfel încât să revitalizeze anvergura unei organizații cu pretenții globale. Cu toate acestea, preluarea de către talibani a puterii statale în Afganistan reprezintă cel mai mare impuls pentru Al-Qaeda de la atacurile din 11 septembrie 2001 și până în prezent. Condițiile favorabile, vidul de putere militară și lipsa guvernării solide a statului, inclusiv declinul ISIS, oferă condiții din ce în ce mai favorabile pentru o reapariție a grupării Al-Qaeda în întreaga regiune.

Șirul evenimentelor ultimilor 20 de ani de conflicte în Afganistan nu relevă nici un dubiu cu privire la prezența continuă și activă, chiar dacă redusă, a Al-Qaeda sau disponibilitatea acesteia de a lupta cot la cot cu talibanii, în ciuda afirmațiilor succesive ale administrațiilor SUA. În decembrie 2020, ministerul afgan al apărării a anunțat uciderea a cincisprezece agenți Al-Qaeda care luptau cu talibanii în sudul provinciei Helmand și reținerea altor câteva zeci de jihadiști. În ultimele săptămâni, numărul combatanților Al-Qaeda și al ISIS-Khorasan, franciza din Afganistan, a crescut după ce talibanii au eliberat aproximativ cinci mii de prizonieri numai din închisoarea Pul-i-Charkhi la Aerodromul Bagram pe 15 august. Într-un mod similar, pe măsura retragerii trupelor coaliției către aeroportul din Kabul, talibanii au reușit eliberarea a mii de deținuți care și-au manifestat rapid opțiunea de aderare la una dintre grupările radicale, în lipsa unei alternative sociale viabile ori chiar forțați de contextul socio-cultural.

Paradoxul mișcării jihadiste constă în modul în care aripa afgană a grupării Statul Islamic a devenit un rival atât al talibanilor, cât și al Al-Qaeda.

Gruparea Stat Islamic din provincia Khorasan, cunoscută și sub acronimele ISIS-K, ISKP și ISK, este afiliatul oficial al mișcării Statului

Islamic care operează în Afganistan, recunoscut de conducerea centrală a grupării Statul Islamic în Irak și Siria. ISIS-K a fost fondată oficial în ianuarie 2015. Într-o perioadă scurtă de timp a reușit să-și consolideze statutul de organizație fundamentalist-islamică prin controlul teritorial al mai multor districte rurale din nordul și nord-estul Afganistanului și a lansat o campanie letală în Afganistan și Pakistan. În primii trei ani, ISIS-K a lansat atacuri împotriva grupurilor minoritare, a zonelor și instituțiilor publice și a obiectivelor guvernamentale din marile orașe din Afganistan și Pakistan. Până în 2018 a devenit una dintre primele patru organizații teroriste cele mai sângeroase din lume, potrivit indicelui global de terorism al *Institute for Economics and Peace*. Însă, după ce a suferit pierderi teritoriale, la nivelul membrilor de bază și o destructurare a conducerii, ca urmare a acțiunilor coaliției condusă de SUA și partenerii săi afgani, care a culminat cu predarea a peste 1.400 de luptători și familiile acestora guvernului afgan la sfârșitul anului 2019 și începutul anului 2020, organizația a fost declarată, de către unii, învinsă.

În urma atacului asupra unei mulțimi adunate în fața aeroportului din Kabul la 26 august 2021, ce s-a soldat cu cel puțin 100 de oameni morți, inclusiv 13 soldați americani, ISIS-K, care și-a asumat răspunderea pentru atacul sinucigaș, a revenit în atenția publicului larg ca o organizație teroristă activă, ce luptă deopotrivă cu regimul taliban, forțele de coaliție și celelalte grupări teroriste pentru a atinge desideratul suprem al organizației Stat Islamic – marele califat islamic. Fondată de foștii membri ultra-radicali ai talibanilor pakistanezi, talibanilor afgani și ai Mișcării Islamice din Uzbekistan, gruparea a reușit de-a lungul timpului să valorifice expertiza locală a acestor luptători și a foștilor comandanți. ISIS-K a început mai întâi să consolideze teritoriul din districtele sudice ale provinciei Nangarhar, care se află la granița de nord-est a Afganistanului cu Pakistanul, folosind pozițiile de frontieră pentru a culege provizii și a recruta adepți din zonele tribale ale Pakistanului, precum și expertiza altor grupuri locale cu care a încheiat alianțe operaționale. Strategia generală a ISIS-K este de a stabili un cap de pod pentru ca mișcarea Statului Islamic să-și extindă așa-numitul califat în Asia Centrală și de Sud. În aceeași măsură ca entitatea centrală a grupului din Irak și Siria, ISIS-K valorifică expertiza personalului său și alianțele operaționale cu alte grupuri pentru a efectua atacuri devastatoare care vizează minorități, cum sunt populațiile Hazara și Sikh din Afganistan, precum și jurnaliști, lucrători guvernamentali, personal de securitate și infrastructura guvernamentală. Scopul ISIS-K este de a crea haos și incertitudine în încercarea de a converti luptătorii dezamăgiți din alte grupări și de a pune la îndoială capacitatea oricărui guvern aflat la guvernare de a oferi securitate populației civile. ISIS-K vede talibanii afgani drept rivalii săi strategici, calificându-i drept „naționaliști spurcați” cu ambiții de a forma un guvern limitat doar la granițele Afganistanului, lucru ce contrazice obiectivul mișcării Statul Islamic de a stabili un califat global.

Concluzii

Speranța că un nou capitol al istoriei moderne a Afganistanului nu va avea aceleași coordonate radicale ca precedentul este cât se poate de falsă deoarece acest nou regim taliban, conectat la actualele capabilități tehnice și informaționale, s-a dovedit din prima lună de la preluarea guvernării la fel de brutal și radical ca cel de dinainte. Ca atare, este evident că anii de război cu Statele Unite și aliații săi nu au reușit nici să extermine elementele radicale ultra-îndoctrinate religios și nici să producă o ruptură a relației cu Al-Qaeda, ci exact contrariul. Așa cum sunt văzuți acum de întreaga lume musulmană, talibanii au învins cea mai puternică forță militară de pe planetă, oferind speranță oricărei națiuni musulmane aflată în conflict. Astfel, Al-Qaeda din Peninsula Arabică, cu sediul în mare parte în Yemen, a anunțat „începutul unei transformări esențiale” la nivel mondial. În Africa de Nord, Al-Qaeda din Maghrebul Islamic a sărbătorit victoriile militare talibane ca dovadă că lupta jihadistă violentă este „singura modalitate de a restabili gloria Ummah”. („Ummah” este termenul arab pentru comunitatea musulmană globală). Victoria talibanilor a dat,

de asemenea, o nouă viață grupurilor îndepărtate, inclusiv unora dintre rivalii Al-Qaeda. „Victoria talibanilor este o poveste care poate fi aplicată pentru a energiza și justifica orice jihad sau răscoală islamistă, indiferent de câți ani de vărsare de sânge ar putea aduce", a afirmat într-un recent interviu Rita Katz fondatoarea și directorul executiv al SITE Intelligence Group, o organizație neguvernamentală de combatere a terorismului.

SITE Intelligence Group a urmărit ecourile succesului talibanilor și aspirațiile diferitelor grupări jihadiste exprimate cu ajutorul canalelor mediatice și a platformelor social-media, observând faptul că întreaga comunitate musulmană percepe acest moment ca fiind o victorie a jihadului. Hamas și Jihadul Islamic palestinian, cu sediul în Gaza, au declarat că retragerea trupelor americane din Afganistan a dovedit că și palestinienii vor realiza, în cele din urmă, întoarcerea lor în fostele teritorii palestiniene din Israel, „cu permisiunea lui Allah". Firul comun al diferitelor mesaje de felicitare și susținere transmise talibanilor este că îndrumarea lui Allah este responsabilă de succesul anilor de lupte continue. Toate aceste narațiuni de încurajare a luptei jihadiste transformă regimul taliban într-un exemplu veritabil de urmat. Poziția talibanilor este acum și mai puternică, având în vedere că SUA încearcă să încheie o înțelegere cu noul regim pentru a combate acțiunile grupării Statul Islamic.

Având acest tablou succint al evenimentelor recente, se poate considera că în Afganistan, victoria talibanilor este și victoria Al-Qaeda. Pe măsură ce se desfășoară această tranziție bruscă și brutală de la încercarea coaliției de stabilire a unui stat de drept cu instituții și organisme statale recunoscute la nivel internațional, la o formă de guvernare pseudo-arhaică, bazată în continuare, pe coalizare prin constrângere a diferitelor entități tribale ori impulsionată de dogme și doctrine radical-religioase, începe un nou capitol în lupta globală împotriva terorismului în care actori pe care comunitatea internațională îi plasează în aceleași cataloage ale grupărilor teroriste se vor afla într-un lung conflict, generat de disensiuni ideologice și ambiții teritoriale, ceea ce ne duce la concluzia crudă că toate încercările coaliților și alianțelor vestice au reușit blocarea manifestării fizice a califatului islamic în Irak și Siria, dar au pierdut din vedere aspectele legate de ideologie.

Bibliografie:

1. BROWN, Vahid and Don Rassler, Fountainhead of Jihad: the Haqqani nexus, 1973-2012. Oxford University Press. 2013. pg. 46;
2. HANDEL, Sarah, "Who Are The Haqqanis?" NPR, 3 Oct. 2011, http://www.npr.org/blogs/thetwo-way/2011/10/03/141016637/who-are-the-haqqanis.
3. RUTTIG, Thomas, "Loya Paktia's Insurgency." Decoding the Neo-Taliban, New York, Columbia University Press, 2009, p. 64-65;
4. "Foreign Terrorist Organizations", US Department of State, 2013, https://www.state.gov/j/ct/rls/crt/2013/224829.htm.
5. NABIL, Rahmatullah and Melissa Skorka, "Commentary: The road to Afghanistan peace does not lie in Kabul." Reuters, 7 Jul. 2017, https://www.reuters.com/article/us-nabil-afghanistan-commentary/commentary-the-road-to-afghanistan-peace-does-not-lie-in-kabul-idUSKBN19W2MS.
6. https://www.washingtonpost.com/world/2021/09/07/alqaeda-evolution-911/.
7. https://govinfo.library.unt.edu/911/report/911Report_Ch7.pdf.
8. https://www.wilsoncenter.org/article/al-qaeda-isis-20-years-after-911.
9. https://nationalinterest.org/feature/isis-vs-al-qaeda-jihadism%E2%80%99s-global-civil-war-12304.
10. https://www.foreignaffairs.com/articles/afghanistan/2021-08-13/osama-bin-ladens-911-catastrophic-success.
11. https://foreignpolicy.com/2021/09/13/taliban-victory-afghanistan-al-qaeda-victory-911/.
12. https://ent.siteintelgroup.com/Statements/aqap-optimistic-of-afghan-taliban-victory-ushering-new-conquests-marking-turning-point-in-muslim-history.html
13. https://www.ctc.usma.edu/situating-the-emergence-of-the-islamic-state-of-khorasan/.

14. https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2019-web.pdf.
15. https://theconversation.com/what-is-isis-k-two-terrorism-experts-on-the-group-behind-the-deadly-kabul-airport-attack-and-its-rivalry-with-the-taliban-166873.
16. https://www.afghanistan-analysts.org/en/reports/war-and-peace/iskps-battle-for-minds-what-are-their-main-messages-and-who-do-they-attract.

[1] https://www.washingtonpost.com/world/2021/09/07/alqaeda-evolution-911/, accesat la 21.09.2021.
[2] https://govinfo.library.unt.edu/911/report/911Report_Ch7.pdf, accesat la 21.09.2021.
[3] https://foreignpolicy.com/2021/09/13/taliban-victory-afghanistan-al-qaeda-victory-911/, accesat la 22.09.2021.
[4]https://ent.siteintelgroup.com/Statements/aqap-optimistic-of-afghan-taliban-victory-ushering-new-conquests-marking-turning-point-in-muslim-history.html
[5] Idem.
[6] https://www.bbc.com/news/world-asia-58632147, accesat la 22.09.2021.
[7]https://www.wilsoncenter.org/article/future-al-qaeda-isis-jihadism?utm_medium=social&utm_source=twitter.com&utm_campaign=wilson, accesat la 22.09.2021.
[8] https://foreignpolicy.com/2021/09/13/taliban-victory-afghanistan-al-qaeda-victory-911/, accesat la 23.09.2021.
[9] Bayʿah (în arabă: بَيْعَة, „Gaj de loialitate"), în terminologia islamică, este un jurământ de loialitate față de un lider. Se știe că a fost practicat de profetul islamic Mahomed. Bayʿah este uneori luat sub un pact scris, dat în numele supușilor de către membrii de frunte ai tribului, cu înțelegerea că atâta timp cât liderul respectă anumite cerințe față de poporul său, ei trebuie să-și păstreze loialitatea față de el. Bayʿah este încă practicat în țări precum Arabia Saudită și Sudan. În Maroc, bayʿah este unul dintre fundamentele monarhiei. https://en.wikipedia.org/wiki/Bay%27ah.
[10] https://www.aljazeera.com/news/2015/8/13/al-qaedas-zawahiri-pledges-allegiance-to-taliban-head, accesat la 23.09.2021.
[11] Rețeaua Haqqani este o organizație militantă islamistă sunnită care operează în regiunea sud-estică a Afganistanului și în zonele tribale administrate federal (FATA) din nord-vestul Pakistanului. Renumitul comandant al mujahidinilor Jalaluddin Haqqani, a format Rețeaua Haqqani la sfârșitul anilor 1970. Unul dintre primii islamiști afgani și un erudit islamic, Jalaluddin Haqqani a jucat un rol esențial în ordinea politică a provinciilor Khost, Paktya și Paktika din sud-estul Afganistanului (denumită în mod colectiv Loya Paktya).Structura de bază a rețelei este în mare parte familială și ierarhică. Mulți dintre liderii proeminenți ai grupului au absolvit *madrassa Dar al-Ulum Haqqaniyya* din Pakistan, instituția de învățământ religios de la care HN și-a derivat numele. Acest seminar *Deobandi* este locul în care Jalaluddin Haqqani a cultivat o rețea de militanți care au jucat roluri de conducere în structurile de comandă militante islamiste (de exemplu, Al-Qaeda, talibanii pakistanezi, Mișcarea Islamică din Uzbekistan și Lashkar-e-Taiba) din regiunea Afganistan-Pakistan.https://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/print_view/363, accesat la 23.09.2021.
[12]https://www.wilsoncenter.org/article/future-al-qaeda-isis-jihadism?utm_medium=social&utm_source=twitter.com&utm_campaign=wilson, accesat la 23.09.2021.
[13] https://www.ctc.usma.edu/situating-the-emergence-of-the-islamic-state-of-khorasan/, accesat la 23.09.2021.
[14] https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2019-web.pdf, accesat la 23.09.2021.
[15] https://theconversation.com/what-is-isis-k-two-terrorism-experts-on-the-group-behind-the-deadly-kabul-airport-attack-and-its-rivalry-with-the-taliban-166873, accesat la 23.09.2021.
[16] https://www.afghanistan-analysts.org/en/reports/war-and-peace/iskps-battle-for-minds-what-are-their-main-messages-and-who-do-they-attract/, accesat la 23.09.2021.
[17] https://foreignpolicy.com/2021/09/13/taliban-victory-afghanistan-al-qaeda-victory-911/, accesat la 24.09.2021.
[18] https://ent.siteintelgroup.com/about-site.html, accesat la data de 24.09.2021. SITE Intelligence Group este o organizație nonguvernamentală americană care urmărește activitatea online a organizațiilor jihadiste.

Direcția Generală de Informații a Apărării