MODELAREA MEDIULUI OPERAȚIONAL PRIN UTILIZAREA ATACURILOR CIBERNETICE

Locotenent-colonel Marian ȘTEFAN
Centrul de pregătire în domeniul informații pentru apărare, București

Actualul context geopolitic și geostrategic, amploarea politicului, economicului, culturalului și interesele religioase, problemele informaționale și cibernetice, criza medicală globală, ca și alte măsuri non-militare ocupă, în zilele noastre, un loc special în conturarea mediului operațional. Importanța acestora se resimte nu numai pe timpul escaladării situațiilor de criză și în procesul de gestionare și control al acestora, ci și în operațiile militare, marcând arhitectura conflictelor contemporane. Paleta de actori prezenți și implicați, împreună cu multitudinea riscurilor și amenințărilor pe care aceștia le generează, schimbă paradigma mediului operațional clasic către abordări operaționale multidimensionale în raport cu cele cinci dimensiuni tradiționale cu care eram familiarizați în literatura militară: terestru, aerian, maritim, cosmic și spectrul electromagnetic, alături de care regăsim, acum, mediul înconjurător și mediul informațional. Suprapunerea acestor medii și crearea unei imagini integrate a spațiului de luptă reprezintă o schimbare de paradigmă ce trebuie înțeleasă și asumată. 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 atât pe timp de pace, cât și în situații de criză sau război.

Acest studiu propune o prezentare holistică a problemelor și provocărilor la nivelul mediului operațional internațional, prezentând diferite tipologii de amenințări identificate la nivelul componentei informaționale prin instrumentarea unor atacuri cibernetice atribuite unor entități statale și non-statale. Modelarea conceptelor teoretice este însoțită de o serie de exemple, prezentate cu scopul de a oferi o perspectivă punctuală asupra unor evenimente care au produs efecte la nivelul mediului informațional.

Cuvinte-cheie: mediu operațional, atacuri cibernetice, agresiuni, criză, tehnologie.

INTRODUCERE

Modalitatea extinsă de abordare a securității s-a îmbogățit, în timp, 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: *„Evoluția relațiilor internaționale, turbulențele și accelerarea integrării și fragmentării Ordinii Internaționale Mondiale au condus la forme și tipuri neașteptate și neconvenționale de amenințări la adresa securității naționale și internaționale. Unele dintre aceste amenințări derivă din procesul dezvoltării tehnologice, altele din impactul tehnologiei asupra societății noastre, altele din creșterea populismului și relevanței identităților și, ultimele, dar nu cele din urmă, sunt generate de 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 în aceste zone, precum și emergența noilor tipuri de conflicte”* (Chifu, 2020, p. 10).

Cu toate că lumea în care trăim cunoaște permanent noi dezvoltări tehnologice, viteza de evoluție a societății noastre, a relațiilor internaționale și securității a introdus noi categorii de amenințări neconvenționale. În acest fel, amenințările din surse externe sunt corelate cu vulnerabilitățile interne, transformate, și acestea, în amenințări. Acest fapt se întâmplă, deoarece, în realitate, acestea corespund tipologiei de amenințări hibride, care sunt generate de surse externe (Chifu, 2018, pp. 23-30). Este cazul tuturor caracteristicilor democrației liberale, valorilor și principiilor pe care le respectăm pentru că reprezintă modul nostru de viață, dar care sunt considerate vulnerabilități de către anumiți actori (statali, în mod special de către Federația Rusă și China, și non-statali, entități și organizații teroriste, grupări de criminalitate organizată), care au construit instrumente pentru a profita de aceste caracteristici ale societății liberal-democratice, privite ca vulnerabilități (Chifu, Țuțuianu, 2017, p. 270).

Noile tipuri de amenințări provin din specularea principiilor și valorilor sistemului de guvernare democratic, profitând de lipsurile și neclaritățile identificate la nivelul

acestor sisteme, generate de evoluția tehnologiei și impactul ei asupra societății (Chifu, 2019, pp. 11-23).

Platformele de socializare și 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.

Contextul geopolitic și geostrategic, amploarea politicului, economicului, culturalului și interesele religioase, problemele informaționale și cibernetice, ca și alte măsuri non-militare ocupă, în zilele noastre, un loc special în conturarea mediului operațional. Importanța acestora se resimte nu numai în timpul escaladării situațiilor de criză și în procesul de gestionare și control al acestora, ci și în operațiile militare, marcând arhitectura conflictelor contemporane.

Multitudinea de actori prezenți și implicați, împreună cu diversitatea și scara riscurilor și amenințărilor pe care aceștia le generează, schimbă paradigma mediului operațional clasic către abordări operaționale multidimensionale, în raport cu cele cinci dimensiuni tradiționale cu care eram familiarizați în literatura militară: terestru, aerian, maritim, cosmic și spectrul electromagnetic, alături de care apar, acum, mediul inconjurator și mediul cibernetic. Suprapunerea acestor medii și crearea unei imagini integrate a spațiului de luptă reprezintă o schimbare de paradigmă ce trebuie înțeleasă și asumată.

Din punctul de vedere al abordării tradiționale, doctrinele militare ale Armatei SUA extind lista componentelor 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)”.* (TRADOC G-2, 2012, p. 5), punând un puternic accent pe utilizarea operațiilor informaționale și cibernetice. Acest tablou asupra mediului operațional actual specific războiului hibrid, incluzând combinații de forțe convenționale și neregulate, oferă o percepție limitată 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 asocierea instrumentelor de putere militare și non-militare întrebuințate pentru atingerea obiectivelor strategice ale unui stat, nu este de ajuns. Natura tacită a conflictului în spațiul cibernetic face dificilă distincția dintre originile și factorii declanșatori și starea finală dorită de actorii care au declanșat agresiunea.

CONTEXTUL INTERNAȚIONAL AL MEDIULUI OPERAȚIONAL

Mediul operațional la nivel internațional 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, care, prin vulnerabilitățile create, oferă oportunități pentru ascensiunea unor actori non-statali care, prin acțiunile lor 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 în actul de guvernare ale actorilor non-statali 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 punctul de vedere al măsurilor și politicilor exercitate, iar pe de altă parte, aceștia pot contesta, prin natura existenței și prezenței lor, monopolul structurilor de forță ale statului-gazdă.

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 geo-politice și geo-economice) între state puternice 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 în care 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.

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, dar stabil din punctul de vedere al politicilor externe ale celor două blocuri de putere, conflictele anilor ’90 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 creșterea 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. Actualul mediu operațional estompează distincția între zone de război și zone de pace, precum și între combatanții legitimi, adversarii neatribuiți și civili.

Una dintre cele mai critice dimensiuni ale conflictului de tip hibrid constă în contopirea eforturilor militare și politice concomitent cu aplicarea suprapusă a agresiunilor informaționale.

Războiul informațional este utilizat, de regulă, în cadrul conflictelor de tip hibrid pentru a crea disensiuni de percepție la nivelul opiniei publice a populației statului-țintă, pentru a genera legitimitate unor acțiuni intruzive prin fabricarea unui pretext credibil, pentru a împiedica sau a încetini reacția de răspuns a statului-țintă la atacurile cinetice și non-cinetice și pentru a reduce șansele de interferență externă prin crearea unor situații de confuzie legislativă. Cea mai reușită campanie hibridă este aceea în care se reușește paralizarea instituțiilor statului-țintă și indisponibilizarea capacităților de a rezista sau a reacționa înaintea introducerii forțate a componentei militare – a cărei natură poate fi caracterizată ulterior ca fiind un instrument de stabilitate (adică, generatori de pace și stabilitate) în locul instrumentului care a creat instabilitatea. Controlul tuturor canalelor mass-media clasice și moderne va conduce la posibilitatea utilizării acestora în scopul influențării publicului intern, iar în condițiile în care acest control va fi realizat încă din starea inițială a declanșării stării de conflict ori într-o formă incipientă, înaintea oricăror alte acțiuni, efectele vor consta în subminarea voinței populației-țintă de a rezista în fața unei agresiuni ulterioare. În situațiile în care temele și mesajele construite de către agresor în scopul dezinformării și intoxicării trebuie să concureze presa internațională și internetul nereglementat, conținutul specific al acestor teme lansate este mai puțin important decât saturația acestor domenii cu dezinformarea pentru a ajuta la mascarea acțiunilor agresorului.

VULNERABILITĂȚILE MEDIULUI INFORMAȚIONAL – ȚINTA AGRESIUNILOR CIBERNETICE

Conceptual, un mediu operațional complex este compus dintr-o multitudine de actori care interacționează cu rapiditate, în moduri diferite, fiind evidențiat de complexitate structurală și interactivitate. Pârghiile care guvernează interacțiunile sunt, uneori, ambigue și pot fi opace pentru actorii externi fără o înțelegere profundă a contextului. Caracteristicile condițiilor dintr-un mediu operațional sunt în continuă evoluție, componenta informațională fiind cea mai dinamică.

Parte a mediului operațional, dimensiunea informațională prezintă complexitate, volatilitate, incertitudine, instabilitate și ambiguitate în evenimente care se schimbă în viteză, ritm și tempo. O serie de amenințări de tip hibrid, care includ agresiuni de tip cibernetic, acțiuni de propagandă și influență și dezinformarea propagată în mediile virtuale, pot extinde impactul asupra operațiunilor militare planificate. Agresiunile cibernetice reprezintă o amenințare din ce în ce mai critică pentru infrastructura tehnologiei informației și capacitatea de a executa în mod eficient comanda unei misiuni. Un potențial adversar va încerca să modeleze un mediu operațional în avantajul lui, schimbând natura conflictului și folosind capabilități pentru care orice forță militară întrebuințată nu este pe deplin pregătită.

Un sistem informațional, la modul general, se poate defini ca fiind ansamblul de elemente implicate în procesul de colectare, transmitere și prelucrare a informației, aceasta având rolul central în cadrul acestui sistem. Într-un sistem informațional se regăsesc următoarele componente: informația vehiculată, documentele purtătoare de informații, personalul care are acces la informație, mijloacele de comunicare, sistemele de prelucrare (de regulă, automată) a informației etc. Unele dintre activitățile desfășurate în cadrul acestui sistem presupun: achiziția informațiilor din sistemul de bază, completarea documentelor și transferul acestora între diferite compartimente, centralizarea datelor etc. În cel mai larg sens, orice sistem informațional se referă la diversele interacțiuni dintre oameni, date, procese, și tehnologii. În acest fel, termenul nu se referă numai la aspectele legate de tehnologiile informaționale și de comunicații pe care o organizație le utilizează, ci și la modul în care oamenii interacționează cu tehnologia în scopul de a oferi suport pentru procesele de prelucrare. Sistemul informațional reprezintă un ansamblu complex de fluxuri de date și circuite informaționale organizate într-o concepție unitară.

Dezvoltarea tehnologiilor informaționale și de comunicații în ultimii 20 de ani a servit ca un catalizator puternic și accelerant pentru schimbarea distribuției puterii în sistemul internațional, precum și a modalităților de utilizare a acestei puteri. Dominația tehnologiilor conexe modifică din ce în ce mai mult fizionomia mediului operațional actual, deoarece capacitatea tehnologică și puterea economică investită în sectorul militar se află într-o strânsă legătură. Apariția spațiului cibernetic, parte integrantă a mediului informațional, a adăugat un teren nou pentru desfășurarea conflictelor între statele lumii sau între organizații non-statale. În ceea ce privește aspectele de guvernare globală și echilibrul adecvat între libertatea individuală și controlul statului, provocările sunt din ce în ce mai mari, deoarece monopolul statelor asupra unor tipuri de informații a fost erodat în favoarea indivizilor și a actorilor non-statali. Revoluția tehnologică perturbă conceptele și doctrinele militare în moduri care par să reducă aportul factorului uman în caz de conflict

și să diminueze unele dintre avantajele de care dispuneau armatele occidentale la sfârșitul Războiului Rece.

Tehnologiile informaționale și de comunicații modelează toate instrumentele de putere ale statelor, inclusiv diplomația, informațiile și utilizarea forței. Progresele în domeniul tehnologiilor și digitalizarea informațiilor au făcut posibilă colectarea mai inteligentă a informațiilor și apariția și implicarea unei game largi de actori. Existența unui volum mare de informații stocate în baze de date controlate de mari concerne particulare sunt privite ca nesigure de către guvernele statelor occidentale, în timp ce conținutul social-media servește ca un depozit de informații personale despre potențialele ținte de informații rămase până acum de neatins pentru instituțiile statului. Marile puteri păstrează un avantaj semnificativ în controlul informațiilor, însă orice stat cu o agenție de telecomunicații are capacitatea de a dezvolta modalități de colectare de genul informații de semnal – SIGINT. China este un exemplu primordial al unui stat ale cărui capabilități de culegere, procesare și stocare de informații au fost transformate dramatic în ultimii 20 de ani prin utilizarea spionajului cibernetic atât în scopuri comerciale, cât și militare. Multe state din Africa, Asia și America Latină folosesc capacități de colectare îmbunătățite pentru a monitoriza sau reprima mai eficient disidența din rândul propriilor populații. Între timp, Coreea de Nord și-a folosit capacitățile cibernetice substanțiale atât pentru a ataca adversarii, cât și pentru a obține venituri prin criminalitatea cibernetică, un caz fiind furtul de 81 de milioane de dolari americani de la banca centrală a Bangladeshului, în 2016.

Faptul că nivelurile de spionaj au devenit atât de omniprezente a creat, probabil, un set nou și fără precedent de circumstanțe. S-a observat, adesea, că, atunci când vine vorba de rețelele digitale, distincția dintre spionaj și sabotaj poate fi determinată doar prin intenție. Acest lucru nu este strict adevărat, având în vedere că orice exploatare digitală care are ca scop spionajul va avea în mod necesar o componentă specifică de sabotaj. Întotdeauna va exista teama că orice exploatare descoperită – și timpul mediu de descoperire poate varia de la 146 de zile, în SUA, la peste 400 de zile în UE (The Impact of the ICT Revolution on International Relations, 2018) – poate avea o componentă de sabotaj prea sofisticată pentru a fi ușor identificată. Statele își folosesc din ce în ce mai mult capacitățile de informații (atât sub forma agențiilor de stat, cât și a entităților non-statale) pentru a penetra rețelele adversarilor în scopul identificării unor vulnerabilități care pot fi activate în moment de tensiune sau conflict, cu scopul de a afecta capacitatea de funcționare a societății în sine. Astfel de exploatări pot avea, de asemenea, o funcție de semnalizare, concepută pentru a descuraja statele să întreprindă acțiuni ostile de teama unui răspuns dăunător.

Acest aspect reprezintă o provocare pentru factorii de decizie atât în statele care se angajează în spionajul cibernetic, cât și în cele care sunt ținte ale unor astfel de activități. Imaginea este, în continuare, destul de neclară, existând riscul unor consecințe nedorite, așa cum, în 2017, NotPetya, un virus de tip ransomware, extrem de virulent, îndreptat, în principal, împotriva agențiilor guvernamentale ucrainene, s-a răspândit pe scară largă în Australia, Europa, Rusia și SUA, provocând pagube de miliarde de dolari. CIA a atribuit virusul agenției ruse de informații militare (GRU), care pare să fi folosit conflictul cu Ucraina ca un teren de test pentru o serie de agresiuni cibernetice. Impactul unor astfel de amenințări materializate evidențiază așa-numitul *„paradox al conectivității”*, prin care cele mai avansate tehnologii dependente de o rețea sunt, de asemenea, cele mai vulnerabile la perturbări cibernetice semnificative.

Astfel de perturbări devin o parte familiară a unei noi abordări a concurenței și a contestației dintre state, sub forma a ceea ce a fost numit *operațiuni din zona gri*. Aceste operațiuni au fost descrise de Comandamentul Forțelor Speciale din SUA drept *„interacțiune competitivă între și în cadrul actorilor statali și non-statali care se încadrează între tradiționalul război și starea de pace”*. (Special Operations Forces within the Competiton Continuum, 2020). Acestea se caracterizează prin ambiguitate cu privire la natura conflictului, opacitatea părților implicate și incertitudine în ceea ce privește politicile și cadrele legale relevante. Nu există nimic nou în mod intrinsec cu privire la astfel de operațiuni, dar dezvoltarea tehnologiilor le-a facilitat enorm evoluția, permițând actorilor să întreprindă (cu costuri reduse și cu posibilitatea de a nega) o serie de activități care provoacă daune fără a se ridica la un nivel ce ar justifica, cu ușurință, un răspuns cinetic. Un exemplu de acest tip de operațiuni sunt atacurile entităților care au acționat în numele statului iranian între anii 2011 și 2013 împotriva sistemului bancar și financiar american, întreprinse ca răspuns la sancțiunile americane legate de programul nuclear iranian.

Cel mai elocvent exemplu este presupusa ingerință a Rusiei în alegerile prezidențiale din 2016, din SUA, care s-a centrat pe exploatarea iscusită a platformelor social-media. Rușii care pretindeau a fi cetățeni ai SUA au deschis un număr mare de conturi de social-media false, predominant pe platformele de socializare Facebook și Twitter. Aceste conturi au fost utilizate pentru a propaga mesaje concentrate pe problemele sociale existente la acea vreme, care, apoi, au fost amplificate de roboți (aplicații software care efectuează sarcini repetitive simple la un ritm mult mai mare decât pot fi oamenii). Acest lucru a creat impresia unei dezbateri naționale reale pe anumite probleme de interes, de la condițiile de imigrare și problemele rasiale la comportamentele candidaților aflați în campanie electorală. În acest mod, politicienii americani s-au simțit obligați să adreseze temele de dezbatere și mass-mediei tradiționale pentru a acoperi vidul de informare credibilă, creând,

astfel, încă o amplificare suplimentară a propagandei false. Cu câteva zile înainte de a avea loc alegerile, hackerii ruși au încercat, de asemenea, să încalce sistemele de vot din SUA, trimițând e-mailuri infectate cu malware către computerele oficialilor electorali de stat.

Obiectivele acestei campanii rusești au evoluat dintr-o intenție inițială de a discredita unul dintre candidații la președinție și de a genera neîncredere în procesul politic al SUA pentru promovarea candidaturii celuilalt politician, considerat a fi persoana cea mai potrivită pentru a ridica sau a diminua sancțiunile asupra Rusiei. Această abordare ilustrează conceptul rusesc de *control reflexiv*, definit drept *„un mijloc de a transmite unui partener sau unui adversar informații special pregătite pentru a-l înclina voluntar să ia decizia predeterminată dorită de inițiatorul acțiunii”*. (Kowalewski, 2017). De fapt, i-a permis Rusiei să provoace daune semnificative integrității procesului democratic din SUA, cu costuri minime, prin exploatarea digitală a fisurilor existente în societatea americană, utilizând sisteme informatice aflate la dispoziția publicului larg și a utilizatorilor domestici. Chiar dacă guvernul american a cunoscut bine ceea ce avea loc și cine a fost responsabil, capacitatea sa de a răspunde la un astfel de comportament în timp util sau de a sancționa efectiv acțiunile respective a fost limitată.

Deși China nu a încercat încă să imite tipul de operațiuni informaționale utilizate de Rusia, statul a folosit progresele tehnologice și avansul cercetărilor în acest domeniu pentru a-și extinde influența într-o varietate de moduri în scopul configurării mediului operațional pe linii favorabile propriilor interese. În arena diplomatică internațională, China și-a asumat rolul de a susține conceptul de *suveranitate cibernetică* și nevoia de noi forme de guvernare globală a domeniului cibernetic. Operațiunile cibernetice ale Chinei relectă o concentrare continuă a eforturilor agențiilor de informații ale statului asupra acțiunilor de spionaj, având anumite intenții coercitive ca obiectiv secundar.

Spre deosebire de China, activitatea cibernetică iraniană este mult mai concentrată pe represalii împotriva vecinilor regionali și a Occidentului decât să servească unui scop coercitiv direct. Atacurile cibernetice împotriva companiilor petroliere saudite au început cu un atac distructiv în 2012, care a dus la distrugerea a aproximativ 30.000 de calculatoare din rețelele companiei petroliere de stat din Arabia Saudită (ARAMCO), dar nu a avut un impact perceptibil asupra operațiunilor petroliere. În 2017, același malware a provocat daune similare companiei petrochimice Tasnee; acel atac a fost urmat de un atac asupra ARAMCO, în august 2017, implicând un soft de tip *malware TRITON intrusion*.

Mediul informațional este o construcție bazată pe ideea că existența și proliferarea sistemelor informaționale creează o dimensiune sau un mediu de funcționare distinct. Ca o combinație de elemente tangibile (sisteme și rețele

de informații fizice) și elemente intangibile (informații și luarea deciziilor), mediul informațional este atât o resursă pentru operații militare, cât și un mediu în care operează forțele armate. În cadrul oricărui mediu operațional, elementul cel mai intangibil, informația, are o importanță supremă. Acest lucru se datorează faptului că, în ciuda lipsei existenței sale fizice, conținutul și fluxul de informații dintr-o zonă geografică specifică produc efecte reale, tangibile în lumea fizică și asupra forțelor militare prezente în mediul de operare. Din aceste motive, înțelegerea asupra mediului informațional trebuie să includă, în final, modul în care conținutul și fluxul de informații afectează executarea operațiilor militare.

Atribuirea atacurilor cibernetice este dificilă, necesitând un proces de colectare a volumelor mari de informații, analiza acestora și luarea unei decizii pentru a identifica cine se face responsabil. Foarte rar, urmele lăsate de un atac cibernetic oferă dovezile clare pentru specialiștii din domeniul informatic, astfel încât să se poată indica sursa generatoare a atacului, fie instituție a statului sau persoană, pentru a putea constitui probe într-o instanță de judecată.

Proliferarea tehnologiilor informației și comunicațiilor, atât în ceea ce privește extinderea utilizării acestor tehnologii, cât și disponibilitatea crescută a mijloacelor distructive, a generat noi modalități de proiecție a instrumentelor de putere (Paleta et al., 2008). Divergențele politice și economice dintre state implică acum rezolvări prin atacuri cibernetice împotriva utilităților, rețelelor financiare, infrastructurii electorale și sistemelor de guvernanță ale altor țări. Atacurile cibernetice ce presupun utilizarea deliberată a unui produs de software special proiectat și direcționat pentru exploatarea sau modificarea codului computerului, a datelor sau a algoritmilor pentru a provoca daune, oferă noi metode pentru a viza infrastructura internetului, rețelele de telecomunicații, sistemele de informații, precum și computerele și sistemele informatice. Astfel de activități ar putea avea ca obiectiv distrugerea sau afectarea bunei funcționări a acestor sisteme, cu efecte negative pentru utilizatorii lor, indiferent dacă sunt state, companii, furnizori de servicii publice sau persoane fizice.

CONCLUZII

Doctrina Aliată Întrunită pentru Operații Informaționale definește mediul informațional ca un spațiu ce *„cuprinde informații, actori și sisteme care permit utilizarea informațiilor”.* (AJP-3.10, 2009, p. 1-1). În acest context, mediul informațional a devenit sistemul în care entități, mijloace informatice, sisteme de comunicații și volumele de date vehiculate acționează simultan pentru un singur scop: comunicarea. Distanțele între generatorii de informații și receptori sau utilizatori s-au disipat odată cu dezvoltarea tehnologică, astfel încât ideile promovate

de oricine în mediul virtual pot fi accesate instant prin utilizarea unei game variate de terminale sau sisteme informatice, devenind, în acest fel, o problematică globală. Mediul informațional global prezintă avantajele tehnologiilor avansate, oferă acces nelimitat la resurse, însă reprezintă un spațiu vulnerabil în fața agresiunilor de natură cibernetică. Practic, această sabie cu două tăișuri oferă entităților guvernamentale și deopotrivă indivizilor nișe de penetrare și modalități de vehiculare a unor date cu caracter de dezinformare. Iar războiul informațional, *„potrivit unei definiții a conceptului, reprezintă crearea unor realități alternative prin pervertirea adevărului pe baza datelor, faptelor și argumentelor concrete și răstălmăcirea lui prin utilizarea unei combinații de fapte, silogisme, sofisme, propagandă, interpretare forțată și o multitudine de minciuni. Realitatea alternativă pervertește percepția unei populații vizate într-o combinație de operațiuni psihologice – PSYOPS, alături de dezinformare și propagandă, utilizând convingeri fundamentale, sentimente și imagini cu impact, cu scopul de a duce publicul-țintă spre o percepție pre-definită”* (Chifu, 2015).

BIBLIOGRAFIE:

1. Chifu, I. (2015). *Război hibrid, Lawfare, Război informațional. Războaiele viitorului.* Conferinţa Ştiinţifică Internaţională *„Strategii XXI”*. Tema: *„Complexitatea şi dinamismul mediului de securitate”*. Bucureşti: Centrul de Studii Strategice de Apărare şi Securitate.
2. Chifu, I., Țuțuianu, S. (2017). *Torn Between East and West: Europe's Border States*. London and New York: Editura Routledge.
3. Chifu, I. (2018). *Războiul hibrid şi reziliența societală. Planificarea apărării hibride*. În Revista *Infosfera.*
4. Idem. (2019). *Technology and Democracy. The Impact of the Evolution of Security and International Relations.* În Conferința Științifică Internațională *„Strategii XXI”*. Strategic Changes and International Relations. Bucureşti: Universitatea Națională de Apărare *„Carol I”*.
5. Idem. (2020). *Ameninţări neconvenționale și noile tipuri de conflicte de natură hibridă în secolul 21.* În revista *Gândirea militară românească*, nr. 1.
6. Kowalewski, A. (2017). *Disinformation and Reflexive Control: The New Cold War*, https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/, accesat la 17 august 2020.
7. Paleta et al. (2008). *Information technology and communication and best practices in it life cycle management*. În *Journal of Technology Management & Innovation*, vol. 3, nr. 4.
8. Williams, P. (2008). *Violent Non-State Actors and National and International Security.* International Relations and Security Network. Zürich: Swiss Federal Institute of Technology, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=93880, accesat la 15 august 2020.
9. AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
10. *The Global Risks Report 2016,* ediția IX, http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf, accesat la 10 iunie 2020.

11. *The Impact of the ICT Revolution on International Relations* (2018), www.iiss.org/publications/strategic-survey, accesat la 12 august 2020.
12. *Special Operations Forces within the Competiton Continuum*, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-05/3-05-D03-SOF-Competition-Continuum.pdf, accesat la 13 august 2020.
13. TRADOC G-2. (2012). *„Operational Environments to 2028: The Strategic Environment for Unified Land Operations".*
14. https://www.iiss.org/publications/strategic-survey/strategic-survey-2018-the-annual-assessment-of-geopolitics/ss18-04-strategic-policy-issues-2, accesat la 11 iunie 2020.
15. https://www.globalpolicy.org/nations-a-states/failed-states.html, accesat la 11 iunie 2020.