ABORDĂRI CONCEPTUALE ASUPRA RĂZBOIULUI INFORMAȚIONAL ȘI ASUPRA UNOR COMPONENTE ALE SALE

Teodor BADIU

absolvent al masterului civil Relații Internaționale și Studii de Intelligence din cadrul Academiei Naționale de Informații „Mihai Viteazul" din București

Când vorbim despre războiul informațional, nu mai există nicio linie de demarcație între starea de pace și starea de război, acesta fiind folosit de către actorii statali și nestatali, având în vedere eficiența sa și dificultatea de a fi detectat și respins. În plus, se știe faptul că Federația Rusă a folosit activitățile informaționale împotriva țărilor din Europa de Vest și de Est și, pentru a vedea specificitatea operațiunilor lor informaționale, trebuie să definim conceptele și componentele care stau la baza războiului informațional și ce perspectivă au gânditorii militari ruși despre activitățile informaționale. Deși articolul nu detaliază toate componentele războiului informațional, este important să se clarifice rolul operațiunilor informaționale și al elementelor sale ca parte a războiului informațional, precum și termenii care sunt adesea folosiți în spațiul public și academic – dezinformare, manipulare, propagandă, știri false etc. Pentru a înțelege mai bine activitatea informațională rusească, articolul oferă câteva exemple specifice din Polonia, Cehia și Slovacia.

Cuvinte-cheie: război informațional, operațiuni psihologice, distorsiune informațională, manipulare, media alternativă.

INTRODUCERE

Deși chestiunea războiului informațional – și, implicit, a operațiunilor informaționale – se regăsește în spațiul public și academic prin abordările referitoare la dezinformare, fake news, manipularea informațiilor, propagandă, scoaterea din context, apariția *„mediei alternative”* etc., în puține cazuri chestiunea a fost abordată mai profund.

Spațiul public european și cetățenii acestuia au fost puternic asaltați, în ultimii ani, de narațiuni conspiraționiste sau radicaliste, de mesaje confuze și părtinitoare, de informații eronate care stârneau emoții și rumori, toate acestea producând reacții sociale care îngreunau funcționarea eficientă a statelor. Trebuie precizat că există o multitudine de actori care au contribuit la diseminarea de informații false, atât statali, precum Federația Rusă, Iran, China, Coreea de Nord (Nemr, Gangware, 2019, pp. 14-25), cât și nestatali, cum ar fi organizațiile teroriste. Rezumându-ne la actorii statali, remarcăm faptul că elementul comun al acestor state constă în scopul operațiunii informaționale de a le favoriza propriile agende naționale, având moduri de operare diferite. Mai precis, Federația Rusă revitalizează spectrul măsurilor active; China inițiază campanii de influențare a percepțiilor publicului pe zona economică, politică și a relațiilor bilaterale personale; Iranul preferă o abordare clasică de diseminare a informațiilor false, asemănătoare cu cea rusească și chineză, axată pe narațiuni pro-palestiniene și anti-israeliene, iar Coreea de Nord folosește un mix între operațiuni de influențare și propagandă, pentru a altera realitatea și pentru a scăpa de sancțiuni (Ib.). Canalele media folosite de aceste state sunt diverse, pornind de la materiale tipărite și până la diseminarea informațiilor în spațiul online, în funcție de obiective, grupuri țintă și capabilități.

Spațiul public european și cetățenii acestuia au fost puternic asaltați, în ultimii ani, de narațiuni conspiraționiste sau radicaliste, de mesaje confuze și părtinitoare, de informații eronate care stârneau emoții și rumori, toate acestea producând reacții sociale care îngreunau funcționarea eficientă a statelor.

Pe de altă parte, operațiunile informaționale săvârșite de aceste state au anumite particularități ce constau în cultura strategică, experiența și tradiția în desfășurarea lor, în modul de operare, doctrine etc. Însă, pentru a putea analiza acțiunile informaționale desfășurate

de aceste state, este necesar să definim, chiar și succint, conceptele și termenii folosiți atunci când ne referim la contextul războiului informațional. Urmărind diversele abordări din spațiul public și din mediul academic, apar uneori neclarități referitoare la modul de operare, ce concepte și instrumente sunt folosite sau care sunt legăturile dintre componente și concepte.

Astfel, lucrarea de față va încerca să lămurească o serie de caracteristici ale războiului informațional, mai ales că acest subiect dezvoltă o întreagă abordare teoretică și practică, plecând de la accepțiunea că, pe timp de pace, războiul informațional este parte a războiului hibrid/amenințărilor hibride, fiind inclus și în spectrul războiului asimetric, iregular, neconvențional, al măsurilor active, al diplomației publice etc. (Theohary, 2018, pp. 4-5). Tot aici, trebuie precizat că vom descrie câteva situații din Polonia, Cehia și Slovacia, axându-ne pe activitatea informațională a Federației Ruse asupra acestor state.

NATO clasifică războiul informațional drept „acțiuni întreprinse pentru obținerea superiorității informatice prin deteriorarea sistemelor informatice inamice și protejarea celor proprii”.

ASPECTE TEORETICE

În privința *războiului informațional*, există două abordări principale care încearcă să îl definească: una pune accent pe specificul tehnic al războiului informațional, unde activitățile informaționale se desfășoară în cyberspace și/sau zona electronică, iar cealaltă abordare privește războiul informațional la nivel comprehensiv, din perspectiva intelligence-ului.

Pentru prima abordare, putem lua ca exemplu perspectiva NATO asupra războiului informațional, care îl clasifică drept *„acțiuni întreprinse pentru obținerea superiorității informatice prin deteriorarea sistemelor informatice inamice și protejarea celor proprii.”* (AAP-6, 2018, p. 430).

Însă, în privința celei de-a doua abordări, războiul informațional reprezintă un cumul de acțiuni organizate în mediul informațional care încearcă să utilizeze toate mijloacele pentru a deține controlul asupra fluxului informațional și a interpretării acestuia (Robinson, 2010, p. 169). Ținta poate fi un decident, opinia publică a unui stat sau cea internațională.

Michael Herman considera că *„Războiul devine ‹război informațional›; războiul începe și se termină cu intelligence-ul... Informația este o resursă critică în război, iar același lucru se aplică* și *competiției*

internaționale, pe timp de pace". (Herman, 1996, p. 347), astfel conflictul devine constant în contextul competiției internaționale și logica războiului informațional se universalizează, implicând metode și instrumente care, în trecut, se limitau la sfera militară.

În acest sens, Edward Waltz definește conceptul de *război informațional* drept *„război bazat pe informații"* (information-based warfare), unde scopul final este de a obține superioritatea informațională prin procurarea, procesarea și exploatarea informației, rezultând cunoaștere, care va fi, ulterior, protejată prin defensivă (information warfare-defend) sau ofensivă informațională (information warfare-attack) împotriva cunoașterii adversarului (Waltz, 1998, pp. 20-21). Definirile referitoare la războiul informațional pot continua, însă, dacă simplificăm acest concept, l-am putea defini drept cumul de acțiuni separate ori integrate, interdisciplinare, desfășurate de cel puțin doi combatanți/competitori al căror scop este de a obține un avantaj strategic în defavoarea celuilalt, folosind canalele disponibile, oportunitățile și mijloacele proprii prin culegerea și diseminarea datelor și informațiilor.

Edward Waltz definește conceptul de „război informațional" drept „război bazat pe informații", unde scopul final este de a obține superioritatea informațională prin procurarea, procesarea și exploatarea informației.

Spațiul în care războiul informațional se desfășoară este *mediul informațional*, care este definit ca *„agregatul de indivizi, organizații și sisteme ce colectează, procesează, diseminează sau acționează pe bază de informații".* (DoD, 2020, p. 104). Acesta este compus, la rândul său, din trei dimensiuni (Waltz, p. 27):

- *dimensiunea fizic*ă, unde acțiunile urmăresc protecția, distrugerea fizică și/sau furtul echipamentelor, materialelor/documentelor, al bazelor de date, nodurilor de comunicații, facilităților de colectare, procesare și diseminare a informațiilor;
- *dimensiunea informațională*, unde acțiunile urmăresc protecția, distrugerea, interceptarea, alterarea și/sau diseminarea de informații false, iar această dimensiune reprezintă legătura dintre dimensiunea fizică și cea cognitivă. Din perspectiva combatanților, acest câmp oferă mai multe oportunități, deoarece poate afecta infrastructura C4 a adversarului fără a presupune riscurile fizice ale unei acțiuni operative a propriilor forțe. Pe de altă parte, desfășurarea operațiunilor de inducere în eroare sau a surprizelor strategice poate avea o eficiență crescută în câmpul infrastructurii informaționale, ca urmare a posibilității de interceptare a datelor și informațiilor,

de a parazita un canal și de a introduce date și informații false/parțial adevărate sau a posibilității de a acționa punctual, în funcție de vulnerabilitățile adversarului;

- *dimensiunea cogniției umane/a percepțiilor*, unde acțiunile urmăresc influențarea și exploatarea emoțiilor, percepțiilor, trendurilor, motivațiilor și comportamentelor unor grupuri sociale țintă, a decidenților sau a populației prin utilizarea instrumentelor specifice distorsiunii informaționale.

În altă ordine de idei, *operațiunile informaționale* trebuie percepute ca element particular (sau pilon) în cadrul războiului informațional, prin care sunt întreprinse, la nivel punctual, acțiuni în sfera operațiunilor psihologice (PSYOPS), a operațiunilor de securitate (OPSEC), a operațiunilor cibernetice, a decepției militare (MILDEC)[1], a războiului electronic (EW) sau a celor care susțin activități militare, subversive, de contrainformații etc.

Operațiunile informaționale trebuie percepute ca element particular (sau pilon) în cadrul războiului informațional, prin care sunt întreprinse, la nivel punctual, acțiuni în sfera operațiunilor psihologice (PSYOPS), a operațiunilor de securitate (OPSEC), a operațiunilor cibernetice, a decepției militare (MILDEC), a războiului electronic (EW) sau a celor care susțin activități militare, subversive, de contrainformații.

Operațiunile informaționale pot fi definite, din perspectivă militară, ca activitate ce integrează capabilitățile informaționale proprii în strânsă legătură cu celelalte linii de operațiuni, cu scopul final de a întrerupe, corupe, uzurpa sau influența factorii de decizie adverși, în timp ce propriile sisteme sunt protejate (DoD, Ib.). Operațiunile informaționale optimizează elementele informaționale în contextul fluxului de date și informații și concentrează acțiunile în mod specific pe anumite subiecte și anumite ținte. Altă abordare clasifică operațiunile informaționale ca acțiuni ale guvernelor sau ale actorilor nestatali de a distorsiona opinia internă sau externă, cu scopul de a obține un rezultat strategic și/sau geopolitic, folosind un spectru de metode compus din dezinformare, informații false sau amplificatori falși – conturi de pe platformele sociale ce încearcă să manipuleze opinia publică (Wardle, Derakhshan, 2017, p. 6).

În cadrul operațiunilor informaționale, putem identifica *distorsiunea informațională* drept un concept relativ nou, subsumată operațiunilor

[1] Utilizarea termenului *„decepție”* (militară-MILDEC) în defavoarea echivalentului său românesc, *„măsuri de inducere în eroare”*, nu reprezintă o traducere nefericită, ci o alegere deliberată, ca urmare a faptului că recentele lucrări referitoare la decepția militară și modul de desfășurare al acestora folosesc decepția drept concept comprehensiv. Utilizarea decepției militare se fundamentează pe patru principii esențiale: 1. adevăr, 2. negare, 3. înșelăciune și 4. inducere în eroare. Deci, *inducerea în eroare* reprezintă doar o parte dintr-un spectru conceptual mult mai cuprinzător al decepției militare (pentru detalii în acest sens, vezi Robert M. Clark, William L. Mitchell, *Deception. Counterdeception and Counterintelligence*, CQ Press, Washington D.C., 2019).

informaționale, ce încearcă să ofere o înțelegere cuprinzătoare a ceea ce este considerat în spațiul public drept fake news. Necesitatea utilizării acestui concept se datorează: 1) utilizării abuzive – și, uneori, neadecvate –, de către oamenii politici și jurnaliști, a termenului în diverse contexte, determinând alterarea înțelesului acestuia; și 2) ca urmare a diferențelor culturale dintre Occident și spațiul estic. Spre exemplu, când ne referim la fake news, înțelegem că termenul vizează o informație falsă sau care induce în eroare. În schimb, în cultura rusă, există termeni precum *„lozh”* (Hamilton, 1986, p. 43), *„dezinformatsiya”* și *„maskirovka”*, care fac referire la aceste înțelesuri, dar fiecare dintre acești termeni diferă în înțelesuri în funcție de particularitățile lingvistice, culturale și contextuale. Astfel, pentru a înțelege corect modul de desfășurare al activităților informaționale din partea unui actor inițiator, este necesar să le analizăm din prisma particularităților lor culturale. În această lumină, utilizarea unui concept cât mai cuprinzător, care să diminueze aceste diferențe culturale dintre inițiator și țintă, devine o necesitate.

Distorsiunea informațională include instrumente și tehnici precum dezinformarea, diseminarea neintenționată de informații false și utilizarea informațiilor scoase din context. Datorită rolului pe care îl are conceptul în a altera realitatea, putem include în suma de tehnici și instrumente cum ar fi propaganda, manipularea informațiilor, propagarea zvonurilor, utilizarea „mediei alternative”.

Distorsiunea informațională include instrumente și tehnici precum dezinformarea, diseminarea neintenționată de informații false și utilizarea informațiilor scoase din context (Ib., p. 20), însă, datorită rolului pe care îl are conceptul în a altera realitatea, putem include în suma de tehnici și instrumente cum ar fi propaganda (albă, gri și neagră)[2], manipularea informațiilor, propagarea zvonurilor, utilizarea *„mediei alternative”*, mistificarea realității, utilizarea meme-urilor, propagarea excepționalismului politico-istoric asupra grupurilor țintă și radicalizarea acestora. Este important de precizat că distorsiunea informațională activează, în general, în cadrul *camerelor cu ecou* (Wardle, Derakhshan, p. 50), care reprezintă spațiile prin care indivizii sau grupurile țintite de distorsiunea informațională pot împărtăși și disemina propriile perspective și păreri. Principala vulnerabilitate a acestor camere este că schimbul de informații este, în general, subiectiv și prezintă biasuri cognitive care, ulterior, pot fi folosite de factorii externi infiltrați pentru a dirija apariția trendurilor, a surescita

[2] Alte abordări definesc *propaganda* ca activitate distinctă din cadrul operațiunilor psihologice, fiind o acțiune acoperită și specifică operațiunilor militare comune [Col. Frank L. Goldstein, col. Daniel W. Jacobowitz, *„Psychological Operations. An Introduction”*, în *Psychological Operations: principles and case studies*; col. Frank L. Goldstein (ed.), col. Benjamin F. Findley (ed.), Air University. Press Maxwell Air Force Base, Alabama, 1996, p. 6].

ținta/țintele pe anumite subiecte sau a determina/stimula acceptarea, refuzul ori acțiunea față de o idee, simbol sau eveniment.

Operațiunile informaționale pot fi privite prin prisma contextului generat de războiul hibrid/amenințările hibride, care, în Europa, a avut implicații semnificative asupra dimensiunii cognitive/a percepțiilor, mai ales când au fost organizate alegeri, referendumuri, proteste etc. În mod general, a reieșit că Federația Rusă a desfășurat în statele europene, în contextul războiului informațional, operațiuni informaționale care au încercat să determine formarea unor trenduri în societățile statelor sau să le influențeze în diverse direcții în funcție de particularitățile civilizaționale ale națiunilor europene și ca parte a conflictului dintre Federația Rusă și Occident (Darczewska, 2014, p. 12). De asemenea, acestea au urmărit, utilizând distorsiunea informațională, diseminarea constantă în spațiul public și social media de mesaje și narațiuni conflictuale care aveau rolul de a convinge audiențele de multiplele versiuni ale adevărurilor, bulversându-le în final (Wardle, Derakhshan, p. 30).

Operațiunile informaționale pot fi privite prin prisma contextului generat de războiul hibrid, care, în Europa, a avut implicații semnificative asupra dimensiunii cognitive/a percepțiilor, mai ales când au fost organizate alegeri, referendumuri, proteste etc.

Astfel, indiferent de modul în care definim operațiunile informaționale, abordarea lor teoretică se va adapta pe specificul gândirii și strategiei militare ruse, unde esența conceptuală își va avea originile în gândirea militară, dar aplicativitatea se va extinde dincolo de sfera militară, către cea civilă.

În acest sens, luând drept exemplu de perspectivă rusă viziunea lui Ivan Vorobev, general-maior cu o lungă carieră militară și expert în domeniul teoriei militare, remarcăm că relevante într-un conflict nu sunt numai dinamica atacului și spațiul de manevră, ci și mijloacele de a stopa accesul adversarului la informații corecte. El definește conceptul *atacului informațional* sau al *șocului informațional* în trei direcții: inițierea de operațiuni ofensive psihologice și de inducere în eroare, utilizarea de măsuri speciale pentru atacuri psihotronice și atacarea calculatoarelor cu scopul afectării sistemelor adverse de comandă și control (Franke, 2015, p. 23). Mai adăuga și faptul că, în timpul desfășurării războiului informațional, trebuie realizată o coordonare a acțiunilor de contrainformații, război electronic, distrugere fizică a punctelor și nodurilor C2 prin bombardamente precise și utilizarea decepției. Alte abordări descriu operațiunile informaționale/războiul

informațional (Ib., pp. 25-26)[3] dincolo de sfera militară, cum ar fi în cazul colonelului Anatolii Streltsov, care duce războiul informațional în sfera politică și guvernamentală. El consideră că principala sarcină a guvernului, în acest context, este de a contracara încercările actorilor ilegitimi de a folosi războiul informațional în zona ideologiei politice, în zona tehnică și în ceea ce privește politicile guvernamentale. În cadrul războiului informațional din sfera politică, el subliniază trei sarcini principale: identificarea și stoparea propagandei ideologice dăunătoare, stimularea societății civile de a contracara propaganda adversă și stoparea dezinformării despre politica de stat (Ib., pp. 28-29).

Remarcăm faptul că perspectiva rusă asupra operațiunilor informaționale ține cont, într-o măsură semnificativă, de experiența măsurilor active – operațiunile psihologice –, ceea ce ne determină să includem în discuție și relevanța componentei PSYOPS.

Operațiunile psihologice reprezintă activitățile întreprinse cu scopul de a influența, într-o direcție favorabilă propriilor forțe, emoțiile, gândurile și comportamentul unor grupuri țintă sau ale decidenților, fiind desfășurate pe timp de pace și război.

Operațiunile psihologice reprezintă activitățile întreprinse cu scopul de a influența, într-o direcție favorabilă propriilor forțe, emoțiile, gândurile și comportamentul unor grupuri țintă sau ale decidenților, fiind desfășurate pe timp de pace și război. Este important de menționat că activitatea operațiunilor psihologice este gândită și desfășurată în sens invers, mai exact conceperea planului de acțiune și punerea sa în practică depind de particularitățile cognitive și comportamentale ale țintei – grup sau individ – și de calitatea produselor de intelligence referitoare la țintă (Robinson, p. 137). Dacă, în cadrul celorlalte componente ale operațiunilor informaționale, utilizarea distorsiunii informaționale este minimă sau opțională, în cazul PSYOPS, putem spune că este maximă, fiind valorificate toate instrumentele și tehnicile ce pot favoriza finalizarea cu succes a operațiunilor. Din perspectiva procesului, operațiunile psihologice pot fi împărțite în trei categorii

[3] La fel ca în Occident, și în cazul Federației Ruse, perspectivele teoretice asupra războiului informațional și operațiunilor informaționale sunt multiple și prezintă un cumul de abordări ce variază de la cele clasice (specifice gândirii militare sovietice) sau neconvenționale până la cele care se fundamentează pe domeniul tehnico-militar sau care încearcă să găsească o relevanță deosebită unei specialități militare anume. Din această cauză, la fel cum menționa și generalul-maior Charis Saifetdinov, anumite concepte – în special, cele din câmpul războiului informațional – pot fi înțelese și interpretate în mod subiectiv, ca urmare a absenței expertizei solide, a principiilor bine definite și/sau a terminologiei care nu este clar înțeleasă. Deși pot exista explicații care să argumenteze că baza teoretică a războiului informațional/a operațiunilor informaționale ruse constă în experiența măsurilor active, conform defectorului KGB, Iuri Bezmenov, măsurile active se rezumă la spectrul de acțiuni specifice războiului psihologic/operațiunilor psihologice (PSYOPS), astfel ele fiind o componentă a războiului informațional și, implicit, a operațiunilor informaționale.

(Findley, 1996, p. 54): a). operațiuni psihologice strategice, prin a căror desfășurare se urmărește îndeplinirea unor obiective pe termen lung, în ideea creării unui mediu ulterior favorabil propriilor acțiuni și obiective; b). operațiuni psihologice operaționale, prin a căror desfășurare este urmărită obținerea unor avantaje pe termen mediu, la nivelul campaniilor militare și non-militare, regional sau global; și c). operațiuni psihologice tactice, prin a căror desfășurare se urmărește îndeplinirea unor obiective pe termen scurt, imediate, având mai mult un rol de suport decât desfășurarea unor operațiuni psihologice independente și de amploare.

În momentul stabilirii țintei, trebuie analizat specificul cultural și mediul din care aceasta provine. Mediul cultural poate determina percepțiile și preconcepțiile, perspectivele acesteia despre viață și lume, comportamentul și înclinațiile spre anumite sisteme de valori și idei. Este esențial ca acordarea operațiunilor psihologice să se plieze pe specificul cultural al țintei pentru a produce efecte.

Deși, în sine, operațiunile psihologice sunt un subiect vast și complex, cu propria metodologie și abordare, în cadrul acestei lucrări, este relevant să subliniem câteva caracteristici comune de care operațiunile psihologice trebuie să țină cont în momentul planificării și desfășurării (Ib., pp. 55-59):

❖ *Diferențele culturale* – în momentul stabilirii țintei, trebuie analizat specificul cultural și mediul din care aceasta provine. Mediul cultural poate determina percepțiile și preconcepțiile, perspectivele acesteia despre viață și lume, comportamentul și înclinațiile spre anumite sisteme de valori și idei. Este esențial ca acordarea operațiunilor psihologice să se plieze pe specificul cultural al țintei pentru a produce efecte.

❖ *Influențele sociale* – în funcție de apartenența socială la o clasă sau un grup, ținta poate avea anumite obiceiuri sau preferințe în ceea ce privește acceptarea sau refuzul unei idei sau perspective promovate de formatorii de opinie. În acest sens, expertiza asupra unei ținte se poate face și în sens invers, plecându-se de la mediile pe care aceasta le frecventează și formatorii de opinie pe care îi urmărește.

❖ *Motivațiile* – există o strânsă legătură între nevoile, motivele și comportamentul unei ținte, toate acestea variind de la necesități primare până la nevoia de autodeterminare. Deși, de obicei, motivele sunt rezultatul satisfacerii sau nesatisfacerii unor nevoi de bază, acestea pot determina conceptualizarea existenței proprii pe baza sentimentelor, percepțiilor, experiențelor, mediului înconjurător, interacțiunilor și, în final, a autoevaluării. Acestea pot fi foarte utile analizei PSYOPS, deoarece, prin motivațiile sale, ținta acționează într-o anumită direcție, oferind indicii însemnate despre cine este sau ce dorește să fie și ce vrea să obțină.

❖ *Percepțiile și atitudinile* – înțelegerea indivizilor, a contextului și a mediului înconjurător se realizează prin intermediul propriilor perspective despre viață și lume, setul de valori pe care și-l asumă, experiență și trendurile la care aderă, toate acestea determinând ca percepția individului să fie selectivă și subiectivă. Atitudinea reprezintă predispoziția individului de a acționa într-o anumită direcție, fiind condiționată de dimensiunea cognitivă, afectivă și comportamentală, afectând în mod direct percepțiile indivizilor. În acest sens, operațiunile psihologice pot acționa asupra: a) schimbării atitudinii și percepțiilor prin utilizarea unui flux constant de informații noi și narațiuni care să fie repetitive, să urmeze o logică narativă și să fie desfășurate pe lungi perioade de timp; și b) schimbării emoțiilor determinate de o acțiune, idee, fapt sau eveniment prin utilizarea informațiilor, prin orice canal, care să fie contradictorii raționamentelor inițiale – percepțiilor preconcepute –, determinând, în final, dezamorsarea pornirilor emotive.

Un ajutor semnificativ în activitatea operațiunilor psihologice constă în intelligence, deoarece acesta poate aduce informații utile, care să ajute la calibrarea și perfecționarea operațiunilor și să ofere analize referitoare la compatibilitatea dintre efectele operațiunilor psihologice și rezultatul dorit.

Trebuie precizat că un ajutor semnificativ în activitatea operațiunilor psihologice constă în intelligence, deoarece acesta poate aduce informații utile, care să ajute la calibrarea și perfecționarea operațiunilor și să ofere analize referitoare la compatibilitatea dintre efectele operațiunilor psihologice și rezultatul dorit. În cazul operațiunilor psihologice (dar nu se limitează la acestea), intelligence-ul (Waltz, p. 219) poate avertiza din timp atunci când o acțiune informațională inamică este în desfășurare, poate oferi o perspectivă reală asupra unei situații, sesizează indicatorii subtili, poate investiga, analiza și face recomandări acolo unde a fost valorificată o vulnerabilitate etc.

Chiar dacă, până acum, am evidențiat, pe scurt, rolul și însemnătatea operațiunilor informaționale, subdiviziunile acestora și activitățile conexe pe care le angrenează în îndeplinirea unui obiectiv demonstrează precizia unui sistem extrem de complex și sincronizat. Pornindu-se de la factori independenți de țintă precum cultura, mediul înconjurător, influențele sociale, se ajunge până la motivele, trăirile, percepțiile și atitudinile unei ținte, operațiunile psihologice având ca scop final utilizarea informațiilor analizate pentru a influența, în mod specific, o țintă.

Având în vedere cele prezentate, definirea războiului informațional și a operațiunilor informaționale reliefează o perspectivă mult mai comprehensivă asupra mediului informațional actual, care este

mai mult decât doar o campanie de dezinformare și de fake news sau propagandă. De asemenea, includerea printre acestea a câtorva abordări ruse asupra războiului informațional evidențiază originea militară în materie de concepție și acțiune, mai ales în sensul în care, prin intermediul operațiunilor psihologice, este revitalizat spectrul măsurilor active asupra unor elemente esențiale din societățile statelor, în acest sens, fiind vorba de influențarea formatorilor de opinie sau a grupurilor ale căror acțiuni pot determina destabilizare, haos sau pot favoriza acțiuni contrare intereselor naționale proprii.

EXEMPLE

Operațiunile informaționale ruse asupra Poloniei au urmărit fracturarea unității societății poloneze prin utilizarea distorsiunii informaționale, mai precis prin intoxicarea mediului informațional cu meme-uri menite să adâncească tensiunile dintre diferite facțiuni, precum xenofobii, naționaliștii și pro-europenii.

Cazurile prezentate nu sunt izolate, iar exemplele în care Federația Rusă a utilizat spectrul războiului informațional asupra momentelor cheie din politica internă a statelor europene nu sunt puține. Însă, spre deosebire de Europa Occidentală, activitatea informațională rusă a fost ceva mai resimțită la nivelul statelor din fostul bloc socialist, ca urmare a moștenirilor marxist-leniniste, a legăturilor culturale, a originilor comune (în anumite cazuri) și a interacțiunilor istorice. Astfel, am luat drept exemple, pentru a evidenția activitatea operațiunilor informaționale ruse, Polonia, Cehia și Slovacia.

Polonia

Deși Polonia cu greu poate fi orientată spre o perspectivă măcar puțin mai *„caldă”* față de Federația Rusă, este totuși supusă războiului informațional. Chiar dacă nu prezintă vulnerabilități ce ar putea să genereze vreo legătură directă cu Federația Rusă, în realitate, există o gamă de oportunități ce sunt exploatate de către Federația Rusă. În cazul Poloniei, încercarea introducerii în percepția opiniei publice a unei narațiuni pro-ruse ar fi o acțiune sortită eșecului, ceea ce înseamnă că aici abordarea trebuie să fie una complexă. Operațiunile informaționale ruse asupra Poloniei au urmărit fracturarea unității societății poloneze prin utilizarea distorsiunii informaționale, mai precis prin intoxicarea mediului informațional cu meme-uri menite să adâncească tensiunile dintre diferite facțiuni, precum xenofobii, naționaliștii și pro-europenii (Lucas, Pomerantsev, 2017, p. 23). Având în vedere că operațiunile informaționale ruse încearcă să susțină și să scoată în prim-plan naționalismul exacerbat polonez, remarcăm faptul că, în acest sens, se folosesc de componenta culturală

a operațiunilor psihologice pentru a determina grupările radicale să promoveze etnocentrismul și sentimentul anti-occidental (alături de cel anti-rusesc). În anumite privințe, site-uri obscure (falanga.org.pl, konserwatyzm.pl) au încercat să elogieze acțiunile grupărilor extremiste din trecutul Poloniei și să compare eficiența lor, determinată de absența corectitudinii politice și a constrângerilor, cu timpurile actuale. Spre exemplu, portalul de știri kresy.pl stabilise un flux regulat, care comemora, în mod repetitiv, masacrul polonezilor din vestul Ucrainei, realizat de Armata Insurecțională Ucraineană (UPA) în timpul celui de-al Doilea Război Mondial (Gajos, Rodkiewicz, 2016, p. 264).

Astfel, distorsiunea informațională generează o cosmetizare a personalităților poloneze cu înclinații etnocentrice și radicale, promovându-le, iar la nivel de societate, încearcă să determine unele trenduri anti-UE și anti-NATO, fundamentate pe criticism negativ, nostalgie față de regimul comunist, antisemitism, urltracatolicism și ideologii antidemocratice (Ib., p. 24). Emoțiile și percepțiile polonezilor asupra existenței lor ca națiune și asupra trecutului lor constituie cele mai semnificative vulnerabilități, fiind susceptibili la fluxurile informaționale ce îi pot radicaliza, mai ales în contextul în care mediul politic polonez – care începe să fie caracterizat de ultraconservatorism – alimentează etnocentrismul și sentimentul anti-.

Emoțiile și percepțiile polonezilor asupra existenței lor ca națiune și asupra trecutului lor constituie cele mai semnificative vulnerabilități, fiind susceptibili la fluxurile informaționale ce îi pot radicaliza, mai ales în contextul în care mediul politic polonez – care începe să fie caracterizat de ultra-conservatorism – alimentează etnocentrismul.

Cehia și Slovacia

La nivel informațional, cazul celor două state este unul remarcabil, deoarece acestea sunt profund penetrate de operațiunile informaționale ruse și pot deveni un punct de lucru pentru diseminarea elementelor războiului informațional.

În aceste două state, operațiunile informaționale ruse încearcă să pună în valoare, în mod general, prezența curentelor antioccidentale, iar în mod particular, a celor antiamericane, din interiorul celor două societăți în încercarea de a le generaliza. Utilizându-se și aici distorsiunea informațională, narațiunea primară se bazează pe antagonizarea adversarului (Occidentul) și, în funcție de context, încearcă să creeze Federației Ruse o imagine, dacă nu favorabilă în sensul unei alternative pentru aceste două state, cel puțin acceptabilă ca partener compatibil de colaborare. Dacă, de obicei, media mainstream acționează ca un element de corecție a distorsiunii informaționale din interiorul social-media și al mass-mediei, în cazul celor două state s-a dezvoltat,

în ultimul timp, o media *„alternativă”* cu puternice influențe pro-ruse (Lucas, Pomerantsev, p. 25). Astfel, în Cehia, media reprezintă canalul principal al desfășurării operațiunilor informaționale ruse, iar datorită acestui fapt, se disting patru tendințe (Vit, 2016, pp. 279-280): 1) media tradițională, înființată după perioada de tranziție, care rezistă în fața presiunilor influențelor informaționale ruse și care este subfinanțată și, treptat, deprofesionalizată; 2) noua media online, conectată la fluxul principal de știri ce s-a format preponderent în perioada 2012-2014, fiind la fel de rezistentă la influențele informaționale ruse; 3) media online, apărută după 2010, care se nișează pe subiecte politice și sociale, făcând abstracție de fluxul principal de știri, și care include în articolele sale și narațiuni rusești *„alternative”*; și 4) revistele online, care pretind că prezintă perspective necenzurate asupra lumii și care își fundamentează articolele pe argumente axate pe dreptul la opinie (subiectivizarea realității în acord cu preconcepțiile publicului țintă), incluzând în argumentație și teorii ale conspirației. Alt aspect foarte interesant constă în modul de acțiune al operațiunilor informaționale ruse în spațiul ceh, deoarece sunt desfășurate operațiuni fățișe și acoperite, unde cele fățișe au rol de distragere. Drept exemplu, site-ul *Aeronet* (Lucas, Pomerantsev, p. 26), fondat inițial de iubitorii de aviație, în 2001, și-a schimbat proprietarii în mai multe rânduri, până a ajuns ca, în 2014, să publice primul articol pro-rus. Acest site poate fi încadrat în zona operațiunilor informaționale acoperite, ca urmare a dificultății de a urmări proprietarii acestui domeniu, titlul site-ului nu este sugestiv pentru conținutul pe care îl distribuie, fiind dificil de interceptat, autorii sunt anonimi sau folosesc pseudonime și conținuturile au surse îndoielnice sau fictive. Suma acestor site-uri acoperite, ce diseminează narațiuni pro-ruse și elemente ale distorsiunii informaționale precum teorii ale conspirației, propagandă gri sau neagră, fake news-uri etc., s-ar putea să o depășească pe cea a site-urilor fățișe, care ar avea scopul de a induce în eroare și de a influența (Sputnik, Russia Today, TASS etc. pot fi încadrate în sfera canalelor fățișe prin care obiectivul principal este influențarea percepțiilor publicului țintă).

În Cehia, media reprezintă canalul principal al desfășurării operațiunilor informaționale ruse, iar datorită acestui fapt, se disting patru tendințe: media tradițională; noua media online; media online și revistele online.

În schimb, în Slovacia, operațiunile informaționale ruse au valorificat, în principal, două vulnerabilități ale statului: dependența statului slovac de importurile de hidrocarburi din Federația Rusă, care au determinat o aprofundare a relațiilor (mai ales diplomatice) dintre cele două state – spre deosebire de Cehia, care și-a diversificat sursele

– și existența problemelor socio-economice, care au generat o tendință a societății slovace de apreciere și nostalgie față de moștenirea marxist-leninistă. De această dată, activitatea informațională rusă asupra publicului slovac s-a orientat pe utilizarea operațiunilor psihologice, ca urmare a faptului că încearcă să determine, la nivel cognitiv, percepții și atitudini nostalgice și favorabile trendurilor anticapitaliste sau antioccidentale. De asemenea, alături de fluxul constant și repetat de mesaje care subiectivizează în mod pozitiv memoria comunismului cehoslovac, este introdusă și tema panslavismului, în încercarea de a fundamenta percepția publicului slovac asupra unei legături cultural-istorice și etnolingvistice cu Federația Rusă (Fischer, 2016, pp. 295, 301).

O problemă majoră a războiului informațional din Cehia și Slovacia este că operațiunile informaționale au dus la producerea subversiunii politice (Rosenau, 2007, pp. 6-7) prin crearea unui mediu informațional prielnic infiltrării factorilor subversivi în instituții cheie, iar în situația în care sunt deconspirați, total sau parțial, aceștia să beneficieze de susținerea sau indiferența publicului. Spre exemplu, în Cehia, operațiunile informaționale ruse au creat o întreagă infrastructură ce a constat, conform serviciului ceh de contrainformații (BIS) (EURACTIV, 2016), în infiltrarea unor agenți de influență și monopolizarea informațională a mass-mediei și a social media. De asemenea, distorsiunea informațională a generat o *„realitate alternativă”* față de Miloš Zeman, ceea ce a contribuit semnificativ la alegerea sa în funcția de președinte al statului, pentru a doua oară. Miloš Zeman (Santora, 2018), în calitate de vector de influență, nu a ezitat să își manifeste, de-a lungul timpului, tendințele etnocentrice și afinitatea față de Federația Rusă și China, în detrimentul partenerilor și aliaților occidentali, dezvoltând o retorică pro-rusă și antioccidentală.

O problemă majoră a războiului informațional din Cehia și Slovacia este că operațiunile informaționale au dus la producerea subversiunii politice prin crearea unui mediu informațional prielnic infiltrării factorilor subversivi în instituții cheie, iar în situația în care sunt deconspirați, total sau parțial, aceștia să beneficieze de susținerea sau indiferența publicului.

Din acest punct de vedere, remarcăm o legătură între operațiunile informaționale și subversiune, deoarece, alături de Zeman, apar alte două personalități care ar avea legături externe sau intenții contrare intereselor naționale ale Cehiei (PBJ, 2020): Vratislav Mynář, ce deține funcția de șef al Biroului Prezidențial, din 2013, însă fără a deține un certificat de securitate din partea Oficiului de Securitate Națională (NBU), și omul de afaceri Martin Nejedlý, ce are legături cu Lukoil și mediul politic rus și care deține un birou în cadrul Biroului Prezidențial, fără a fi plătit din fondurile publice, dar care, deseori, îl însoțește

pe președinte în călătoriile externe. În Slovacia, se încearcă o formă de subversiune politică ce se poate exemplifica prin activitatea fostului prim-ministru Jan Čarnogurský, președinte al Asociației Slovaco-Ruse, cu sediul la Bratislava, care, în 2015, a încercat să adune semnături pentru un referendum pe tema rămânerii sau a părăsirii NATO de către Slovacia. În schimb, la nivelurile societății, operațiunile informaționale ruse încearcă propagarea panslavismului atât în interiorul Slovaciei, cât și în extern, prin promovarea unui vehicul informațional, precum Clubul slovac de motocicliști *„Lupii nopții”* (Gotev, 2018). Elementele ce particularizează acest club de motocicliști[4] constau în faptul că unii membri au contribuit efectiv la procesul anexării Peninsulei Crimeea în 2014, sunt promotori ai naționalismului rus și susținători ai lui Vladimir Putin, iar în 2018 au inițiat proiectul *„Lumea Slavă”*, ce presupunea un tur de promovare a proiectului prin majoritatea statelor est-europene și, probabil, de transmitere a unui mesaj de susținere sau de surescitare a indivizilor și grupurilor adepte ale panslavismului, ultranaționalismului sau susținătoare ale acțiunilor Federației Ruse. Este de menționat că, prin exemplul *„Lupilor nopții”*, remarcăm rolul activităților informaționale și subversive ruse de a pune în valoare orice vehicul care le poate ajuta la îndeplinirea obiectivelor/misiunii și nu se limitează la activitățile clasice ale serviciilor de intelligence.

În Slovacia, se încearcă o formă de subversiune politică ce se poate exemplifica prin activitatea fostului prim-ministru Jan Čarnogurský, care, în 2015, a încercat să adune semnături pentru un referendum pe tema rămânerii sau a părăsirii NATO de către Slovacia.

CONCLUZII

Așa cum am văzut, dinamica mediului de securitate se schimbă și, dacă până nu demult, elemente ce țineau de amenințările militare erau tratate ca atare, infuzia acestor elemente în zona civilă poate fi datorată războiului hibrid și amenințărilor pe care le generează. Războiul informațional poate fi perceput ca o amenințare hibridă, deoarece, cum am văzut în cazul Poloniei, Cehiei și Slovaciei, țintele sale constau în grupuri specifice (cu anumite preferințe religioase și ideologice, din anumite clase sociale, cu anumite particularități

În schimb, la nivelurile societății, operațiunile informaționale ruse încearcă propagarea panslavismului atât în interiorul Slovaciei, cât și în extern, prin promovarea unui vehicul informațional, precum Clubul slovac de motocicliști „Lupii nopții”.

4 Clubul de motociclism reprezintă o organizație atât formală, cât și informală, compusă din pasionați ai motocicletelor, care își dezvoltă propriul stil de viață și reguli cutumiare. Legăturile dintre membri sunt puternice, iar în cadrul organizației, există o ierarhie bine stabilită, fundamentată, de obicei, pe grade militare recunoscute și aplicate doar în interiorul organizației. Datorită caracterului său libertin și, uneori, antisistem, unele cluburi de motocicliști au fost implicate în activități specifice crimei organizate, precum trafic de persoane, droguri și armament, șantaj și amenințare, spălare de bani, crime la comandă etc.

culturale etc.), iar ambiguitatea momentului desfășurării, a formei și a practicilor folosite îl face greu de prevenit și de stopat.

Este interesant că amenințarea războiului informațional se mulează pe particularitățile statelor și vânează vulnerabilitățile sale. Spre exemplu, în Polonia, am văzut că se axează pe flagelul radicalismului aflat în societatea polonă.

În acest sens, istoria și geopolitica pot oferi destule oportunități de exploatare în cazul mai multor state, fiind greu de interpretat dacă acțiunile informaționale sunt determinate de un stat agresor sau doar aparțin unor grupuri ce au interese proprii. De asemenea, mai rămâne dilema protejării decidenților politici și militari care, fiind parte a societății, sunt conectați la fluxul informațional din social media și mass-media, iar expunerea lor regulată la degenerările informaționale duce la condiționare și, ulterior, la alterarea percepției corecte a realității în care trăiesc.

Astfel, definirea și oferirea unor concepte operaționale care să clarifice rolul și însemnătatea războiului informațional și a operațiunilor informaționale, împreună cu componentele sale, devin esențiale. Având în vedere contextul actual, în care confruntările din mediul informațional nu mai fac distincția dintre starea de pace și război, devine imperios ca statele să își clarifice conceptele și să își dezvolte propriile strategii și arme informaționale – la fel ca în cazul armamentelor și doctrinelor convenționale –, prin care să obțină avantaje, să se protejeze sau să limiteze oportunitățile adversarului. Deși literatura de specialitate vorbea, încă din anii ’90, de rolul tot mai semnificativ pe care informația îl va avea pentru cetățeni și decidenți, în prezent, încă mai sunt perspective care clasifică războiul informațional și operațiunile informaționale ca desfășurându-se doar în cadrul universului militar și al serviciilor de intelligence. Tot aici, utilizarea superficială a termenilor și tehnicilor distorsiunii informaționale determină necesitatea recurgerii la noi concepte și redimensionarea felului în care percepem activitățile informaționale, mai ales în contextul în care abordări, concepte și tehnici ce aparțineau cândva domeniului militar și al serviciilor de intelligence au început să se extindă și spre mediul civil.

Având în vedere contextul actual, în care confruntările din mediul informațional nu mai fac distincția dintre starea de pace și cea de război, devine imperios ca statele să își clarifice conceptele și să își dezvolte propriile strategii și arme informaționale – la fel ca în cazul armamentelor și doctrinelor convenționale –, prin care să obțină avantaje, să se protejeze sau să limiteze oportunitățile adversarului.

În final, putem spune că ceea ce conferă războiului informațional perspectiva de a se dezvolta constă în eficacitatea sa datorată ambiguității și imprevizibilității cu care acționează, indiferent de țintă.

Însă, cel mai interesant fapt este că războiul informațional este un concept fundamentat pe gândirea militară ce produce efecte dincolo de sfera militară.

BIBLIOGRAFIE:

1. Čižik, T. (ed.). (2017). *Information Warfare – New Security Challenge for Europe*. Bratislava: Centre for European and North Atlantic Affairs (CENAA).
2. Darczewska, J. (2014). *„The anatomy of Russian information warfare: the Crimean operation, a case study”*. Varșovia: Centre for Eastern Studies.
3. Findley, B.F., *„Blending Military and Civilian PSYOP Paradigms”*. În *Psychological Operations: principles and case studies*, Goldstein, L., Frank, col. (ed.), col. Findley, F. Benjamin (ed.). (1996). Alabama: Press Maxwell Air Force Base. Air University.
4. Franke, U. (2015). *„War by non-military means: Understanding Russian information warfare”*. Swedish Defence Research Agency (FOI).
5. Goldstein, L., Frank, col. (ed.), col. Findley, F. Benjamin (ed.). (1996). *Psychological Operations: principles and case studies*. Alabama: Press Maxwell Air Force Base. Air University.
6. Gotev, G. (2018). *„Slovak president sees security risk in ‘Putin’s motorcycle club’ activity”*. În *EURACTIV*, publicat la 01.08.2018, republicat la 02.08.2018, https://www.euractiv.com/section/global-europe/news/slovak-president-sees-security-risk-in-putins-motorcycle-club-activity/, accesat la 28 martie 2021.
7. Hamilton, L.D. (1986). *Deception in Soviet Military Doctrine and Operations*. California: Naval Postgraduate School Monterey.
8. Herman, M. (1996). *Intelligence power in peace and war*. Royal Institute of International Affairs.
9. Lucas, E., Pomerantsev, P. (2017). *„Winning the Information War Redux. Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe”*. Center for European Policy Analysis (CEPA).
10. Nemr, C., Gangware, W. (2019). *„Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age”.* PARK ADVISORS.
11. Pynnöniemi, K. (ed.), Rácz, A. (ed.). (2016). *Fog of Falsehood. Russian Strategy of Deception and the Conflict in Ukraine*. The Finnish Institute of International Affairs.
12. Robinson, P. (2010). *Dicționar de securitate internațională*. Traducere de Monica Neamț. Cluj-Napoca: Editura CA Publishing.
13. Rosenau, W. (2007). *„Subversion and Insurgency”.* RAND Corporation: National Defense Research Institute.
14. Santora, M. (2018). *„Czech Republic Re-elects Milos Zeman, Populist Leader and Foe of Migrants”*. În *The New York Times*, 27 ianuarie 2018,

https://www.nytimes.com/2018/01/27/world/europe/czech-election-milos-zeman.html, accesat la 21 februarie 2021.
15. Theohary, A.C. (2018). *„Information Warfare: Issues for Congress”.* Congressional Research Service.
16. Waltz, E. (1998). *Information Warfare: Principles and Operations*. Boston, Londra: Artech House.
17. Wardle, C., Derakhshan, H. (2017). *„Information Disorder”*. Consiliul Europei.
18. AAP-6 (2018). *Glosar de termeni* și *definiții NATO* (engleză, franceză și română). Agenția de Standardizare NATO (ASN).
19. Department of Defense (DoD) (2020). *Dictionary of Military and Associated Terms*. Joint Publication (JP).
20. *EURACTIV* (2016). *„Russian secret services wage information war, says Prague”*, 2 septembrie 2016, https://www.euractiv.com/section/global-europe/news/russian-secret-services-wage-information-war-says-prague/, accesat la 28 martie 2021.
21. *Prague Business Journal (PBJ)* (2020). *„Zeman's Dream Team: VratislavMynar and Martin Nejedly”*, 31 ianuarie 2020, https://praguebusinessjournal.com/zemans-dream-team-vratislav-mynar-and-martin-nejedly/, accesat la 28 martie 2021.