RĂZBOIUL INFORMAȚIONAL, INTELLIGENCE-UL DE SECURITATE ȘI INTELLIGENCE-UL MILITAR – O SCURTĂ ABORDARE TEORETICĂ –

Teodor BADIU
Academia Națională de Informații, București

În domeniul cercetării, în cadrul discuțiilor din spațiul public și în materialele concepute și diseminate de trusturile mass-media, problema războiului hibrid/amenințărilor hibride este, adesea, analizată fie ca fenomen, fie ca factor specific al unui eveniment. Cu toate acestea, datorită complexității subiectului, se face o oarecare confuzie sau conceptele sunt amestecate, pe măsură ce subiectul devine și mai ambiguu. În plus, utilizarea excesivă, în spațiul public, a unor termeni precum „manipularea informațiilor", „propagandă", „dezinformare", „influență" a condus la o modificare a sensului acestora și la o ambiguitate a efectelor pe care acești termeni le au asupra percepției amenințării.

Pe de altă parte, în acest context, rolul și relevanța securității și a informațiilor militare în gestionarea și limitarea războiului hibrid/amenințărilor hibride au fost puțin discutate. Ca atare, această lucrare încearcă să detalieze într-un mod succint, plecând de la complexitatea subiectelor, la nivel teoretic, conceptele de informații de securitate, informații militare și război informațional.

Cuvinte-cheie: război informațional, securitate, decepție/înșelare, exerciții multinaționale, confruntări asimetrice

INTRODUCERE

Plecând de la experiența ucraineană și de la situațiile de ingerințe informaționale asupra treburilor interne ale altor state, *războiul hibrid/amenințările hibride* reprezintă factorul de instabilitate și insecuritate ce acționează în funcție de specificul operațiunilor, indiferent de natura actorilor. Acesta acoperă mediul internațional de securitate, cu precădere spațiul european, datorită acțiunilor Federației Ruse din anul 2014, care au reamintit Uniunii Europene și Alianței Nord-Atlantice că Federația Rusă este dispusă să utilizeze toate mijloacele pentru a-și atinge obiectivele strategice, inclusiv redobândirea sferei sale de influență asupra statelor est-europene.

Din această privință, putem privi *războiul hibrid* drept factorul ce stabilește contextul de desfășurare a războiului informațional și care determină diminuarea distanței dintre intelligence-ul de securitate – cu rol de a securiza elementele ce pun în funcțiune sistemul național precum societatea, economia, mediul politic, infrastructura etc. – și cel militar –, a cărui funcție este de a aduna informații despre forțele armate ale adversarului sau ale unuia posibil, diseminând informațiile obținute unui *decident militar* ce poate formula strategii sau organiza/reorganiza forțele militare în funcție de necesități. În mod tradițional, activitatea acestora se intensifica atunci când între cel puțin doi actori exista o stare de conflict declarat, însă, în prezent, *războiul hibrid* există fără ca statele să declare acțiunile pe care le desfășoară și fără a exista vreun conflict declarat. O problemă majoră a *războiului hibrid* este că acesta ambiguizează originile și formele amenințărilor, ceea ce a determinat intensificarea activităților de monitorizare, prevenție sau combatere de către instituțiile specializate în intelligence-ul militar și de securitate. Chiar și în privința războiului informațional, contextul *războiului hibrid* a produs modificări, precum: dacă, în mod tradițional, războiul informațional reprezenta o componentă ce se regăsea în cadrul conflictelor armate dintre actori (de ex., confruntări asimetrice sau iregulare, abordări neconvenționale, măsuri active etc.), sfera sa de activitate s-a extins și spre cea civilă, fără a mai necesita declararea oficială a începerii ostilităților.

În continuare, vom aborda, din punct de vedere teoretic, relevanța războiului informațional, a intelligence-ului de securitate și a celui militar pentru a înțelege câteva dintre particularitățile acestora.

DEFINIREA RĂZBOIULUI INFORMAȚIONAL, A INTELLIGENCE-ULUI DE SECURITATE ȘI A INTELLIGENCE-ULUI MILITAR

Războiul hibrid este un concept operațional care integrează o gamă largă de elemente, iar în acest sens, este previzibil ca acesta să afecteze domenii pornind de la cel economic, politic și militar până la cel social și cultural. Cu toate acestea, evenimentele din ultimii ani, începând cu 2014 – anexarea Peninsulei Crimeea și apariția de forțe separatiste în estul Ucrainei, ascensiunea politică a grupurilor extremiste în Europa, implicările străine în alegeri și referendumuri, proliferarea armamentelor convenționale între NATO și Federația Rusă, jocurile de război[1] inițiate în timpul exercițiilor multinaționale, campaniile de dezinformare și delegitimare inițiate de Federația Rusă, tentativa de asasinare a agentului defector Serghei Skipal, necesitatea de regândire a măsurilor de protecție de tip CBRN (contextul răspândirii la nivel internațional a virusului COVID-19) –, demonstrează necesitatea de a include intelligence-ul de securitate și intelligence-ul militar într-o abordare comună și integratoare. În ansamblu, aceste evenimente pot fi înțelese ca segmente ce compun războiul hibrid, iar dacă, până acum, se discuta despre specificitatea intelligence-ului de securitate și intelligence-ului militar, mutațiile amenințărilor au dus la un amalgam de acțiuni informaționale și militare, ale căror efecte s-au resimțit mai ales în Europa de Est.

Un rol esențial în înrăutățirea mediului de securitate îl are *războiul informațional*. Acesta este un termen asociat războiului hibrid (dar nu numai, fiind conexat și cu războiul asimetric, iregular, neconvențional, măsurile active, diplomația publică etc.) (Theohary, 2018, pp. 4-5), care are dublă valență, ofensivă și defensivă, și care are forme de manifestare distincte, în funcție de starea de război sau de pace. NATO definește conceptul în termeni strict militari, întrucât războiul informațional constă în: *„acțiuni întreprinse pentru obținerea superiorității informatice prin deteriorarea sistemelor informatice inamice și protejarea celor proprii". (*AAP-6, 2018, p. 430). Dar, așa cum am vorbit despre context, observăm că războiul informațional nu se manifestă doar în sfera militară, ci se poate extinde și spre zona socială și politică sau poate fi interdisciplinar.

Spectrul larg în care poate acționa războiul informațional îl face să fie o armă mult mai eficientă, ca urmare a faptului că (Molander et al., 1996, pp. 15-29):

- raportul cost-beneficii poate fi maximizat datorită costurilor relativ scăzute. Spre deosebire de întreținerea și desfășurarea unei armate a cărei existență să reprezinte o amenințare sau să ducă la o dilemă de securitate, infuzia unui mediu informațional cu zvonuri, informații parțial adevărate sau ambigue,

[1] Jocurile de război reprezintă o formă analitică ce simulează aspecte tactice, operaționale și strategice ale unei confruntări convenționale. De obicei, sunt folosite pentru examinarea conceptelor de luptă, pregătirea analiștilor și a comandanților, dezvoltarea de scenarii și evaluarea efectelor.

poate determina percepții eronate și o escaladare a fricii. De asemenea, susținerea și organizarea războiului informațional pot fi susținute de un număr restrâns de indivizi, fiind destul de accesibil;

- estomparea granițelor tradiționale datorate interdependențelor economice, sociale, politice și militare a dus la o alterare a individualității actorilor statali. Racordarea statelor, dar și a actorilor privați la sistemul informațional global (prin internet, spre exemplu) a produs amplificarea dificultății de distincție dintre amenințările externe și interne în contextul războiului informațional;
- percepțiile și gestionarea acestora pot fi problematice în sensul în care fluxul informațional abundă în informații oficiale, neoficiale, secvențiale, conspiraționiste, eronate, false, ambigue etc., făcând societatea vulnerabilă la alterări ale realității sau intoxicări. Manipularea informațiilor prin tehnici și tehnologii poate permite unei game largi de actori să submineze autoritatea și chiar legitimitatea instituțiilor, a statelor sau a organizațiilor internaționale;
- dificultatea de avertizare din timp și de evaluare rapidă a impactului determină o vulnerabilitate majoră în fața atacurilor informaționale-surpriză, actorii fiind limitați ca posibilitate de prevenire sau răspuns. Dublată și de dificultatea de a vedea, în cel mai scurt timp, care a fost ținta, evaluarea efectelor poate necesita timp și costuri suplimentare;
- interoperabilitatea dintre aliați sau membrii unei organizații internaționale duce la sincronizarea sistemelor C4I pentru a asigura coerență, însă, chiar dacă sistemele proprii sunt bine securizate, slăbiciunea unui sistem aliat poate duce la penetrarea sistemului general.

În privința războiului informațional, trebuie apreciat că pilonul său constă în *operațiunile informaționale (OI)*, care pot fi definite drept desfășurarea integrată a capabilităților informaționale în acord cu alte linii de operațiuni pentru a influența, întrerupe, corupe sau uzurpa factorii de decizie ai adversarilor, în timp ce sistemele proprii sunt protejate (*Dictionary of Military and Associated Terms*, 2020, p. 104). În principiu, *operațiunile informaționale* servesc scopului de a face adversarul/ținta să se comporte, sau nu, într-o direcție anume prin utilizarea de informații segmentate (extragerea informației dintr-un context specific), propagandă și dezinformare intenționată (determinată de o acțiune deliberată și organizată) sau neintenționată (determinată de acțiuni eronate, înțelegerea greșită sau degenerarea involuntară a informației). *Operațiunilor informaționale* li se subsumează următoarele tipologii de operațiuni (Theohary, ibid., p. 3):

- Operațiuni psihologice (PSYOPS) – presupun tipul de operațiuni inițiate cu scopul de a influența și exploata emoțiile, motivațiile, percepția și comportamentul țintei la nivel cultural și cognitiv;

- Operațiunile de securitate (OPSEC) – reprezintă acțiunile și măsurile întreprinse în scop defensiv, prin care sunt identificate și analizate informațiile esențiale, factorii perturbatori a unei operațiuni în desfășurare, dar și protejarea tuturor elementelor ce contribuie la îndeplinirea operațiunii. În scop ofensiv, înseamnă culegerea de informații care să faciliteze înțelegerea adversarului, fiind și procesul de încetinire a posibilității de a lua o decizie în timp util de către decidenții adversarului;
- Războiul electronic – este definit drept cumul de acțiuni tehnice militare, desfășurate prin utilizarea undelor electromagnetice și a semnalelor pentru a sprijini operațiunile în desfășurare, a proteja tehnica proprie și a ataca sistemele informatice ale adversarilor. Ca activități mai cunoscute, putem menționa bruiajul sistemelor de comunicații, criptarea și decriptarea canalelor, utilizarea sistemelor de poziționare prin sateliți (GPS) etc.;
- Operațiuni cibernetice – sunt acțiunile desfășurate în spațiul cibernetic, care pot varia de la întreruperea și virusarea sistemului până la sprijinirea sistemelor integrate și protecția sistemelor proprii;
- Decepția/înșelarea – poate angrena toate sau o bună parte din tipurile de operațiuni prezentate cu scopul de a decepționa adversarul. Poate fi realizată prin transmiterea *„accidentală”* de rapoarte și documente false agenților străini, falsificarea unor canale radio ce sunt interceptate, organizarea de afișaje înșelătoare etc. (Herman, 1996, p. 170), iar în funcție de informațiile pe care adversarul le deține, pot fi valorificate oportunități care să determine confuzii la nivel decizional.

Având în vedere tipologiile de operațiuni, remarcăm faptul că *operațiunile informaționale* pot avea un caracter coercitiv, care se poate traduce prin influențarea, în direcții dirijate, a factorilor de decizie sau a mediului civil, prin operațiuni acoperite. Dacă discutăm de abordarea soft, operațiunile informaționale pot contribui prin crearea unei imagini pozitive în raport cu alți actori, ceea ce va determina legitimitate sau avantaje pe termen lung ori doar element de suport în diplomația publică.

Deși operațiunile informaționale sunt inițiate și planificate, în general, de specialiști ce aparțin domeniului militar sau al serviciilor de informații, aplicabilitatea lor se extinde dinspre zona militară către cea civilă. Așa încât, în ultimii ani, discuțiile referitoare la *distorsiunea informațională* (Wardle et al., 2017, p. 20) – concept mult mai cuprinzător, care înglobează fake news-urile, false news-urile, dezinformarea și propaganda gri –, ce se propagă în mass-media, cu preponderență în momente-cheie, precum alegerile, referendumurile, protestele majore, stările de criză etc., s-au intensificat, având în vedere că acestea produc efecte în relația dintre grupurile sociale, dar și între autorități și propriii cetățeni. Putem spune că spectrul

distorsiunii informaționale poate contribui la procesul de decepție/înșelare, deoarece livrează unei ținte anumite informații parțial adevărate sau false, ceea ce presupune că trebuie să-i creeze o percepție specifică ori să o facă să acționeze într-o anumită direcție. Văzută din perspectivă psihologică, esența distorsiunii informaționale constă în subiectivismul țintei, unde nu este important felul în care este prezentată povestea, ci povestea însăși, care poate favoriza un context dat.

Pentru a exemplifica, putem aborda chestiunea platformelor social-media, precum Facebook și Twitter, care se confruntă, tot mai des, cu distorsiunea informațională ce se folosește de infrastructura acestora. Drept urmare, încă din anul 2016, aceste platforme au încercat să inițieze acțiuni și măsuri de reglementare ceva mai austere, referitoare la postarea și distribuirea de conținuturi, la eliminarea acestora sau a conturilor care sunt dubioase și răspândesc informații eronate și contradictorii (Polyakova, Fried, 2019, p. 12). Pe de altă parte, alte companii, ca Google și YouTube, au manifestat o transparență redusă referitoare la măsurile adoptate. Mai precis, Google a permis factorilor perturbatori cunoscuți, precum Sputnik sau Russia Today, să rămână în topul motoarelor de căutare, în timp ce YouTube a schimbat doar termenii și condițiile referitoare la conținuturile video cu tentă extremistă și insultătoare, fără a susține o campanie solidă de eliminare a acestora (Ibid., pp. 13-14). În această privință, atentatul de la Christchurch, din Noua Zeelandă, în 2019, când un individ radicalizat a transmis live, pe internet, atacul asupra a două moschei, poate fi abordat ca exemplu al incapacității platformelor de a stopa răspândirea informațiilor toxice. Doar după acest incident, YouTube a înlăturat de pe platforma sa videoclipul *Remove Kebab*, considerat a fi un cântec de propagandă antimusulman din perioada războaielor iugoslave. Este de menționat faptul că acest cântec era ascultat de ucigaș în drum spre cele două moschei...

Social-media încearcă să blocheze, în diferite proporții, instrumentele și efectele *operațiunilor informaționale*, dar acestea nu vor putea face față tocmai din cauza specificului distinct. *Operațiunile informaționale* sunt de sorginte militară, fundamentate pe o doctrină militară, unde planificarea și execuția se fac de către un personal civil-militar. Din cauza acestui fapt, companiile private din sfera social-media se află în dezavantaj, deoarece răspunsul acestora este dintr-o perspectivă strict tehnică, iar din punct de vedere cultural, sunt legate de principiile pieței economice. Organizarea unui răspuns adecvat și eficient ar presupune formarea unui departament specializat, compus din personal instruit în domeniul intelligence-ului, care nu ar fi, probabil, legal și sustenabil din prisma relației cost-beneficii.

Astfel, observăm că, în privința *operațiunilor informaționale* și, implicit, a războiului informațional, statele sunt cele care trebuie să reacționeze, deoarece acestea sunt singurele care dispun de personal calificat în execuție și combatere,

legitimitate morală și legală, resurse materiale consistente, aparat birocratic complex și instituții specializate. În această privință, statul poate deține monopolul, iar în contextul competiției internaționale, nevoia de securitate poate acutiza însemnătatea și activitatea intelligence-ului de securitate și a celui militar.

După al Doilea Război Mondial, Sherman Kent introduce în literatura de specialitate noțiunea de *intelligence de securitate* ca formă distinctă de *intelligence-ul militar*. El îl definește în două direcții: drept intelligence-ul din spatele muncii polițienești, care se ocupă cu protejarea statului și a cetățenilor, și ca activitate destinată identificării acelor factori perturbatori interni, precum agenții clandestini, trădătorii, elementele de crimă organizată și persoanele care încalcă legea (federală) (Kent, 1965, pp. 209-210). Această perspectivă asupra intelligence-ului de securitate tinde să se aproprie de munca polițienească, însă, dacă vom compara instituțiile mai multor țări care se ocupă cu intelligence-ul de securitate, vom vedea că acestea și-au dezvoltat un specific ce ține de cultură, de trecutul și tradiția instituției, regimul din care fac parte, importanța instituției în raport cu alte instituții de profil, resursele financiare de care dispun, gradul de calificare și numărul personalului etc. În mod general, subiectele de interes ale intelligence-ului de securitate constau în contraterorism, combaterea operațiunilor subversive desfășurate pe teritoriul național, contraspionaj și combaterea activităților crimei organizate. Intelligence-ul de securitate, în teorie, exclude activitățile din domeniul politic, economic și tactico-militar și este considerat a fi diferit de securitatea informațiilor, intercalându-se doar în privința contraspionajului – intelligence-ul de securitate și securitatea informațiilor ar avea ca scop comun prevenirea/combaterea scurgerilor de informații și protejarea sistemelor informaționale (Robinson, 2010, pp. 113, 207). Și, cu toate că, în mod teoretic, instituțiile acreditate pe zona de intelligence de securitate ar trebui să se ocupe numai pe zona de protecție internă, în practică, există particularități ale instituțiilor din diverse state, ce duc la apariția unor diferențe notabile.

Luând ca exemplu MI5 (Security Service) din Marea Britanie, FBI din SUA și FSB (Serviciul Federal de Securitate) din Federația Rusă, putem remarca abordări distincte în materie de securitate națională, fiecare incluzând activități ce depășesc zona securității interne sau orientându-se pe arii specifice. În acest sens, putem exemplifica situația FSB-ului, care, după fuziunea sa cu Agenția Federală a Comunicațiilor și Informațiilor Guvernamentale/FAPSI, are atribuții nu numai defensive, ci și ofensive prin întreprinderea de activități specifice războiului electronic, în comparație cu MI5, care oferă o atenție sporită contraterorismului și care își extinde aria spre apărarea bunăstării economice și a regimului democratic parlamentar – ca și componentă ideologică/identitară (Ibid., pp. 92, 209). Michael Herman explică intelligence-ul de securitate ca entitate separată de

factorii de decizie al căror rol ar trebui să fie de a oferi informații și nu consultanță. Cu toate că intelligence-ul de securitate trebuie să se ocupe de amenințările interne, acestea, oricât de interne ar părea, au o proveniență externă, astfel încât este vital, în procesul de informare a decidenților, ca analizele și prognozele să cuprindă și elementele externe (Herman, p. 34). Această adaptare se datorează tranziției paradigmei de securitate de la sistemul Războiului Rece, fundamentat pe un conflict ambivalent dintre blocul Tratatului de la Varșovia și NATO, la un sistem multipolar, marcat de incertitudinile războiului hibrid. Dacă, în ceea ce privește munca de intelligence, perioada Războiului Rece a fost orientată spre culegerea de informații, organizarea și destructurarea operațiunilor subversive, de spionaj și contraspionaj, pentru a înțelege intențiile adversarului, în prezent, asistăm la un paradox. Nu este un caz rar când intelligence-ul extern este cules și din teritoriul național, în timp ce intelligence-ul de securitate este cules din afara granițelor naționale, iar țintele pot consta mai mult în subiecte decât în actorii propriu-ziși, mai ales în contextul diluării sensului strict intern al intelligence-ului de securitate (Ibid., pp. 47-49).

În privința intelligence-ului militar, se poate spune că există formată o tradiție îndelungată, ca urmare a necesității armatelor de a cunoaște informații vitale, precum capacitățile, numărul, specializările, moralul, dispunerea trupelor, strategiile, centrele de comandă etc. ale forțelor adverse. Astfel, definirea intelligence-ului militar începe cu perspectiva lui Carl von Clausewitz, care descria culegerea de informații pe timp de război drept necesară, dar contradictorie. Fie există situația în care o parte din informații sunt false și altă parte este compusă din informații incerte care, la un moment dat, se vor contrazice, fie informațiile se susțin una pe cealaltă și, în vâltoarea luptei, o decizie care părea oportună se dovedește a fi greșită din cauza informațiilor eronate, mincinoase sau exagerate (Clausewitz, 2014, p. 38). Pe scurt, intelligence-ul militar reprezintă acea componentă a intelligence-ului care este preocupată de subiecte specifice zonei militare, capabilitățile statelor, ale organizațiilor străine sau operațiuni militare multinaționale în desfășurare (DoD, p. 91). Mai putem adăuga că intelligence-ul militar încearcă să descopere, pe de o parte, punctele vulnerabile în arhitectura militară inamică, oferind comandamentului șansa de a-și eficientiza acțiunile combative cu riscuri minime, iar pe de altă parte, analizează și descoperă punctele nevralgice din sistemul de apărare propriu și al aliaților. Totuși, în lumina proliferării armamentelor convenționale și a jocurilor de război din ultimii ani, subiectele intelligence-ului de apărare par să rămână încă în centrul atenției instituțiilor de securitate. *Intelligence-ul de apărare* poate fi considerat o subcategorie a intelligence-ul militar, ale cărui subiecte sunt de interes și pentru mediul politic. Obiectul de activitate este axat pe supravegherea acțiunilor militare externe și războaiele locale sau regionale, cuprinzând insurecții autonome sau susținute de ajutor extern; situații în care politica, violența și operațiunile

subversive cumulate duc la utilizarea forțelor armate; eșuarea statelor în urma conflictelor inter-etnice, religioase, ideologice etc. (Herman, p. 50). Pe lângă subiectele de interes pentru intelligence-ul de apărare, mai sunt și industriile de apărare, exporturile de armament, evoluțiile tehnologice în materie de tehnică militară, proliferarea armelor de distrugere în masă (tactice și balistice) etc.

Un aspect fundamental al intelligence-ului, care nu poate fi neglijat, fie dacă vorbim de intelligence-ul de securitate sau de cel militar, constă în *decepție.* NATO o definește ca *„măsuri de inducere în eroare a inamicului prin manipularea, distorsiunea și/sau falsificarea realității, astfel încât acesta să reacționeze într-un mod dezavantajos pentru el”.* (AAP-6, p. 272). Aceasta nu este o practică nouă, ea fiind folosită încă din Antichitate, de către lideri și generali în îndeplinirea obiectivelor, însă, din punct de vedere conceptual, varianta complexă a decepției constă în *decepția militară (MILDEC)*. Vorbind strict de caracterul său operațional, decepția militară nu ar putea fi considerată parte a intelligence-ului, având în vedere că este un conglomerat de elemente și activități specifice, ca OPSEC, PSYOPS, război electronic, culegerea de informații, contraspionaj etc. Însă, poate fi luată în considerare ca mijloc defensiv în cazul intelligence-ului de securitate și ofensiv în cel al intelligence-ului militar. Deși pare straniu că este atribuit și primei categorii, în contextul războiului informațional, MILDEC poate genera diverse forme de percepție țintelor politico-militare, dar și celor civile, determinând acțiuni eronate sau inacțiuni inoportune ale guvernelor ori poate determina societatea civilă să pună presiune pe guverne, într-o direcție dirijată. În mod special, remarcăm că spectrul de activități soft al MILDEC este compus din agenți de influență, operațiuni informaționale, operațiuni acoperite de finanțare ale grupurilor politice sau ale unor trusturi media, iar spectrul hard este compus din suport acoperit față de grupurile de opoziție, forțele de rezistență, insurgență sau teroriste și activități de sabotare și operațiuni paramilitare (Herman, p. 55).

În privința decepției/înșelare/inducere în eroare militare, literatura de specialitate este abundentă și cuprinde detalieri cuprinzătoare, de la țintele și obiectivele decepției până la canalele, rețelele și filtrele utilizate în decepție. Subiectul MILDEC reprezintă în sine – ca și celelalte, precizate în lucrare – o temă de cercetare vastă, ce îmbină aspectele teoretice și practice într-o artă subtilă, însă, pentru acest studiu, vom evidenția câteva aspecte teoretice fundamentale.

Rolul MILDEC este de a crea o *poveste a decepției* pe care adversarul să o poată prelua ca atare, iar în acest sens, toate dovezile să îi indice că povestea este conformă cu realitatea. Povestea decepției este o narațiune sau o declarație succintă, construită în funcție de perspectiva și specificul țintei – structura mentală, valorică, culturală și așteptările sale – și care este servită prin evenimente de inducere

în eroare (Field Manual 3-13.4, 2019, p. I-5). În privința tipurilor de decepție, pot fi identificate două categorii:

1) amplificarea ambiguității, care are scopul de a genera confuzie și conflict interior asupra factorilor de decizie adverși printr-un flux continuu de informații aparent plauzibile, atrăgând atenția lor de la un set de activități la altul;

2) diminuarea ambiguității, care are în vedere manipularea și exploatarea gândirii și a convingerilor preexistente ale factorilor de decizie adverși, prin îndrumarea țintei spre locul nepotrivit, la timpul nepotrivit, în condiții de maximă vulnerabilitate (Ibid., pp. I-6-I7). Deopotrivă, mai pot fi regăsiți, în literatura de specialitate, termeni alternativi precum decepție Tip-A (ambiguity-increasing), pentru amplificarea ambiguității, și decepție Tip-M (misleading deception), pentru diminuarea ambiguității, fiind identificate și forme pasive și active ale decepției. Forma pasivă este bazată pe acțiunile de acoperire și camuflaj a intențiilor și/sau a capacităților proprii față de adversar, în timp ce forma activă este constituită din acțiunile deliberate proprii, de a-i prezenta adversarului intențiile sau capabilități pe care nu le posedă (Shaw, 2014, p. 3). Ca tactici, MILDEC se folosește de o gamă restrânsă, care să servească în mod concret obiectivelor situaționale, astfel:

- *Șiretlicurile* – acțiuni deliberate de alterare a realității prin informații.
- *Diversiunea* – distragerea intenționată a adversarului de la un subiect/obiectiv de interes sau de la desfășurarea unui atac.
- *Fenta* – acțiuni ofensive ce presupun contactul direct cu adversarul și al căror scop este de a induce în eroare adversarul referitor la locul și/sau momentul când un atac va avea loc.
- *Demonstrația* – spectacol de forțe inițiat cu scopul de a determina adversarul să aleagă cel mai dezavantajos curs al acțiunii sale.
- *Acoperirea* – acțiuni orientate spre mascarea pregătirilor sau a inițierii unei operațiuni ofensive, fiind, în funcție de situație, asociat și cu *condiționarea*.
- *Expunerea* – acțiuni organizate pentru a susține povestea decepției prin simulare, deghizare și/sau evidențierea capacităților și a alcătuirii forțelor aliate (Ibid., p. 6).

Trebuie reafirmat că în centrul acestor acțiuni se află povestea decepției, care este un produs al imaginației. Aceasta necesită o gândire organizată și disciplinată, întrucât logica poveștii să nu se întrerupă, iar ținta să o poată percepe vizibil – exagerarea subtilității sale poate duce la ignorarea poveștii decepției. Formularea trebuie făcută din perspectiva țintei, iar ansamblul său este o prezentare generală a întregii decepții. Astfel, povestea decepției trebuie să fie verificabilă (ținta să o poată confirma prin canalele proprii sau cu ajutorul structurilor de intelligence aliate), executabilă (existența autorității și a resurselor necesare), credibilă (diminuarea suspiciunilor și a îndoielilor din partea țintei) și consistentă (inițiatorii decepției

trebuie să cunoască gradul de pregătire al țintei, pentru a nu exagera sau a diminua complexitatea poveștii). (Field Manual 3-13.4, pp. II-10 – II-11). Din acest motiv, în cadrul proceselor de inducere în eroare, sunt folosite deseori maxime specifice domeniului, care să faciliteze organizarea operațiunilor de decepție. Astfel, detaliem câteva dintre aceste maxime (CIA, pp. 5-20, 22-26, 32-33), relevante pentru acest studiu:

a) *Principiul lui Magruder* urmărește valorificarea convingerilor adversarului, utilizarea acestora în alterarea realității și examinarea posibilităților ce pot fi în dezavantajul său. Acest principiu poate fi exemplificat prin momentul planificării invaziei Normandiei, unde informațiile arătau că germanii se așteptau la o ofensivă aliată în regiunea Pas-de-Calais, fiind un revers al planurilor germane de a invada Marea Britanie.

b) *Limitările umane ale procesării informației* sunt procese ale cogniției umane care, în mod aproape universal, în situații specifice, prezintă sincope ale proceselor. În acest sens, sincopele pot fi exploatate, ceea ce ne duce spre *legea numerelor mici* și la predispoziția spre *condiționare*. Legea numerelor mici se referă la tendința umană de a generaliza în cazul seturilor mici de date. Condiționarea este obișnuirea adversarului cu o anumită situație sau stare, care a fost săvârșită în timp, prin transmiterea unor stimuli repetitivi. Altă limitare constă în tendința umană de a omite micile schimbări sau detaliile.

c) *Formele multiple ale surprizei* constau în locație, capacitățile forței, intenție, stilul specific și sincronizare. Deși, în cadrul unei operațiuni, nu toate elementele pot fi atinse, accentul trebuie pus pe limitarea unui număr de elemente care au relevanță. Utilizarea alarmelor false constituie unul dintre principalele elemente de surpriză, pe de o parte, prin condiționarea adversarului de a nu mai răspunde imediat la aparentele amenințări iminente, iar pe de altă parte, prin inducerea în eroare, întrucât adversarul își orientează atenția, resursele și efectivele acolo unde indică alarmele false.

d) *O alegere dintre tipurile de decepție* este absolut necesară, ca urmare a faptului că utilizarea extensivă a acestora poate duce la neîncrederea țintei în aparențele ce i se servesc. Astfel, se optează, în această situație, pe reducerea ambiguității, cu toate că, dacă ținta deține deja anumite informații reale, se poate recomanda accentuarea *„zgomotelor”* – creșterea posibilităților de acces ale țintei la informații alternative false și/sau la dovezi care să adeverească informațiile alternative false.

e) *O regulă de secvențiere* se referă la necesitatea ca activitățile de inducere în eroare să fie succesive și susținute cât de mult posibil, pentru a consolida povestea decepției.

Trebuie precizat că procesul decepției este unul constant, datorită schimbului de informații care se realizează între echipele de analiză și organizare și cele operative.

Dar, probabil, culegerea de informații despre adversar, analizarea și interpretarea acestora pot fi considerate acțiuni fundamentale ale întregii operațiuni de inducere în eroare. Pentru a influența comportamentul țintei, este vital să existe ajutor din partea structurilor de intelligence și să se mențină un flux constant al informării asupra felului în care aceasta percepe mediul înconjurător, al felului în care procesează informațiile și al modului de luare a deciziilor, urmând analizarea variabilelor din mediile politice, militare, economice, sociale și informaționale ale țintei ce o pot influența (Field Manual 3-13.4, pp. II-3, II-14).

O altă precizare importantă constă în modul în care ținta percepe, la nivel cognitiv, amenințarea și remarcăm că există o tendință a indivizilor de a percepe lucrurile ca urmare a propriilor așteptări, unde și acestea sunt modelate de context. Modul lor de gândire poate prezenta câteva vulnerabilități ce constau în:

a) tendința de formare a unor raționamente pripite, ce ulterior se pot schimba doar printr-un efort psihologic deliberat considerabil;

b) asimilarea seturilor de informații noi, care pot fi contradictorii, și utilizarea lor în consolidarea raționamentului inițial;

c) expunerea îndelungată la informații ambigue sau neclare, ceea ce determină ca o expunere ulterioară la un nou set de informații să necesite o sumă de informații suplimentare, chiar dacă acestea pot reliefa din primele momente imaginea de ansamblu (Heuer, 1999, pp. 7-14). Deși pot exista dovezi solide care să demonstreze imprecizia raționamentului inițial, procesele mentale fac ca reorganizarea datelor și a informațiilor asimilate să fie o muncă anevoioasă în schimbarea unei percepții. Cu toate că dinamica evenimentelor denotă alte tendințe, există o rezistență interioară referitoare la perceperea noilor schimbări. Chiar dacă individul este dispus, din punct de vedere psihologic, să reanalizeze datele și informațiile, perspectivele diferite la care ajunge vor avea legătură, în continuare, cu raționamentul inițial, neputând fi schimbat sau eradicat (Ibid, p. 125).

Având în atenție aceste detalii, ambiguitatea relației dintre războiul informațional, intelligence-ul de securitate și intelligence-ul militar pare a se diminua. Războiul informațional este, în sine, ofensiv, însă are tendința de a angrena actori din voința lor proprie ori ca victime. Ca urmare, intelligence-ul de securitate trebuie să se adapteze la noile provocări și să răspundă în timp util unor amenințări care, în actualul context, nu sunt ușor de reperat și anticipat. Însă, incertitudinile mediului de securitate al secolului XXI au dus la o extindere a ariei intelligence-ului de securitate și, practic, au generat micșorarea delimitărilor dintre acesta și intelligence-ul militar. Proiecția puterii unui stat față de altul prin informații și decepția asupra inexistenței sau existenței unor capabilități naționale însemnate generează, de asemenea, dileme de securitate. Toate acestea produc, în fond, percepții ca rezultat al unor acțiuni voite sau ca efect necalculat, însă riscul ca percepțiile să degenereze și să se transforme în frică este foarte real.

CONCLUZII

După cum am observat, războiul informațional și, în special, decepția încearcă să amăgească percepția indivizilor într-o anumită direcție. Percepția poate întruchipa înțelegerea greșită a unei situații reale, determinând: un stat să acționeze pripit în raport cu un altul; un guvern să nu perceapă corect nevoile propriei populații și să acționeze în defavoarea ei; sau populația, influențată de sentimente negative și neajunsuri, să recurgă la proteste masive față de autoritatea centrală, până la război civil. Perceperea eronată a unui factor extrem de important sau a unui eveniment posibil ori în desfășurare poate genera panică și frică neîntemeiate, acțiuni inoportune, pasivitate nocivă, agresivitate disproporționată etc., determinând, astfel, probleme de securitate națională. De asemenea, percepția realității nu este un lucru standardizat, el fiind diferit în funcție de informațiile pe care indivizii le asimilează și le interpretează, folosind filtre, precum experiența personală, educația, cultura, contextul spațial și temporal, afilierea la un grup sau la un set de norme și valori specifice etc.

Pe de altă parte, adăugându-se și contextul pe care războiul hibrid îl stabilește, acesta determină maximizarea ambiguității referitoare la originea, natura și impactul inițial al amenințării informaționale și militare. Coroborat cu surpriza strategică și decepția, există riscul ca factorii de decizie să fie incapabili să acționeze ori să acționeze inoportun în momente-cheie, ca urmare a fluxurilor informaționale la care au fost supuși în acord cu propriile percepții. Cel mai relevant exemplu, în acest sens, este cazul Ucrainei, unde cumulul de acțiuni militare și non-militare ale Federației Ruse au dus la anexarea Crimeii și destabilizarea estului Ucrainei (apariția conflictelor armate în regiunile Donețk și Luhansk), ceea ce a determinat o surpriză strategică, pe care conducerea de la Kiev nu o prevăzuse și care i-a cauzat imposibilitatea de a răspunde în timp util.

În acest sens, datorită dinamicii mediului de securitate, rolul și relevanța intelligence-ului de securitate și militar cresc exponențial, din două motive:

a) pot constitui sursa distorsiunii informaționale și a decepției, mai ales că instituțiile specializate în activitatea de intelligence au capacitatea de a desfășura acțiuni ofensive și defensive;

b) datorită complexității acestora, pot desfășura un spectru larg de măsuri de protecție ce pornește de la obiective strategice până la decidenții politici și militari care, fiind parte a societății, sunt conectați la fluxurile informaționale.

În final, putem afirma că evoluțiile tehnologice, teoretice și geopolitice afectează forma conceptelor războiului informațional și ale intelligence-ului de securitate și militar, deoarece dinamica mediului de securitate accentuează necesitatea unei abordări neașteptate, inteligente și surprinzătoare. Indiferent de starea de pace

sau de război, de țintă, combatanții (declarați sau nu) vor încerca să obțină, prin toate mijloacele, avantaje și câștiguri strategice drept alternativă pentru folosirea directă și în masă a forței.

BIBLIOGRAFIE:

1. Clausewitz, von C. (2014). *Despre război.* Editura ANTET.
2. Herman, M. (1996). *Intelligence power in peace and war*. Royal Institute of International Affairs.
3. Heuer, J.R.Jr. (1999). *Psychology of Intelligence Analysis*. Central Intelligence Agency: Center for the Study of Intelligence.
4. Kent, S. (1965). *Strategic Intelligence for American World Policy*. Connecticut: Archon Books. Hamden.
5. Molander, C.R., Riddile, S.A., Wilson, A.P. (1996). RAND: *„Strategic information warfare: a new face of war".*
6. Polyakova, A., Fried, D. (2019). Atlantic Council: *„Democratic Defense against Disinformation 2.0"*.
7. Robinson, P. (2010), *Dicționar de securitate internațională*. Trad. de Monica Neamț. Cluj-Napoca: Editura CA Publishing.
8. Shaw, J.E. (2014). *„Military Deception at the Operational Level War"*. The United States Naval War College: Joint Military Operations Department.
9. Theohary, A.C. (2018). *„Information Warfare: Issues for Congress".* Congressional Research Service.
10. Wardle, C., Derakhshan, H. (2017). *„Information Disorder".* Council of Europe.
11. AAP-6, *Glosar de termeni și definiții NATO (engleză, franceză și română)*. (2018). Agenția de Standardizare NATO (ASN).
12. Central Intelligence Agency, *„Deception Maxims: Factand Folklore"* (1981). Washington: Office of Research and Development.
13. Clark, M.R., Mitchell, L.W. (2019). *Deception. Counter deception and Counterintelligence*. Washington D.C.: CQ Press.
14. Department of Defense (DoD) (US), *Dictionary of Military and Associated Terms*. (2020). Joint Publication (JP).
15. Field Manual 3-13.4, *Army Support to Military Deception* (2019). Washington: Headquarters, Department of the Army.