OPINII PRIVIND DEFINIREA ȘI INTERPRETAREA UNOR CONCEPTE DIN GÂNDIREA ȘI TEORIA MILITARĂ RUSĂ

Teodor BADIU

Academia Națională de Informații „Mihai Viteazul”, București

DOI: 10.55535/GMR.2022.2.01

Există o abundență de perspective și interpretări referitoare la practicile și acțiunile Federației Ruse asupra statelor și indivizilor, în special la nivel informațional. Însă, în anumite privințe, perspectivele occidentale tind să simplifice acțiunile rusești și să le catalogheze drept jocuri de sumă nulă. În acest sens, lucrarea încearcă să interpreteze modul de acțiune al Federației Ruse, mai ales la nivel informațional, prin definirea unor concepte-cheie și încearcă să ofere o perspectivă asupra felului în care teoreticienii militari ruși folosesc noțiunea de „acțiuni ostile” în contextul conceperii operațiunilor pe timp de pace. În plan secund, este evidențiată complexitatea fondului teoretic militar rusesc, cu succinte comparații între formele teoretice ale unor concepte din perioada sovietică și din prezent. De asemenea, lucrarea revizuiește anumite concepții referitoare la forma hibridă a acțiunii ruse, încearcă să sintetizeze anumite opinii ale unor teoreticieni militari ruși și, având ca reper cultura strategică rusă, să arate care sunt nivelurile de acțiune în contextul desfășurării unei serii de operațiuni. În final, lucrarea propune un model orientativ care abordează o perspectivă holistică referitoare la modul în care acțiunile, subversive și informaționale, ale Federației Ruse pot influența politica și securitatea unui stat având ca ținte individul, societatea și sistemul politic.

Cuvinte-cheie: abordare indirectă, război informațional, mijloace nonmilitare și asimetrice, măsuri active, maskirovka.

INTRODUCERE

Din 2014 până în prezent, literatura de specialitate referitoare la amenințările hibride/asimetrice și la războiul hibrid a tot înflorit, încercând, în diverse procedee, să descrie, să explice și să interpreteze modurile prin care Federația Rusă operează, fățiș și acoperit, în mediul internațional. Însă, în ultimii ani, au început să apară și voci care introduc ideea că perspectiva occidentală tinde să transforme subiectul războiului hibrid/amenințărilor hibride într-o abordare mai apropriată de cultura strategică occidentală.

Pe de altă parte, nu trebuie exagerată această observație, având în vedere că lucrările științifice și analitice care abordează acest subiect, în mod public, se fundamentează pe culegerea informațiilor din surse deschise, neclasificate. În acest sens, riscul apariției unei dihotomii dintre direcțiile de cercetare sau analiză și realitatea obiectivă este dat de volumul mare de informații și de calitatea informațiilor publice (care pot fi incomplete, false sau compromise). Tot aici, un aspect problematic este dat de imposibilitatea de a verifica certitudinea cercetării sau analizei publice cu informații obținute din surse clasificate (HUMINT, SIGINT, IMINT etc.) din cauza restricțiilor ce țin de protecția informațiilor. De asemenea, obținerea unui produs informațional relevant pentru un anumit subiect/temă (analiză sau lucrare științifică) depinde nu doar de informație, ci și de o serie de caracteristici personale, precum experiența, abilitățile, deprinderile, cunoștințele despre subiect/temă (Chiru, 2019, p. 71).

Obținerea unui produs informațional relevant pentru un anumit subiect/ temă (analiză sau lucrare științifică) depinde nu doar de informație, ci și de o serie de caracteristici personale, precum experiența, abilitățile, deprinderile, cunoștințele despre subiect/ temă.

Având în vederea acestea, lucrarea de față exprimă unele opinii referitoare la definirile și interpretările unor concepte și perspective teoretice militare ruse cu intenția de a genera o imagine de ansamblu. Lucrarea va urmări formele și metodele de acțiune rusească, accentuând specificul culturii strategice a Federației Ruse și felul în care decurge, din perspectivă rusă, desfășurarea unui conflict, în special în mediul informațional. Astfel, ne va interesa să observăm cum percep teoreticienii ruși rolul informației într-un conflict, care sunt țintele unei operațiuni informaționale ruse, când o folosesc și cum este

informația integrată ca armă în cadrul unei serii de operațiuni (etapizate sau sincronizate). Pe parcursul lucrării nu ne vom concentra doar pe elementul informațional, ci vom explica și defini și alte concepte, precum războiul informațional, abordarea indirectă, operațiunile asimetrice și nonmilitare. Totodată, vom încerca să explicăm modurile de acțiune ale decepției militare ruse *(maskirovka),* alături de măsurile active și controlul reflexiv, ca parte a unei serii de operațiuni. În final, vom evidenția un model orientativ de acțiune rusească ce urmărește afectarea mediului informațional (dimensiunea informațională și cognitivă) cu scopul de a realiza o schimbare de regim sau de a schimba structura social-politică.

OPERAȚIUNI INDIRECTE/NONMILITARE SAU RĂZBOI HIBRID/AMENINȚĂRI HIBRIDE?

În cadrul gândirii militare ruse, putem identifica trei stadii în care un stat se poate găsi: pace – stare generală, la nivel intern și extern; acțiuni ostile – stare conflictuală ambiguă; război – stare social-politică, definită ca formă combativă a activităților ostile.

În privința gândirii și artei militare ruse referitoare la războiul hibrid, atât teoreticienii militari, cât și cei civili preferă să evite utilizarea conceptului de *război hibrid* în favoarea altor termeni, precum *abordare/strategie indirectă*, *măsuri/operațiuni nonmilitare*, *acțiuni asimetrice/indirecte*, *strategii de uzură*. Din punctul lor de vedere, războiul hibrid reprezintă una dintre opțiunile valabile atunci când este gândită o posibilă acțiune militară. După analizarea particularităților posibilului teatru de operații și a contextului conflictului, acțiunea militară este proiectată în așa fel încât să permită, în mod fluid, comutarea la diverse modalități de acțiune pentru îndeplinirea scopurilor militare și/sau politice (Kabernik, 2019, p. 59). În acest sens, în cadrul gândirii militare ruse, putem identifica trei stadii în care un stat se poate găsi (Ib., pp. 60-61): a) pace – stare generală, la nivel intern și extern, caracterizată de absența acțiunilor ostile; b) acțiuni ostile – stare conflictuală ambiguă, caracterizată de intenția de a elimina sau suprima un adversar prin măsuri violente sau acțiuni indirecte ori acoperite al căror scop este de a schimba structura socială, politică sau culturală; c) război – stare social-politică, definită ca formă combativă a activităților ostile (cu origini în gândirea lui Clausewitz și Lenin), la nivel intern și extern, unde este folosită, fățiș și direct, violența prin intermediul operațiunilor militare.

Echivalentul occidental al *„acțiunilor ostile”* ar consta în spectrul acțiunilor sub acoperire, pe care l-am putea defini drept *„...activități precum acordarea de ajutor în mod secret unor susținători politici*

din alte țări, dezinformarea, propagandă neagră și alte tipuri de operațiuni psihologice, provocări, sabotaj, subversiune, asasinate și susținerea insurgenților, a loviturilor și a terorismului". (Robinson, 2010, p. 14). Totuși, în mod tradițional – în gândirea și arta militară occidentală –, acțiunile sub acoperire sunt executate în timpul unui conflict declarat[1], fiind cumulate cu acțiunile directe ale forțelor armate. Pe de altă parte, teoreticienii militari ruși adaugă celor două stări clasice, de pace și război, această stare a acțiunilor ostile care nu se încadrează în logica războiului clasic, însă care este mai mult decât simpla competiție dintre state, sugerând că statele sunt mereu rău intenționate (în principal, pe timp de pace), intențiile acestora fiind de tip *realpolitik*. Prin urmare, acțiunile ostile urmăresc modificarea structurii sociale, a celei politice și culturale ale unui stat într-o anumită direcție. Putem presupune că, din acest raționament, reiese îngrijorarea Federației Ruse față de izbucnirea *„revoluțiilor colorate"* și tendința centralizării exacerbate a puterii pe plan intern.

Acțiunile ostile urmăresc modificarea structurii sociale, a celei politice și culturale ale unui stat într-o anumită direcție. Din acest raționament, reiese îngrijorarea Federației Ruse față de izbucnirea „revoluțiilor colorate" și tendința centralizării exacerbate a puterii pe plan intern.

Totuși, în cadrul gândirii și teoriei militare ruse putem identifica o sumă de păreri, concepte și abordări teoretice care nu sunt mereu clare, iar uneori acestea acționează ca o *„ceață"* în identificarea unui tipar de acțiune rus. Acest fapt este enunțat și de generalul-maior (r.) Charis Saifetdinov, care considera că există anumite arii pe care cercetarea și deciziile ulterioare ale factorului de decizie (în Federația Rusă) ar trebui să le stabilească, mai concret este necesară o universalizare a terminologiei (în contextul războiului informațional), obiectivele ar trebui să fie definite clar, principiile referitoare la modurile de îndeplinire a obiectivelor trebuie fundamentate, iar, în final, unitățile și resursele necesare trebuie identificate și alocate (Franke, 2015, p. 25). În acest sens, chiar dacă o parte dintre aceste aspecte au fost rectificate, corectate și/sau ajustate de Federația Rusă, încă este puțin probabil ca să existe o uniformizare completă a conceptelor și a termenilor.

[1] Chiar dacă există o linie destul de subțire între acțiunile acoperite desfășurate de structurile de securitate pe timp de pace și război, acestea trebuie diferențiate în funcție de context și scop. Spre exemplu, pe timp de război, efortul comun al tuturor instituțiilor se concentrează pe a obține victoria sau doar a descuraja adversarul prin toate mijloacele, iar pe timp de pace (în contextul competiției internaționale), acțiunile acoperite sunt desfășurate, în mod exclusiv, de organizațiile de intelligence și cuprind spionajul, utilizarea operațiunilor psihologice sau informaționale, provocările, subversiunea, finanțarea și susținerea unor forțe insurgente/separatiste/de gherilă etc.

Rezumându-ne, în continuare, la sfera *„acțiunilor ostile”*, putem remarca faptul că, pe timp de pace, spațiul de luptă este desfășurat, preponderent, în mediul informațional – cu excepția implicării forțelor speciale și a factorilor subversivi –, cuprinzând acțiuni ofensive și defensive în sfera HUMINT, operațiunilor electronice, operațiunilor cibernetice, operațiunilor psihologice, operațiunilor informaționale, inducerea în eroare a factorilor de decizie și așa mai departe.

În susținerea acestei idei, putem evidenția unele perspective (comprimate) ale teoreticienilor militari și civili, precum:

- *colonelul (r.) Serghei Cekinov și generalul-locotenent (r.) Serghei Bogdanov*: aceștia se concentrează pe acțiunile în mediul informațional (războiul informațional), unde domină mijloacele nonmilitare și indirecte. Cei doi argumentează relevanța abordării indirecte în actualul context ca instrument al celor mai buni strategi. Ei conceptualizează abordarea indirectă drept o acțiune menită să lovească adversarul în punctele sale slabe, folosind surpriza strategică, manevra rapidă și exploatarea oportunităților de atac. Aceștia consideră că, în timp ce decepția militară este un element comun folosit în conflicte, influențarea prin informații a atins un nivel ce le-ar permite până și lor să execute sarcini strategice (Ib., pp. 38-39);
- *generalul-maior Ivan Vorobev*: din perspectiva acestuia, dincolo de atacurile cinetice și spațiul de manevră, contează și capacitatea proprie de a stopa accesul adversarului la informații corecte. Astfel, Vorobev separă conceptul atacului informațional sau al șocului informațional în trei direcții: a) atacuri informațional-psihologice care urmăresc dezinformarea și înșelarea adversarului; b) atacuri psihotronice care au funcția de a afecta psihicul adversarului prin mijloace speciale[2]; și c) atacuri asupra calculatoarelor adversarului pentru a afecta sistemele C2. Având în minte această separație, generalul accentuează importanța executării acestor atacuri în mod sincronizat și coordonat (Ib., pp. 23-24);
- *colonelul Iuri Starodubțev și locotenent-coloneii Vladimir Buharin și Serghei Semenov*: aceștia, în contextul războiului informațional, identifică două direcții de acțiune: a) influențarea civililor

Colonelul (r.) Serghei Cekinov și generalul-locotenent (r.) Serghei Bogdanov conceptualizează abordarea indirectă drept o acțiune menită să lovească adversarul în punctele sale slabe, folosind surpriza strategică, manevra rapidă și exploatarea oportunităților de atac.

[2] Cu toate că încă nu avem concluziile unei cercetări referitoare la *„Sindromul Havana”*, descrierea generalului-maior Ivan Vorobev evidențiază unele similitudini cu acest caz.

sau a personalului militar al unei alte țări prin diseminarea unor anumite informații (probabil, se referă la distorsiunea informațională) care să țintească grupuri sau factori de decizie; și b) obținerea superiorității informaționale față de adversar prin dezafectarea sistemelor informaționale de procesare și culegere a informațiilor (probabil, referindu-se la partea de război electronic) (Ib., p. 40);

- *generalul Mahmut Ahmetovici Gareev*: acesta considera că amenințările către Federația Rusă au legătură cu operațiunile informaționale și subversive care acționează din interiorul statului. Astfel, principalul efort al Federației Ruse ar trebui să se concentreze pe distrugerea mediului informațional, a surselor de informații și a sistemelor de navigare, ghidare și C3 adverse. Pentru a îndeplini acest deziderat, forțele ruse se pot folosi de acțiuni indirecte, pentru a influența adversarul, care activează în sfera politică, economică și psihologică prin intermediul dezinformării. Tot aici, generalul include acțiunile indirecte în sfera mijloacelor nonmilitare, coroborându-le cu distorsiunea informațională, stratagemele, intelligence-ul și contrainformațiile (Thomas, 2016, p. 15);
- *generalul-colonel Andrei V. Kartapalov*: acesta adaugă forțelor armate clasice (terestre, aeriene și navale) o a patra, care ține de spațiul informațional. Pornind de la perspectivele teoretice americane, generalul acordă o atenție sporită operațiunilor asimetrice executate de un adversar mai slab care, confruntându-se cu problema resurselor limitate, acționează prin mijloace economice, diplomatice, informaționale (incluzând și *„lovituri informaționale”*) și indirecte (de natură militară). De asemenea, din perspectiva sa, în arsenalul abordărilor combative ale Federației Ruse pot fi incluse și măsurile asimetrice, care cuprind utilizarea forțelor speciale, a agenților străini, a formelor diverse ale armelor informaționale și a altor forme nonmilitare. Cu ocazia fiecărui conflict, va fi generată câte o operațiune asimetrică (probabil, în acord cu specificul conflictului) (Ib., pp. 19-20);
- *generalul-maior (r.) I. N. Vorobiov și colonelul (r.) V. A. Kiselev*: cei doi consideră că strategia abordării indirecte câștigă teren în defavoarea strategiilor ce utilizează forța, prima fiind

Generalul-colonel Andrei V. Kartapalov acordă o atenție sporită operațiunilor asimetrice executate de un adversar mai slab care, confruntându-se cu problema resurselor limitate, acționează prin mijloace economice, diplomatice, informaționale și indirecte.

caracterizată de o diversitate a formelor și metodelor specifice acțiunii militare – incluzând războiul informațional, lovituri electronice, operațiuni anti-satelit etc. O atenție deosebită o acordă armelor informațional-psihologice, pe care le cataloghează ca fiind arme speciale și care acționează asupra psihicului uman cu scopul de a-l influența (Ib., pp. 30-31);

- *Andrew Koribko*: acesta încearcă să dezvolte o teorie complexă și pretențioasă plecând de la accepțiunea că războiul hibrid are o bază teoretică de factură occidentală și îl definește ca *„abordare adaptivă indirectă”* menită să determine schimbări de regim. Teza lui gravitează în jurul practicilor războiului neconvențional și al *„fabricării revoluțiilor colorate”*. Tot aici, el arată cum succesul unei *„revoluții colorate”* implică recrutarea indivizilor folosind tehnici ideologice, psihologice și informaționale și cum acest proces depinde de specificul țării, caracteristicile conducătorilor și puterea (capacitatea) guvernului și a instituțiilor de securitate din subordine (Koribko, 2015, pp. 29-30). Astfel, *„revoluțiile colorate”* sunt rezultatul unor campanii informaționale care țintesc populația unui stat, iar *„acestea trebuie să fie persuasive pentru a ajunge la un public cât mai numeros* (în anumite cazuri, poate fi mai strategic să vizeze doar anumite părți ale populați*ei pentru a le determina să se ‹răscoale›* și să exacerbeze fracturile etnice preexistente din inter*iorul societății, spre exemplu)”.* (Ib., p. 29).

Andrew Koribko arată cum succesul unei „revoluții colorate” implică recrutarea indivizilor folosind tehnici ideologice, psihologice și informaționale și cum acest proces depinde de specificul țării, caracteristicile conducătorilor și puterea (capacitatea) guvernului și a instituțiilor de securitate din subordine. „Revoluțiile colorate” sunt rezultatul unor campanii informaționale care țintesc populația unui stat, iar „acestea trebuie să fie persuasive pentru a ajunge la un public cât mai numeros”.

Perspectivele și abordările pot continua, mai ales că sunt unii teoreticieni militari care atribuie o semnificație aparte, în acest context, componentei SIGINT sau cibernetice/sistemelor informatice; care pun accent pe perioada inițială a unui conflict[3], pe capacitatea de prognoză a viitoarelor tendințe sau pe formele și mijloacele ce trebuie utilizate în desfășurarea unei operațiuni; ori care conferă mai multă valoare armamentelor high-tech, pregătirii continue a trupelor sau a deținerii de arme de distrugere în masă (nucleare, chimice, biologice

[3] Un teoretician militar rus care are o semnificativă influență asupra gândirii și artei militare ruse, mai ales în privința luptelor de profunzime, este Alexander A. Svechin (1878-1938), care considera că, înaintea declanșării ostilităților, prioritare sunt înțelegerea fundalului istoric, stabilirea unor obiective realiste și pregătirea intensă a trupelor. Tot acesta susținea că fiecare război reprezintă un caz special (sau unic) ce necesită dezvoltarea unui comportament strategic specific, care să se plieze pe logica particulară a acelui conflict, evitându-se aplicarea modelelor stereotipice (Sinclair, 2020, pp. 13-14).

sau radiologice). Toate sunt relevante și conferă indicii referitoare la modul real de operare al Federației Ruse, în ansamblu însă, trebuie să menționăm că, pentru o înțelegere cât mai corectă, fiecare abordare teoretică rusă ar merita o cercetare în sine.

Totuși, nu putem să nu remarcăm că, în anumite puncte, putem identifica asemănări cu abordările conceptuale occidentale, mai ales în privința utilizării eficiente a informației, atât în cadrul sistemelor proprii, cât și ca armă împotriva adversarilor. Remarcăm că, în cazul conceptelor referitoare la conflict, avem de-a face cu un ansamblu teoretic format din reutilizarea și actualizarea unor concepte sovietice și rezultatele cercetărilor occidentale în domeniul teoriei militare (Kabernik, p. 54) și al intelligence-ului.

Ceea ce este interesant este faptul că sunt reliefate anumite concepte cheie care ne atrag atenția, mai precis *strategie/abordare indirectă*, *război/atac/șoc informațional*, *mijloace nonmilitare*, *operațiuni/măsuri asimetrice*, și care ar merita o detaliere a semnificației acestora.

În cazul *strategiei/abordării indirecte,* putem spune că aceasta reprezintă o adaptare a teoriei strategiei abordării indirecte a lui B.H. Liddell Hart (1895-1970). Teoria lui Hart abordează nevoia de schimbare a formei de desfășurare a conflictelor, mai precis de la luptele directe dintre forțele opozante la *„strategia abordării indirecte, care caută să disloce echilibrul inamicului cu scopul de a determina o decizie”* și de a-l ademeni sau surprinde într-o ipostază prin care *„propriul său efort [al adversarului] este transformat în pârghia răsturnării sale”* (Hart, 1929, 2008, pp. 19, 123). Strategia abordării indirecte a lui Hart încurajează exploatarea liniilor de rezistență minimă; limitarea utilizării de forțe armate, unde elementul esențial constă în gradul ridicat de mobilitate care este dublat de capacitatea de răspuns rapid (Ib., p. 138); iar la nivel tactic sau strategic, strategia abordării indirecte urmărește deținerea *„...un[ui] plan care se poate potrivi cu ușurință circumstanțelor întâlnite; de a păstra o asemenea adaptabilitate în timp ce își menține inițiativa...”.* (Ib., p. 133). De asemenea, într-o confruntare, Hart considera că *„...dislocarea echilibrului fizic și psihologic al adversarului a fost preludiul vital pentru o încercare reușită de a-l răsturna”.* (Ib., p. 15). În acest sens, strategia ar trebui concepută în așa fel încât să diminueze capacitatea de rezistență a adversarului prin exploatarea surprizei (strategice) și a capacității

Teoria lui Hart abordează nevoia de schimbare a formei de desfășurare a conflictelor, mai precis de la luptele directe dintre forțele opozante la „strategia abordării indirecte, care caută să disloce echilibrul inamicului cu scopul de a determina o decizie” și de a-l ademeni sau surprinde într-o ipostază prin care „propriul său efort [al adversarului] este transformat în pârghia răsturnării sale”.

de manevră, iar în situația unui conflict cu mai mulți adversari, ar fi avantajos concentrarea eforturilor, mai întâi, asupra aliaților slabi ai adversarului decât să încerce un efort singular, constant și obositor de a-l doborî pe adversarul cel mai puternic în speranța că ceilalți din jurul său vor renunța la luptă (Ib., pp. 128, 123).

Chiar dacă Hart era occidental, nu putem spune că este o coincidență prezența unor idei ale sale în teoria militară rusă, mai ales că, așa cum scria un autor în 1986, arta militară sovietică avea la bază principiile a) vitezei și șocului (utilizarea mobilității și a spațiului de manevră), b) concertării efortului (utilizarea superiorității în locul și momentul potrivit), c) surprizei și securizării, d) menținerii inițiativei, e) conservării eficienței în luptă, f) conformității cu scopul/obiectivul, g) coordonării dintre forțe (Hamilton, 1986, p. 63).

În episodul invadării Crimeii, folosindu-se de surpriza strategică, forțele ruse au acționat cu mare rapiditate și flexibilitate, mai întâi prin transportarea unor unități speciale de dimensiuni reduse în peninsulă, în contextul în care acestea făceau parte dintr-un exercițiu desfășurat la granița estică a Ucrainei, care inspecta capacitatea de intervenție rapidă. Odată ajunse pe teritoriul advers, unele unități chiar au simulat că ar fi parte a miliției locale, inducând în eroare populația autohtonă și ocupând Parlamentul Crimeii.

Deși aspectele prezentate sunt doar o porțiune din viziunea lui Liddell Hart, putem remarca totuși similitudinile între teoria strategiei abordării indirecte și strategia/abordarea indirectă de care vorbesc teoreticienii militari ruși. Spre exemplu, în contextul exploatării punctelor de rezistență minimă, a surprizei strategice, a dislocării echilibrului adversarului și a maximizării capacității de manevră, episodul invadării Crimeii în 2014 evidențiază aceste asemănări. Folosindu-se de surpriza strategică, forțele ruse au acționat cu mare rapiditate și flexibilitate, mai întâi prin transportarea unor unități speciale de dimensiuni reduse în peninsulă, în contextul în care acestea făceau parte dintr-un exercițiu desfășurat la granița estică a Ucrainei, care inspecta capacitatea de intervenție rapidă. Odată ajunse pe teritoriul advers, unele unități chiar au simulat că ar fi parte a miliției locale, inducând în eroare populația autohtonă și ocupând Parlamentul Crimeii (Kofman et al., 2017, pp. 12-13). Această surpriză, practic, a determinat efecte atât fizice, cât și psihologice, prin care i-a conferit Federației Ruse avantaj la nivel tactic, operațional și strategic, în timp ce căile de reacție a Ucrainei au fost treptat anulate. Alt exemplu care are legătură cu limitarea utilizării forțelor armate constă în intervenția militară rusească în Siria, în 2015. În acest caz, Federația Rusă a operat (Sinclair, 2020, pp. 15-17): pe cale politică, prin influențarea guvernului sirian de a refuza accesul ONG-urilor finanțate de Occident în teritoriul aflat sub controlul forțelor guvernamentale; pe cale diplomatică, prin blocarea unei rezoluții ONU care să favorizeze SUA și lărgirea parteneriatelor cu statele din regiune precum Turcia, Arabia Saudită, Irak și Israel; și pe cale militară,

prin asigurarea de suport aerian, securizare, furnizarea de armament, pregătire de specialitate și coordonare. În această privință, trupele din teatru erau limitate și erau compuse din forțe navale, aeriene, speciale și contractori independenți, însă cu precizarea că înfruntările terestre directe erau evitate pe cât posibil, iar pentru a compensa economia forțelor proprii, rușii s-au axat pe un sistem terestru comun, robust, de comandă și control (Ib.).

Având în vedere aceste exemple (fără a mai menționa și exemplele pe care le putem extrage din recentele exerciții militare ruse), remarcăm că strategia/abordarea indirectă rusă reprezintă un hibrid conceptual compus din cultura strategică rusă/sovietică și teoria militară occidentală pe care teoreticienii militari ruși continuă să o dezvolte și să o îmbunătățească în acord cu noile evoluții tehnologice.

În privința *războiului/atacului/șocului informațional,* remarcăm că, deși există terminologii diferite în abordările conceptuale ruse și occidentale, intenția va fi asemănătoare: în dimensiunea informațională, scopul rezidă în distrugerea, coruperea, uzurparea informațiilor și/sau a mediului informațional advers; iar în dimensiunea cognitivă, este urmărită afectarea rețelelor umane și a sistemelor care pot influența factorii de decizie, manipularea conținuturilor și a structurii informațiilor și influențarea sistemelor care pot afecta procesul de decizie (FM 3-13, 2016, pp. 1-4). Pe scurt, este vorba despre obținerea superiorității informaționale față de adversar în timp ce propriile sisteme sunt protejate.

Strategia/ abordarea indirectă rusă reprezintă un hibrid conceptual compus din cultura strategică rusă/ sovietică și teoria militară occidentală pe care teoreticienii militari ruși continuă să o dezvolte și să o îmbunătățească în acord cu noile evoluții tehnologice.

Din acest punct, asemănările între modelele de gândire occidentală și rusă se estompează ca urmare a unor diferențe ce țin de terminologie, structură și rol. În gândirea militară occidentală (dicționare, documente strategice, manuale etc. NATO), întâlnim utilizarea termenului de *operațiuni informaționale* pentru a descrie capabilitățile și desfășurarea activităților care afectează mediul informațional, iar termenul de *război informațional* este utilizat atunci când se fac referiri la tacticile, activitățile și capabilitățile adverse (Giles, Seaboyer, 2019, pp. 6-7). În contrast, gândirea militară rusă atribuie conceptului *război informațional* o aplicabilitate mult mai largă și dinamică, acesta folosind informația ca instrument, domeniu al operațiunilor sau fiind ținta/obiectul care trebuie afectat. Conform abordării teoretice ruse, războiul informațional este un concept-umbrelă, căruia i se subsumează operațiunile cibernetice, operațiunile psihologice, comunicarea strategică,

operațiunile de influențare, războiul electronic, distorsiunea informațională (dezinformarea, falsificarea informațională, propaganda etc.), activitățile de intelligence (HUMINT, SIGINT, IMINT, GEOINT, OSINT etc.), contrainformațiile, maskirovka (echivalentul occidental fiind decepția militară – MILDEC) și alterarea/distrugerea echipamentelor (Ib., p. 6). De asemenea, organizarea și desfășurarea războiului informațional revine comunității de intelligence ruse (GRU, FSB, SVR etc.) și forțelor de securitate (structuri specializate pe securitatea și ordinea internă), unde activitățile de analiză, culegere și diseminare de informații sunt combinate cu acțiuni directe precum subversiunea, sabotajul și asasinatul, toată această activitate având ca țintă civilii, militarii și factorii de decizie (Ib., p. 7). Pentru a putea identifica și exploata vulnerabilitățile mediilor informaționale ale statelor, Federația Rusă și-a format *„trupe informaționale”,* care sunt compuse, alături de ofițerii de informații și militari, din hackeri, specialiști în comunicare strategică și în operațiuni psihologice, jurnaliști și lingviști (Giles, 2016, pp. 35-36), care să înțeleagă particularitățile lingvistice și culturale ale statelor vizate de războiul informațional. Tot aici, mai trebuie spus că, în funcție de obiective și ținte, războiul informațional rus se divide în (Ib., p. 9): a) război psihologic-informațional, a cărui țintă sunt forțele armate și populațiile adverse; și b) război tehnologic-informațional, a cărui țintă sunt sistemele tehnice de colectare, procesare și transmitere a datelor și informațiilor. De precizat că ambele tipologii includ și folosirea activităților cibernetice, deoarece, în viziunea lor, războiul cibernetic se referă la transmiterea și transferul de informații prin orice mijloace, în acest sens rușii atribuind sensuri similare acțiunii de parazitare/infectare a unui calculator și acțiunii de a distorsiona realitatea prin intermediul media clasice sau a social media (Ib., p. 10).

Abordarea teoretică (și practică) rusească este una defensiv-ofensivă, unde, pe plan intern, este asigurat un control strict ale fluxurilor informaționale ce provin din afara Federației Ruse. În acest scop, Federația Rusă are capacitatea de a se decupla, informațional, de restul lumii și poate influența fragmentele informaționale ce se strecoară din exterior, astfel încât populația rusă să nu aibă o percepție cât mai obiectivă asupra evenimentelor, de pe plan intern și extern și, astfel, să fie vulnerabilă propagandei propriului stat.

După cum putem observa, caracterul războiului informațional rus este unul ofensiv, însă acesta este dublat și de unul defensiv în ceea ce privește mediul informațional intern. Practic, abordarea teoretică (și practică) rusească este una defensiv-ofensivă, unde, pe plan intern, este asigurat un control strict ale fluxurilor informaționale ce provin din afara Federației Ruse. În acest scop, Federația Rusă are capacitatea de a se decupla, informațional, de restul lumii și poate influența fragmentele informaționale ce se strecoară din exterior, astfel încât populația rusă să nu aibă o percepție cât mai obiectivă asupra evenimentelor de pe plan intern și extern și, astfel, să fie vulnerabilă propagandei propriului stat (Ib., pp. 29-30).

Această abordare defensiv-ofensivă poate fi interpretată ca un sistem de securitate informațional, unde emoțiile și atenția cetățenilor ruși sunt canalizate către adversarii externi desemnați de Federația Rusă în încercarea de a preveni izbucnirea revoltelor față de abuzurile autorităților, moralul trupelor este ținut la cote ridicate, iar sistemele C4I rămân protejate. În același timp, pe plan extern, sunt exploatate, prin războiul informațional, percepțiile, atitudinile și emoțiile populațiilor din alte state în încercarea de a genera destabilizare sau de a schimba guverne ori regimuri; sunt influențați factorii de decizie; sunt determinate personalități cheie ale statelor să defecteze prin șantaj, amenințare sau mită; și sunt urmărite penetrarea, coruperea sau dezafectarea sistemelor militare și guvernamentale ale statelor vizate.

Mijloacele nonmilitare și *operațiunile/măsurile asimetrice* le putem aborda în comun, deoarece, deși sunt discutate ca termeni separați de teoreticienii militari ruși, în practică, remarcăm faptul că sunt niște concepte care se completează.

În acest sens, teoreticienii militari ruși pornesc de la teoria războiului de generație a șasea[4], unde obiectivele principale constau în: 1) înfrângerea forțelor armate ale adversarului pe propriul teritoriu, 2) distrugerea activității și potențialului economic al adversarului și 3) schimbarea sau subversiunea sistemului politic al adversarului (Mattsson, 2015, p. 62). În îndeplinirea acestor obiective este evidentă o abordare indirectă, de la distanță, care să se materializeze prin măsuri nonmilitare și asimetrice. În susținerea acestei idei, aceștia consideră că primul pas constă în luarea inițiativei în lansarea unui război psihologic, război informațional și recrutarea sau introducerea unor agenți de influență (componenta nonmilitară) care să destabilizeze statul victimă din interior și să creeze condiții optime. Ulterior, prin lansarea unui atac coordonat, sunt desfășurate operațiuni asimetrice, folosind forțele speciale, arme dirijate de la distanță, voluntari și miliții care să pătrundă adânc în teritoriul advers (Ib., pp. 62-63).

Teoreticienii militari ruși pornesc de la teoria războiului de generație a șasea, unde obiectivele principale constau în: înfrângerea forțelor armate ale adversarului pe propriul teritoriu, distrugerea activității și potențialului economic al adversarului și schimbarea sau subversiunea sistemului politic al adversarului.

[4] Războiul de generație a șasea reprezintă o abordare teoretică de sorginte rusească asupra fenomenului și tendințelor războiului, iar acesta, în mod particular, se referă la caracterul tot mai informațional al conflictelor, rolul tot mai semnificativ al sistemelor de arme de înaltă precizie, compactarea efectivelor și maximizarea mobilității acestora etc., dar include și aspecte abstracte, precum *„război fără contact”*, *„război cultural”* sau *„război existențial”*. Pentru un punct de vedere, vezi https://jamestown.org/program/russian-sixth-generation-warfare-and-recent-developments/, accesat la 12 februarie 2022.

Totuși, există situații în care utilizarea oricăror forțe armate, sub orice formă, poate determina riscuri mai mari decât beneficiile, astfel încât sunt accentuate mijloacele nonmilitare ca parte a operațiunilor asimetrice, fiind exprimate prin:

- acțiuni de discreditare și delegitimarea instituțiilor cheie și a factorilor de decizie prin fluxuri informaționale constante care subliniază limitările și inabilitățile autorităților în gestionarea problemelor și a guvernării;
- acțiuni de inducere a stării de haos în rândul populației, care să determine senzația de degradare rapidă a ordinii și stabilității și apariția unei tendințe antisistem în rândul populației;
- acțiuni de decepție/inducere în eroare, care urmăresc distragerea atenției adversarului sau determinarea sa de a acționa sau nu într-un anumit moment;
- acțiuni de supraveghere și evaluare, care urmăresc, de la distanță, capacitățile adversarului, modul și timpul de reacție și posibilele vulnerabilități. (Duțu, 2013, p. 36)

Perspectiva accentuării mijloacelor nonmilitare desfășurate sub umbrela acțiunilor asimetrice urmărește îndeplinirea unor obiective strategice, substituind utilizarea clasică de forțe armate, iar prin acest fapt, adversarul – nefiind supus unei amenințări militare – nu poate oferi un răspuns simetric.

În acest sens, remarcăm că această perspectivă a accentuării mijloacelor nonmilitare desfășurate sub umbrela acțiunilor asimetrice urmărește îndeplinirea unor obiective strategice, substituind utilizarea clasică de forțe armate, iar prin acest fapt, adversarul – nefiind supus unei amenințări militare – nu poate oferi un răspuns simetric (Renz et al., 2016, p. 54). Mai trebuie spus că ne confruntăm cu un paradox în contextul mijloacelor nonmilitare și al operațiunilor/măsurilor asimetrice ruse, deoarece, oricât de mult ar tinde să excludă componenta militară, toate aceste acțiuni sunt organizate și desfășurate sub egida structurilor militare ruse, iar arsenalul *„armelor dirijate de la distanță”* poate fi compus din organizații, grupuri ori indivizi care primesc finanțare și instrucțiuni din partea Federației Ruse, acționând împotriva intereselor de securitate ale statului în care operează (Ib., pp. 56, 57).

Pe de altă parte, în cadrul teoriei militare ruse referitoare la războiul de generație a șasea, remarcăm că este acordată o atenție semnificativă utilizării mijloacelor nonmilitare. Conform abordării militare ruse, aceste mijloace ar avea rolul de a slăbi și corupe adversarul înaintea desfășurării atacului, ca parte a perioadei inițiale a conflictului/războiului, unde desfășurarea lor este acoperită și urmărește subminarea sau diminuarea capacității statului vizat

de a mai rezista (Göransson, 2021, pp. 86, 88). Însă, această idee își are originea în principalele obsesii de securitate ale Federației Ruse, una dintre cele mai semnificative fiind schimbarea de regim prin *„revoluții colorate”*. În acest sens, autoritățile ruse au acuzat, în repetate rânduri, Statele Unite și NATO de faptul că ele desfășoară activități subversive de susținere a *„revoluțiilor colorate”* în Orientul Mijlociu și Europa de Est. În acest registru, rușii au clasificat acțiunile occidentale drept *„operațiuni multidimensionale hibride”*, compuse din măsuri politice, diplomatice, informaționale, propagandistice, financiare, economice și militare care acționează prin intermediul partidelor politice, al ONG-urilor, migrației și companiilor militare private (deși nu este explicat rolul lor ca parte a măsurilor nonmilitare) (Ib., p. 89). Trebuie să avem în vedere că, empiric, ceea ce a clasificat Federația Rusă drept riscuri la adresa securității sale au reprezentat indicii referitoare la acțiunile pe care le-a executat împotriva altor state, fățiș sau acoperit, probabil având ca repere propriile acțiuni desfășurate împotriva altor state. De asemenea, există o ambiguitate și o confuzie conceptuală, intenționată sau nu, referitoare la mijloacele nonmilitare și operațiunile/măsurile asimetrice care, într-o anumită măsură, induc în eroare mediile academice și analiștii, generând interpretări și perspective diferite, fără a se putea clarifica adevăratele forme și metode ale acțiunii ruse. Un astfel de exemplu îl regăsim în interpretarea pe care au oferit-o diverși specialiști occidentali (Mark Galeotti, Roger McDermott, Pavel Felgenhauer etc.) referitor la existența unei *„Doctrine Gherasimov”* sau a subestimării intențiilor Federației Ruse de a-și putea proiecta puterea pe arena internațională. În fapt, intențiile generalului Valeri Gherasimov nu urmăresc aprofundarea mijloacelor nonmilitare, asimetrice, informaționale etc. de către armată în detrimentul celorlalte arme/specialități, ci atrag atenția că *„...Rusia are nevoie să își creeze capabilitatea materială și doctrinală a unei forțe de intervenție de înalt profesionalism, ce are potențialul de a acționa la nivel mondial, sub protecția unei umbrele nucleare foarte eficiente și modernizate”* (Fridman, 2019, p. 109), pentru a-și proteja interesele pe plan extern.

Intențiile generalului Valeri Gherasimov nu urmăresc aprofundarea mijloacelor nonmilitare, asimetrice, informaționale etc. de către armată în detrimentul celorlalte arme/specialități, ci atrag atenția că „...Rusia are nevoie să își creeze capabilitatea materială și doctrinală a unei forțe de intervenție de înalt profesionalism, ce are potențialul de a acționa la nivel mondial, sub protecția unei umbrele nucleare foarte eficiente și modernizate”, pentru a-și proteja interesele pe plan extern.

În urma acestei sinteze, remarcăm, într-adevăr, o diversitate conceptuală care se tot extinde și care, în unele situații, reprezintă adaptări ale conceptelor militare occidentale, iar în altele, constă în preluări și îmbunătățiri ale conceptelor sovietice. În acest sens, din cele prezentate, reiese că tendința forțelor armate ruse este de a pune

accent pe interoperabilitate, mobilitate, tehnologizare, flexibilitate și utilizarea economică a forței, direct proporțional cu caracteristicile teatrului de operații. Pe de altă parte, forțelor militare ruse li se adaugă componentele informațională și nonmilitară, care pot fi desfășurate în comun cu acțiunea militară sau independente (folosind tehnici militare cu mijloace civile), având scopul de a destabiliza un stat din interior.

Cu toate acestea, sunt necesare prudența și rezervarea în interpretarea teoriei și gândirii militare ruse, deoarece: a) documentele strategice disponibile sunt abstracte și accesul la documentele clasificate revine unei mici porțiuni de specialiști; b) diferențele lingvistice și de cultură strategică reprezintă o barieră în înțelegerea modului lor de acțiune; iar c) unele abordări ruse pot fi contaminate de biasuri și teorii ale conspirației rezultate din reminiscențele moștenirii ideologice marxist-leniniste și din erorile dezvoltate de cercurile restrânse ale comuniștilor sovietici din cadrul structurilor de securitate (Andrew, Mitrokhin, 1999, 2000, 2018).

Conform unui raport special declasificat de CIA în 2006, măsurile active se referau la operațiuni întreprinse de sovietici cu scopul de a afecta politica domestică a statelor vizate, fiind distincte de acțiunile de spionaj, și urmăreau să afecteze relațiile dintre state, discreditarea oponenților Uniunii Sovietice și subminarea liderilor, instituțiilor și valorilor externe.

MĂSURILE ACTIVE, MASKIROVKA ȘI CONTROLUL REFLEXIV

Când introducem în discuție *abordarea indirectă, război informațional, mijloace nonmilitare* sau *operațiuni asimetrice*, trebuie să avem în vedere că, în cadrul liniilor de operațiuni sau în mod auxiliar, sunt desfășurate *măsuri active*, *maskirovka* și/sau *controlul reflexiv*. Includerea acestor termeni în spectrul acțiunilor militare ruse, fățișe sau acoperite, este obligatorie, datorită rolului, tradiției și evoluției lor în cultura strategică sovietică/rusească.

Începând cu *măsurile active*, din punct de vedere istoric, acestea erau gândite de Serviciul A, care reprezenta ramura pregătită în măsuri active ale direcției KGB specializată în informații externe, iar execuția era atribuită ofițerilor Liniei PR (departamentul de informații politice din cadrul rezidenței KGB), care lucrau din rezidențele legale (parte a misiunilor diplomatice) și ilegale aflate pe teritoriile statelor vizate și care trebuiau să confere măsurilor active, în mod teoretic, 25% din totalul activităților întreprinse (Ib., p. 292). Conform unui raport special declasificat de CIA în 2006, *măsurile active* se referau la operațiuni întreprinse de sovietici cu scopul de a afecta politica domestică a statelor vizate, fiind distincte de acțiunile de spionaj, și urmăreau să afecteze relațiile dintre state, discreditarea oponenților Uniunii Sovietice și subminarea liderilor, instituțiilor și valorilor externe

(Bureau of Public Affairs, 1981, p. 1). *Măsurile active* erau desfășurate în mod subversiv/sub acoperire și foloseau tehnici precum:

- manipularea agențiilor de presă scrisă din țările vizate prin inserarea, de către agenții sovietici, de falsuri informaționale;
- utilizarea falsurilor și a dezinformării prin producerea și diseminarea de documente false sau parțial adevărate (propagandă neagră și gri) și prin răspândirea zvonurilor, insinuărilor și a distorsionării faptelor/evenimentelor;
- controlarea organizațiilor comuniste locale și internaționale;
- radiodifuzarea de informații prin stații clandestine;
- utilizarea manipulării economice prin influențarea prețurilor (acolo unde se putea) și diseminarea de informații reale și false către oamenii de afaceri locali și decidenții politici în încercarea de a le dirija planurile de investiții în funcție de interesele Uniunii Sovietice;
- desfășurarea de operațiuni de influențare politică prin exploatarea contactelor din mediul politic, mediul economic și media statelor vizate. O atenție deosebită le era oferită oamenilor politici, în cazul cărora acest tip de operațiuni încerca să îi fidelizeze și să îi folosească pe canalele private cu oficialii guvernamentali străini;
- odată influențați, Uniunea Sovietică le inducea, în mod fals, impresia unei relevanțe deosebite prin invitarea acestora de a se întâlni cu oficiali sovietici de rang înalt. În realitate, prin intermediul oamenilor politici locali fidelizați, Uniunea Sovietică transmitea amestecuri de informații false, reale și distorsionate, care favorizau agenda sovietică;
- utilizarea academicienilor și a jurnaliștilor, unde primii ajungeau să se supună ordinelor sovietice, iar ultimii ajungeau să reprezinte indirect Uniunea Sovietică și să disemineze propagandă comunistă (Ib., pp. 2-3).

Măsurile active erau desfășurate în mod subversiv/ sub acoperire și foloseau tehnici precum: manipularea agențiilor de presă scrisă din țările vizate prin inserarea, de către agenții sovietici, de falsuri informaționale; controlarea organizațiilor comuniste locale și internaționale; sau radiodifuzarea de informații prin stații clandestine.

În această lumină, *măsurile active* reprezentau acțiuni pe care, în prezent, le-am include în sfera operațiunilor psihologice, a operațiunilor informaționale și a celor HUMINT. Totuși, în cadrul teoriei militare sovietice/ruse, *măsurile active* – denumite și *operațiuni active* – au forme multiple. În general, acestea vizează utilizarea influenței utile asupra aspectelor ce țin de politica internă și externă a statului vizat; implementarea unor soluții în chestiuni internaționale; inducerea

în eroare, subminarea și slăbirea adversarului; perturbarea activității ostile a adversarului; și îndeplinirea altor scopuri (Mitrokhin, 2002, 2004, p. 13). Atunci când sunt desfășurate de serviciile de informații externe, în mod particular, *măsurile active* își extind sfera de activitate și către aspectele militare, economice și ideologice ale adversarului. Ca metode utilizate, putem menționa dezinformarea, expunerea, discreditarea, compromiterea, persuasiunea sau coerciția – exercitarea de presiuni psihologice asupra indivizilor pentru a-i convinge sau pentru a-i determina să se comporte într-un anumit fel –, acțiunea/presiunea pozitivă specială – exercitarea influenței asupra guvernelor, partidelor sau a personalităților politice și publice folosind forme și materiale diverse prin intermediul agenților și contactelor racolate/cultivate –, acțiunile clandestine etc. (Ib., pp. 13, 67-68). Tot aici mai precizăm că *măsurile active* joacă un rol și în contextul acțiunilor de contrainformații, fiind diferite de măsurile de protecție, unde scopul este de a penetra logica adversarului, a preveni apariția oportunităților pentru adversar, a spori ambiguitatea, a expune și întrerupe activitățile ostile încă din etapele incipiente, a bloca posibilitățile de inițiativă ale adversarului, a-l frustra și a-l face să acționeze în condiții nefavorabile (Ib., p. 251).

Măsurile active joacă un rol și în contextul acțiunilor de contrainformații, fiind diferite de măsurile de protecție, unde scopul este de a penetra logica adversarului, a preveni apariția oportunităților pentru adversar, a spori ambiguitatea, a expune și întrerupe activitățile ostile încă din etapele incipiente, a bloca posibilitățile de inițiativă ale adversarului, a-l frustra și a-l face să acționeze în condiții nefavorabile.

Din experiența ultimilor ani, vedem că există puține diferențe între *măsurile active* din trecut și cele din prezent. Însă, diferențele notabile ar consta în valorificarea experienței prin profesionalizarea *măsurilor active*, utilizarea tehnologiei și valorificarea mediului permisiv al statelor occidentale generat de inadaptarea sistemelor de protecție proprii la *măsurile active* actuale. În acest sens, rezumându-ne la elementul tehnologic, vom face câteva referiri.

Astfel, generalizarea mediului virtual și utilizarea pe scară largă a platformelor digitale care generează conținut, distribuie informații și constituie foruri de discuții, toate acestea au determinat apariția unui mediu informațional alternativ/paralel la cel clasic. Dincolo de avantajele evidente ale interconectării informatice și informaționale, s-au generat și dezavantaje acute, precum: diseminarea, între utilizatori, de conținuturi și informații fundamentate pe emoții, enclavizarea digitală a utilizatorilor pe baza reprezentărilor și a credințelor comune, promovarea ignoranței față de fenomenele științifice, accentuarea poveștii în detrimentul evenimentelor reale, proslăvirea unor modele de viață utopice, dramatizarea și alterarea realității obiective etc.

(Wardle, Derakhshan, 2017, pp. 12, 13, 15). Aceste tendințe constituie un mediu propice pentru *măsurile active* (inclusiv pentru racolarea/cultivarea de agenți), spațiul virtual reprezentând atât canalul, cât și locul de întâlnire. Datorită acestei subiectivizări, oamenii preferă să se constituie în grupuri virtuale, denumite *camere de ecou*, prin care aceștia își pot exprima credințele și ideile comune, fără a mai exista fenomenul dezbaterii, și unde își pot exprima neîngrădit, radical și necenzurat viziunile despre viață și lume (Ib., pp. 49-50).

Odată cu subiectivizarea percepției realității a individului, rolul componentei psihologice s-a accentuat, ca parte a *măsurilor active*, ceea ce a dus la o eficientizare în identificarea și valorificarea indivizilor. Deși nu putem indica în mod exact etapele folosite de ruși, putem spune că, înainte de lansarea *măsurilor active*, instituțiile organizatoare execută ample cercetări referitoare la statul vizat, care stabilesc particularitățile civilizaționale determinate de geografie, evoluție istorică și compoziție, origini etnice, religie, statutul economic și structura societății (Gordon, 1996, p. 205). Însă, trebuie menționat că, la nivel deductiv, pre-analiza nu este executată înaintea stabilirii planului de acțiune, a obiectivelor și a scopurilor care vor fundamenta desfășurarea operațiunilor active *(măsurilor active)*. Apoi, sunt culese informații care sunt supuse analizelor, având în atenție atitudinile latente ale anumitor grupuri sau ale populației asupra subiectelor ce țin de domeniile politic, economic, militar și social, iar ulterior este realizată o altă analiză, ce încearcă să identifice vulnerabilitățile posibile, având în vizor o țintă specifică, întrucât analiza stabilește nivelul disensiunilor, al fricilor și al nemulțumirilor ce vor fi exploatate (Ib.). În funcție de informațiile obținute, este luată o decizie referitoare la metodele și tehnicile ce vor fi folosite, mijloacele de comunicare favorabile, conținuturile și mesajele diseminate, spațiile în care se desfășoară măsurile active (virtual și/sau real), personalul implicat (propriu, clandestin sau/și recrutat din statul vizat) etc., urmând ca toată activitatea să fie monitorizată, evaluată și ajustată (Ib., p. 206). Chiar și cu un volum impresionant de cunoaștere despre adversar, succesul operațiunilor active nu este garantat, din cauza activităților protecționiste ale structurilor de securitate din statul țintă și a particularităților lingvistice și culturale ale populației acestuia.

Măsurile active continuă să fie un instrument de influențare a Federației Ruse, care este supus constant perfecționării și care produce

Chiar și cu un volum impresionant de cunoaștere despre adversar, succesul operațiunilor active nu este garantat, din cauza activităților protecționiste ale structurilor de securitate din statul țintă și a particularităților lingvistice și culturale ale populației acestuia.

efecte, în general, pe termen mediu și lung. Deși am prezentat doar aspecte teoretice, nu putem atribui hazardului unele concordanțe dintre acest cadru teoretic și anumite evenimente (declanșarea unor proteste, contradicțiile declarațiilor/deciziilor unor oficiali guvernamentali din interiorul aceluiași stat, acutizarea fluxurilor informaționale false în momente sensibile etc.). Astfel, putem constata că intensitatea manifestării acestora nu este diferită față de perioada Războiului Rece, ceea ce ne obligă să depunem eforturi sporite pentru a ne apăra.

Maskirovka este un concept cu o evoluție îndelungată în gândirea și teoria militară rusă, care are o aplicabilitate și adaptabilitate extinsă. Așa cum preciza Barton Whaley, orientalii au fost cei care au descoperit potențialul manipulării informațiilor în timpul unui război prin blocade informaționale, desfășurarea de operațiuni de inducere în eroare, supraîncărcarea comunicațiilor cu informații confuze, până când adversarul este înnebunit.

Maskirovka este un concept cu o evoluție îndelungată în gândirea și teoria militară rusă, care are o aplicabilitate și adaptabilitate extinsă. Așa cum preciza Barton Whaley (1969, 2007), orientalii au fost cei care au descoperit potențialul manipulării informațiilor în timpul unui război prin blocade informaționale, desfășurarea de operațiuni de inducere în eroare, supraîncărcarea comunicațiilor cu informații confuze, până când adversarul este înnebunit. Cu timpul, tehnici și forme de decepție militară au fost preluate, în principal, de la Sun Tzu (și nu numai) și adaptate la războaiele occidentale (de Antoine Henri Jomini, Carl von Clausewitz, B.H. Liddell Hart).

Rezumându-ne la decepția militară rusă, aceasta nu este foarte diferită de cea occidentală, însă, așa cum am menționat, are o aplicabilitate largă. Spre exemplu, în munca de intelligence, maskirovka se referă la utilizarea condițiilor naturale, crearea unor situații artificiale și utilizarea de dispozitive pentru a ascunde și camufla activitatea propriilor agenți și ofițeri de informații (Mitrokhin, p. 64). Maskirovka este folosită și în contrainformații, unde constituie un set de măsuri speciale proiectate să ascundă sau să inducă adversarul în eroare referitor la adevărata natură a măsurilor luate de structurile de securitate alături de forțele implicate și resursele folosite (Ib., p. 247). În această privință, remarcăm o ușoară asemănare cu ceea ce ar reprezenta măsurile OPSEC (Operations Security).

În sfera militară, *maskirovka* este un concept-umbrelă, care este compus din alte trei concepte, precum *camuflajul, ascunderea* și *decepția militară* (care include utilizarea adevărului, minciunii, înșelăciunii și inducerea în eroare), iar aplicabilitatea sa se întinde la nivel strategic, operațional și tactic (Hamilton, p. 65). La nivel strategic, *maskirovka* asigură dezorientarea adversarului prin ascunderea pregătirilor de desfășurare a unor operațiuni, a strategiei, intențiilor

și armelor implicate; la nivel operațional, scopurile *maskirovka* sunt diminuate ca dimensiune și se focalizează pe simulări, dezinformare, fente și acoperirea pregătirilor operațiunilor ce vor fi desfășurate; iar la nivel tactic, *maskirovka* se concentrează pe acoperire și demonstrații (crearea de poziții de luptă false, camuflaj al trupelor și al echipamentelor etc.) (Maier, 2016, pp. 16-17).

Mai putem adăuga că sunt perspective care consideră că o aplicabilitate mai consistentă a *maskirovka* o întâlnim la nivel operațional, deoarece, de obicei, sarcinile constau în: mascarea mișcărilor de trupe sau a retragerii acestora atunci când au fost reperate de adversar; alterarea percepției adversarului și/sau stoparea posibilității de a putea identifica propriul armament; distragerea atenției adversarului; supraîncărcarea cu date și informații a structurilor de intelligence ale adversarului; divagarea atenției adversarului de la amenințările reale și simularea forței pentru acoperirea vulnerabilităților proprii sau pentru a-i conferi adversarului o falsă impresie de siguranță; condiționarea adversarului cu o anumită rutină/comportament, care să îi determine prejudecăți; și inducerea în eroare a adversarului, în așa fel încât să nu înțeleagă acțiunile proprii în curs de desfășurare și să nu poată răspunde prompt la un incident/eveniment (Dick, 2013, p. 190).

Maskirovka, ca orice operațiune militară, se bazează pe o planificare ce ține cont, în general, de:

- inițiativă – preferința de a pătrunde și influența procesul decizional al țintei în încercarea de a genera confuzie, indecizie și greșeli;
- plauzibilitate – planurile trebuie să fie plauzibile, ca și construcție, din perspectiva țintei;
- consecvență și sincronizare;
- diversitate – pentru a preveni standardizarea sau stereotipizarea în planificare, este recomandată desfășurarea unor măsuri de decepție militară multiple, credibile și înrudite, încât fiecare să se poată confirma pe cealaltă, iar astfel cumulate, să contribuie la povestea decepției. (Hamilton, pp. 66-67)

Maskirovka, ca orice operațiune militară, se bazează pe o planificare ce ține cont, în general, de: inițiativă, plauzibilitate, consecvență, sincronizare și diversitate.

Tot în cadrul aceluiași plan, conform perspectivei sovietice/ruse, este importantă și folosirea categoriei optime de *maskirovka*, acesta fiind constituită din: măsuri de camuflare, care reprezintă măsuri clasice de ascundere a echipamentului prin folosirea culorilor, vegetației naturale, terenului etc.; imitare, care pornește de la folosirea momelilor

(în inducerea în eroare) până la folosirea spectrului electromagnetic, pentru a imita semnale radio ale adversarului; demonstrații de forțe, care au rol dublu, dat de intenția de a spori sau diminua ambiguitatea față de capacitățile și intențiile proprii și de intenția de a simula intenția de a ataca adversarul pentru a-i monitoriza reacția sau a-l face să ia o decizie nefavorabilă; și dezinformare, care are scopul de a furniza adversarului, prin diferite canale și forme, fluxuri informaționale eronate, parțial reale, false (Ib., pp. 68-69).

Pe baza cadrului teoretic al *maskirovka*, inițiatorul încearcă să înfățișeze o reprezentare a realității, falsă și credibilă, încât să atragă atenția țintei în puncte moarte, dar și să genereze condiții favorabile propriilor intenții. Trebuie menționat că, în acest efort, *maskirovka* se folosește, preponderent, de surpriza strategică și de influențare – care asigură conservarea forței de luptă, micșorează riscurile și acționează ca multiplicatoare ale forței –, este un proces puternic centralizat și coordonat, iar limitările nu există, indiferent dacă ținta este una militară, guvernamentală sau civilă, procesul fiind constrâns doar de relația cost-beneficiu și de riscurile aferente (Maier, pp. 6-7). În gândirea militară rusă, *maskirovka* este cea mai bună cale prin care se poate obține surpriza strategică, generând deschideri în apărarea adversarului care, în mod tradițional, s-ar fi obținut cu costuri mult prea mari; *maskirovka* reprezintă varianta optimă de a altera percepția realității factorilor de decizie adverși astfel încât să îi ademenească în a lua decizii inoportune sau eronate; în câmpul tactic, *maskirovka* este folosită pentru protecția forțelor proprii prin mascarea forțelor și prin diseminarea de informații false sau eronate care să îndrepte efectele armelor adverse în direcții irelevante pentru acțiunea combativă (Ib., pp. 8-9).

În gândirea militară rusă, maskirovka este cea mai bună cale prin care se poate obține surpriza strategică, generând deschideri în apărarea adversarului care, în mod tradițional, s-ar fi obținut cu costuri mult prea mari; maskirovka reprezintă varianta optimă de a altera percepția realității factorilor de decizie adverși astfel încât să îi ademenească în a lua decizii inoportune sau eronate.

După cum putem remarca, acest termen este folosit mai mult în chestiunile militare, spre deosebire de măsurile active. Însă, având în vedere scopul său de a altera realitatea și faptul că operațiunile informaționale ruse sunt gândite și executate de un mix de personal civil-militar, putem presupune că *maskirovka* este folosită și în afara teatrului de operații. Utilizarea sa, ca formă a războiului informațional, și în spațiul virtual împotriva țintelor civile, dar și în cel al factorilor de decizie, ne trimite cu gândul la ideile exprimate de teoreticienii militari ruși referitoare la utilizarea abordării indirecte sau la perspectiva schimbării de regim prin mijloace nonmilitare/asimetrice.

Controlul reflexiv (această denumire fiind regăsită mai mult în literatura de specialitate occidentală) sau managementul percepțiilor este un concept complementar al *maskirovka*, dezvoltat încă din anii '60, iar, în general, *maskirovka* și *controlul reflexiv* sunt desfășurate împreună. Spre deosebire de componentele discutate, *controlul reflexiv* pune accent pe confruntarea intelectuală a adversarilor, unde ofițerii examinează obiectiv situația dată și, în funcție de experiență și pregătire, aceștia caută metode de a manipula câmpul tactic în favoarea lor prin analizarea tiparelor și a tendințelor adversarului, coroborând informațiile obținute cu propriile prognoze de acțiune posibilă (Thomas, 2019, pp. 4-1–4-2). Conform gândirii militare ruse, *controlul reflexiv/managementul percepțiilor* este desfășurat în mediul informațional și urmărește obținerea unor efecte informaționale și psihologice împotriva factorilor de decizie în încercarea de a-i convinge, prin diverse canale, să renunțe la planurile inițiale și să acționeze în detrimentul propriilor interese sau obiective (Ib., p. 4-2). Practic, *controlul reflexiv* caută să genereze condițiile optime pentru acțiunile ruse, folosindu-se de *maskirovka* și *măsurile active*, cu mențiunea că nu este căutată surclasarea militară a adversarului, ci proiectarea/simularea unei anumite imagini sau stări de fapt care să distorsioneze realitatea obiectivă și să afecteze capacitatea de prognoză, anticipare și acțiune a adversarului prin bulversarea decidentului.

Controlul reflexiv pune accent pe confruntarea intelectuală a adversarilor, unde ofițerii examinează obiectiv situația dată și, în funcție de experiență și pregătire, aceștia caută metode de a manipula câmpul tactic în favoarea lor prin analizarea tiparelor și a tendințelor adversarului, coroborând informațiile obținute cu propriile prognoze de acțiune posibilă.

Cu toate acestea, ca urmare a evoluțiilor sociale, politice și tehnologice, în concepția rusă, *controlul reflexiv* se poate extinde dincolo de arta militară, spre acțiuni precum inducerea în eroare sau înșelarea experților străini, coruperea rețelelor de calculatoare și manipularea social media sau/și a opiniei publice a unui stat, astfel având aplicabilitate în:

- negocieri – utilizarea unui mix între tehnici de marketing și control reflexiv;
- decepție și doctrină militară – publicarea de documente oficiale programatice și doctrinare care să proiecteze o anumită imagine referitoare la intențiile și direcțiile de acțiune ale Federației Ruse;
- descurajare – în contextul arsenalelor nucleare, părțile încearcă să se convingă de futilitatea acțiunilor de șantaj și presiune militară;

În viziunea rusă, controlul reflexiv este un proces pe baza căruia inițiatorul încearcă să exploateze vulnerabilitățile din sistemul valoric al adversarului, care este compus din „filtre", unde filtrele sunt constituite din conceptele, cunoașterea, ideile și experiența adversarului. Astfel, după identificarea unui punct de rezistență minimă, este folosită o armă informațională (compusă din metode și tehnici ale distorsiunii informaționale) care să aibă capacitatea de a genera schimbări în procesele și sistemele informaționale (civile și militare) adverse.

- exerciții militare – organizarea de acțiuni militare care să transmită mesaje diferite de intențiile reale și care să se desfășoare simultan în diferite zone;
- stratageme – implementarea unor seturi de măsuri, interconectate prin caracteristici ca scop, loc și timp, pentru a zădărnici planurile adversarului, utilizând ascunderea, mascarea, inducerea în eroare, înșelăciunea etc.;
- C4 – parazitarea sistemelor de comandă și control, informatice și de comunicații cu date și informații distorsionate sau false, care să determine executarea, de către adversar, a unor acțiuni care să compromită liderii militari și/sau politici în fața subordonaților și să convingă societatea civilă de intențiile anti-naționale ale acestora;
- războiul psihologic-informațional – modelarea comportamentului adversarului prin utilizarea unor măsuri complexe militare, politice și diplomatice;
- analiză și abordare reflexivă – analiza descoperă obiectivele probabile ale adversarului și mijloacele prin care dorește să le obțină, iar abordarea reflexivă încearcă să obțină superioritatea intelectuală față de adversar pe baza analizei;
- internet – manipularea trendurilor sau a emoțiilor sociale prin determinarea unor grupuri/indivizi țintă să acționeze într-o anumită direcție (Ib., pp. 43-46).

Subiectul *controlului reflexiv* este amplu discutat atât în literatura de specialitate occidentală, cât și în cea rusă, iar definițiile, metodele și aplicabilitatea acestui concept sunt mai extinse decât detaliile prezentate. Cu toate acestea, ne interesează, îndeosebi, relevanța pe care teoreticienii militari ruși o atribuie *controlului reflexiv* în contextul războiului psihologic-informațional (sau războiului informațional). În acest sens, *controlul reflexiv* are rolul de a determina adversarul să se deziluzioneze singur și să ia acele decizii care să-i determine carențe în organizarea sistemelor proprii. În viziunea rusă, *controlul reflexiv* este un proces pe baza căruia inițiatorul încearcă să exploateze vulnerabilitățile din sistemul valoric al adversarului, care este compus din *„filtre"*, unde filtrele sunt constituite din conceptele, cunoașterea, ideile și experiența adversarului (Pynnöniemi, 2019, p. 219). Astfel, după identificarea unui punct de rezistență minimă, este folosită o armă informațională (compusă din metode și tehnici ale distorsiunii

informaționale) care să aibă capacitatea de a genera schimbări în procesele și sistemele informaționale (civile și militare) adverse (Ib.). Este important de precizat că, în momentul desfășurării armei informaționale, ținta este atacată de către mai mulți atacatori/din mai multe direcții simultan și, în acest fel, victima nu mai reușește să facă distincția dintre aliat și adversar, ceea ce, în final, duce la pierderea noțiunii de amenințare (Ib., p. 220). În acest fel, remarcăm faptul că acțiunea *controlului reflexiv* bulversează ținta, întrucât aceasta produce efecte în două direcții posibile: latență în capacitatea de reacție la amenințările obiective și directe sau subiectivizează amenințările, determinând reacții exacerbate și distrăgând atenția de la evenimentele periculoase imediate.

Făcând o comparație între *controlul reflexiv* și *măsurile active*, remarcăm faptul că există similitudini în materie de forme și tehnici, ambele vizând dimensiunea cognitivă a țintei. Diferența cea mai vizibilă constă în scopul și focalizarea acțiunilor, unde *controlul reflexiv* este destinat țintelor exclusiv externe, în timp ce măsurile active au o aplicabilitate mai generală, intern-externă. Totuși, există o nuanță de care trebuie să ținem cont: *măsurile active, maskirovka* și *controlul reflexiv* sunt concepte cu o îndelungată evoluție, astfel încât acestea au fost proiectate să fie desfășurate în comun, să se completeze și să fie adaptabile noilor concepte operaționale, tehnologii și nevoi.

MODEL ORIENTATIV

Având în vedere conceptele, noțiunile și ideile prezentate, propunem, în continuare, un model orientativ, care să evidențieze modul de acțiune al Federației Ruse, punând accent pe ideea schimbării de regim prin intermediul coruperii/ afectării mediului informațional al statului vizat. Considerăm că acest model poate contribui la o înțelegere mai clară a modului de acțiune rusesc asupra statelor membre ale Uniunii Europene și ale NATO, având în vedere că utilizarea forței militare împotriva acestor state este încă o mișcare riscantă.

Așa cum am precizat, înainte de inițierea unor acțiuni împotriva unui stat/unor state, sunt realizate pre-analize și analize care identifică punctele de rezistență minimă ale acestora, ulterior exploatându-le particularizat. Totuși, chiar dacă vorbim de state membre ale UE și ale NATO, sunt unele vulnerabilități generale valabile în sistemele lor democratice, care facilitează aplicarea formelor și măsurilor

Înainte de inițierea unor acțiuni împotriva unui stat/unor state, sunt realizate pre-analize și analize care identifică punctele de rezistență minimă ale acestora, ulterior exploatându-le particularizat. Chiar dacă vorbim de state membre ale UE și ale NATO, sunt unele vulnerabilități generale valabile în sistemele lor democratice, care facilitează aplicarea formelor și măsurilor nonmilitare, a războiului informațional sau a ideii de schimbare de regim.

nonmilitare, a războiului informațional sau a ideii de schimbare de regim.

În sistemele democratice, există o distincție între individ și stat, unde cele două entități au nevoi și obiective diferite, iar securitatea este percepută sub forme diverse. Spre exemplu, statul poate fi interesat să își asigure, pe plan internațional, securitatea teritorială și o oarecare vizibilitate și relevanță în cadrul organismelor internaționale din care face parte, dar individul s-ar putea să fie mai interesat de prosperitatea sa economică și de împlinirea profesională, sentimentală sau ideologică. Totuși, existența acestei distincții reprezintă fundamentul care poate duce la erodarea puterii și legitimității statului, întrucât poate determina: enclavizarea societății, unde indivizii resimt o fidelitate sporită față de elementele mai apropiate de viața lor, precum familia, clanul, comunitatea religioasă, regiunea de care aparțin etc.; și enclavizarea statului, alături de instituțiile sale, unde rolul său se rezumă la componenta administrativă (Buzan, 2017, p. 90). Astfel, în ideea de a diminua această falie dintre stat și individ/societate, sistemul politic joacă rolul de mediator în raporturile sociale conflictuale, fenomenele politice fiind fapte sociale, în special prin faptul că nu există delimitări clare care să limiteze politizarea vieții sociale (Denni, Lecomte, 2004, pp. 21, 25). Iar din acest punct apar vulnerabilitățile ce pot fi exploatate de Federația Rusă, îndeosebi la nivel informațional.

În sistemele democratice, există o distincție între individ și stat, unde cele două entități au nevoi și obiective diferite, iar securitatea este percepută sub forme diverse. Spre exemplu, statul poate fi interesat să își asigure, pe plan internațional, securitatea teritorială și o oarecare vizibilitate și relevanță în cadrul organismelor internaționale din care face parte, dar individul s-ar putea să fie mai interesat de prosperitatea sa economică și de împlinirea profesională, sentimentală sau ideologică.

Partidele politice contribuie la educarea politică a individului și, astfel, au capacitatea de a structura opinia publică prin faptul că acestea analizează, în scop electoral, situația statului, propun teme de dezbatere politică și vin cu soluții, dar diseminează bătălia politică la toate nivelurile societății, prin orice canale (Bréchon, 2004, pp. 119-120). În mod natural, societatea nu este un sistem omogen și armonios, fiind marcată de conflicte generate de existența stratificării sociale și a intereselor divergente ale diferitelor grupuri sociale (Denni, Lecomte, p. 73). Însă, cu cât conflictul politic este exprimat mai violent în societate (adăugându-se tensiunilor preexistente), cu atât șansele apariției partidelor extremiste cresc, iar dacă sunt infuzate, în toiul conflictului, și elemente ale distorsiunii informaționale, fricile care se vor naște în interiorul societății sau al grupurilor sociale vor genera forme ideologice embrionare (ultranaționalism, antiglobalism, fanatism religios, anarhism etc.) cu potențial de dezvoltare (Bréchon, pp. 80, 110). Totuși, aici sunt generate alte două probleme: a) partidele

politice sunt condiționate, în oferta politică, de starea și preferințele opiniei publice/societății, așa încât agenda politică nu poate fi prea îndepărtată de aceste preferințe (Ib., p. 92); și b) statul poate face față unei perioade îndelungate de dezordine a vieții politice, însă, pentru individ, acutizarea unei lupte politice violente devine o sursă de insecuritate (Buzan, pp. 83-84), care îl radicalizează și, ulterior, îi schimbă sistemul valoric.

Aceste aspecte, practic, stau la baza ideilor ruse referitoare la influențarea adversarului în sfera politică (decizională) și a populației. Astfel, ca prim pas, aceștia trebuie să obțină supremația asupra mediului informațional advers prin luarea inițiativei care să determine șocul informațional. În acest sens, Federația Rusă poate desfășura o serie de operațiuni care să includă *măsuri active, maskirovka* și *control reflexiv* orientate, în primă instanță, către individ și societate, iar ulterior către mediul politic. În această primă etapă, operațiunile ar urmări să blocheze capacitatea societății de a-și organiza modalități de mediere a conflictelor sociale (Denni, Lecomte, p. 31), determinând fragmentarea acesteia în urma escaladării conflictelor care se înmulțesc și nu se mai rezolvă.

Federația Rusă poate desfășura o serie de operațiuni care să includă măsuri active, maskirovka și control reflexiv orientate, în primă instanță, către individ și societate, iar ulterior către mediul politic. În această primă etapă, operațiunile ar urmări să blocheze capacitatea societății de a-și organiza modalități de mediere a conflictelor sociale, determinând fragmentarea acesteia în urma escaladării conflictelor care se înmulțesc și nu se mai rezolvă.

Aceste forme și măsuri pot fi atât de bruște, încât sistemele de securitate ale statului vizat pot fi supuse surprizei strategice și, astfel, pot reacționa târziu la atacurile informaționale ruse, iar prin expunerea indivizilor la fluxurile informaționale ruse pe o perioadă îndelungată pot determina alterarea mediului informațional, astfel încât să se obțină efectele dorite. Cu toate acestea, condiționarea nu este suficientă, deoarece Federația Rusă acționează simultan sau etapizat (în funcție de particularitățile statului țintă) în mai multe direcții. Mai precis, în primă instanță, este destul de probabil să își concentreze efortul în a stopa accesul populației/unor grupuri la informații corecte, cu scopul de a le subiectiviza realitatea, ulterior penetrând societatea cu agenți de influență activi și pasivi (activi – ofițeri de informații/ agenți recrutați care se ocupă cu măsuri active; pasivi – oameni influenți care nu au legături directe cu acțiunile externe, dar sunt parte la acestea). După asigurarea unui mediu informațional propice, Federația Rusă poate disemina informații false prin diverse canale, în special prin camerele de ecou din social-media, și să se asigure că este instaurată confuzia, nemulțumirea și, în final, radicalizarea.

De asemenea, Federația Rusă poate opera și în direcția mediului politic al statului vizat cu scopul de a-l vulnerabiliza, în așa fel încât acesta să nu își mai poată asuma rolul de reglator și de păstrător al unității valorice și sociale globale împotriva elementelor destabilizatoare (Ib., p. 35). În acest sens, conform perspectivelor teoretice prezentate, vulnerabilizarea mediului politic se poate realiza prin acțiuni acoperite, precum înșelarea și inducerea în eroare, șantajul, amenințarea, coruperea *(figura nr. 1)*, dar și prin acțiuni mai directe, cum ar fi infiltrarea unor vectori de influență care să genereze și să mențină

Vulnerabilizarea mediului politic se poate realiza prin acțiuni acoperite, precum înșelarea și inducerea în eroare, șantajul, amenințarea, coruperea, dar și prin acțiuni mai directe, cum ar fi infiltrarea unor vectori de influență care să genereze și să mențină un anumit grad de instabilitate, subversiunea, sabotajul și chiar asasinatul (operațiuni umede).

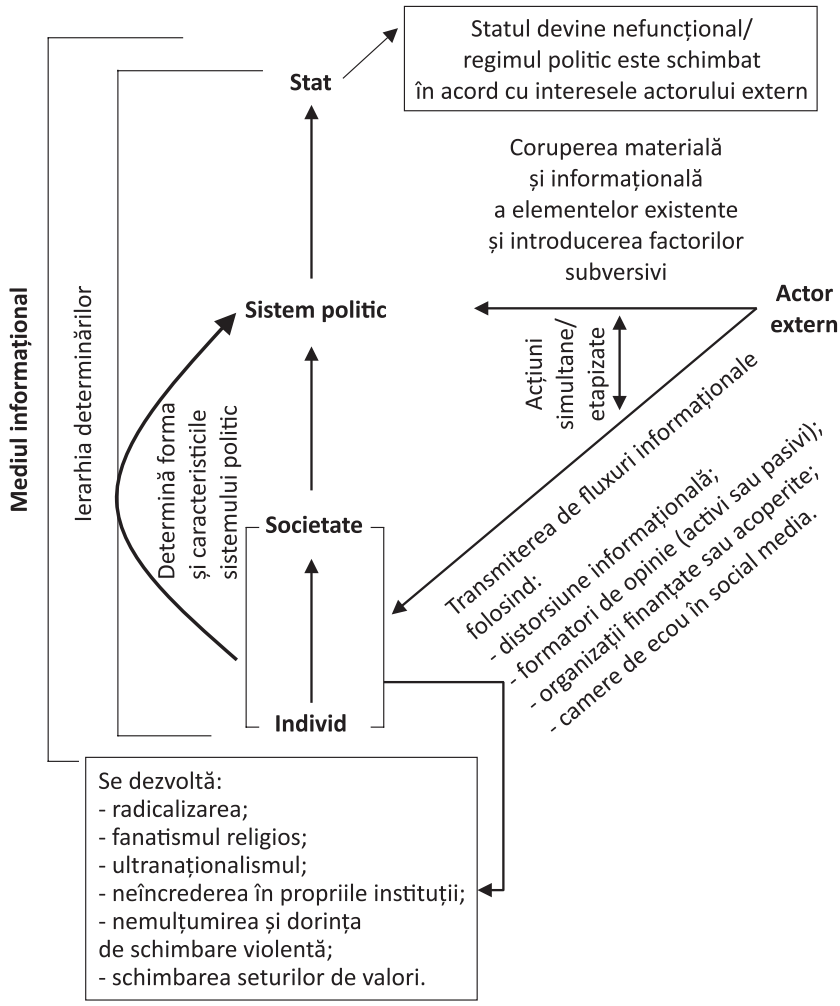

Figura nr. 1: Model orientativ al schimbării structurii social-politice a unui stat prin afectarea mediului său informațional (Sursa: autorul)

un anumit grad de instabilitate, subversiunea, sabotajul și chiar asasinatul (operațiuni umede). Acțiunile informaționale ruse pot urmări (așa cum am mai precizat), în general: 1) discreditarea și delegitimarea instituțiilor statului și a mediului politic, 2) inducerea stării de haos în rândul populației, 3) inducerea în eroare și distorsionarea realității și 4) monitorizarea, evaluarea efectelor și ajustarea formelor și mijloacelor, în caz de nevoie.

Trebuie precizat că, înaintea radicalizării individului, atacurile informaționale au rolul de a asigura distrugerea încrederii și respectului cetățeanului față de ordinea preexistentă din interiorul statului și să îl motiveze să acționeze pentru a o schimba/dărâma. Executarea acestor operațiuni informaționale poate fi desfășurată pe termen mediu și lung pentru fundamentarea, la nivel cognitiv, a mistificării realității/inducerii în eroare. Cu trecerea timpului, apar primele semne ale modificării sistemelor valorice în rândul societății și al mediului politic, precum partidele extremiste, ultranaționalismul, fundamentalismul religios, antiglobalismul, izolaționismul, antieuropenismul, antiamericanismul etc. Odată ce schimbările de atitudine încep să devină vizibile, indivizii și societatea vor determina schimbări în mediul politic – care a fost, și el, supus influenței externe – și, la rândul său, va determina schimbări în aparatul de stat pornind de la structură până la legi organice și fundamentale. Desigur, în cadrul unei operațiuni ce vizează un stat sunt analizate și utilizate diverse tehnici și mijloace, iar detaliile sunt consistente și constau în cât mai multe particularități care pot contribui la îndeplinirea cu succes a *„acțiunilor ostile”* ruse.

Înaintea radicalizării individului, atacurile informaționale au rolul de a asigura distrugerea încrederii și respectului cetățeanului față de ordinea preexistentă din interiorul statului și să îl motiveze să acționeze pentru a o schimba/dărâma.

În această secțiune, am încercat să construim un model orientativ care se fundamentează pe unele aspecte esențiale, dar generale ale statelor democratice. Bazându-ne pe conceptele și perspectivele militare ruse prezentate, am construit acest model ipotetic, pentru a evidenția cât de reală este posibilitatea unei acțiuni de a destabiliza un stat din interior sau de a-i schimba regimul politic pentru a genera condițiile optime unor acțiuni rusești ulterioare.

CONCLUZII

Definirile și interpretările prezentate au rolul de a construi o sinteză asupra unor concepte fundamentale din arsenalul teoretic al Federației Ruse și de a clarifica (pe cât posibil) unele ambiguități referitoare la forme și practici rusești. Însă, tot în acest registru, lucrarea încearcă

să atragă atenția asupra complexității conceptuale militare ruse, în special în contextul în care unii analiști/cercetători clasifică acțiunile ruse drept joc de sumă nulă. După cum am prezentat, atât perspectivele militare ruse, cât și conceptele lor se fundamentează pe o planificare complexă, care înglobează diferite forme și măsuri, coordonate sau sincronizate, unde scopurile sunt variate și țintesc militarii, civilii și factorii de decizie. În această logică, indiferent dacă Federația Rusă lansează operațiuni asimetrice, măsuri nonmilitare sau un război psihologic-informațional folosindu-se de forme precum *măsurile active, maskirovka* și *controlul reflexiv*, acțiunile vor urmări îndeplinirea unei linii de operațiuni prin care să influențeze ținta în direcțiile dorite/prognozate. Astfel, putem afirma că aceste acțiuni, deși lente ca efect, urmăresc generarea unor condiții optime de acțiune pentru Federația Rusă, ceea ce ne determină să luăm în considerare faptul că o operațiune de influențare a unei ținte poate fi etapizată și poate fi desfășurată pe termen lung (referindu-ne la o durată de ani).

Având în vedere că majoritatea statelor autocratice se folosesc, în diverse măsuri, de operațiuni informaționale pentru a influența ținte în diverse direcții, considerăm că se impune, la nivel NATO, redimensionarea teoretică și conceptuală în ceea ce privește utilizarea militară a informației.

De asemenea, chiar dacă au sau nu capacitățile materiale, umane și financiare de a desfășura operațiuni pe durata anilor, trebuie recunoscut faptul că, la nivel teoretic, au un avantaj în fața statelor membre ale NATO, deoarece acestea dezvoltă și îmbunătățesc conceptele operaționale care se fundamentează pe inițiativă, surpriză strategică, flexibilitate și manevrabilitate, influențare, inducere în eroare și exploatarea punctelor de rezistență minimă. În acest sens, un aspect foarte problematic îl regăsim în faptul că încadrează *„acțiunile ostile”* între starea de pace și război, lucru pe care nu îl regăsim în concepția NATO. Teoretizarea războiului informațional în formele sale psihologic-informațional și tehnic-informațional determină un alt dezavantaj conceptual pentru NATO.

Având în vedere că majoritatea statelor autocratice se folosesc, în diverse măsuri, de operațiuni informaționale pentru a influența ținte în diverse direcții, considerăm că se impune, la nivel NATO, redimensionarea teoretică și conceptuală în ceea ce privește utilizarea militară a informației. Odată create niște instrumente generale, structurile de securitate ale statelor membre pot folosi, particularizat și în funcție de specificul cultural, pentru a contracara sau anula abordările indirecte, atacurile informaționale, operațiunile asimetrice sau măsurile nonmilitare rusești, dar nu numai.

În final, putem doar estima că amenințările de natură militară și informațională nu se vor estompa, ci se vor amplifica, determinând forme și mai complexe și greu de contracarat. Timpul este un aliat pentru cei care știu să îl folosească optim, astfel că statele membre ale NATO și ale UE trebuie să valorifice timpul rămas pentru a-și proteja mediile informaționale, sistemele de apărare, factorii de decizie și societățile de ingerințele ruse.

BIBLIOGRAFIE:

1. Andrew, C., Mitrokhin, V. (1999, 2000, 2018). *The Mitrokhin Archive: The KGB in Europe and the West*. Vol. I. Penguin Books.
2. Bréchon, P. (2004). *Partidele politice*. Trad. Marta Nora Țărnea, Adina Barvinshi. Cluj-Napoca: Editura Eikon.
3. Buzan, B. (2017). *Popoarele, statele și frica: O agenda pentru studii de Securitate internațională în epoca de după Războiul Rece*. Trad. Vivia Săndulescu. Chișinău: Editura Cartier.
4. Chiru, I. (2019). *Analiza în intelligence: de la artă la știință*. București: Editura Tritonic.
5. Clark, R.M., Mitchell, W.L. (2019). *Deception: counterdeception and counterintelligence*. Washington, D.C.: CQ Press.
6. Denni, B., Lecomte, P. (2004). *Sociologia politicului*. Vol. I. Trad. Marta Nora Țărnea. Cluj-Napoca: Editura Eikon.
7. Dick, C.J. (2013). *Catching NATO Unawares: Soviet Army Surprise and Deception Techniques*. În Barton Whaley (ed.), Hy Rothstein (ed.). *The Art and Science of Military Deception* (pp. 181-192). Boston, Londra: Artech House.
8. Duțu, P. (2013). *Amenințări asimetrice sau amenințări hibride: delimitări conceptuale pentru fundamentarea securității și apărării naționale*. București: Editura Universității Naționale de Apărare *„Carol I”*.
9. Franke, U. (2015). *War by non-military means: Understanding Russian information warfare*. Swedish Defence Research Agency (FOI).
10. Fridman, O. (2019). *On ‘Gerasimov Doctrine’: Why the West Fails to Beat Russia to the Punch*. În *Prism*, 8(2), 101-112.
11. Giles, K., Seaboyer, A. (2019). *The Russian Information Warfare Construct*. Defence Research and Development Canada.
12. Giles, K. (2016). *Handbook of Russian Information Warfare*. Roma: NATO Defense College, Research Division.
13. Gordon, J.S. (1996). *Intelligence and Psychological Operations.* În Benjamine F. Findley (ed.). Frank L. Goldstein (ed.), *Psychological Operations: principles and case studies* (pp. 203-211). Alabama: Air University. Press Maxwell Air Force Base.

14. Göransson, M. (2021). *Understanding Russian thinking on gibridnaya voyna*. În Mikael Weissmann (ed.), Niklas Nilson (ed.), Björn Palmertz (ed.), Per Thunholm (ed.). *Hybrid Warfare. Security and Asymmetric Conflict in International Relations* (pp. 83-94). Londra, New York, Dublin: I.B. TAURIS, Bloomsbury Publishing Plc.
15. Hamilton, D.L. (1986). *Deception in Soviet military doctrine and operations*. Monterey, California: Naval Postgraduate School.
16. Kabernik, V. (2019). *The Russian Military Perspective*. În Ofer Fridman (ed.), Vitaly Kabernic (ed.), James C. Pearce (ed.). *Hybrid Conflicts and Information Warfare: new labels, old politics* (pp. 43-65). Boulder, London: Lynne Rienner Publishers.
17. Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., Oberholtzer, J. (2017). *Lessons from Russian's Operations in Crimea and Eastern Ukraine*. RAND Corporation.
18. Koribko, A. (2015). *Hybrid Wars: the Indirect Adaptive Approach to the Regime Chance*. Moscova: Peoples' Friendship University of Russia.
19. Liddell Hart, B.H. (1929, 2008). *Strategy*. BN Publishing.
20. Maier, M. (2016*). A Little Masquerade: Russia's Evolving Employment of Maskirovka*. Kansas: US Army School for Advanced Military Studies, Fort Leavenworth United States.
21. Mattsson, P.A. (2015). *Russian Military Thinking – A New Generation of Warfare*. În *Journal of Baltic Security 1(1)*, 61-70.
22. Mitrokhin, V. (ed.). (2002, 2004). *KGB lexicon: The Soviet Intelligence Officer's Handbook*. Londra, New York: Frank Cass & Co. Ltd.
23. Pynnöniemi, K. (2019). *Information-Psychological Warfare in Russian Security Strategy*. În Roger E. Kanet (ed.), *Routledge Handbook of Russian Security* (pp. 214-226). Londra, New York: Routledge Taylor & Francis Group.
24. Renz, B., Smith, H., Bukkvoll, T., Echevarria, A.J., Giles, K., Scheipers, S., Strachan, H., Thornton, R. (2016). *Russia and Hybrid Warfare: definitions, capabilities, scope and possible responses*. Kikimora Publications, Aleksanteri Institute, University of Helsinki.
25. Robinson, P. (2010). *Dicționar de securitate internațională*. Trad. Monica Neamț. Cluj-Napoca: CA Publishing.
26. Sinclair, N. (2020). *A Logic All Its Own. Russian Operational Art in the Syrian Campaign*. În *Military Review 100(1)*, 12-21.
27. Thomas, T.L. (2016). *Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*. Foreign Military Studies Office.
28. Thomas, T.L. (2019). *Russian Military Thought: Concepts and Elements*. The MITRE Corporation.
29. Wardle, C., Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for researh and policymaking*. Strasbourg: Council of Europe.

30. Whaley, B. (1969, 2007). *Stratagem. Deception and Surprise in War*. Norwood: Artech House.
31. Bureau of Public Affairs (1981). *Soviet „Active Measures". Forgery, Disinformation, Political Operations*. Washington D.C.: United States Deparment of State.
32. FM 3.-1. (2016). *Information Operations*. Headquarters, Department of the Army.