MODALITĂȚI DE CONTRACARARE A AMENINȚĂRII HIBRIDE LA ADRESA SECURITĂȚII STATELOR

Marius Titi POTÎRNICHE
Dan PETRESCU

Concepte și teorii

Centrul de Studii Strategice de Apărare și Securitate
SSAS

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
Centrul de Studii Strategice de Apărare și Securitate

Marius Titi POTÎRNICHE
Dan PETRESCU

MODALITĂȚI DE CONTRACARARE A AMENINȚĂRII HIBRIDE LA ADRESA SECURITĂȚII STATELOR

Studiu de specialitate

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
BUCUREȘTI, 2019

Descrierea CIP a Bibliotecii Naţionale a României
POTÎRNICHE, MARIUS TITI
Modalități de contracarare a amenințării hibride la adresa securității statelor : studiu de specialitate / Marius Titi Potîrniche, Dan Petrescu. - București : Editura Universității Naționale de Apărare "Carol I", 2019
Conține bibliografie
ISBN 978-606-660-402-4

I. Petrescu, Dan
355.45

- *Lucrarea face parte din Planul de cercetare științifică al Universității Naționale de Apărare „Carol I" și este distribuită conform reglementărilor în vigoare*
- *Lucrarea a fost avizată în şedinţa Consiliului Ştiinţific al CSSAS; responsabilitatea privind conţinutul revine în totalitate autorilor*

ISBN 978-606-660-402-4 (tipărit)
ISBN 978-606-660-403-1 (online)

CUPRINS

WAYS OF COUNTERING HYBRID THREAT TO STATE SECURITY

Argument ■ Hybrid threat – conceptual definition ■ Operationalisation of hybrid threat and hybrid aggression ▪ NATO, EU and Russian approach to hybrid war ■ **Hybrid aggression in the contemporary operational environment** ■ Operational environment of hybrid threat ▪ Configuration model of the hybrid threat ■ **Countering hybrid threat** ▪ Regional initiatives ▪ Strategic models for countering hybrid threat ▪ Countering hybrid threat – military implications ■ **Conclusions** ■ **Bibliography**

Within the four main chapters of the paper, we emphasize that the modern approach to threat generates extremely complex situations that shift the scope of countering its manifestation −the aggression −from defence to a security issue. The first objective of the study is to settle down the concepts of *hybrid threat* and *hybrid aggression* and their understanding at scientific and operational level. The second objective is to describe the environment in which hybrid aggression may occur and its configuration. The aim of this study is to analyse the possibility of an actor state to counter hybrid threats and to highlight several keypoints that must be followed in order to detect and prevent it before materializing violently. Based on the analysis of specialized literature, strategic and official documents, official declarations, statistics and case studies, the paper concludes that each hybrid threat has a unique configuration based on a hybrid strategy used in the hybrid aggression, perpetrated by a hybrid aggressor against a target actor. The latter will have to develop a "whole of government" type system, corresponding to its intrinsic characteristics, integrated in that of the partners and adapted to the configuration of the hybrid aggression, which allows to counteract it: detection, prevention (deterrence), resilience (defence, impact resistance and recovery) and combat (implementation of countermeasures that constitute the response to hybrid aggression). The hybrid threat countering system must implement a coherent strategy, using all instruments of power in actions carried out in all areas that define the state actor (PMESII) to achieve all security objectives set at national level for achieving its asigned purpose.

ARGUMENT

Evoluția evenimentelor politico-militare din ultimele decenii a fost marcată de profunde transformări în modul de abordare a conflictelor de către actorii participanți. Apariţia şi dezvoltarea fulminantă a unor mijloace de ordin tehnologic cu efecte semnificative în ecuaţia conflictului, modificările de natură conceptuală privind modul de abordare a luptei armate şi diferenţa creată din punct de vedere al puterii de luptă între actorii angajaţi în conflict au dus la transpunerea în fapt a unor profunde transformări privind configuraţia mediului operaţional actual şi viitor şi a acţiunilor desfăşurate.

Este de necontestat faptul că acţiunile de tip hibrid generează în mediul de securitate contemporan situaţii de o complexitate deosebită. Această certitudine a conflictului prezent şi viitor impune nevoia identificării unor modalităţi de a reduce gradul de incertitudine al acţiunilor militare desfăşurate în mediul operaţional. Formularea unor metode ştiinţifice eficiente de analiză a mediului operaţional prezent, a modalităţilor de estimare a configuraţiei mediului operaţional viitor şi a posibilităţilor de identificare a cursurilor de acţiune optime pentru atingerea scopurilor urmărite constituie o necesitate de necontestat şi determină motivaţia desfăşurării demersului ştiinţific prezentat în continuare.

Aceste realităţi au adus în atenţia specialiştilor militari de pe mapamond necesitatea concentrării eforturilor de analiză a evoluţiei fenomenului război cu direcţionarea acestora în sensul previzionării aspectului conflictului militar şi adaptării tuturor componentelor care cristalizează puterea de luptă în scopul contracarării ameninţărilor actuale şi viitoare. Considerăm că aprofundarea cunoaşterii conceptului de *ameninţare de tip hibrid*, care conturează aspectul modern al fenomenului război, însoţită de dezvoltarea unui instrument avansat, puternic, eficient şi flexibil care să vină în sprijinul previzionării situaţiilor de criză viitoare şi planificării modului de prevenire sau rezolvare a lor, constituie un demers de importanţă majoră în domeniul ştiinţelor militare.

Ţinând cont de complexitatea mediului de securitate, în special a componentei lui operaţionale, şi de nivelul ridicat de incertitudine care îi incumbă, în demersul ştiinţific întreprins pornim de la ipoteza că cea mai potrivită abordare a eforturilor integrate de identificare şi contracarare a

ameninţării de tip hibrid şi de soluţionare a crizelor pe care le generează este abordarea proactivă. Aceasta trebuie să fie fundamentată pe un mod de gândire prospectiv, a cărui dezvoltare, concretizată prin sporirea ratei de succes şi a acurateţei privind anticiparea acţiunilor probabile ale adversarului de tip hibrid este, nu numai din punct de vedere cronologic, prima şi poate cea mai importantă cerinţă a pregătirii forţei. Analiza mediului operaţional, a actorilor prezenţi şi a relaţiilor dintre ei, dar şi a strategiilor prin care ei vizează realizarea scopurilor urmărite constituie o condiţie obligatorie pentru pregătirea forţei şi planificarea acţiunilor.

Dezvoltarea conceptuală a agresiunii de tip hibrid se realizează ca o abordare cuprinzătoare a modurilor de manifestare a ameninţărilor în contextul mediului de securitate contemporan. De aceea, considerăm extrem de importantă definirea conceptuală a cadrului în care se desfăşoară agresiunea de tip hibrid, iar această activitate trebuie să se constituie într-o analiză exhaustivă şi documentată a mediului de securitate şi a configuraţiei ameninţării de tip hibrid, elemente ce modelează paleta de acţiuni desfăşurate în acest context. Luând în considerare aceste deziderate, studiul mediului de securitate contemporan trebuie să fie structurat având la bază un model cuprinzător, cum este cazul *PMESII*, care urmăreşte evoluţia celor mai semnificative domenii în care pot evolua relaţiile dintre actori. După prezentarea aspectelor definitorii referitoare la ameninţarea de tip hibrid, dezvoltate în cadrul comunităţii ştiinţifice interne şi internaţionale, realizăm analiza modului de desfăşurare a acţiunilor posibile care compun agresiunea de tip hibrid şi tendinţele în configurarea acesteia într-o imagine structurată a elementului generator al situaţiei de criză. Studiul se concentrează, apoi, pe identificarea unor modalităţi de contracarare a ameninţării de tip hibrid, atât în etapa de pregătire a acesteia, orientat pe descurajare şi pe diminuarea efectelor acţiunilor destinate să modeleze mediul operaţional şi de securitate din zona ţintei, cât şi în etapa atacului, cu generarea răspunsului la agresiunea de tip hibrid, aflată în plină desfăşurare. În acest sens, am valorificat nu doar bibliografia de specialitate, ci şi baze de date, analize şi studii actuale realizate de către membri marcanţi ai comunităţii ştiinţifice naţionale şi internaţionale.

Capitolul 1

AMENINŢAREA DE TIP HIBRID – DEFINIRE CONCEPTUALĂ

Ideea că un actor poate genera în mediul operaţional o ameninţare care combină forţele convenţionale, guvernate de regulile și normele militare tradiționale, cu forțe neconvenționale, care execută acţiuni din registrul celor neregulate[1] (cum ar fi acţiunile de gherilă), a existat de multă vreme. De-a lungul istoriei s-a întâmplat deseori ca un actor inferior din punct de vedere militar să vizeze vulnerabilitățile adversarilor mai puternici și să profite de mijloacele de care dispune pentru a-şi realiza scopurile strategice prin acţiuni asimetrice, deseori neconvenţionale, combinate cu cele convenţionale. Exemple istorice de acţiuni de tip hibrid pot fi întâlnite încă din antichitate, deși termenul *amenințare hibridă* este relativ recent, definind acţiuni mult mai sofisticate.

În Roma antică, o forţă formată din bandiți, criminali, soldați din forţele regulate și mercenari au întrebuinţat diverse metode de luptă într-o combinaţie de bătălii şi ambuscade organizate pe căi de comunicaţii, utilizând arme de asediu furate, împotriva legiunilor romane ale lui Vespasian pe timpul rebeliunii evreilor din anul 66 AD (Timothy McCuloh şi Richard Johnson). Până de curând nu i-am fi spus acestei forțe „hibridă”. În peninsula Iberică, în anul 1806, o forță (*de tip hibrid*) formată de gherile spaniole, combinate cu forțe regulate britanice și portugheze au încercat să obțină efecte militare decisive asupra Marii Armate a lui Napoleon. În al Doilea Război Mondial, între 1941 şi 1945, pe Frontul de Est, armata sovietică a integrat și sincronizat o forță neregulată slab echipată, neconvenţională, cu forțele militare convenționale pentru a genera mai multe efecte (*de tip hibrid*). În războiul din Vietnam, Armata Populară a Vietnamului (armata regulată

[1] N.A.: în continuare, vom utiliza acest termen pentru a defini acţiunile care nu se încadrează în spectrul celor militare tradiţionale şi care sunt desfăşurate de către forţe armate regulate (*irregular* – en.)

nord-vietnameză) şi-a sincronizat operațiile cu Viet Cong-ul, o forţă formată din gherile şi armate regulate, pentru a susține un conflict de lungă durată împotriva a două dintre cele mai puternice forţe convenționale ale lumii: Franța și SUA.

În războiul Israel-Hezbollah din 2006, actorul nestatal libanez Hezbollah a combinat mijloace tehnice, armament şi acţiuni specifice războiului convențional și neconvențional pentru a lupta împotriva celei mai mari puteri militare convenționale din Orientul Mijlociu, Forţele Israeliene de Apărare (Israel Defense Forces – *IDF*). Privind apariţia amenințării de tip hibrid, Hezbollah, o grupare relativ amorfă, este reprezentativă din multe puncte de vedere. Cele 34 de zile de luptă (12 iulie -14 august) din sudul Libanului au scos în evidenţă unele deficienţe ale Forţelor Israeliene de Apărare, aspecte de care planificatorii americani au ţinut cont în acţiunile ulterioare ale forţelor proprii. Prin mixarea unei mișcări politice organizate cu celule descentralizate care au folosit tactici specifice în zonele neguvernate, Hezbollah a arătat că poate provoca foarte multe pierderi. Celulele sale formate din luptători extrem de bine pregătiți şi disciplinaţi, distribuite în teren într-o configuraţie descentralizată, au acţionat împotriva unei forţe convenționale moderne, folosind un amestec de tactici de gherilă, dar și armament şi tehnică de luptă moderne, în centrele urbane dens populate. Hezbollah, ca şi apărătorii extremişti islamici în luptele din Fallujah în Irak (aprilie – noiembrie 2004), au exploatat abil zonele urbane pentru a crea ambuscade şi a evita să fie descoperiţi, organizând totodată puternice fortificații defensive în imediata apropiere a necombatanților[2]. Liderii Hezbollah descriau forţele lor ca fiind o combinaţie între forţe militare regulate şi forţe de gherilă, fiind convinşi că au dezvoltat o nouă structură de forţe. Această structură de forţe consta într-un amestec de miliţii şi grupuri de luptători extrem de bine instruiţi care întrebuinţau armament şi tehnică ultramoderne cum ar fi rachete antitanc dirijate, rachete operative şi tactice, drone, rachete antinavă şi echipamente de

[2] Andrew Exum, *Hizballah at War: A Military Assessment*, Policy Focus #63, Washington Institute for Near East Policy, Washington DC, Decembrie 2006, disponibil la http://www.washington institute.org/uploads/Documents/pubs/PolicyFocus63.pdf accesat la 11.04.2019.

supraveghere radio. Misiunile acestei forţe ocupau o paletă diversă, de la acţiuni de luptă directă şi până la acţiuni de gherilă, hărţuire sau operaţii informaţionale. Toate acestea recomandă războiul Israel-Hezbollah din 2006 ca pe un exemplu „de manual" pentru confruntarea de tip hibrid. Desigur că după aceea configuraţia ameninţării de tip hibrid s-a modificat dramatic, în combinaţie intrând multe alte componente, cele mai multe cu un caracter subversiv, orientate pe abordarea *soft-power*, aşa cum va fi prezentat în continuare.

În fiecare dintre aceste cazuri istorice se pot observa variante de manifestare a ameninţării hibride împotriva unor actori care întrebuinţează, în mod preponderent, forţe armate regulate în acţiuni convenţionale. Pe baza lor se pot crea analize care să ducă la anticiparea modului de manifestare a amenințărilor hibride în viitor. Dacă în istorie acest model de aplicare a artei operative a dus la rezultate diferite în funcție de actor, posibilităţile de coordonare şi organizare a acţiunilor convenționale și neconvenționale desfăşurate în mediul operaţional modern creează o nouă paradigmă în ceea ce priveşte caracterul amenințării, organizarea și gândirea militară.

În continuarea acestui capitol vom prezenta definirea din punct de vedere etimologic şi conceptual a termenului *ameninţare hibridă*.

Ameninţare – termenul *ameninţare* provine din cuvântul latin *amminaciare* şi presupune actul de „a arăta intenția de a face rău cuiva (pentru a-l intimida sau pentru a obține ceva de la el)"[3]. Alte definiţii ale ameninţării sunt „cineva sau ceva care poate cauza probleme sau poate face rău" sau „posibilitatea ca ceva rău să se întâmple"[4]. Nivelul de ameninţare al unei acţiuni este apreciat în funcţie de capacitatea de a produce rău împreună cu intenţia de a face rău. Aducând conceptul de ameninţare în planul securităţii naţionale şi internaţionale, „amenințările reprezintă capacități, strategii, intenții ori planuri ce pot

[3] ***, *Dicţionarul explicativ al limbii române* (ediţia a II-a revăzută şi adăugită), Editura Univers Enciclopedic Gold, 2009, disponibil la http://dexonline.ro/definitie/amenintare

[4] ***, *Merriam Webster Dictionary*, disponibil la http://www.merriam-webster.com/dictionary/threat

afecta valorile, interesele şi obiectivele naţionale de securitate”[5]. Un actor poate să aibă un potenţial suficient pentru a ataca un alt actor, dar dacă nu îşi manifestă intenţia să o facă, el nu este considerat o ameninţare. De asemenea, un actor poate avea intenţia de a ataca un alt actor dar dacă potenţialul acestuia de a provoca pierderi celuilalt este unul scăzut, el este considerat o ameninţare de nivel scăzut (spre exemplu Cuba *vs.* SUA, în anii ‘60). Desigur că dacă adăugăm conceptului de ameninţare şi probabilitatea de a se manifesta şi îl privim prin prisma efectelor generate, obţinem riscul, ca efecte (consecinţe) posibile ale unei ameninţări probabile.

Hibrid – termenul *hibrid* provine din cuvântul latin *hybrida* fiind preluat apoi în limba franceză ca *hybride*. În sens propriu, el este utilizat în biologie, pentru a descrie „un organism provenit din încrucișarea a doi indivizi de specii, de soiuri, de genuri sau de rase diferite”[6]. În alte domenii, termenul a fost preluat cu sens figurativ, pentru a defini concepte (noţiuni, idei şi acţiuni) rezultate din combinarea unor elemente fără o legătură evidentă între ele şi, oarecum, lipsite de armonie.

Ameninţare hibridă – deşi s-a făcut de multe ori referire la termenul *ameninţare hibridă*, acesta nu a fost utilizat în mod explicit sau definit până spre sfârşitul primei decade a anilor 2000, după ce o serie de cercetători, cum ar fi Frank Hoffman sau Russel W. Glenn, au încercat să găsească o sintagmă care să caracterizeze războiul dintre Israel şi gruparea Hezbollah (2006). În plus, putem remarca faptul că *ameninţarea hibridă* este adesea confundată din punct de vedere conceptual cu termenii *război hibrid* sau cu *război combinat* (*compound war*[7]) ajungându-se la o anumită omisiune doctrinară și conceptuală. Mai mult, termenii agreaţi în limba engleză sunt *hybrid threat* (utilizat în special de către forţele armate) şi *hybrid warfare* (specific mediului academic), iar dacă pentru primul se poate găsi o traducere adecvată în

[5] ***, Strategia naţională de apărare a ţării pentru perioada 2015 - 2019, Bucureşti 2015, Cap. III, p. 14.
[6] ***, *Dicţionarul explicativ al limbii române* (ediţia a II-a revăzută şi adăugită).
[7] N.A.: vezi lucrarea lui Thomas M. Huber, *Compound Warfare: That fatal knot*, publicată în anul 2002.

limba română (*ameninţare*), pentru cel de-al doilea nu există un singur cuvânt care să aibă aceeaşi semnificaţie în limba română precum cea din limba engleză (*războială* nu are un caracter ştiinţific). În literatura de specialitate românească este utilizat des termenul *război hibrid* ca o traducere inexactă a termenului *hybrid warfare*. Pe lângă aceasta, termenul de *război* este unul cu sens general, având o conotaţie chiar metaforică, fără un fundament ştiinţific sau, mai mult, juridic (deşi termenul *stare de război* există în legislaţia românească, fără ca termenul *război* să fie definit[8]). De aceea, considerăm că, probabil, cei mai potriviţi termeni pentru a reda semnificaţia constructului *hybrid warfare* sunt, în funcţie de context, *agresiune hibridă* sau *acţiune hibridă specifică războiului*, deşi acesta din urmă este uneori prea lung şi dificil de utilizat în construcţii literare.

Un alt aspect al problemei legată de terminologie se referă la diferenţa dintre *ameninţare hibridă* şi *agresiune hibridă*. Termenul a*meninţare hibridă* este utilizat în virtutea faptului că, atâta timp cât agresiunea de tip hibrid nu a fost definită complet şi, ca atare, nu poate fi demonstrată şi incriminată, cea mai bună modalitate de a implementa contramăsurile necesare este prevenirea manifestării acesteia în mod deschis, adică transformarea ei în *agresiune hibridă*. În acest fel, *contracararea ameninţării de tip hibrid* trebuie privită, în special, ca un set de acţiuni ce trebuie să se încadreze într-o abordare proactivă. Cu alte cuvinte, actorul care ajunge să întrebuinţeze agresiunea de tip hibrid implementează o combinaţie inteligentă de acţiuni atât de disimulate, care nu pot fi dovedite, şi într-o configuraţie atât de nouă încât, deocamdată, la nivel internaţional nu există o legislaţie care să conţină criterii de incriminare şi acţiuni de amendare a acesteia. Întrucât o mare parte dintre aceste acţiuni sunt îndreptate împotriva subminării instrumentelor de putere a statului ţintă, astfel încât în faza de atac, adică de manifestare propriu-zisă a ameninţării de tip hibrid (agresiunea de tip hibrid), ţinta să nu se mai poată apăra, abordarea proactivă este pe deplin cea mai justificată.

[8] N.A.: vezi legea nr. 355/2009 privind regimul stării de mobilizare parţială sau totală a forţelor armate şi al stării de război.

În prezent, în rândul specialiştilor militari de pe mapamond se află în curs de desfăşurare o dezbatere cu privire la ameninţările din mediul operaţional al viitorului. La prima vedere, aceasta poate fi încadrată ca o alegere dihotomică între acţiuni de tip convenţional şi neconvenţional, lucru care ar simplifica oarecum planificarea apărării şi luarea deciziilor de alocare a resurselor. În realitate, situaţia comportă un aspect total diferit, întrucât tendinţele contemporane indică existenţa unor oponenţi care pot angaja simultan multiple forme de acţiune aparţinând ambelor categorii. Astfel de ameninţări multimodale au fost denumite *ameninţări hibride*. Adversarii care implementează componente ale ameninţării de tip hibrid întrebuinţează combinaţii de capabilităţi pentru a genera agresiuni hibride în scopul obţinerii unui avantaj semnificativ în cadrul unei confruntări. Angajarea capabilităţilor militare superioare a dus la încercările unor posibili oponenţi de a identifica unele capacităţi şi capabilităţi asimetrice, „de nişă", combinaţii de mijloace tehnologice şi tactici noi, pentru a elimina acest dezechilibru de forţe şi a obţine avantaje de nivel strategic, operativ sau tactic. Aceste încercări au dus la apariţia *ameninţării hibride* care generează, prin manifestarea acesteia, *agresiunea hibridă*[9]. Pe parcursul acestui studiu vom întrebuinţa în mod frecvent cele două concepte (ameninţare hibridă şi agresiune hibridă), în funcţie de context, cu sensurile prezentate mai sus.

În continuare vom detalia definirea conceptuală a termenului de *ameninţare hibridă*, prezentând câteva dintre variantele propuse de către specialiştii militari, adăugând la fiecare dintre ele comentarii pentru ca, în final, să concluzionăm prin prezentarea variantei proprii.

Analistul militar american Russel W. Glenn defineşte termenul *ameninţare hibridă* ca „un adversar care întrebuinţează în mod adaptiv şi simultan o combinaţie de mijloace politice, militare, economice, sociale şi informaţionale, în cadrul unor metode de acţiune convenţionale,

[9] Frank G Hoffman, James N. Mattis, „Future warfare: The rise of hybrid wars", *Proceedings Magazine*, Issue: November 2005, Vol. 132/11/1,233, 2005, https://www.usni.org/magazines/proceedings/archive/story.asp?print=...

neregulate, catastrofice, teroriste și disruptive[10]/criminale. Acest tip de adversar poate include în combinație actori statali și nestatali”[11]. Termenul „*catastrofice*” presupune evenimentele să fie definite ca „orice incident natural sau provocat de om, inclusiv terorismul (anumite forme), care cauzează un număr mare de victime, pagube sau distrugeri sau care afectează grav populația, infrastructura, mediul, economia, moralul și/sau funcţionarea guvernului”[12].

În urma *Conferinţei privind războiul hibrid (U.S. Joint Forces Command hybrid war conference),* care a avut loc pe 24 februarie 2009 în Washington, ameninţarea hibridă a fost definită ca fiind „orice adversar care, în mod adaptiv şi simultan, întrebuinţează în mediul operaţional o combinaţie de mijloace sau activităţi convenţionale, neregulate, teroriste şi criminale. Acest adversar este mai degrabă o combinaţie de actori statali şi nestatali, decât o singură entitate”[13]. În cadrul aceleiaşi conferinţe, Russel W. Glenn a specificat faptul că acest concept este un amalgam sofisticat de activităţi fără restricţie. O ameninţare hibridă este caracterizată prin conducere descentralizată, activităţi militare şi non-militare întrebuinţate simultan, combinarea tradiţionalului, confruntărilor asimetrice, acţiunilor teroriste şi metodelor criminale disruptive în condiţii de mediu operaţionale complexe, toate cu intenţia de a folosi timpul şi spaţiul pentru a realiza decizia adecvată situaţiei[14].

În doctrina americană, amenințarea de tip hibrid a fost adoptată în 2011, fiind definită ca o combinație diversă și dinamică de forțe regulate, forțe neregulate, elemente criminale sau o combinație a acestor forțe și

[10] N.A.: aici, termenul „disruptiv” semnifică o caracteristică a ceva care cauzează probleme în cadrul unui sistem, prin aceasta întrerupând sau afectând funcţionarea normală a acestuia şi împiedicându-l să funcţioneze aşa cum a fost realizat iniţial.

[11] N.A.: această definiție apare în articolul „Evolution and Conflict: Summary of the 2008 Israel Defense Forces” a lui Russell W. Glenn, prezentat în cadrul *Hybrid Threat Seminar War Game*, Santa Monica, 2009.

[12] ***, JP 1-02, *DOD Dictionary of Military and Associated Terms*, US Department of Defense, mai 2017, p. 32, disponibil la http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf

[13] Russell W. Glenn, „Thoughts on “Hybrid” Conflict”, *Small Wars Jurnal*, 2009 disponibil la http://smallwarsjournal.com/ accesat la 12.04.2019.

[14] Petre Duțu, *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale,* Editura UNAp. „Carol I”, Bucureşti 2013, p. 46.

elemente unificate pentru a obține efecte în interes comun[15]. Amenințările hibride combină operaţiile desfăşurate de forţele regulate, care acţionează conform legilor dreptului internaţional, normelor şi tradiţiilor militare, cu forțe neregulate care acționează fără restricții de violență pentru atingerea obiectivelor urmărite. Forțele neregulate pot include teroriști, trupe de gherilă și criminali şi combină abilitățile de a întrebuinţa arme și tactici cu caracter regulat şi neregulat, tranziţia între ele realizându-se în funcţie de situaţie. Aceste abilități generează amenințări hibride care, întrebuinţate împotriva vulnerabilităţilor unui inamic convenţional, devin extrem de eficace[16].

În mod neîndoielnic, delimitările dintre acţiunile actorilor statali şi nestatali (insurgenţi, terorişti, gherile şi membri ai crimei organizate) sunt dificil de evidenţiat, existând permanent posibilitatea confruntării cu un adversar care utilizează mijloace convenţionale şi neconvenţionale. Situaţia creată poate duce la apariţia unui amalgam de ameninţări, aplicate de actori aparent întâmplători sau necoordonaţi, denumite ameninţări hibride când sunt utilizate într-o manieră simultană şi coordonată de către un adversar determinat. Aceşti adversari utilizează ameninţările hibride pentru a exploata vulnerabilităţile forţelor proprii, iar situarea lor în afara cadrului legal şi etic le permite să genereze provocări de natură militară care se manifestă în moduri dificil de anticipat.

Contracararea ameninţărilor hibride este posibil să solicite concentrarea eforturilor pentru acţiuni cu efect în domeniul moral, cărora le urmează câştigarea încrederii populaţiei. Totodată, adversarii pot opta pentru o strategie pe termen lung, prin care să evite înfrângerea în locul câştigării victoriei. Este foarte probabil ca succesul în contracararea ameninţărilor hibride să nu fie obţinut prin întrebuinţarea exclusivă a instrumentului militar, în aceste situaţii fiind necesară o nouă

[15] Fleming, Brian P, *Hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art*, United States Army Command and General Staff College, 2011 disponibil la https://apps.dtic.mil/dtic/tr/fulltext/u2/a545789.pdf, accesat la 04.05.2019.
[16] ***, ADRP 3-0 *Unified Land Operations*, Washington, noiembrie 2016.

abordare cuprinzătoare, sprijinită de efortul concertat a tuturor instrumentelor de putere, inclusiv de operaţii informaţionale[17].

Frank G. Hoffman defineşte ameninţarea hibridă ca „orice adversar care întrebuinţează în mod simultan şi adaptiv o combinaţie de arme convenționale, tactici neregulate, terorism și comportament criminal în spațiul de luptă pentru a-şi atinge obiectivele politice”[18]. Se observă că în definiţia lui, Hoffman foloseşte termeni care fac referire la acţiuni de nivel tactic-operativ. El nu include în definiţia lui acţiuni cu efect strategic din mediul politic, economic sau social. În continuare, Hoffman consideră că există o legătură foarte strânsă între acţiuni cu caracter asimetric cum ar fi terorismul, crima organizată, traficul de droguri şi de fiinţe umane şi acţiuni întreprinse în scopul subminării legitimităţii guvernului sau autorităţilor locale şi generării sau amplificării crizei. Producţia de opium în Afganistan sau grupurile de crimă organizată pe continentul american (în special în Mexic) sunt factori perturbatori care vin în sprijinul teoriei sale.

În esenţă, în conflictul modern, nu mai există ameninţări separate, cu abordări fundamental diferite. Oponenţii întrebuinţează diferite forme de acţiune şi tactici, de cele mai multe ori simultan. În războiul de tip hibrid se poate observa o convergenţă a unor ameninţări de tip neregulat, în care adversarii au o abordare cuprinzătoare pentru a-şi atinge obiectivele. Reiterăm faptul că, ameninţarea hibridă nu este una vizibilă şi ca atare nu poate fi dovedită şi amendată de legile internaţionale. Sunt întrebuinţate mijloace tehnologice de ultimă generaţie în operaţii de tip asimetric urmându-se tactici neaşteptate. Cu alte cuvinte, sistemele de armament şi tehnica militară sunt întrebuinţate, uneori chiar şi de către intermediari, în moduri noi, utilizând tactici, tehnici şi proceduri inovative.

Fizionomia conflictului prezentată anterior se aplică perfect situaţiei din Ucraina, de vreme ce sunt întrebuinţate simultan acţiuni de gherilă, combinate cu acţiuni specifice războiului informaţional,

---

[17] ***, *Doctrina Armatei României*, Bucureşti, 2012, art. 0208, Al. (4).

[18] Frank G. Hoffman, „Hybrid vs. compound war”, *Armed Forces Journal*, 1 octombrie 2009, disponibil la http://www.armedforcesjournal.com/hybrid-vs-compound-war/ accesat la 11.04.2019.

cibernetic, economic şi chiar politic, pe fondul unei ample operaţii psihologice, menită să expună vulnerabilităţile statului şi să provoace destabilizarea autorităţilor publice şi haos.

Pentru analiză, abordarea rusească a ameninţării de tip hibrid presupune întrebuinţarea concertată a cinci elemente cheie, pe care le prezentăm mai jos[19].

1. *Toate acţiunile se desfăşoară sub acoperirea legii (по закону)* – elementul central în strategia rusească este crearea unui aspect de legalitate în scopul evitării răspunderii în faţa organismelor de securitate internaţionale. Un exemplu relevant este desfăşurarea referendumului privind statutul peninsulei Crimeea. Acesta a avut loc fără supraveghere internaţională, Moscova reuşind să orchestreze anexarea acestui teritoriu ca o urmare a „voinţei populaţiei locale".

2. *Demonstraţia de forţă militară* – Rusia a dislocat importante forţe şi mijloace militare în proximitatea graniţei cu Ucraina în scopul pregătirii şi, la nevoie, intervenţiei în forţă pe teritoriul acesteia pentru rezolvarea situaţiei de criză.

3. *Balul mascat al lui Putin (zece verzi mititei)* – Rusia a întrebuinţat pe teritoriul Ucrainei structuri de forţe speciale fără însemne militare care au acţionat ca „forţe de securitate locale". Scopul acestor operaţii a fost crearea posibilităţii intervenţiei ruseşti în zonă pentru a proteja populaţia de naţionalitate rusească, fără ca acest lucru să atragă o răspundere în mediul internaţional.

4. *Avantajul creat de tensiunile din zonă şi de miliţiile locale* – înainte de a începe acţiunile militare, Rusia „şi-a protejat cetăţenii din zonă" prin gruparea şi susţinerea minorităţilor ruseşti nemulţumite. Prin aceasta şi-a asigurat un paravan pentru a desfăşura intervenţii în forţă pe teritoriul Ucrainei.

5. *Propagandă sau simple minciuni nevinovate?* Conştientă fiind de importanţa mass-media la nivel regional şi global, Rusia a transformat informaţia într-o armă redutabilă, desfăşurând o amplă

[19] Rebecca Blum, *The future of NATO in the face of hybrid conflict*, Bernard El Ghoul, International Relations, Academic year 2014/2015.

campanie de dezinformare şi manipulare a maselor, care a inclus mai multe componente:

-*dezinformare sistematică şi ţintită* – a fost întrebuinţată de multe ori, un exemplu fiind mişcarea populară *Euromaidan* (21 noiembrie 2013 – 23 februarie 2014) care a fost caracterizată ca fiind fascistă în scopul activării sentimentului de luptă a poporului rusesc împotriva Germaniei naziste;

-*negare credibilă* – oficialii ruşi au oferit explicaţii bizare privind unele din acţiunile presupuse a fi desfăşurate de către Rusia pe teritoriul Ucrainei şi scopurile urmărite. Spre exemplu, putem menţiona argumentul adus în sprijinul negării apartenenţei „verzilor mititei" la Rusia, potrivit căruia uniformele lor pot fi cumpărate din orice magazin de haine *second-hand*;

-*acoperirea umanitară* – Kremlinul a încercat să atragă sprijinul din partea mediului internaţional prin motivarea acţiunilor sale cu argumente umanitare;

-*Noua Rusie (Novorossiya)* – au fost invocate argumente istorice care să motiveze ajutorul dat de către ruşi rebelilor din estul Ucrainei.

Analizând aceste definiții ale termenului *ameninţare hibridă* se poate observa că punctul lor comun constituie faptul că provocarea este cu siguranţă mai mult decât una militară. Exemplul celui de-al doilea război din Liban susține această teză. Acele 34 zile din iulie-august 2006 au fost doar un vârf de violență în timpul unui conflict care a durat ani de zile și continuă și astăzi. O victorie rapidă ar fi fost mult mai reconfortantă pentru cetățenii Israelului, însă nici aceasta nu ar fi pus capăt conflictului. Hezbollah este mai mult decât o forță militară, este o organizaţie politică şi paramilitară și tocmai acest lucru îi conferă puterea reală. Ea are componente politice, sociale, diplomatice și informaționale care creează fundamentul pentru structura sa militară. Această fundație, constituită şi consolidată de-a lungul anilor prin asigurarea de ajutor umanitar, construirea infrastructurii fizice şi educarea cetăţenilor libanezi ar fi rămas chiar și în urma înfrângerii militare. Ca şi rădăcinile adânci ale unei plante, celelalte componente

care dau forţă organizaţiei Hezbollah ar fi generat în timp noi forțe pentru a le înlocui pe cele pierdute în luptă.

Tot din analiza definiţiilor de mai sus, rezultă o serie de probleme care se pot constitui în criterii privind atribuirea caracterului hibrid al ameninţării: *modul de acţiune şi structura forţelor; simultaneitatea; fuziunea; multimodalitatea.*

Modul de acţiune şi structura forţelor – acest criteriu determină apariţia unor întrebări. Ameninţarea poate fi considerată hibridă după criteriul modului de desfășurare a luptei sau după structura forţei? Este de ajuns satisfacerea unei singure condiţii sau sunt necesare ambele? Considerăm că aspectul hibrid al unei amenințări este dat, în primul rând, de modul de manifestare al acesteia, astfel încât, este suficient ca agresorul să întrebuințeze simultan metode convenționale și neconvenționale pentru atingerea obiectivelor urmărite. Forța care aplică amenințarea are structura impusă de situație.

Simultaneitatea – ameninţarea poate fi considerată hibridă dacă are în compunere tipurile prezentate în majoritatea definiţiilor în mod simultan sau este de ajuns ca ele să se manifeste succesiv, pe toată durata conflictului? Putem considera că amenințarea are caracter hibrid dacă presupune manifestarea în mod simultan a agresiunii în cel puțin două domenii dintre cele enumerate.

Fuziunea – ameninţarea poate fi considerată hibridă dacă forţele regulate şi neregulate acţionează împreună sau dacă ele acţionează în zone diferite? Iar dacă acţionează în zone diferite, acţiunile celor două tipuri de forţe trebuie să fie coordonate sau nu? Indiferent de zona în care acționează sau de nivelul de coordonare realizat, condiția care trebuie îndeplinită este ca obiectivul urmărit de către cele două tipuri de forțe să fie comun.

Multimodalitatea – ameninţarea poate fi considerată hibridă dacă se întrebuinţează toate cele patru tipuri de ameninţare sau sunt suficiente două sau trei? Un actor care întrebuințează amenințări de tip hibrid va include cât mai multe tipuri de acțiuni, în funcție de resursele de care dispune și de vulnerabilitățile oponentului. Considerăm că două sau mai multe tipuri de amenințare întrebuințate combinat duc la o rezultantă de tip hibrid.

În articolul său *Thoughts on "Hybrid" Conflict*, publicat în *Small wars journal* în anul 2009, Russel W. Glenn realizează o relaţionare între termenii *abordare cuprinzătoare (comprehensive approach)*, *guvern unitar (whole of government)* şi *operaţii în întregul spectru (full spectrum operations)*[20] utilizând tocmai exemplul războiului Israel-Hezbollah, prezentat mai sus. Cheia puterii organizaţiei Hezbollah este o capacitate pe care multe naţiuni dezvoltate o caută în dinamica lor spre atingerea obiectivelor strategice şi anume abordarea cuprinzătoare. Armata canadiană a făcut progrese importante în înţelegerea şi realizarea practică a relaţiei dintre *abordarea cuprinzătoare* şi *guvernul unitar*. David Lambert, ofiţer în armata canadiană, explică faptul că abordarea cuprinzătoare presupune utilizarea tuturor instrumentelor de putere pentru a accesa toate sistemele prezente în mediul operaţional şi care pot avea un rol în managementul crizei în curs.

În virtutea celor prezentate anterior, un stat trebuie să întrebuinţeze diverse agenţii cu obiect de activitate din diferite domenii pentru realizarea unui scop comun. Este legea unităţii acţiunilor aplicată la scară naţională. Dacă nivelul este restrâns la nivelul instituţiilor guvernamentale, se deduce termenul de *guvern unitar*. Pe acelaşi principiu, în cadrul abordării cuprinzătoare sau, mai exact, în cadrul acţiunilor desfăşurate la nivel de guvern unitar, componenta militară execută operaţii în întregul spectru. R.W. Glenn evidenţiază faptul că, în statele cu un nivel de dezvoltare ridicat, aplicarea legii unităţii acţiunilor în operaţiile desfăşurate pentru atingerea obiectivelor strategice întâmpină greutăţi din cauza „multiplelor straturi ale structurii organizaţionale şi a birocraţiei care le acompaniază".

În definirea termenului de *ameninţare hibridă* trebuie să avem în vedere faptul că aspectul hibrid al ameninţărilor din mediul operaţional contemporan se manifestă în cel puţin două planuri: *structural* şi *acţional*.

[20] N.A.: în doctrina militară americană, termenul „*full spectrum operations*" a fost înlocuit cu „*decisive actions*" prin publicarea în 16 mai 2012 a ADRP 3-0 (Army Doctrine reference publication).

În *plan structural,* ameninţările de tip hibrid pot fi utilizate atât de către actorii statali, cât şi de către cei nestatali. Indiferent de structura organizaţională a acestora, configuraţia forţelor care aplică aceste ameninţări este cea care are un caracter hibrid. De cele mai multe ori, aceste forţe sunt constituite ca o „mixtură" mai mult sau mai puţin organizată de forţe regulate, forţe neregulate, forţe speciale şi indivizi sau grupuri cu abilităţi în domenii speciale, cum ar fi operaţiile psihologice, operaţiile informaţionale (manipularea maselor, spionaj etc.), influenţarea deciziilor la nivel politic sau economic etc.

În *plan acţional* se vizează atingerea obiectivelor stabilite prin utilizarea oricăror metode sau mijloace de acţiune, atât de natură convenţională, cât şi neconvenţională. Trecerea de la convenţional la neconvenţional se face rapid, în funcţie de situaţie (adversar, mediu, vulnerabilităţi, timp la dispoziţie etc.).

Ținând cont de toate aspectele analizate mai sus, putem defini amenințarea hibridă ca un adversar de tip statal sau nestatal care întrebuinţează în mod adaptiv și concertat mijloace politice, militare, economice, sociale sau informaţionale, în cadrul unor combinații de metode de acţiune convenționale și neconvenționale, executate sub acoperire sau descoperite, sub limita pragului de stare de război declarată oficial, în scopul realizării obiectivelor urmărite.

Termenul *ameninţare hibridă* are o construcţie interesantă şi valoroasă, întrucât cu ajutorul lui se realizează următoarele deziderate:

- descrierea caracterului evolutiv al conflictului modern;
- schimbarea modului de gândire tradiţional și impulsionarea analiştilor militari în efortul lor de a găsi noi metode şi mijloace de adaptare acţională şi organizaţională a forţei la provocările mediului operaţional contemporan;
- evidenţierea provocărilor pe care le generează conflictele moderne sub forma unei perspective mult mai complexe decât manifestarea în mod disparat a unor ameninţări;
- evidenţierea necesităţii ridicării gradului de conştientizare a riscurilor potențiale din mediul operaţional al viitorului.

Pentru a avea o abordare structurată, vom prezenta în continuare tipologia ameninţărilor în mediul operaţional contemporan, pornind de la faptul că ameninţările reprezintă state, naţiuni, organizaţii, indivizi, grupuri sau condiţii care pot pune în pericol viaţa cetăţenilor, resursele vitale sau instituţiile. Pregătirea şi aplicarea acestor ameninţări presupune întrebuinţarea tuturor instrumentelor de putere afectând toate variabilele mediului operaţional, în special pe cele din sfera politică, militară, informaţională şi economică.

În încercarea de a conceptualiza ameninţările prezente în mediul operaţional viitor, Andrew J. Bacevich a identificat două tabere antagoniste: *cruciaţii* şi *tradiţionaliştii*[21]. Primii susţin faptul că ameninţările viitorului se vor concentra pe ameninţări asimetrice urmând modelul contrainsurgenţei. Ca atare, forţa militară cu misiunea de a contracara un asemenea tip de ameninţări trebuie să-şi concentreze eforturile pentru a fi suficient de flexibilă încât să facă faţă unui oponent care întreprinde acţiuni neregulate, complexe şi, de cele mai multe ori, neconvenţionale. Pe de altă parte, tradiţionaliştii susţin faptul că în continuare, ameninţările prezente în conflictele viitorului vor fi de tip convenţional şi, ca atare, forţa întrebuinţată trebuie să aibă o structură care să desfăşoare acţiuni de luptă împotriva unui oponent convenţional.

La rândul lui, Frank G. Hoffman identifică patru curente prezente pe eșichierul conceptual american: *contrainsurgenţii* – configurează viitorul oponent ca unul neregulat, *tradiţionaliştii* – susţin predominanţa inamicului convenţional, *variaţioniştii* – consideră că o forţă suficient de agilă, pregătită pentru a executa întregul spectru de operaţii, va putea contrabalansa multiplele riscuri şi ameninţări şi *diviziunea muncii* – consideră că forţa viitorului trebuie să fie compusă din structuri specializate pentru contracararea câte unui tip de ameninţare[22].

[21] Andrew J. Bacevich, „The Petraeus Doctrine", *The Atlantic*, octombrie 2008, disponibil la https://www.theatlantic.com/magazine/archive/2008/10/the-petraeus-doctrine/306964/, accesat la 12.04.2019.

[22] Frank G. Hoffman, *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies, National Defense University, Strategic Forum No. 240, Aprilie 2009, disponibil la http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=98862 accesat la 13.05.2019.

Nathan Freier a fost unul dintre iniţiatorii conceptului *ameninţare hibridă* pe vremea când lucra la Strategia Naţională de Apărare în Biroul Secretarului Apărării din SUA. El a introdus termenul *patru cadrane (quad chart)* care defineşte cele patru tipuri de ameninţări: *tradiţionale* (convenţionale), *neregulate* (neconvenţionale), *catastrofice* şi *perturbatoare*[23]. Inamicul poate întrebuinţa una sau mai multe tipuri de ameninţări, consecutiv sau simultan, pentru a-şi atinge scopurile urmărite, rezultatul fiind manifestarea unei ameninţări de tip hibrid. Concepţia prin care un actor implicat în conflict întrebuinţează ameninţarea de tip hibrid se bazează pe exploatarea tehnologiei şi/sau a oricăror metode de ducere a luptei pentru a contrabalansa sau chiar a anula superioritatea militară a adversarului. Această idee a fost preluată în strategia militară de apărare şi în doctrina militară americană care consemnează faptul că cel mai complex tip de ameninţare este o combinaţie a tuturor celor patru[24].

Ameninţările tradiţionale sunt realizate, de regulă, prin capabilităţi convenţionale. Forţele sunt bine definite şi întrebuinţează tactici, tehnici şi proceduri prezente în doctrinele proprii, precum şi sisteme de armament convenţional care vizează în primul rând forţa militară a oponentului, fie că sunt forţe armate regulate sau forţe pentru operaţii speciale. Confruntarea tradiţională dintre cele două forţe se desfăşoară prin ducerea luptei armate caracterizată de acţiuni cu caracter militar, în spaţiul aerian, terestru şi naval, cu respectarea tratatelor şi convenţiilor internaţionale şi a normelor privind dreptul internaţional umanitar. Atunci când ne referim la convenţii, înţelegem în primul rând acele aspecte legale şi morale (tradiţii, reguli şi obiceiuri), completate de limite materiale (dimensiune tehnologică) şi fizice (caracteristicile mediului de confruntare), cunoscute şi acceptate de către beligeranţi.[25]

Statele cu un nivel ridicat de dezvoltare şi alianţele militare de pe mapamond au dezvoltat forţe convenţionale cu o mare putere de luptă pentru a fi în măsură să realizeze superioritatea militară în orice conflict

[23] N.A.: Termenul în limba engleză este *disruptive*.
[24] Frank G Hofmann, *Hybrid vs. Compound war*, 1 octombrie 2009, disponibil la http://www.armedforcesjournal.com/hybrid-vs-compound-war/ accesat la 15.07.2019.
[25] Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013, p. 10.

ar fi implicate. Această superioritate are şi rolul de a descuraja un eventual agresor. Însă, problema actuală cea mai importantă şi totodată caracteristica esenţială o reprezintă faptul că, în cazul ameninţărilor de tip hibrid, operaţiile axate pe ameninţări convenţionale poate reprezenta doar o parte, alături de care se manifestă celelalte tipuri de ameninţări. Este important de precizat faptul că în ansamblul ameninţării de tip hibrid, proporţia ameninţărilor de tip neconvenţional este mult mai mare, ameninţările de tip convenţional (adică acţiunile de luptă de tip *force-on-force*) reprezentând doar o mică parte (sau chiar lipsind) din eșichierul acţiunilor desfăşurate împotriva oponentului. În acest sens, manifestarea ameninţării de tip convenţional este bivalentă: acţiunile militare tradiţionale sunt desfăşurate cu titlu de demonstraţie de forţă, în vederea intimidării oponentului sau sunt desfăşurate ca acţiune decisivă, dar de o anvergură redusă, întrucât oponentul este mult slăbit din cauza efectelor produse de către manifestarea în prealabil a celorlalte tipuri de ameninţări.

Ameninţările de tip neregulat sunt cele generate de către un oponent care foloseşte mijloace neconvenţionale, de cele mai multe ori în contextul unui conflict de tip asimetric, pentru a contrabalansa superioritatea forţei de tip convenţional. Un actor mai slab din punct de vedere militar foloseşte ameninţările de tip neregulat pentru a atrage oponentul într-un război de durată şi a supune forţele acestuia unui grad de uzură ridicat care duce la pierderea sau diminuarea voinţei de a lupta şi, implicit, a forţei de care dispune. Ameninţările de tip neregulat includ *terorismul, insurgenţa, războiul de gherilă, pirateria, extremismul, acţiunile desfăşurate de grupuri de partizani (de rezistenţă), crima organizată* precum, şi *acţiuni subversive*, în special în mediul economic şi politic.

Terorismul – normele de drept internaţional definesc terorismul ca fiind: „folosirea deliberată şi sistematică a unor mijloace de natură să provoace, pe scară largă, teroarea, în vederea atingerii unor scopuri criminale”[26]. Dicţionarul explicativ al limbii române defineşte terorismul ca „totalitatea actelor intenționate de violenţă comise de un grup sau de

[26] Vasile Crețu, *Drept internațional penal*, Editura Societății “Tempus”, București, p. 245.

o organizație pentru a provoca o teamă generalizată și pentru atingerea unor scopuri politice”[27]. În legislaţia românească, terorismul este definit ca „ansamblul de acţiuni şi/sau ameninţări care prezintă pericol public şi afectează securitatea naţională având următoarele caracteristici: sunt săvârşite premeditat de entităţi teroriste, motivate de concepţii şi atitudini extremiste, ostile faţă de alte entităţi, împotriva cărora acţionează prin modalităţi violente şi/sau distructive; au ca scop realizarea unor obiective specifice, de natură politică; vizează factori umani şi/sau factori materiali din cadrul autorităţilor şi instituţiilor publice, populaţiei civile sau al oricărui alt segment aparţinând acestora; produc stări cu un puternic impact psihologic asupra populaţiei, menit să atragă atenţia asupra scopurilor urmărite”[28].

În opinia unor juriști cu renume în drept internațional terorismul este atașat, de regulă, anumitor revendicări care, în imaginaţia autorilor săi, se pot realiza numai prin ameninţări sau alte acte de violenţă menite să arate determinarea lor şi care provoacă teroare. Terorismul este un act în măsură să provoace teamă de un rău oarecare sau de o situaţie nefavorabilă şi care reprezintă o intimidare din toate punctele de vedere. Acesta constă în folosirea actelor de violenţă fizică sau psihică pentru a influenţa indivizi sau grupuri, pentru a semăna spaima generală şi care, prin natura sa, creează un pericol general. Actele de violenţă pot fi comise de indivizi, grupuri sau regimuri politice, de regulă totalitare, având intensitate variabilă.

Se poate afirma că, în esenţa sa, terorismul se realizează prin acte comise într-un anumit mediu, a căror natură produc un sentiment de panică, de insecuritate, de rău inevitabil, generând atât efecte fizice, cât şi psihologice. Ceea ce amplifică gravitatea actului terorist este faptul el că nu poate fi prevăzut, nici ca loc, nici ca moment şi nici ca mod de manifestare şi, ca atare, poate fi prevenit prin măsuri specifice doar într-o oarecare măsură. Se poate afirma cu certitudine faptul că acţiunile de tip terorist sunt acţiuni ilegale, organizate şi desfăşurate sistematic de

[27] ***, *Dicţionarul explicativ al limbii române* (ediţia a II-a revăzută şi adăugită), Editura Univers enciclopedic Gold, 2009, disponibil la http://dexonline.ro/definitie/terorism
[28] ***, Legea nr. 535 din 25 noiembrie 2004 privind prevenirea şi combaterea terorismului.

anonimi, împotriva ordinii de drept, alimentate de puternice motivaţii etnice, religioase, politice sau de altă natură.

Ţinând cont de aceste aspecte, precum şi de evenimentele recente, apreciem că terorismul, pe lângă statutul de faptă penală, a dobândit un caracter de fenomen social generat de cauze bine determinate şi, din păcate, este tot mai bine organizat şi structurat, indiferent dacă se manifestă individual sau în grup. Efectele devastatoare şi caracterul extins al acestui fenomen au determinat necesitatea analizării exhaustive a acestuia în mediul ştiinţific internaţional. Din studiile efectuate, putem realiza o clasificare după diferite criterii a acestui flagel care se manifestă într-o diversitate de forme. În esenţă, ţinând cont de mobilul şi intenţia care generează actul de violenţă în sine, se poate evidenţia terorismul naţional, internaţional, politic, social, de stat, de drept comun, individual şi de grup.

În concluzie, putem afirma că terorismul presupune desfăşurarea de către indivizi sau grupuri special constituite şi organizate, de acte de violenţă sau ameninţare cu violenţa în scopul influenţării unor persoane sau a unui grup ţintă, aflat dincolo de victimele imediate. Acest fenomen este un conflict asimetric dintre un grup sau un număr variabil de indivizi din afara vreunei structuri statale şi una sau mai multe instituţii de stat, organizaţii, categorii sociale, grupuri sau indivizi, purtat de pe poziţii diferite de forţă. Teroriştii utilizează tehnici şi tactici de luptă asimetrice şi mijloace neconvenţionale în scopul atingerii prin acte de violenţă şi sabotaje a unor obiective politice, ideologice, etnice, economice sau de altă natură. Efectul produs este paralizant din punct de vedere psihologic, fiind realizat prin frică şi intimidare şi finalizat prin impunerea prin presiunea exercitată asupra ţintelor, a unor condiţii care să le facă să acţioneze potrivit scopurilor de tip terorist.

Insurgenţa – termenul *insurgent* provine din latinescul *insurgens* şi defineşte o persoană care participă la o insurecţie, adică la o „formă de luptă armată, având ca scop înlăturarea regimului politic existent sau a unei armate ocupante”[29]. În terminologia americană, termenul insurgenţă

[29] ***, *Dicţionarul explicativ al limbii române* (ediţia a II-a revăzută şi adăugită), Editura Univers enciclopedic Gold, 2009, disponibil la http://dexonline.ro/definitie/insurecţie

este definit ca „acțiunile unui grup sau mișcare organizată, motivate adesea ideologic, care încearcă să contribuie sau să împiedice schimbări politice sau să răstoarne o autoritate guvernamentală într-o țară sau într-o regiune, axate pe convingerea sau forțarea populației prin utilizarea violenței și a subversiunii”[30]. Putem deduce că insurgenţa este o acţiune cu un caracter subversiv şi violent desfăşurată în scopul înlocuirii sau răsturnării regimului politic dintr-o zonă sau îndreptate împotriva unei forţe armate ocupante. Deseori, ea este precedată de o stare de revoltă care apare în rândul maselor indigene şi este urmată de insurecţie, care reprezintă forma cea mai violentă de manifestare. Astfel, putem afirma că, de cele mai multe ori, conflictul începe cu mult timp înainte, lucru care permite insurgenţei să se răspândească în rândul populaţiei. Aceasta dezvoltă în cadrul ei grupuri organizate, răspândite pe tot teritoriul ocupat, care acţionează în mod descentralizat, însă urmărind realizarea unui scop comun.

Din analiza conflictelor recente sau încă în desfăşurare rezultă că există o tendinţă de implicare a unor elemente teroriste transnaţionale pentru a completa paleta de acţiuni desfăşurate de către grupurile insurgente indigene. O altă tendinţă este lărgirea ariei acţiunilor desfăşurate de grupurile insurgente, acestea pătrunzând în domeniul politic, comercial, informaţional sau financiar. Rezultă o mişcare cu un caracter complex care, din punct de vedere spaţial, depăşeşte limitele zonei stabilite iniţial, iar acţional, defineşte o mişcare cu un aspect combinat, menit să diminueze puterea politică sau militară a ţintei, facilitând atingerea obiectivelor urmărite.

Spre deosebire de ameninţările convenţionale, în acţiunile de insurgenţă sunt întrebuinţate şi mijloace neletale sau civile care, de cele mai multe ori, sunt extrem de eficiente. Acest tip de acţiuni polarizează voinţa populară indigenă sau internaţională, ducând la diminuarea credibilităţii şi a sprijinului oferit sistemului politic de guvernământ sau forţei militare ocupante. Scopul urmărit este diminuarea nivelului de

[30] ***, AAP-6, *NATO glossary of terms and definitions*, NATO Standardization Agency, 2015, p. 2-I-5.

control şi a legitimităţii acţiunilor puterii politice sau militare stabilite ca ţintă.

Considerăm necesar să precizăm faptul că acţiunile de insurgenţă se desfăşoară de-a lungul unor perioade mari de timp, din cauza faptului că grupările insurgente dispun de resurse limitate şi, din punct de vedere al acţiunilor convenţionale, au o putere de luptă mult redusă faţă de cea a oponentului. Din acest motiv, ele evită confruntarea directă şi decisivă şi execută acţiuni în cadrul cărora exploatează terenul şi populaţia ca acoperire. Modul de acţiune constă în alegerea şi lovirea unor obiective în locul şi momentul în care sunt vulnerabile şi contribuie cel mai mult la atingerea propriilor obiective. Întrebuinţând o combinaţie de acţiuni în forţă, propagandă, acţiuni subversive, intimidare şi influenţă politică, insurgenţii caută să diminueze şi să discrediteze autoritatea politică sau forţa militară, subminându-i capabilităţile, puterea şi voinţa de a lupta, fără a fi necesară confruntarea armată. De cele mai multe ori, aceste acţiuni se bazează pe efectul lor gradual şi cumulativ, amplificat prin propagandă şi aplicat pe o perioadă mare de timp. În final, insurgenţa duce fie la obligarea guvernului sau forţei ocupante să treacă la negocieri, fie la pierderea controlului în zonă, fie la confruntarea armată, în situaţia în care grupările insurgente devin o forţă care să fie în măsură să învingă prin confruntare armată directă guvernul sau armata ocupantă considerată ţintă.

Insurgenţa generată de obiective comerciale sau infracţionale (carteluri de droguri, trafic de fiinţe umane etc.) are un caracter aparte întrucât obiectivul acesteia nu constă în răsturnarea regimului politic existent şi asumarea guvernării zonei. În această situaţie, obiectivul urmărit este controlul aparatului de stat prin intimidare, mită, violenţă sau alte mijloace care să permită insurgenţilor desfăşurarea fără restricţii a activităţilor ilicite, în timp ce sistemul politic existent îşi continuă activităţile de guvernare a populaţiei indigene.

Războiul de gherilă – denumit şi *micul război,* provine din limba spaniolă (*guerilla*), fiind preluat în franceză sub forma *guérilla* şi reprezintă denumirea dată partizanilor din Spania şi ţările Americii Latine. În limba spaniolă, membrii *guerillei* sunt denumiţi

guerrillero dacă sunt bărbaţi sau *guerrillera* dacă sunt femei. El defineşte grupuri sau detaşamente, de regulă paramilitare, formate din adepţi ai unei doctrine sau idei de sorginte diversă, care luptau pentru atingerea unor obiective comune. În terminologia NATO, războiul de gherilă este definit ca „operaţii militare sau paramilitare desfăşurate în teritoriul ostil sau deţinut de către inamic de către forţe neregulate, predominant indigene”[31].

Obiectivele acestui tip de acţiuni sunt, în general, la nivel local şi vizează obţinerea unor drepturi, schimbarea regimului politic local, eliberarea teritoriului propriu, separatism teritorial, autonomie sau independenţă statală. Tacticile utilizate sunt bazate în special pe acţiuni cu mobilitate ridicată, cum ar fi ambuscadele, atentatele, incursiunile, raidurile, sabotajul și atacurile surpriză asupra unor ținte vulnerabile ale inamicului. În esenţă, acţiunile de gherilă se bazează pe superioritatea cunoaşterii terenului şi pe sprijinul populaţiei din zonă. Ele se desfăşoară fără respectarea regulilor luptei armate, fără o ritmicitate sau logică şi fără a se ţine cont de anotimp, timp sau starea vremii, în grupuri mici, de regulă înarmate cu armament uşor. Obiectivele urmărite sunt uzarea fizică şi morală a inamicului prin provocarea de pierderi materiale sau umane fără o confruntare directă.

Pirateria – termenul provine din limba franceză (*piraterie*) şi este definit ca „faptă prin care membrii echipajului unui vas, prin amenințări și violență, răpesc un alt vas ori bunurile sau persoanele aflate la bordul acestuia”[32]. Ulterior, a apărut şi *pirateria aeriană* care presupune „un act de amenințare și de violență săvârșit de o persoană sau de un grup înarmat asupra echipajului unui avion în scopul schimbării rutei acestuia”[33]. Totuşi, pirateria pe mare constituie principala formă de manifestare a acestui fenomen, care se estimează că produce daune în valoare de aproximativ 16 miliarde de dolari pe an. În prezent, acte de piraterie sunt semnalate în special în zona dintre Marea Roşie şi Oceanul

[31] ***, AAP-6, *NATO glossary of terms and definitions*, NATO Standardization Agency, 2015, p. 2-G-4.
[32] ***, *Dicţionarul explicativ al limbii române* (ediţia a II-a revăzută şi adăugită), Editura Univers enciclopedic Gold, 2009, disponibil la http://dexonline.ro/definitie/piraterie
[33] *Ibidem.*

Indian, în zona coastelor Somaliei, în strâmtoarea Malacca şi în zona portului Singapore. Actele de piraterie săvârşite în zona Somaliei au determinat încredinţarea unor misiuni de patrulare în zona Cornului Africii unei forţe multinaţionale, condusă de către SUA, la care au participat şi nave româneşti.

Modul de operare al piraţilor în epoca modernă se bazează pe atacuri desfăşurate cu nave de mici dimensiuni, cu grupuri mici de piraţi care profită de efectivele reduse ale marinarilor de pe navele de transport moderne. Piraţii întrebuinţează şi nave de dimensiuni mai mari pentru a aproviziona navele de bordaj. De obicei atacurile se dau în zone în care ţărmurile sunt apropiate (strâmtori), unde navele de mari dimensiuni sunt vulnerabile. Pirateria este, de asemenea, prezentă şi în zonele de conflict dintre doi actori regionali. Fenomenul se manifestă prin atacarea navelor uneia dintre părţi şi apoi evitarea urmăririi prin pătrunderea în apele controlate de către cealaltă parte. În ultimii ani acest fenomen a luat amploare, numărul atacurilor crescând în mod îngrijorător.

Crima organizată – potrivit Legii nr. 39/2003 privind prevenirea și combaterea criminalității organizate, prin *crimă organizată* înţelegem activităţile desfăşurate de orice grup constituit din cel puţin trei persoane, între care există raporturi ierarhice sau personale, care permit acestora să se îmbogăţească sau să controleze teritorii, pieţe ori sectoare ale vieţii economice şi sociale, interne sau străine, prin folosirea şantajului, intimidării, violenţei ori coruperii, urmărind fie comiterea de infracţiuni, fie infiltrarea în economia reală.

Cu alte cuvinte, crima organizată este definită de existenţa unor grupări infracţionale la nivel naţional sau internaţional care desfăşoară activităţi ilicite în scopul obţinerii de profit. Aceste grupări fac parte din diferite categorii sau „branşe”, în funcţie de tipul de activitate infracţională pe care o desfăşoară. Activităţile desfăşurate includ acţiuni violente (crima, ultrajul, hărţuirea, ameninţarea, şantajul etc.), infracţiuni financiare (evaziunea fiscală, contrabanda, falsificarea de bunuri), acţiuni ilicite în spaţiul cibernetic (fraude pe internet, încălcarea dreptului de autor, lansarea de viruşi informatici), corupţie (trafic de influenţă), trafic de droguri, de arme sau de fiinţe umane.

Grupurile de crimă organizată au, în general, o structură piramidală, cu diferite forme de organizare: bande, triade, familii mafiote, carteluri de droguri etc. Liderul organizaţiei are un stil de conducere autoritar, bazat pe loialitate deplină, pedepsirea aspră şi exemplară a abaterilor de la regulile impuse şi suprimarea libertăţii de acţiune a membrilor. Acţiunile ilicite sunt agresiuni îndreptate fie împotriva populaţiei locale, fie împotriva autorităţilor. Prezenţa acestor grupuri este semnificativă în special în statele subdezvoltate sau eşuate, în zonele în care autorităţile au un nivelul de control mai scăzut sau inexistent. Ameninţarea pe care o reprezintă acest tip de activitate este una semnificativă în contextul mediului operaţional, întrucât ea duce la apariţia sau creşterea nivelului de instabilitate în zonă, în special pe fondul discreditării autorităţilor locale sau a forţei militare prezente în zonă.

Acţiunile subversive – acţiunile subversive presupun acele activităţi desfăşurate de către actori statali sau nestatali care duc la subminarea puterii guvernului, a economiei naţionale, a sistemului politic existent sau sunt întreprinse în mod conspirativ împotriva ordinii sociale şi politice oficiale. Modul de manifestare a acestui tip de acţiuni se bazează în special pe coruperea sau manipularea (prin şantaj, ameninţări, violenţă etc.) unor factori de decizie în domeniul subminat, fie în scopul producerii de daune, fie în scopul obţinerii unor avantaje politice, economice sau de altă natură. Acest tip de ameninţare este îndreptat în special împotriva actorilor statali şi duce la diminuarea puterii politice, militare şi economice a acestora şi, implicit, creşterea nivelului şi diversificarea vulnerabilităţilor care pot fi exploatate.

Ameninţările de tip catastrofic implică întrebuinţarea armelor de distrugere în masă chimice, biologice, radiologice şi nucleare (ADMCBRN). Acest tip de armament dă unui potenţial inamic posibilitatea de a genera efecte catastrofice, dacă este utilizat. Chiar şi când nu sunt utilizate, posesia acestor arme poate genera efecte de natură psihologică, materializate prin descurajarea unui eventual oponent. Este adevărat că descurajarea poate funcţiona ca un mijloc de contracarare a ameninţării de tip catastrofic, însă considerăm necesar să subliniem

faptul că acest tip de răspuns funcţionează preponderent împotriva actorilor de tip statal, la nivelul cărora decizia de întrebuinţare a acestui tip de armament se ia în urma unui proces de anvergură, bazat pe anumite raţiuni şi reglementări internaţionale. În situaţia actorilor de tipul grupărilor teroriste, spre exemplu, situaţia este diferită. Cu alte cuvinte, nu trebuie să ne fie frică de cineva care are câteva zeci de focoase cu încărcătură chimică, biologică, radiologică sau nucleară. Trebuie să ne fie frică de cel care are doar unul.

„ADM şi mijloacele de întrebuinţare a acestora vor prolifera semnificativ dacă nu sunt supuse unui control strict. Un număr limitat de state vor putea dezvolta capabilităţi nucleare militare fără un ajutor extern, însă un număr semnificativ au deja posibilitatea de achiziţie a armelor biologice şi chimice” [34]. În Doctrina Armatei României se evidenţiază faptul că actorii nestatali care pot achiziţiona ADM sunt mult mai dificil de identificat şi contracarat sau descurajat decât actorii statali. Alte tipuri de arme de distrugere în masă care pot deveni accesibile, chiar şi actorilor nestatali, sunt sistemele de armament care utilizează impulsul electromagnetic sau cele cu termen întârziat de letalitate sau nonletale, cum ar fi sistemele de armament radiologic şi cel chimic cancerigen.

Ameninţările perturbatoare (disruptive, en.) constituie un tip de ameninţare care implică, de cele mai multe ori, întrebuinţarea unor instrumente cu grad ridicat de tehnologizare sau metode sofisticate de realizare pentru a reduce avantajele oponentului în domenii cheie. O categorie a acestor domenii este cea legată în special de mediul cibernetic ce include comunicaţiile, capabilităţile de culegere (senzori), prelucrare şi diseminare a informaţiei, capacitatea de a dirija diferite tipuri de armamente etc. Un atac în mediul cibernetic poate duce la dezafectarea sistemelor automatizate, de cele mai multe ori fără a se putea identifica sursa problemei sau a se putea întreprinde contramăsuri. O altă categorie de domenii o reprezintă cele care ţin de mediul informaţional şi de cel moral. Aici se încadrează operaţiile informaţionale (INFOOPS) şi cele psihologice (PSYOPS). Atacurile disruptive pot utiliza metode şi

[34] ***, *Doctrina Armatei României*, Bucureşti, 2012, art. 0208, Al. (2).

mijloace tehnologice care să genereze un asemenea grad de confuzie, încât ţinta să nu înţeleagă natura sau sursa ameninţării.

Agresiuni în mediul cibernetic – în condiţiile mediului operaţional modern tehnologia informaţiei şi comunicaţiilor sunt un *sine qua non* pentru orice tip de putere, militară, politică sau economică. Dinamica acțiunilor care țin de mediul cibernetic este foarte mare, iar importanța acestora în contextul operațiilor militare este una covârșitoare. De aceea, considerăm că amenințările specifice acestui domeniu sunt de prim rang în paleta amenințărilor de tip hibrid. Puterile militare supertehnologizate, bazate aproape exclusiv pe capabilitățile din domeniul cibernetic prezintă unele vulnerabilități care pot fi exploatate de către oponenți net inferiori. Aceștia pot acționa fie direct asupra sistemelor informatice militare prezente în zona de desfășurare a conflictului, fie asupra sistemelor informatice și de securitate din statele care furnizează puterea militară.

Atacurile cibernetice din zona de conflict pot fi executate asupra rețelelor de calculatoare și de comunicații militare şi pot avea obiective variate, cum ar fi întreruperea/interzicerea realizării conexiunii, spionajul cibernetic sau chiar introducerea în sistem a unor informații false.

În ceea ce privește modul de manifestare a amenințării în teritoriul statelor generatoare de forță militară (*homeland*), un scenariu posibil îl constituie atacul asupra unor rețele informatice care gestionează procese de importanță strategică (sistemul de gestionare a distribuției de energie electrică, sistemul de telecomunicații național, sisteme de comunicații interbancare etc.). Preluarea controlului asupra unor astfel de sisteme de către teroriștii cibernetici pot genera efecte devastatoare, pornind de la paralizarea domeniului de activitate atacat și până la manipularea acestuia în interesul atacatorului.

Indiferent de țintă, amenințarea în mediul cibernetic se manifestă într-o dinamică foarte mare pornind de la identificarea vulnerabilităților sistemului atacat, continuând cu desfășurarea atacului sau implementarea virusului informatic și degenerând în preluarea controlului asupra sistemului atacat sau alterarea funcționării lui. În mod paradoxal, avansul tehnologic pe care societatea îl dorește în scopul creșterii eficienței

activităților de orice fel este chiar cel care creează vulnerabilități ce pot fi exploatate de către indivizi sau grupuri cu intenții criminale. Cea mai bună soluție ce poate elimina acest tip de amenințare rămâne stimularea și educarea resursei umane, situație care să ducă la asigurarea superiorității în mediul cibernetic și securizarea beneficiilor aduse de tehnologie.

Amenințări la adresa mediului înconjurător – acest tip de amenințări sunt exercitate prin întrebuinţarea unui nou tip de arme, numite *geofizice*, al căror efect este îndreptat împotriva mediului înconjurător.

Introducerea restricţiilor de ordin ecologic în legislaţia de drept internaţional umanitar privind întrebuinţarea armelor cu efecte grave asupra mediului înconjurător, nu a făcut decât să diversifice preocupările pentru disimularea metodelor şi mijloacelor de întrebuinţare a acestora sub forma unor fenomene naturale cu manifestare firească. În acest sens, considerăm că, prin modul de întrebuinţare în secret, eludând tratatele şi prevederile internaţionale de neproliferare a acestui tip de armament, se creează o diferenţiere semnificativă faţă de armamentul convenţional şi chiar faţă de armele de distrugere în masă (ADMCBRN). Acest aspect conferă tuturor dispozitivelor, metodelor, mijloacelor tehnice sau de altă natură care au ca efect modificarea mediului înconjurător în scopuri militare, caracterul de armament neconvenţional.

În opinia noastră, abordarea problematicii efectelor de tip geofizic în conceptul ameninţării de tip hibrid trebuie considerată o prioritate pentru analiza modului de îndeplinire a finalităţilor politice pe care şi le propune un ipotetic adversar. În identificarea şi exploatarea vulnerabilităţilor adversarului, de cele mai multe ori net superior ca potenţial militar, un actor care întrebuinţează ameninţarea hibridă va urmări ca printr-un efort minim şi o cantitate redusă de energie să genereze efecte maxime. Întrebuinţarea armamentului cu efecte asupra mediului înconjurător, pe lângă urmările directe pe care le are, generează traume în mentalul colectiv, sporeşte sentimentul colectiv de nesiguranţă şi duce la apariţia neîncrederii în capacitatea guvernului şi autorităţilor de a asigura protecţia naţiunii, punând presiune asupra factorului politic

în scopul obţinerii victoriei fără angajarea instrumentului de forţă militar.

Operaţii informaţionale – acest tip de operaţii presupun acţiuni care vizează două aspecte extrem de importante privind percepţia realităţii operaţionale. Un prim aspect se referă la distorsionarea modului de înţelegere a situaţiei reale curente şi a evoluţiei probabile a acesteia în mediul operaţional. Al doilea priveşte protejarea capacităţii şi elementelor de decizie proprii şi a mijloacelor de care dispun acestea în cadrul operaţiei.

În accepţiunea doctrinară românească, operaţiile informaţionale sunt definite ca „acţiuni militare coordonate şi realizate în scopul influenţării procesului de luare a deciziilor a unui adversar pentru a sprijini realizarea obiectivelor politice şi militare prin influenţarea voinţei acestuia, în acelaşi timp protejând proprii comandanţi şi procese”[35].

Obiectivul operaţiilor informaţionale este cucerirea şi menţinerea superiorităţii decizionale ale forţelor proprii prin angajarea în mod integrat a unei palete largi de capabilităţi, tehnici şi instrumente pentru obţinerea efectelor specifice în dimensiunea informaţională a mediului operaţional. Din aria operaţiilor informaţionale fac parte operaţiile psihologice, securitatea informaţiilor, războiul electronic, înşelarea, dezinformarea, distrugerea fizică a infrastructurii informaţionale, operaţiile în reţeaua informatică şi angajarea liderilor cheie.

Acţiunile desfăşurate în cadrul operaţiilor informaţionale se pot situa pe trei paliere: de influenţare, de protecţia informaţiilor şi împotriva comenzii. Activităţile de influenţare sunt realizate prin manipularea percepţiilor şi acţiunilor adversarului. Activităţile de protecţia informaţiilor se concretizează prin acţiuni destinate protecţiei sistemului propriu de gestionare a informaţiilor şi sunt realizate în scopul menţinerii libertăţii de acţiune în mediul informaţional şi a creării condiţiilor optime de desfăşurare a procesului decizional. În final, activităţile îndreptate împotriva comenzii presupun atacuri împotriva sistemelor şi mijloacelor de culegere, procesare şi diseminare a datelor şi informaţiilor ale

[35] ***, *Doctrina Armatei României*, Bucureşti, 2012, p.137.

adversarului, precum şi împotriva sistemelor de comandă-control, de supraveghere şi de achiziţie a ţintelor.

În contextul ameninţării de tip hibrid, acţiunile de influențare se desfăşoară de către agresor, în mod preponderent asupra populaţiei din statul ţintă, folosind metode şi mijloace informaţionale multiple pentru manipularea percepţiei indivizilor şi grupurilor din cadrul acesteia în scopul îndeplinirii anumitor obiective. Scopul influenței în context hibrid este de a slăbi sau/și dezavantaja ținta propusă prin producerea de efecte la nivelul populaţiei. Ţinta amenințării trebuie să facă față dificultății de a discerne între influențare şi informare şi de a identifica autorul acestora. Acţiunile de influenţare sunt greu de identificat iar în situaţia în care sunt descoperite, actorul le poate nega cu vehemență. Pentru agresor, este este important să execute aceste activități încă din timpul fazei de pregătire a agresiunii, la granița dintre război și pace, adică pe timpul escaladării situaţiei tensionate înspre situaţia de criză, pentru ca acțiunile de contracarare să fie cât mai greu de implementat. Un aspect important pentru ţintă este faptul că protecţia împotriva acţiunilor de influenţare nu necesită mereu o astfel de analiză, mult mai important fiind identificarea propriilor vulnerabilități, educarea populaţiei și conştientizarea posibilelor consecințe ale propriilor măsuri, chiar și a celor indirecte. În esenţă, influențarea în contextul ameninţării hibride este bazată în special pe exploatarea și menținerea vulnerabilităților existente.

Centrul European de Excelență pentru Contracararea Amenințărilor Hibride a împărțit manifestarea amenințării hibride în două faze: faza de pregătire şi faza operaţională. În faza de pregătire, agresorul face pregătirile pentru acțiunile de influențare prin crearea sau identificarea unor canale de transmitere a mesajelor. În practică, acest lucru înseamnă observarea și crearea anumitor vulnerabilități care să fie exploatate, testarea impactului acțiunilor asupra acestora sau folosirea acestora ca o diversiune. În faza operațională, agresorul urmărește să-și atingă obiectivul prin combinarea unor metode diferite de influențare, selectate şi aplicate unor segmente de audienţă ţintă.

Nu trebuie uitat faptul că agresiunea hibridă este o acțiune coordonată și sincronizată care în mod voluntar țintește sistematic vulnerabilitățile populaţiei şi a unor instituții de stat printr-o mare varietate de metode. Activitățile care compun acest ansamblu tind să exploateze vulnerabilităţile producând efecte sub pragurile de detecție și atribuire precum și la granița dintre război și pace. Scopul este de a influența diferite forme de luare a deciziei la nivel local sau regional, aparţinând statului sau unor instituții pentru a favoriza sau atinge un scop strategic ce afectează ținta. Alături de influențarea informațională, agresorul mai poate întrebuinţa şi alte metode de influențare cum ar fi influențarea financiară, influențarea psihică, influențarea politică, atacurile cibernetice precum și violența politică. Acțiunea de influenţare poate fi o combinație a metodelor prezentate mai sus. De exemplu, dacă toate operațiile care folosesc internetul sunt considerate operații cibernetice, atunci toate acțiunile de acest fel pot în mod fi simultan percepute şi ca acțiuni de influențare informaționale. Similar, influențarea informațională poate fi legată de influența politică, cum ar fi modificarea consecințelor unei anumite legi pentru favorizarea unui anumit grup. Într-o societate democratică, decizia politică ca și opinia rezidenților poate fi influențată. Aceste metode sunt deseori combinate pentru atingerea obiectivului de influențare într-un mod mai eficient. De asemenea, influența poate fi percepută ca o amenințare. Amenințarea este ceva ce nu este de dorit, iar aceasta poate fi cu ușurință clasificată în sens legal pentru că de cele mai multe ori reprezintă activități criminale.

Capitolul 2

OPERAŢIONALIZAREA CONCEPTELOR „AMENINŢARE HIBRIDĂ” ŞI „AGRESIUNE HIBRIDĂ”

Ţinând cont de faptul că războiul a fost şi mai este, în forma sa convenţională, un fenomen politico-militar *per se*, ar fi normal ca cea mai relevantă dintre abordările acțiunilor de luptă de tip hibrid să fie din perspectivă militară. Aceasta definește conceptul într-un mod simplu, prin folosirea concomitentă a forțelor armate regulate și neregulate în aceeași campanie militară. Peter R. Masour, ca istoric militar, definește acțiunile militare hibride ca fiind *„*un conflict care implică o combinație de forțe militare convenționale și neregulate (insurgenți, gherilă și teroriști) care pot include atât actori statali cât și actori nestatali cu scopul atingerii unui obiectiv politic*”*.[36] Din această perspectivă, acțiunile militare hibride, în mod clar, nu reprezintă ceva nou. Există numeroase exemple de tehnici și metode „hibride” la nivel tactic, operativ, chiar și strategic al artei militare, care au fost aplicate de-a lungul istoriei, pornind din cele mai vechi timpuri, cum ar fi acţiunile militare descrise în Războiul Peloponeziac al lui Tucidide sau în scrierile lui Sun Tzu. De-a lungul timpului, acțiunile forțelor de gherilă au avut un impact deosebit asupra unor campanii militare convenționale. Ar fi de ajuns să amintim exemplele campaniei militare desfăşurată de către Napoleon în peninsula Iberică (războiul Peninsular, 1807–1814) sau acţiunile desfăşurate de către Armata Nord-vietnameză, în combinaţie cu forţele de gherilă ale grupării politice Viet Cong, în războiul din Vietnam. Venind în contemporaneitate, operațiile de contrainsurgență din Irak și Afganistan au arătat cât de dificil este să învingi grupuri insurgente fără a comite abuzuri privind drepturile omului împotriva populației locale, subminând astfel sprijinul public local și internațional

[36] Peter R. Mansour, „Hybrid War in History”, în *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present,* Editura Williamson Murray and Peter R. Mansour, Cambridge University Press, 2012, p. 2.

pentru campania militară. În ceea ce priveşte configuraţia agresiunii de tip hibrid, considerăm că este momentul oportun să precizăm că una dintre caracteristicile cele mai importante ale acesteia (care o şi diferenţiază de acţiunile de luptă „hibride" desfăşurate în trecut) este faptul că dimensiunea militară a acţiunilor desfăşurate este mult diminuată, privind amploarea, ba chiar poate să lipsească, aşa cum se va demonstra în continuare. Totuşi, dacă ea există, suntem în asentimentul lui Thomas Huber care, cu un deceniu înaintea lui Masour, a denumit combinaţia dintre acţiunile convenţionale şi cele neconvenţionale, în domeniul luptei armate, drept *acţiuni de luptă compuse* (*compound warfare*).

"Hibrid" este un adjectiv foarte comun care a fost folosit pentru a descrie un anume tip de război, chiar înainte de introducerea conceptelor *ameninţare hibridă*, *agresiune hibridă* sau *„război hibrid"*. Într-adevăr, termenul a fost folosit în anul 2003 de Tatiana Carayannis pentru a caracteriza războaiele contemporane din Africa în care, „...războaiele complexe hibride combină războiul civil, războiul interstatal și insurgența transfrontalieră".[37] Această utilizare se pare că a rămas necunoscută susținătorilor conceptului. Foarte diferit de Tatiana Carayannis a fost folosirea termenului de către Eric Simpsons pentru a descrie conflictele care nu sunt intrastatale și nici interstatale, dar sunt duse de un stat împotriva unui grup de actori nestatali în afara teritoriului lor.[38] Totuşi, este important să precizăm faptul că, ţinând cont de menţiunea lu Frank Hoffman[39], primul care a folosit termenul de „război hibrid" a fost Robert G. Walker, în lucrarea sa de disertaţie cu titlul „Spec Fi: The US. Marine Corps and Special Operations", relizată în anul 1998.

Ceea ce avea să devină mai târziu conceptul *acțiuni specifice războiului hibrid* [40], a apărut pentru prima dată în anul 2005 în articolul

[37] Tatiana Carayannis, „The complex wars of the Congo: towards a new analytic approach". Journal of Asian and African Studies. 38(2-3), 2003, p. 232.
[38] Erin Simpson, „*Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims*", http://www.allacademic.com/meta/p84945_index.html, 2005, accesat la 12.06.2019.
[39] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007, p. 9.
[40] N.A.: vom folosi acest termen pentru a traduce „hibrid warfare".

„Future Warfare: The Rise of Hybrid Wars" scris de generalul James Mattis și locotenent colonelul Frank G. Hoffman și publicat la Institutul Naval al SUA. Articolul s-a concentrat în principal pe tipul viitorului război ce va fi dus de SUA. Autorii criticau preocuparea anterioară a Pentagonului privind Revoluția în Afacerile Militare și superioritatea tehnologică și, referindu-se la războaiele din Irak și Afganistan, reiterau dimensiunea umană a conflictului și nevoia de a lua în calcul acest element atunci când se planifică viitoarele războaie. Deși au apreciat faptul că la acea vreme se identificaseră viitoarele provocări cărora armata trebuia să le facă față – tradițional, neregulat, catastrofic și perturbator[41] – ei și-au menținut teoria că războiul va fi o contopire a unor noi metode și mijloace de ducere a acțiunilor de luptă, și au numit acest lucru „război hibrid". Ei dezvoltau de fapt un concept al generalului Charles Krulak intitulat „Războiul în trei Monoblocuri" (în esență acest concept se referea la faptul că armata SUA va fi nevoită să desfășoare operații militare de luptă armată, de menținere a păcii și de sprijin umanitar, fără ca între aceste trei tipuri de acțiuni să fie distincte în spațiu şi timp). Autorii arătau că „într-un «război hibrid» este de așteptat ca, simultan, să aibă de a face cu dezintegrarea unui stat eșuat care deține armament chimic sau rachete dar care a pierdut controlul asupra lor şi să lupte împotriva unor forțe paramilitare care sunt motivate etnic și a unor teroriști radicali care au fost strămutați din pricina conflictului."[42] Pentru F. Hoffman, cel care este considerat inițiatorul acestui demers, „hibrid" însemna deci folosirea simultană a forțelor, pe același câmp de luptă, în diferite acțiuni, asupra unui adversar. Mai târziu acesta a abordat subiectul amenințărilor neregulate, cu referire la conceptele Războiul de Generația a IV-a, Războiul în trei Monoblocuri şi Războiul Nerestricționat, ca posibilități de înțelegere a „războiului hibrid" și cu includerea terorismului în cadrul acţiunilor de luptă neregulate.

[41] N.A.: în original, termenul uilizat de către William Lind în constructul „the quad chart" este *disruptive*.

[42] Frank G. Hoffman, „Small Wars Revisited: The United States and Nontraditional Wars", *Journal of Strategic Studies*. 28(6), 2005, p. 913.

Tot Hoffman a interpretat conflictul Israel – Hezbollah din 2006 ca fiind un conflict hibrid, punând succesul Hezbollahului pe seama abilității acestei organizații de a-și elabora strategia de acțiune prin atacarea vulnerabilităților forțelor armate israeliene și eșecul israelienilor de a fi mult prea încrezători în capacitățile lor militare. Astfel, el evidenţia faptul că deosebit de importantă este adaptarea acţională şi organizațională, competențe cheie pentru viitorul câmp de luptă, precum și importanța aspectelor non-cinetice ale acțiunilor de luptă neregulate, în special lupta informațională și comunicarea strategică. Acesta trata astfel acțiunile de luptă hibride, ca pe un caz particular al acțiunilor de luptă neregulate: „războaiele neregulate, în general și acțiunile de luptă hibride, în particular reflectă un stil de război în care «găsirea și fixarea» adversarului într-o zonă urbană aglomerată sau pe un teren complex sunt, de obicei, mult mai dificile decât «distrugerea lui»".[43] Trăsătura de „neregulat" a acțiunilor hibride este subliniată prin caracterul de lungă durată a acestui tip de acțiune (care vine în contrast, totuși, cu războiul din Liban care a ținut cu puțin mai mult de o lună). Aspectul de convențional al acțiunilor Hezbollah este dat în principal de folosirea armamentului convențional și nu de tacticile folosite. Nu în ultimul rând, Hoffman evidenţiază importanţa forţelor terestre, pe care le consideră esențiale în contextul „războiului hibrid".

În consecinţă, putem afirma faptul că dezbaterea asupra conflictelor contemporane și a mediului de securitate a fost bazată pe această caracteristică de *hibrid*. Creșterea importanței și popularității acesteia a făcut ca, aparent, să devină un laitmotiv în cercul dezbaterilor despre apărare, fie că dezbaterea este despre transformarea NATO, evenimentele de la Marea Neagră, conflictul din estul Ucrainei, Liban, Afganistan sau împotriva Statului Islamic, fie că se vorbeşte despre proliferarea armamentul de orice categorie sau despre transferul tehnologiilor moderne către actorii nestatali, despre mediul cibernetic

[43] Frank G. Hoffman, *Lessons from Lebanon: Hezbollah and Hybrid Wars*, Foreign Policy Research Institute, 2006, disponibil la http://www.fpri.org/articles/2006/08/lessons-lebanon-hezbollah-and-hybrid-wars accesat la 14.05.2019.

sau securitate energetică. Trebuie să avem în vedere faptul că „atunci când este posibil să suferim de indigestie intelectuală, să nu ezităm să ne punem o întrebare esențială, despre ce anume vorbim”.[44] Alături de amenințare hibridă, agresiune hibridă și război hibrid, au apărut şi alţi termeni cum ar fi actori hibrizi, acţiuni de luptă hibride, efecte hibride etc., în special de când a început conflictul din estul Ucrainei, care pot fi deranjanți atât în mediul academic cât și în cel politic. Actori importanți de securitate, cum sunt UE sau NATO au preluat termenii de bază și acționează, sau intenționează să acționeze pe baza acestora.

O asemenea creștere dramatică de folosire a termenilor a provocat dezordine în dezbaterile despre conflictele contemporane. Deseori nu există o utilizare liniară a termenilor, în sensul semnificaţiei acestora și, mai mult, există o foarte mică înțelegere a conceptelor din spatele acestor termeni. Nu numai că mulți autori folosesc termenii fără să explice relația dintre ei, dar unii îi tratează ca fiind interschimbabili. Cum cititorul de limbă română este sau nu este familiarizat cu conceptele, se poate observa și în literatura de specialitate autohtonă aceeași invazie de scrieri care alătură adjectivul „hibrid” oricărui substantiv. Este nevoie deci de un număr limitat de concepte de bază, pentru a nu genera construcţii literare nefolositoare sau cu un sens prea larg care pot deveni derutante dacă nu sunt bine definite și bine diferențiate de alte concepte. Elementul „hibrid” pare să fie prezent în număr destul de mare în articolele cu tentă politică, în ziare și comunicate de presă unde, deloc surprinzător, nu fac altceva decât să contribuie la confuzie și nu la clarificare. Mult mai îngrijorător este faptul că de multe ori se susține că definiția termenilor de bază trebuie să rămână „flexibilă” pentru a putea fi schimbată în funcție de caracterul și evoluția fenomenului. Acest fapt ar putea genera erori întrucât amenință să deconecteze fenomenul asociat conceptului de definiția sa. Definiția trebuie să fie suficient de cuprinzătoare pentru a include şi cazurile particulare ale fenomenului. Schimbarea definiției conceptului în funcție

[44] Colin S. Gray, „Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional”, *Strategic Studies Institute*, U.S. Army War College, Carlisle, 2012, p. 41.

de evoluţia fenomenului fără a şti dacă situațiile particulare ale acestuia sunt sau ar trebui să fie efectiv parte a conceptului plasează posibilitatea includerii în concept în afara discuției.

Pentru mulți analiști militari occidentali, termenul *hibrid* a părut a fi cea mai bună metodă de a descrie varietatea și combinația de mijloace și metode întrebuințate de Federația Rusă pe timpul conflictului din Ucraina din anul 2014. Tehnicile rusești au cuprins o combinație mai mult sau mai puțin tradițională de operații de luptă convenționale și neregulate, pe fondul sprijinului acordat protestelor politice, constrângerilor economice, operațiilor cibernetice și, în mod particular, unei intense campanii de dezinformare. Într-un interviu din luna iulie 2014, Secretarul General al NATO, Anders Fogh Rasmussen a denumit tacticile rusești ca fiind „acțiuni militare hibride" pe care el le-a definit drept „o combinație de acțiuni militare, operații ascune și un program agresiv de dezinformare".[45] Ediția din 2015 a *Military Balance* prezintă o definiție destul de largă a agresiunii hibride punând accentul pe metodele întrebuințate – „folosirea mijloacelor militare și non-militare într-o campanie cu scopul de obține surpriza, menține inițiativa și de a câștiga un avantaj psihologic și psihic folosind mijloace diplomatice, informații rapide și sofisticate, operații cibernetice și electronice, acțiuni militare sub acoperire și uneori descoperite precum și operații informaționale şi presiune economică".[46] Se poate observa din această definiție că accentul este pus pe aspecte altele decât cel militare privind metodele, cu precădere pe cele specifice, operațiile informaționale. Întrebuințarea operațiilor informaționale coercitive reprezintă caracteristica principală a celor mai recente abordări ale descrierii acțiunilor militare hibride și acest lucru permite să se poată face o comparație între campaniile Statului Islamic în Orientul Mijlociu și războiul cu totul diferit, ca de altfel și teatrul de operații, din Ucraina. Statul Islamic a combinat în mod eficient tacticile convenționale și de

[45] M. Landler, R. Gordon Michael, „NATO Chief Warn of Duplicity by Putin on Ukaine", *The New York Times*, 08 iulie, 2014, disponibil la www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html, accesat la 09.05.2019.

[46] ***, „Complex Crises Call for Adaptable and Durable Capabilities", *The Military Balance* 115.1 2015, disponibil la https://www.tandfonline.com/doi/pdf/10.1080/ 04597222.2015.996334, accesat la 10.02.2019.

gherilă cu actele de terorism, dar de asemenea a exploatat acțiunile de propagandă și cele informaționale la un nivel nemaiîntâlnit pentru un actor nestatal. Campaniile sofisticate de social media au glorificat cauza lor, iar propaganda vizuală de înaltă definiție a contribuit la creșterea capacității grupului de a recruta mii de luptători străini. În desfăşurarea acțiunilor, operaţiile militare informaționale au reprezentat, de asemenea, elementul central al succesului campaniei ruse. La nivel tactic, războiul electronic și atacurile cibernetice au neutralizat capacitatea autorităților ucrainene de a răspunde eficient, în timp ce tehnicile de anvergură ale mass media au făcut ca linia de demarcație dintre fals și adevărat să devină neclară, creând o realitate alternativă pentru acei observatori care au acceptat astfel punctul de vedere al Rusiei asupra evenimentelor. Campania strategică informațională a Rusiei în Ucraina a urmărit exploatarea vulnerabilităților sociale, slăbirea instituțiilor statului, a capacității guvernului de a conduce și subminarea perceperii legitimității statului. La fel ca Statul Islamic, Rusia a folosit operațiile informaționale pentru a influența și modela opinia publică, element care tinde să devină centrul de greutate al conflictelor armate contemporane.

Nu pare deloc surprinzător că factorii de decizie ruși consideră acțiunile militare informaționale și psihologice drept elemente de bază pentru obținerea victoriei în ceea ce ei numesc „*noua generație de război*”.[47] Generalul Philip Breedlove, fost SACEUR, reflecta cu aceeași consternare, ca mulți oficiali occidentali, descriind campania rusă drept „una dintre cele mai deosebite acțiuni militare informaționale de tip «blitzkrieg» care s-a putut vedea în istoria războaielor informaționale.”[48] Un fost producător rus de televiziune spunea că acest „blitzkrieg” merge mult mai departe de operațiile informaționale tradiţionale, arătând că „Rusia nu numai că se folosește de o dezinformare meschină, falsuri,

[47] Serghei G. Chekinov, Serghei A. Bogdanov, „The Nature and Content of New Generation War”, *Voyenna Mysl* 4, 2013, pp. 12-23, disponibil la http://www.eastviewpress.com/Files/MT_from%20the%20current%20issue_No.4_2013.pdf, accesat la 05.03.2019.

[48] John Vandiver, „SACEUR: Allies Must Prepare for Hybrid Warfare”, *Star and Stripes*, 04 septembrie 2015, disponibil la www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464, accesat la 03.09.2019.

pătrunderea în sisteme electronice și sabotajul cibernetic, forme asociate cu acțiunile militare informaționale, ci reinventează realitatea."[49]

Unele definiții ale agresiunii hibride sunt similare teoriei chineze de „*acţiuni de război nerestricţionate*". Acest concept, prezentat pe larg în cartea „Unrestricted Warfare", publicată în anul 1999 de către doi ofițeri chinezi[50], propune metode de ducere a acțiunilor specifice războiului care să permită unor țări precum China, să se poată confrunta cu un adversar superior din punct de vedere al tehnologiei militare, cum ar fi SUA. Similar conceptului de acțiuni militare hibride, acțiunile de război nerestricţionate implică folosirea unei multitudini de mijloace, atât militare cât și non-militare, pentru a răspunde unui adversar pe timpul conflictului. Unul dintre autori spunea într-un interviu că „prima regulă a acțiunilor de război nerestricţionate este aceea că nu există reguli, nimic nu este interzis".[51] Prin urmare, metodele acțiunilor de război nerestricţionate includ atacul reţelelor de calculatoare, atacul sistemelor bancare și a pieței de bunuri, manipularea ratelor de schimb (război financiar), terorismul, dezinformarea prin mass-media, luptă urbană, etc. Autorii susțin că dezvoltarea fără precedent a sistemului informatic și globalizarea au schimbat radical modul de ducere a războiului, care în mod normal a trecut de la preponderenţa covârşitoare a domeniul militar la „*un nou concept de arme"* cum ar fi virusarea sistemului informatic în timpul unei operații militare.[52] Aceste tehnici „noi" de ducere a acțiunilor militare sunt numite în mod destul de curios „*armament pentru copii",* dar modul lor de utilizare rămâne unul clausewitzian. „Un război pentru copii în care vărsarea de sânge poate fi evitată este totuși un război. Ar putea fi afectat procesul de cruzime al războiului dar sub nicio formă nu poate fi schimbată esența războiului,

[49] Peter Pomerantsev, „How Russia Is Revolutionizing Information warfare", *Defence One*, 09 september 2014, disponibil la www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635 accesat la 09.05.2019.
[50] Qiao Liang, Wang Xiangsui, „Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, 1999, p. 2, disponibil la www.oodalooo.com/documents/unrestricted.pdf, accesat la 10-13.2019.
[51] *Ibidem* 8, p. 2.
[52] *Ibidem* 8, p. 25.

care este una de constrângere și de aceea nu poate fi afectat cruntul rezultat al acestuia”.[53]

Nu există nicio îndoială că acțiunile militare asimetrice au avut o contribuţie la conceptul de agresiune hibridă. Acest concept de acţiuni asimetrice (sau, mai degrabă, „confruntări asimetrice”) a fost popularizat după Războiul Rece și a fost caracterizat prin acele tactici și strategii întrebuințate de state și oponenții nestatali ai SUA sau NATO pentru a contracara avantajul tehnologic și puterea de foc copleșitoare a acestora. Metodele asimetrice pot devia cu ușurință în în afara domeniului militar, extinzând „zona gri” dintre război și pace pe care Rusia a axploatat-o în Ucraina. De regulă, așa numitele acțiuni militare asimetrice erau întrebuinţate de către un actor mai slab în încercarea de a eroda puterea unui actor superior, contribuind deseori la succesul strategiei militare. Multe dintre elementele identificate ca fiind specifice acțiunilor militare asimetrice apar și în discuțiile legate de „*generaţia a patra de război*”[54], o teorie oarecum contestată de la începutul anilor 1990[55], ca să nu mai vorbim despre cea referitoare la „*generația a cincea de război*”.[56] Ideea principală a conceptului de „*generația a patra de război*” era exploatarea potențialului informațional tehnologic care se contura, tendinţă ce permitea actorilor militari nestatali să erodeze capacitatea de luptă a statelor prin atacarea centrelor de comandă și influenţarea populaţiei prin rețeaua globalizată a mass-media și a internetului. Prin urmare, conceptul „războiul” trebuie extins pentru a include acele dimensiuni unde puterea militară este mai puțin relevantă și anume cea culturală, socială, legală, psihologică și morală.

---

[53] *Ibidem* 8, p. 30.

[54] N.A.: prezentată în articolul „The Changing Face of War: Into the Fourth Generation” de către William Lind în *Marine Corps Gazette (pre-1994)*, octombrie 1989, disponibil la https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html, accesat la 12.08.2019.

[55] N.A.: un exemplu este oferit de către Antulio J. Echevarria II în lucrarea „Fourth-generation war and other myths”, 2005, disponibil la https://ssi.armywarcollege.edu/ pdffiles/pub632.pdf?fbclid=IwAR1IGbj-2EjcZBam5fb2ijpi9FYFTHixEex UbGrmT2ke GZbM7 EL39lYimMY, accesat la 18.02.2019.

[56] Tim Benbow, „Talking About Our Questions? Assesing the Concept of Four-Generation Warfare”, Comparative Strategy 27:2, 2008, pp. 148-163.

Acțiunile specifice agresiunii hibride tind să fie folosite pentru a descrie toate tipurile de războaie care nu sunt strict convenționale dar care se duc între actori statali (de regulă) care posedă forțe armate legal constituite. De aceea termenul de agresiune hibridă poate părea prea vag pentru a fi cu adevărat de ajutor analiștilor militari și politicienilor. „Cuvântul hibrid este atrăgător, deoarece el reprezintă un amestec de nimic."[57]

Includerea mijloacelor non-militare în definiția agresiunii hibride deschide riscul de a descrie competiția normală între state și conflictul ca făcând parte din război chiar și în absența unei amenințări evidente sau a folosirii violenței armate. Paradigma realistă a relaţiilor internaționale deja postulează relațiile între state ca fiind în mod natural într-o competiție și în conflict. Ea descrie mediul internaţional ca fiind unul în care statele suverane, preocupate de securitatea lor, acționează pentru urmărirea intereselor naționale și luptă pentru putere, cooperând și intrând în competiție cu alte state, în funcție de modul în care obiectivele sunt cel mai bine îndeplinite. Mijloacele economice, diplomatice și informatice folosite în competiția între state nu sunt clasificate în mod normal ca acțiuni de luptă, în absența unei amenințări cu forţa sau a folosirii forței.

2.1. Abordarea conceptului „amenințare hibridă" în cadrul NATO

Dezbaterile în cadrul NATO cu privire la amenințările hibride au început cu mult înainte de conflictul din estul Ucrainei. Primul document public cu privire la amenințarea hibridă a fost scris în anul 2010: „*Bi-SC Input for a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*", un document colectiv scris de ofițerii din SHAPE în colaborare cu alte structuri NATO și experți din statele membre. Documentul dă următoarea definiție amenințării hibride: „amenințarea hibridă constituie acele amenințări generate de

[57] Janis Berzins, „A New Generation of Warfare", *Per Concordiam* 6:3 (2015), p. 24, disponibil la www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/per Concordiam /pC_V6N3)en.pdf, accesat la 09.05.2019.

adversari care au capacitatea ca simultan, în funcție de situație, să poată întrebuința mijloace convenționale şi neconvenționale pentru îndeplinirea obiectivelor sale."[58] Pe lângă această definiție, documentul face referire la mediul operațional care se transformă radical ca urmare a globalizării, a accesului tot mai facil la resursele internaționale și la mijloacele moderne de comunicare și ca urmare a instabilităţii regionale care face din amenințarea hibridă o mare provocare.[59] De asemenea, sunt analizate şi câteva puncte particulare privind amenințarea hibridă contemporană. Interconectarea aduce împreună un număr de adversari care pot colabora, pot folosi dezinformarea cu ajutorul sistemelor informatice în mod instantaneu, pot exploata regulile şi legile, incluzând aici restricțiile naționale, regulile de angajare şi legile internaționale, pentru toate acestea utilizând mijloace și metode dintre cele mai diverse. Acest ultim aspect necesită o atenție mult mai mare pentru că el completează definiţia amenințării hibride, explicitând principalele sale componente. Documentul arată că „amenințarea hibridă poate conține o combinație de armament convențional letal și nonletal, chimic, biologic, materiale radiologice și nucleare, terorism, spionaj, atacuri cibernetice și criminale, sprijinite de un sistem informațional de răspândire a știrilor false și de organizații de afaceri cu legitimitate.[60]

Mijloacele și modalitățile prezentate în document corespund celor pe care F. Hoffman le-a identificat însă între cele două variante există unele diferenţe. Deşi componentele de criminalitate, terorism și armament convențional sunt aceleași, operațiile informaționale au fost menționate uneori de F. Hoffman dar nu au fost niciodată incluse în definiția sa. Divergența dintre cele două abordări constă în menționarea în mod explicit a spionajului și atacurilor cibernetice, a materialelor CBRN, precum și a posibilității de utilizare a mijloacelor nonletale. Acest aspect este destul de interesant întrucât F. Hoffman și-a construit teoria amenințarea hibridă în special pe aspectul letal al acțiunilor de

[58] ***, NATO, *Bi-SC Input to a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats,* 2010, p. 2, disponibil la http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf, accesat 09.05.2019.
[59] *Ibidem,* p. 3.
[60] *Ibidem,* p. 8.

luptă.[61] O altă diferență importantă dintre definiţii este aceea că cea NATO enumeră acţiunile posibile din cadrul unei ameniţări hibride în timp ce F. Hoffman citează componentele necesare ale acesteia. Ultima divergență importantă pleacă de la faptul că NATO consideră că „amenințarea hibridă va avea elemente care sunt relevante pentru apărare. Caracterul lor nu este unul pur militar dar capabilitățile militare pot contribui la prevenirea acestora. Amploarea lor solicită ca NATO să fie pregătită să dea un răspuns coordonat între membrii Alianței și comunitatea internațională".[62] Acest aspect constituie o rupere a tradiției. Problema dacă responsabilitatea pentru contracararea amenințării hibride revine instituțiilor militare sau civile a fost introdusă de F. Hoffman și Freier iar răspunsul celor doi a fost că este de preferat instituția militară.[63] Documentul NATO face evidentă preferința pentru forța militară deşi precizează că aceasta nu mai este de mult o prioritate, atâta timp cât se observă o tendință către aspectul tot mai civil al amenințării hibride. Acest document NATO este unul destul de cuprinzător despre amenințarea hibridă și agresiunea hibridă dar se pare că a fost uitat sau neluat în seamă de mulți autori pe acest subiect care au scris, în special, după conflictul din estul Ucrainei.

De la apariția documentului NATO analizat mai sus, au fost trei lucrări esențiale care au extins problematica introdusă de acesta. Prima a fost scrisă de o echipă de autori în Prism Magazine.[64] Probabil, unul sau mai mulți dintre autori au participat la anumite exerciții conduse de NATO înainte de publicarea articolului, întrucât se fac unele referiri la acestea și oferă o vedere interesantă asupra abordării NATO a aspectelor

[61] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007, p. 7.
[62] ***, NATO, *Bi-SC Input to a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats*, 2010, p. 8.
[63] Frank G. Hoffman, „On Not-So-New Warfare? Political Warfare vs. Hybrid Threats", *War on the Rocks*, 2014, disponibil la http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ asccesat la 24.03.2019; Nathan Freier, „Hybrid Threats and Challenges: Describe… Don't Define", *Small Wars Journal*, 2009, disponibil la http://smallwarsjournal.com/blog/journal/docs-temp/343-freier.pdf, accesat la 23.03.2019.
[64] Michael Aaronson, Sverre Diessen, Yves de Kermabon, Mary Beth Long, Michael Miklaucic, „NATO Countering the Hybrid Threat", *Prism*. 2(4), 2012, pp.111-124, disponibil la http://mercury.ethz.ch/serviceengine/Files/ISN/133803/ichaptersection_singledocument/fee9d9be-0d38-4db7-ab4a-31e7c2bfde19/en/Chapter8.pdf, accesat la 06.02.2019.

amenințării hibride înainte de conflictul din estul Ucrainei. Pe timpul exercițiilor accentul a fost pus pe cooperarea NATO cu organizațiile civile importante, implicarea NATO în industrie, în mod particular în sectoarele energetic și cibernetic, comportamentul privind amenințarea de securitate non-militară, adaptarea birocrației NATO la noile provocări și evoluția NATO într-un mediu în schimbare rapidă şi care prezintă amenințări complexe la adresa securității.[65] Studiul menționează faptul că la exerciții au participat aproape o sută de persoane din sectorul privat ceea ce constituie o evidență clară a modului în care actorii civili fac parte din dezbaterea cu privire la acțiunile militare hibride. Atât problemele evidențiate de aceste exerciții precum și participarea în număr mare a specialiștilor din sectorul privat ilustrează noua abordare non-militară a amenințării hibride.

O altă ilustrare importantă a schimbării modului de abordare a amenințării hibride este introducerea unui element problematic, acela de atribuire a amenințării hibride unui anumit sector, problemă aflată în strânsă legătură cu introducerea în cadrul agresiunii hibride a unui element legat de atacurile cibernetice și includerea unui scenariu de posibilă amenințare hibridă neletală. Autorii studiului au admis faptul că amenințarea hibridă este umbrela sub care se află o largă varietate de circumstanțe și acțiuni cum ar fi terorismul, migrația, pirateria, corupția, conflictul etnic și altele. Ceea ce este nou, totuși, este posibilitatea ca NATO să fie nevoită să facă față folosirii sistematice și în mod adaptiv a unor asemenea acțiuni de către adversari care urmăresc obiective politice pe termen lung, opus modului obișnuit de până acum.

Un alt articol, publicat în anul 2011 și care reflectă efortul NATO de a face față amenințării hibride[66] s-a concentrat în totalitate pe atacurile cibernetice și a demonstrat impactul practic al diferitelor abordări a ameniţării hibride. Autorul a folosit amenințarea hibridă ca pe un termen general care cuprinde diferite amenințări în curs de dezvoltare

[65] *Ibidem* 13, p. 112.

[66] Sascha-Dominik Bachmann, „Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management", *Amicus Curiae*, Vol. 88, 2011, pp. 14-17, disponibil la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989808, accesat la 17.07.2019.

și care au legătură cu atacurile cibernetice. Este o înțelegere clară a faptului ca atacul cibernetic, ca atare, este chiar esenţa amenințării hibride. O asemenea înțelegere poate fi împotriva concepţiei NATO și este cu certitudine incompatibilă cu opinia lui F. Hoffman, atâta timp cât ambele se bazează în definirea și înțelegerea acestui fenomen al amenințări hibride pe combinația mai multor mijloace și modalități diferite, reprezentate în mod ponderat, în funcţie de vulnerabilităţile ţintei. Această reprezentare a amenințării hibride a fost la fel susținută după participarea la exercițiile NATO de un alt autor, H. Gunneriusson care a și-a făcut cunoscută concepţia într-un mod mult mai explicit decât predecesorul său. Acesta s-a folosit de ideea clasică a conceptului de „război hibrid" care este o combinație de tehnologie avansată ce poate fi la dispoziția chiar şi a unui actor nestatal sau a unui actor slab, motiv pentru care a tratat atacurile cibernetice și chiar social media ca fiind principalele componente ale amenințării hibride. Mai mult el a făcut referire la nanotehnologie și furtul de biotehnologie ca viitoare componente majore ale amenințării hibride. Autorul nu a dat o definiție a amenințării hibride dar a tratat termenul ca fiind o combinație de viitoare surprize tehnologice, el introducând ideea de „oportunități hibride", motiv pentru care a făcut apel la o mai strânsă colaborare între sectorul militar și cel civil, cu precădere cel privat.[67]

Cel care a sesizat cel mai bine lipsa unei dezbateri ferme la nivelul NATO pe această temă a fost Rex Brynen care a arătat cum conceptul de amenințare hibridă la nivel NATO „pare să fie ceva desfăşurat cu scopul de a ușura redirecționarea atenției și chiar schimbarea terminologiei pentru a deschide noi discuții cu privire la nivelul de instruire, pregătire, capabilități, analize și noi parteneriate pentru a face față noilor provocări ale secolului XXI".[68] El l-a numit un concept ambiguu, plin de birocrație, scos pe piață în numeroase variante și care este de ajutor pentru NATO, pentru a face față aspectelor mai puțin plăcute, chiar

[67] Hâkan Gunneriusson, „Nothing is Taken Serious Until It Gets Serious: Countering Hybrid Threats", *Defence Against Terrorism Review* (4)1, 2012, pp. 47-70.
[68] Rex Brynen, „Countering Hybrid Threats AAR", *Pax Sims*, 2011, disponibil la https://paxsims.wordpress.com/2011/05/15/countering-hybrid-threats-aar/ accesat la 28.03.2019.

„murdare”[69] ale unui război neconvențional în care ar putea fi implicată această organizaţie. Ideea generală era că termenul hibrid începea să fie folosit pentru amenințări mai puțin sau mai greu de anticipat şi care pot produce efecte dificil de estimat.

2.2. Abordarea conceptului „amenințare hibridă” în cadrul UE

Printre documentele cu privire la amenințările hibride se numără și *Cadrul comun privind contracararea amenințărilor hibride al UE*.[70] Documentul se concentrează pe strategia de contracarare a amenințărilor hibride în timp ce se evită cumva definirea clară a acestor amenințări, susținând că definițiile despre acțiunile militare hibride variază foarte mult dar este nevoie ca ele să rămână flexibile pentru a răspunde caracterului lor evolutiv. Acest punct de vedere este criticat pentru că vorbește despre un fenomen care nu este definit iar faptul că există mai multe definiţii ale acestuia nu poate justifica evitarea formulării uneia proprii. Încercarea de folosire a unei definiții mai largi, mai flexibile pentru a putea include mai multe cazuri diverse poate fi de înțeles pe de o parte, dar în această situaţie paleta largă de acţiuni şi efecte înglobate poate duce la multe confuzii. Comisia Europeană a dat, totuşi, dovadă de multă flexibilitate în definirea amenințării hibride reușind performața să publice trei definiții în aceeași zi. Definiția propusă în Cadrul comun privind contracararea amenințărilor hibride al UE arată că amenințarea hibridă „urmărește să înglobeze amestecul de activități coercitive și subversive, de metode convenționale și neconvenționale (de exemplu, diplomatice, militare, economice, tehnologice), care pot fi utilizate într-un mod coordonat de actorii statali sau nestatali pentru a realiza obiective specifice, rămânând însă sub limita pragului de stare de război declarată oficial.”[71] O altă definiție, puțin diferită de cea de mai sus este propusă în același document „...un amestec de acțiuni convenționale și neconvenționale, militare și non-militare, descoperite și sub acoperire

[69] *Ibidem* 17.
[70] UE, *Joint Framework on countering hybrid threats: A European Union response*. Bruxelles, 2016, disponibil la https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX% 3A52016J C0018, accesat la 15.03.2019.
[71] *Ibidem,* p. 2.

care pot fi utilizate într-un mod coordonat de actorii statali sau nestatali pentru a realiza obiective specifice, rămânând însă sub limita pragului de stare de război declarată oficial". Cea de-a treia definiție a acțiunilor militare hibride a fost dată printr-un comunicat de presă care însoțea apariția Cadrului comun, și care spunea că amenințările hibride se referă la un amestec de activități care de cele mai multe ori combină metodele convenționale și neconvenționale care pot fi utilizate într-un mod coordonat de actorii statali sau nestatali pentru a realiza obiective specifice, rămânând însă sub limita pragului de stare de război declarată oficial.

Obiectivul nu este doar de a produce distrugeri și a exploata oportunitățile, dar și de a destabiliza societatea și de a crea ambiguitate cu scopul de a periclita procesul de luare a deciziilor. Diferențele între definiții nu sunt foarte mari dar îndeajuns ca să creeze confuzie. Este evident că se acordă atenție sporită încă de la început unor elemente ale agresiunii hibride, cu referire la mijloacele convenționale și neconvenționale, actorilor statali și nestatali și mijloacelor de coordonare. Acțiunile sub acoperire din cea de a doua variantă, precum și acțiunilor subversive din prima variantă arată clar că sunt inspirate din opinii apărute ca reacție la modul în care Rusia a desfășurat acțiunile din estul Ucrainei și din Crimeea. UE pune accentul pe aspectul civil al agresiunii hibride și pe posibilitățile de exploatare a vulnerabilităților în anumite zone esențiale cum ar fi securitatea alimentară, infrastructura critică și mediul cibernetic.

2.3. Abordarea rusească a conceptului „război hibrid"

Mulţi analişti militari ruşi resping complet conceptul „război hibrid" argumentând că nu este nimic nou şi că diferite forme ale acestuia au fost puse în practică de la începutul războaielor.[72] Unii critici arată, de asemenea, că multe dintre analizele despre „războiul hibrid" dau o importanță exagerată statutului forţelor convenţionale[73] şi că acest

[72] Andrew Monaghan, "The "War" in Russia's 'Hybrid Warfare'", *Parameters* 45(4)(Winter 2015), pp. 66-68.
[73] *Ibidem*, pp. 68-69.

concept nu reuşeşte să capteze manipularea specifică politică şi informaţională pe care Rusia o execută în sprijinul atingerii obiectivelor sale.

De aceea, este nevoie de un concept mai bun atunci când se descriu perspectivele Rusiei, probabil unul prezent în gândirea rusă. Se consideră că elemente specifice concepţiei acestui tip de război au fost exprimate de generalul Vladimir Gherasimov în faimosul său articol din anul 2013[74]. Dezbaterile între cei care au considerat articolul ca pe o vedere generală, descriptivă a mediului operaţional sau ca pe un mijloc inteligent de comunicare a unui concept doctrinar au dat naştere unor articole în publicaţiile de specialitate dintre cele mai diverse, conceptul „*război hibrid"* căpătând valenţe atotcuprinzătoare. Acestea sunt „mijloacele noi" prin care Rusia îşi exercită influenţa, atât în apropierea graniţelor cât şi pe glob. Termenul folosit de către Gherasimov este cel de *război non-liniar* şi reprezintă, de fapt, o încercare de a ajunge din urmă realităţile războiului modern cu care SUA, de exemplu, se luptă de mai mult de un deceniu în Irak, Afganistan şi în alte zone de conflict.[75] Pe de altă parte, în literatură de specialitate rusă, „războiul hibrid" este considerat a fi un „război indirect", iar Rusia este cea care trebuie să facă faţă „războiului hibrid" declanşat de puterile Occidentale împotriva ei. Conceptul de agresiune hibridă este foarte diferit perceput de către Rusia și Occident. Cuvântul cheie care poate descrie agresiunea hibridă, aşa cum este definită de Occidentali, este „multimodalitate", în timp ce cuvântul cheie pentru a descrie paradigma războiului ofensiv non-liniar din punctul de vedere al ruşilor este „penetrare".

Ceea ce poate ajuta este înţelegerea faptului că anumite elemente „noi", care apar în articolul generalului Gherasimov, au la bază concepte vechi, adaptate realităților operaționale ale secolului XXI. Concret, elemente cheie ale presupusei „doctrine Gherasimov" sunt derivate din conceptele *operaţii în adâncime*, *măsuri active* şi *control reflexiv*.

[74] N.A.: Șeful Statului Major General al Forţelor Armate Ruse şi prim locţiitor al ministrului apărării, numit de preşedintele Vladimir Putin în anul 2012. Articolul se intitulează „Valoarea ştiinţei în predicţie", a fost publicat în revista *VPK* nr. 8 (476) din 27 februarie 2013, disponibil la http://www.vpk-news.ru/articles/14632, accesat 17.04.2019.

[75] M. Kofman, M. Rojanski, „A Closer Look al Russia Hybrid War", Kennan Cable, Wilson Center. No. 7, 2015.

Operaţii în adâncime

Unul dintre analiştii militari tradiţionali, la care generalul Gherasimov a făcut referire în articolul său a fost Georgy Isserson, catalogat ca un profet de către analiştii militari ruși. G. Isserson a fost un mare susţinător al teoriei operaţiilor în adâncime, împreună cu un alţi analişti militari proeminenţi ai erei sovietice cum ar fi Mikhail Tukhachevsky şi Vladimir Triandafillov. Operaţiile în adâncime (inventate de Triandafillov şi Tukhachevsky, inspiraţi, desigur, de Napoleon şi perfecţionate de Isserson) au ca scop (aşa cum este menţionat şi în următorul paragraf) distrugerea unor obiective de importanţă majoră aflate în adâncimea dispozitivului inamicului urmată de încercuirea acestuia şi nu lovirea forţelor inamicului pe întreaga adâncime a dispozitivului său. De regulă, lovirea inamicului pe toată adâncimea dispozitivului său (ideal, realizată în mod simultan şi nu succesiv) este asociată conceptului de război non-contact, e adevărat, o dezvoltare a operaţiilor în adâncime.[76]

Spre deosebire de gândirea militară Occidentală, teoria operaţiilor în adâncime nu pune accentul pe identificarea unui singur centru de greutate şi, apoi, direcţionarea întregului efort către distrugerea acestuia. În schimb, operaţiile în adâncime presupun atacurile asupra unei game variate de obiective importante dispuse în adâncimea dispozitivului inamicului, contribuind semnificativ la obţinerea succesului în operaţie.[77] De-a lungul timpului, sovieticii au transformat această idee în doctrina de manevră, prin folosirea străpungerii în forţă pentru a permite forţelor mobile să pătrundă adânc în dispozitivul tactic de apărare al inamicului, reuşind să asigure încercuirea forţelor. Rezultatul ar fi fost colapsul forţelor de apărare de nivel tactic, fie prin nimicirea lor efectivă fie prin prelungirea izolării, în timp ce forţele mobile ar fi înaintat spre îndeplinirea unor obiective de nivel operativ.[78]

---

[76] Vladimir Triandafillov, „The Nature of the Operations of Modern Armies", Ed. Taylor & Francis, p. XI, 1994.

[77] ***, Department of the Army, FM 100-2-1, The Soviet Army: Operations and Tactics (Washington, DC: Department of the Army, 1984), pp. 2-12; N.A.: not once is the term "centre of gravity" mentioned when referring to Soviet operational and tactical doctrine.

[78] Charles Pickar, „Tactical Deep Battle: The Missing Link, Monograph (Fort Leavenworth, Kansas: School of Advanced Military Studies, 1991)", pp. 10, 37.

Deşi mulţi analişti Occidentali au început să combine expresiile din teoria manevrei cu teoria ca atare, alţi analişti au avertizat asupra acestei interpretări *ad-litteram*, arătând că adepţii acestui curent lasă deseori să se înţeleagă că există un nivel înalt de flexibilitate.[79] Teoria operaţiilor în adâncime încă are un rol important în doctrina militară rusă, aşa cum este evidenţiat şi de recentele reforme militare. Ca parte de programului de modernizare militară aflat în desfăşurare, se pare că Rusia acordă un rol deosebit dezvoltării forţelor sale aeromobile şi aeropurtate. Acest lucru îi conferă capabilităţi ridicate de desfăşurare rapidă, care pot intimida ţările din apropierea frontierelor sale, iar în cazul unui conflict convenţional, pot contribui semnificativ la exploatarea succesului forţelor mecanizate prin operaţii pe verticală în adâncimea teritoriului inamicului.[80]

Teoria operaţiilor în adâncime a influenţat foarte mult reforma militară în Rusia, Doctrina Militară a Federaţiei Ruse din 2014 impunând o coordonare mai apropiată a resurselor statului pentru îndeplinirea scopurilor finale ale acesteia. Într-un paragraf în care se descrie mediul operaţional, se arată că „...folosirea integrată a forţelor militare, politice, economice, informaţionale şi a altor măsuri non-militare" şi „...efectul asupra inamicului de-a lungul întregii adâncimi a teritoriului acestuia în spaţiul global informaţional, aerian, terestru şi pe mare" sunt caracteristici ale războiului modern. Secţiuni din acest document sunt dedicate cartografierii interdependenţei dintre instituţiile militare, economice şi politice, ca elemente de bază ale mobilizării naţionale.[81]

În mod similar, Strategia Naţională de Securitate rusă din anul 2015 tratează căile de realizare a unei abordării unitare de către guvern a descurajării şi securităţii naţionale, dar şi a mobilizării sociale.[82]

---

[79] *Ibidem,* p. 9.

[80] Can Kasapoglu, „Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control", Research Paper No. 121 (Rome: NATO Defence College, 2015), pp. 8-9.

[81] Russian Federation, „Military Doctrine of the Russian Federation (Moscow: Government of the Russian Federation, 2014)", paragraphs 15, 43-44, 48-51 şi 52-53.

[82] Olga Oliker, "Unpacking Russia's New National Security Strategy", Center for Strategic and International Studies, 7 ianuarie 2016, disponibil la https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy, accesat la 9.02.2019.

Accentul pus pe operaţiile în adâncime în procesul de reforma militară a Rusiei şi pe integrarea guvernului în acest proces poate avea, de asemenea, o aplicare ofensivă. În loc să folosească numai forţele militare, istoria recentă arată că Rusia este mai mult decât dispusă să lovească un adversar în multe moduri posibile, în mod simultan, prin folosirea instrumentelor de putere naţionale diplomatice, informaţionale, militare şi economice, după modelul teoriei operaţiilor în adâncime. Mai mult, noua filozofie de ducere a acţiunilor militare încearcă să pună un accent mai redus pe implicarea forţelor armate încă din prima fază, acestea având doar rolul de a finaliza o acţiune dusă cu alte mijloace.

În faza iniţială a războiului ruso-georgian din 2008, Rusia a lansat o serie de acţiuni coordonate, destinate să paralizeze Georgia şi să o forţeze să renunţe la politica ei de apropiere faţă de NATO. Pe cale diplomatică, Rusia a încercat afectarea legitimităţii preşedintelui Georgiei, Mikhael Saakashvili, prin încurajarea protestelor împotriva guvernului, stabilind contacte directe cu guvernele nerecunoscute din Ossetia de sud şi Abkhazia şi prin ridicarea sancţiunilor de interzicere a exportului de armament în aceste regiuni.[83] Totodată, în mediul informaţional, Rusia a răspândit acuzaţii cu privire la atrocităţile comise de către forţele georgiene în Ossetia de Sud şi a lăsat să se înţeleagă că forţele ruseşti prezente în zonă execută misiuni în sprijinul păcii.[84] În plan economic, Rusia a impus sancţiuni Georgiei în domeniul financiar, al energiei şi comerţului, ca pedeapsă pentru apropierea sa de NATO.[85] În cele din urmă, Rusia a desfăşurat o serie de acţiuni militare de mică amploare, iar în luna iulie 2008 a desfăşurat un exerciţiu militar cu scopul de a intimida Georgia pentru ca, în final, să se pregătească pentru invazie.[86] De aceea, invazia Rusiei în Georgia a venit în urma unei vaste campanii pregătitoare în cadrul căreia au fost desfăşurate acţiuni care au

[83] Ariel Cohen, Robert Hamilton, „The Russian Military and the Georgia War: Lessons and Implications", *ERAP Monograph*, Fort Leavenworth, Kansas: Strategic Studies Institute, 2011, p. 15.
[84] *Ibidem*, pp. 15-16.
[85] Randall Newnham, "Georgia on my mind? Russian sanctions and the end of the 'Rose Revolution'", *Journal of Eurasian Studies* (6/2015).
[86] Ariel Cohen, Robert Hamilton, „The Russian Military and the Georgia War: Lessons and Implications", *ERAP Monograph*, Fort Leavenworth, Kansas: Strategic Studies Institute, 2011, pp. 17-18, 23-27.

vizat o serie de obiective strategice, printre care legitimitatea preşedenţiei lui Saakashvili, legăturile Georgiei cu Ossetia de Sud şi Abkhazia, precum şi reputaţia internaţională şi activitatea economică a Georgiei. Distrugerea acestor obiective din adâncimea strategică a Georgiei, a dus la slăbirea statului până în punctul în care atunci când forţele convenţionale ruseşti au intrat în ţară, voinţa politică a Georgiei a ajuns în colapsul preconizat de teoria operaţiilor în adâncime. Deşi, într-un anumit mod, mijloacele Rusiei descrise mai sus par a fi convenţionale, în conflictul ruso-georgian din 2008 s-au folosit în mod extensiv războiul cibernetic şi forţele neregulate.[87] Folosirea unor asemenea forţe şi a unor „trucuri murdare" nu a reprezentat ceva nou pentru Rusia, iar aceste mijloace îşi au originea într-un alt concept moştenit din perioada Uniunii Sovietice, denumit „măsuri active".

Măsuri active

Este un concept care descrie multe dintre metodele non-militare şi asimetrice întrebuinţate în abordarea rusească, de tip non-liniar, a agresiunii.[88] Deşi definiţia rusească exactă este vagă, multe dintre definiţiile Occidentale ale măsurilor active arată că ele constau într-o formă de război politic dus de serviciile de informaţii şi securitate pentru a influenţa cursul unor evenimente mondiale. Măsurile active includ o gamă largă de acţiuni, preponderent informaţionale, de la „manipularea media până la acţiuni speciale care implică diferite niveluri de violenţă şi pot include dezinformări, propagandă, falsificarea unor documente oficiale, asasinate şi represiune politică.[89] Deşi conceptul a fost dezvoltat pentru a sprijini răspândirea comunismului prin mijloace neconvenţionale, multe din elementele sale sunt evidente prin mijloacele folosite în prezent de către Rusia pentru a-şi promova interesele. Negarea folosirii de către Rusia a forţelor neregulate, a războiului cibernetic şi a diasporei, precum şi manipularea media, a partidelor politice şi a „think tank-urilor", sunt toate manifestări contemporane ale

[87] *Ibidem*, pp. 26-28, 44-49.
[88] Marius Potîrniche, „Război non-liniar versus rãzboi hibrid", *Gândirea Militară Românească*, 1-2/2018, p. 15.
[89] ***, "*Terms and Definitions of Interest for Counterintelligence Professionals*", Department of Defense, Public Intelligence, 09 iun. 2014, pp. 4-5.

unui vechi concept sovietic. Deşi colapsul Uniunii Sovietice a determinat suspendarea întrebuinţării unor asemenea tactici pentru o perioadă de timp, deprinderile lăsate în urmă au continuat să supravieţuiască în cadrul serviciilor de securitate ruse, iar ele au fost exploatate pe plan intern de către preşedintele Vladimir Putin.[90]

Departe de a fi o artă moartă, măsurile active îşi găsesc acum expresia atât pe plan intern, pentru a apăra regimul lui Putin, cât şi pe plan internaţional, ca mijloace de urmărire a intereselor sale. Există dovezi semnificative că Rusia a folosit măsurile active în Ucraina, în mod particular în regiunea de est. Se pare că agitatori ruşi s-au deplasat în Ucraina pentru a agrava nemulţumirile etnicilor ruşi şi pentru a submina legea şi ordinea, provocând răspunsul Ucrainei.[91] Acest răspuns a fost apoi folosit pentru a declanşa o serie de acţiuni ale unor grupuri de forţe neregulate formate din ruşii pan-slavi, aşa numiţii „Patrioţi", partidele locale pro-ruse, cazacii şi aventurieri/mercenari, toţi înarmaţi şi aprovizionaţi de serviciile de securitate şi forţele pentru operaţii speciale ruse.[92] Conduşi de către ofiţeri de informaţii ruşi, deteşamentele de rebeli au atacat, aparent în mod prioritizat, facilităţile de comunicaţii, în încercarea de a suprima diveritele mesaje ale rebelilor care descriau revolta ca pe o reacţie la o criză umanitară pregătită de Kiev.[93] În tot acest timp, Rusia a negat implicarea, dar a susţinut aceste forţe neregulate cu armament şi echipamente, precum şi cu acţiuni militare convenţionale directe.[94]

---

[90] Andrew Wilson, "Russian Active Measures: Modernized Tradition", The Institute for Statecraft, 03 ian 2016, disponibil la http://www.statecraft.org.uk/research/russian-active-measures-modernised-tradition, accesat la 23.06.2019.

[91] Andrew Roth, "From Russia, 'Tourists' Stir the Protests", *The New York Times*, 03 mar. 2014, disponibil la https://www.nytimes.com/2014/03/04/world/europe/russias-hand-can-be-seen-in-the-protests.html, accesat la 26.06.2019.

[92] Andrew Higgins, "Armed Men Seize Police Station in Eastern Ukraine City", *The New York Times*, 12 apr. 2014, disponibil la http://www.nytimes.com/2014/04/13/world/europe/ukraine.html, accesat la 18.03.2019.

[93] Jill Dougherty, „Everyone Lies: The Ukraine Conflict and Russia's Media Transformation", Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, iulie 2014, disponibil la https://shorensteincenter.org/wp-content/uploads/2014/07/d88-dougherty.pdf, p. 4-5, accesat la 19.02.2019.

[94] Galeotti, „Hybrid War' and 'Little Green Men': How Does It Works and How It Doesn't", disponibil la http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/, accesat la 11.02.2019.

Astfel, situaţia din estul Ucrainei a avut toate caracteristicile măsurilor active: manipularea politică internă a unui stat suveran, folosirea violenţei prin intermediul unor forţe intermediare (proxy) şi manipulare informaţională, toate coordonate pentru a asigura un final prevăzut. În plus, faţă de folosirea violenţei, măsurile active au constat în componente privind manipulare media, dezinformare şi propagandă. Spre deosebire de acţiunile Rusiei în Crimeea, situaţia din estul Ucrainei nu a dus la o victorie rapidă. Mai mult, conflictul este astăzi îngheţat şi el a dus la aplicarea unor sancţiuni economice, la revigorarea NATO şi la creşterea asistenţei militare acordate Ucrainei şi ţărilor est europene.[95] Totuşi, prin reînsufleţirea controlată a insurgenţei, Rusia poate aştepta un moment oportun pentru a relua iniţiativa.

Control reflexiv

Controlul reflexiv este o teorie comportamentală care conectează elementele informaţionale, şi este definită ca "…un mijloc de a transmite unui partener sau unui oponent, o informaţie special pregătită pentru a îl determina ca, în mod voluntar, să ia o anumită decizie în sensul dorit de iniţiatorul acţiunii."[96] Controlul reflexiv este o teorie militară bine conturată, apărută în anii '60, care a evoluat într-un câmp interdisciplinar, cu propriile publicaţii şi experţi.[97]

Termenul „reflex" în cadrul controlului reflexiv se referă la un model comportamental construit pentru a înţelege procesul de luare a deciziei al unei anumite ţinte. Dacă un actor înţelege modelul comportamental al ţintei sale, acesta poate manipula planurile, concepţiile şi modul de ducere a luptei de către respectiva ţintă.[98] Rădăcinile controlului reflexiv în cadrul teoriei comportamentale au pus accentul pe influenţarea luării unei anumite decizii, sau adoptării unui anumit comportament cu legătură către adevăr, moralitate sau motiv.[99]

---

[95] *Ibidem,* p. 25.
[96] Timothy L. Thomas, „Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies*, 17: 237–256, 2004, p. 237.
[97] *Ibidem*, pp. 237, 238-243.
[98] *Ibidem*, pp. 241-243.
[99] *Ibidem,* p. 250; N.A.: aceasta este o diferenţă majoră între controlul reflexiv şi percepţia occidentală cu privire la conceptul de management al percepţiei, întrucât managementul percepţiei ia în calcul încrederea şi etica.

Folosirea de către Rusia a controlului reflexiv poate fi observată în cadrul operaţiilor informaţionale din anul 2014, odată cu anexarea Crimeii. Scopul informaţional primordial al Rusiei a părut a fi crearea unei profunde stări de confuzie şi îndoială la nivel internaţional, chiar până la nivelul de convingere a audienţei externe că toate ştirile şi rapoartele din regiune erau suspecte.[100]

Acest lucru a redus posibilitatea activării unui răspuns eficient din partea NATO şi SUA, pe măsură ce „poluarea informaţională" a slăbit opinia publică necesară politicienilor Occidentali pentru a trece la acţiuni ferme. Deşi au existat evidenţe clare că „omuleţii verzi" din Crimeea erau soldaţi ruşi, etica jurnaliştilor din Vest i-a obligat către diseminarea rapoartelor de negare emise de oficialii ruşi, pe fondul informaţiilor rezultate din urmărirea unor ziare şi posturi de ştiri deţinute de ruşi, cumulate cu „armata de luptători cibernetici" ce transmiteau comentarii fabricate.[101] Acest lucru a consolidat „legitimitatea" ştirilor false ale unor aşa-zişi localnici revoltaţi din Crimeea şi a creat suficientă incertitudine în măsură să slăbească hotărârea politicienilor Occidentali.

În timp ce publicul în democraţiile Occidentale se lupta să înţeleagă mesajele, transmise în mod deliberat confuze şi contradictorii, ce veneau din Crimeea, Rusia, în mod meticulos, a influenţat decidenţii din Ucraina. Pe măsură ce tensiunile au crescut, forţele armate ale Federaţiei Ruse au organizat în mare grabă un exerciţiu la graniţa cu Ucraina, distrăgând atenţia Ucrainei de la problema Crimeii către o ameniţare în termeni de supravieţuire a statului, care a indus temeri de lungă durată în sânul naţiunii ucrainiene.[102] Concomitent, Rusia a folosit atacul în adâncime pe canalele media (în special televiziunea) în cadrul comunităţilor etnice ruso-ucrainiene pentru a alimenta sentimentul de

[100] Keir Giles, „Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power", Chatham House, London: The Royal Institute of International Affairs, 2016, disponibil la https://www.chathamhouse.org/publication/russias-new-tools-confronting-west, accesat la 14.06.2019.
[101] *Ibidem*, p. 31.
[102] Adrian Croft, „NATO says Russia has big force at Ukraine's border, worries over Transdniestria", Reuters, 23 mar. 2014, disponibil la http://www.reuters.com/article/us-ukraine-crisis-nato/nato-says-russia-has-big-force-at-ukraines-border-worries-over-transdniestria-idUSBREA2M0EG20140323, accesat la 18.03.2019.

sprijin al anexării Crimeii în cadrul referendumului.[103] Aceste combinaţii de presiune informaţională au paralizat guvernul de la Kiev, împiedicând un răspuns eficient şi ferm la problema ocupării facilităţilor din Crimeea.[104] Departe de a fi o exercitare a managementului percepţiei, folosirea de către Rusia a controlului reflexiv pe timpul anexării Crimeii a subminat abilitatea politicienilor Occidentali de a se confrunta cu Rusia pe tema acţiunilor acesteia, prin exploatarea înţelegerii procesului decizional din Occident. Între timp, în Ucraina, Rusia a creat condiţiile unui referendum, considerat ulterior ilegal, care a asigurat pretextul pentru anexare prin direcţionarea mesajelor către etnicii ruso-ucrainieni, amplificând apoi teama ucrainienilor cu o posibilă invazie. Rezultatul final a constat în deciziile (sau non-deciziile) care au sprijinit obiectivele Rusiei.

Noua gândire militară a Rusiei subliniază tendinţa către „războiul nedeclarat" şi modul non-liniar de ducere a luptei. În practica acţiunilor militare ruse s-a produs o schimbare de la metodele tradiţionale, în care declaraţia de război era urmată de operaţii militare care începeau printr-o desfăşurare strategică, marile unităţi ducând lupte sub o ierarhie strictă, iar forţa umană şi puterea de foc fiind principalele elemente determinante ale războiului. Acum, noua gândire militară se concentrează efortul pe „lupte noncontact între unităţi cu mare mobilitate pe câmpul de luptă, acţiuni militare pe timp de pace, folosirea „civililor înarmaţi", precum şi managementul trupelor într-un cadru centralizat al mediului informaţional".[105]

Sunt aduse în prim plan câteva ameniţări la adresa securităţii. În primul rând, deşi retorica Moscovei cu privire la ultimele sale intervenţii aduce în discuţie legalitatea acţiunilor sale, calculul geopolitic rusesc

[103] Bret Perry, „Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations", in *Small Wars Journal*, 14 oct. 2015, disponibil la http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera, accesat la 11.03.2019.

[104] Mark Galeotti, „Hybrid War' and 'Little Green Men': How Does It Works and How It Doesn't", disponibil la http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt, accesat la 15.03.2019.

[105] J. Berzins, „Russia New Generation Warfare in Ukraine: Implications for Latvian Defene Forces", National Defence Academy of Lavtvia Center for Security and Strategic Research, 2014, p. 4.

este cel care stă la baza modului non-liniar de ducere a războiului şi el se bazează pe expansionismul necesar care să asigure securitatea în apropierea graniţelor. În al doilea rând, Rusia acţionează pentru paralizarea principalelor funcţii ale statului atacând prin toate mijloacele necesare şi folosind „operaţiile în adâncime". În al treilea rând, Rusia a desfăşurat rachete balistice cu rază mare de acţiune şi înaltă precizie, precum şi avioane şi sisteme avansate de apărare antiaeriană în regiunea Kaliningrad, fapt ce trimite un puternic semnal politico-militar UE, NATO şi SUA. Nu în ultimul rând, actuala doctrină militară a Rusiei (2014) menţionează NATO ca una din „principale pericole militare externe".[106] Aplicarea unor sintagme ale lui Clausewitz în noua perspectivă rusească de ducere a luptei, presupune promovarea pe scară largă a termenului de „ceaţă a războiului" (*fog of war*), prezentarea pentru inamic a unui „centru de greutate" ambiguu, concomitent cu reducerea la minimum a „factorului de fricţiune" în campania sa de război *non-liniar* (*hibrid* pentru Occident). O asemenea gândire necesită o structură politico-militară centralizată la nivel înalt, în paralel cu o descentralizare a libertăţii de acţiune, a stării de operativitate şi a capabilităţilor de luptă întrunite, cel puţin la nivel batalion, pentru unităţile de elită.

Gândirea militară rusă a început să acorde importanţă deosebită unităţilor de arme întrunite, în principal batalioanelor care rămân în luptă pentru o perioadă lungă de timp. În acest context militar, planificatorii nu mai percep războiul convenţional ca fiind potrivit numai misiunilor infanteriei uşoare, ci efortului combinat al diferitelor genuri de armă, tancurile îndeplinind misiuni vitale împreună cu infanteria, sprijinite de geniu şi de focul direct al artileriei.[107]

Rusia are nevoie de o „deghizare strategică" a acţiunilor de luptă armată (şi nu numai) şi de unele forme de „război politic" semi-acoperite pentru strategia sa complexă de război non-liniar. Deşi mulţi analişti ar fi tentaţi să afirme că elita politică şi militară din Rusia va

[106] ***, Doctrina Militară a Federaţiei Ruse, 2014.
[107] K. Gilles, A. Monagham, „Russian Military Modernization – Goal in Sight", *The Letort Paper,* SSI, 2014, pp. 2-3.

inventa o metodă nouă pentru a duce la îndeplinire aceste sarcini, de fapt ei se raportează la elemente adânc înrădăcinate în studiile teoretice sovietice, pentru care au destulă practică şi experienţă, şi anume „controlul reflexiv”.

Rusia se teme de o lovitură globală. Kremlinul este convins că ţările NATO se pregătesc pentru o lovitură globală care poate distruge Rusia în câteva minute, de aceea Rusia se străduieşte să arate SUA că este pregătită să răspundă unei astfel de provocări. Rusia crede că sunt posibile 3 războaie: primul este cel cu Ucraina, al doilea implică pregătirea pentru un război nuclear, iar al treilea război este cel de combatere a terorismului.[108]

[108] Oleh Starykov, “Military expert Starykov: Zapad-2017 war games in Belarus designed to demonstrate Russia’s military power”, disponibil la http://euromaidanpress.com/ 2017/08/30/military-expert-starykov-zapad-2017-war-games-in-belarus-designed-to-demonstrate-russias-military-power/, accesat la 09.06.2019.

Capitolul 3

ASPECTUL AGRESIUNII DE TIP HIBRID ÎN MEDIUL OPERAȚIONAL CONTEMPORAN

În secolul XXI, Europa este poziţionată într-un mediu strategic dinamic în care oponenții pot fi afectați semnificativ prin strategii hibride ce implică desfăşurarea unui ansamblu de acţiuni în multiple domenii, printre altele, în cel politic, militar sau social. Agresiunile violente din partea unor state sau a unor actori nestatali au loc într-un spectru larg, de-a lungul unor linii de operații convenționale și neconvenționale ce includ instrumente ale puterii de natură diplomatică, informațională, militară și economică. Capabilități cum ar fi cele A2/AD (anti-acces, area denial) compromit libertatea de acțiune în mediile de ducere a acțiunilor de luptă: aerian, terestru, maritim, cosmic și cibernetic.[109]

3.1. Mediul operaţional de manifestare a amenințării hibride

Caracteristicile care conduc spre evoluția aspectului conflictului modern includ abordarea cuprinzătoare şi integratoare, un amestec de activități directe și indirecte, creșterea nivelului de utilizare a unor mijloace de înaltă tehnologie și rolul particular jucat de operațiile informaționale. Toate acestea au dus războiul de la clasicul câmp de luptă într-o zonă gri între război și pace. Anul 2014 a marcat o schimbare dublă a paradigmei pentru Europa. În primul rând, conflictul ruso-ucrainean a evidențiat că folosirea forței armate și a violenței de către actorii statali pentru atingerea intereselor politice, a revenit în Europa. În al doilea rând, natura provocărilor de securitate a devenit în mod preponderent de natură hibridă. Analizând din punct de vedere geografic situaţia de securitate în zona euroaltlantică, precum şi în estul

[109] Luis Simon, „A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy”, în *War on the Rocks*, disponibil la https://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/ 03 mai 2016, accesat la 18.03.2019.

și în nordul Europei, putem afirma că Rusia a devenit, din nou, una dintre principalele cauze de ingrijorare. Două aspecte ies în evidență: comportamentul agresiv al Rusiei în estul Europei și militarizarea zonei Artice. La sud, Europa trebuie să facă față la numeroase provocări de securitate ca rezultat al situației complexe și instabile din Orientul Mijlociu și Nordul Africii (MENA). Statul Islamic a devenit o amenințare importantă, nu numai prin destabilizarea acestei regiuni, dar și ca urmare a recrutărilor luptătorilor și instruirii pe care o acordă acestora, luptători care, la un moment dat se întorc în țările lor de origine din Europa.

Un alt aspect îl reprezintă valul de emigranți și refugiați care continuă să vină în Europa din MENA. Această mișcare a creat serioase probleme economice, umanitare și chiar politice. În același timp, această mișcare creează oportunități pentru organizațiile extremiste violente și cel de crimă tranfrontalieră să obțină avantaje din această criză pentru a avea acces către Europa. Europa, de asemnea, se luptă cu viitoarele provocări la adresa securității ce includ creșterea capabilităților rachetelor balistice ale adversarilor, proliferarea armelor de distrugere în masă, răspândirea bolilor infecțioase, atacurile cibernetice, terorismul internațional și național, narco-terorismul și traficul ilicit. O contribuție la complexitatea mediului de securitate european o reprezintă și provocarea financiară întrucât câteva economii europene nu sunt în forma cea mai bună, ducând la instabilitate.

În viitor, forțele militare naționale sau ale Alianței vor continua să opereze într-un mediu din ce în ce mai complex, care va lansa provocări din ce în ce mai variate și mai neașteptate. De aceea, este necesară formularea de previziuni și opinii privind configurația mediului operațional al viitorului și tendințelor privind amenințările ce pot apărea în acest context. Aceste proiecții ale conflictelor viitorului permit planificatorilor militari o mai bună înțelegere a contextului în care vor opera forțele și stabilesc direcții și concepte pentru dezvoltarea capabilităților militare ale forței armate a viitorului.

Mediul operațional va continua să evolueze, prezentând forțelor militare provocări variate sub forma amenințărilor generate de către

oponenți care desfășoară acțiuni al căror caracter variază de la convențional la neconvențional, cu capabilități care presupun armament și tehnologie de ultimă generație. Aceşti oponenţi pot include în compunerea lor forţe convenţionale extrem de bine pregătite şi echipate şi forţe specializate în desfăşurarea acţiunilor de luptă neregulate, rezultatul fiind o forţă care întrebuinţează ameninţarea de tip hibrid. În plus, în cele mai multe cazuri, nu se poate conta pe sprijinul populației locale în eliminarea acestor amenințări.

Deși conflictele ultimilor ani au avut un caracter asimetric, posibilitatea ca în viitor să apară operații majore de tip combat nu este de neluat în seamă. Aşa cum se specifică şi în literatura de specialitate internaţională, ipoteticul adversar al conflictelor viitoare va continua să fie unul care utilizează forţe neregulate, cuprinzând elemente care variază de la insurgenţi bine antrenaţi şi cu o mare experienţă de luptă care urmăresc schimbarea guvernării locale sau realizarea unor deziderate de ordin religios şi până la grupări criminale sau tribale care urmăresc menţinerea controlului în anumite zone pentru a-şi atinge obiectivele economice. În majoritatea cazurilor, este de aşteptat ca aceste tipuri de forţe să acţioneze împreună, rezultând ameninţarea hibridă, ca o combinaţie între forţe, echipamente şi tactici convenţionale şi neconvenţionale.

Indiferent de scopul urmărit, oponentul din mediul operaţional viitor va fi unul extrem de adaptabil şi „fluid”, fiind în măsură să utilizeze o paletă largă de mijloace tehnologice, echipamente şi proceduri, combinate cu armament convenţional şi mijloace improvizate. În multe zone de posibil conflict, cultura de tip tribal şi sentimentul intrinsec de repulsie manifestat de către populaţia indigenă va duce, cel puţin în faza iniţială, la o lipsă de cooperare cu forţele proprii. Soluţia constă în acţiuni menite să convingă populaţia locală că obiectivul final al prezenţei militare în zonă este de a-i reda şi proteja valorile vitale, cum ar fi securitatea pe termen lung şi un nivel acceptabil de trai. Astfel, mediul operaţional viitor se configurează ca unul extrem de ambiguu şi nesigur, în care forţele proprii trebuie să lupte cu un inamic bine pregătit şi extrem de motivat, cu o bună cunoaştere a

terenului, uneori sprijinit de către grupuri formate din localnici şi care este în măsură să întrebuinţeze ameninţări hibride.

Doctrina britanică evidenţiază extrem de pragmatic caracterul conflictelor militare viitoare: „Conflictul viitorului nu va fi o ştiinţă exactă: el va rămâne o activitate umană unică şi imposibil de prevăzut cu exactitate. Adversarii (statali sau nestatali) şi ameninţările (convenţionale şi neconvenţionale) vor fi în configuraţie mixtă. Paleta ameninţărilor se va extinde, incluzând proliferarea armelor de nimicire în masă, atacurile cibernetice şi alte noi ameninţări neregulate”[110].

În ceea ce priveşte actorii care vor evolua în mediul operaţional viitor, trebuie să-i analizăm ţinând cont de tipul lor: statali, nestatali şi suprastatali.

Actorii statali – estimăm că în viitor va creşte numărul statelor care vor urmări accesul şi controlul asupra resurselor şi influenţei, situaţie care, coroborată cu eşuarea anumitor state va genera stări de instabilitate şi de conflict, în special în Africa, America Centrală, Asia Centrală şi Orientul Mijlociu. Este de aşteptat ca unii factori adiţionali, cum ar fi extremismul religios sau etnic, să adauge mai multă volatilitate acestor situaţii conflictuale. Rivalitatea dintre aceste state poate duce la apariţia unor războaie purtate prin intermediari, o formă de conflict foarte greu de controlat. Proliferarea armelor de distrugere în masă şi controlul acestora readuce în atenţie ameninţarea de tip catastrofic, caracteristic acestor actori.

Actorii nestatali – din punct de vedere al nivelului ameninţărilor viitoare, diferenţa dintre actorii statali şi cei nestatali se va diminua sensibil. Actorii nestatali violenţi vor avea acces din ce în ce mai mult la mijloace tehnologice avansate, în special în domeniul informaţiilor, şi vor fi în măsură să le exploateze pentru atingerea unor obiective de importanţă deosebită, cum ar fi influenţarea opiniei publice interne şi internaţionale, afectarea legăturilor economice şi de comunicaţii. Ei îşi vor dezvolta mijloace şi metode de atac (chiar arme de distrugere în

[110] ***, *Strategic trends programe. Future character of conflict*, UK Ministery of Defence, 02.02.2010, p. 6, disponibil la https://www.gov.uk/government/publications/future-character-of-conflict, accesat la 17.03.2019.

masă) cu efecte suficient de puternice încât să penetreze sistemele de protecţie ale forţelor convenţionale. Toate aceste argumente contribuie la concretizarea concluziei că în mediul operaţional viitor, actorii nestatali nu vor reprezenta ameninţări „de mâna a doua”.

Actorii suprastatali – este de aşteptat ca, şi în viitor, alianţele şi coaliţiile militare să reprezinte principalul tip de actor care să exercite influenţa instrumentului militar. Interesul global va impune permanent un răspuns multinaţional configurat pe un sistem internaţional de reguli şi relaţii. Alianţele pot predefini în mod eficient interesele privind securitatea şi apărarea colectivă, precum şi ameninţările asociate şi tipul de răspuns la acestea. Cerinţa de a sprijini stabilitatea sau de a întreprinde activităţi în sprijinul păcii în regiuni „volatile” cum ar fi Balcanii sau în state eşuate va persista, alături de necesitatea contracarării ameninţărilor generate de actorii nestatali atât asupra elementelor instrumentului militar prezent în zonă, cât şi asupra populaţiei, infrastructurii şi mediului cibernetic „de acasă”. Proliferarea armelor de distrugere în masă şi a atacurilor în mediul virtual necesită dezvoltarea capabilităţilor credibile în măsură să contracareze acest tip de ameninţări, în special prin prevenţie.

Războiul rămâne un cameleon iar gri a devenit noua culoare a acestuia. Când vorbim despre „gri”, doi actori sunt evidențiați: Rusia și așa numitul Stat Islamic (IS/Islamic State).

Rusia a dezvoltat conceptul de agresiune hibridă pe baza studiilor aprofundate asupra Occidentului și a comportamentului altor actori de succes și a elaborat cu multă atenție un cadru conceptual, pe care l-a testat și în final l-a aplicat în operații.[111] Cadrul conceptual a fost prezentat pentru prima dată de generalul Valery Gherasimov, șeful Statului Major General al Federației Ruse în ianuarie 2013, la o întânire anuală a Academiei Militare de Științe ruse: „Experiența conflictelor militare confirmă faptul că un stat prosper poate, în numai câteva luni sau zile, să fie transformat într-o zonă de conflict armat feroce, să devină a victimă a intervenției străine, să se scufunde în haos, să devină o

[111] Ralph Thiele, „Crisis in Ukraine – The Emergence of Hybrid Warfare”, ISPSW Strategy Series, 2015.

catastrofă umanitară, un război civil...[112]. La un an şi două luni după această declaraţie, Crimeea devenea teritoriu rusesc în urma a ceea ce a fost considerat de către specialişti drept agresiune de tip hibrid de manual. Considerate în ansamblu, prezentarea şi apoi aplicarea conceptului de „război neliniar", aşa cum a fost denumit de către Gherasimov, constituie o lecţie dură dată comunităţii internaţionale.

IS a apărut ca o organizație hibridă *per se*, urmând cumva modelul Hezbollah, adică o parte de rețea teroristă, o parte de armată de gherilă și o parte de entitate statală. Principalele sale trăsături sunt:

- tactici diferite – forțele IS cuprind unități paramilitare foarte apropiate de cele militare tradiționale precum și celule mai mici, semi-autonome, ce combină atât tactici şi proceduri de luptă tradiționale cu cele de gherilă. Forțele IS dețin o mare varietate de armament, inclusiv de ultimă generaţie, de la mijloace explozive improvizate la mine la rachete, drone și arme chimice.

- structură flexibilă și adaptabilă – IS este capabilă să absoarbă și să desfășoare rapid resursele la dispoziție. Chiar dacă dispune permanent de noi recruți şi mercenari, noi mijloace de luptă sau dețin teritorii noi, organizaţia este capabilă ca în mod constant să încorporeze aceste mijloace în strategia sau structura lor şi să le întrebuinţeze rapid în luptă.

- terorism – prin acte de violență exagerate, uneori grotești, IS își comunică ideologia către audiența globală.

- propagandă și război informațional – campaniile de social media ale IS accentuează clar și atent mesajele. Fiecare postare, video sau blog conţine componente care urmăresc să glorifice și recruteze membri pentru cauza lor.

- activitate criminală – IS folosește o varietate de metode pentru finanțarea acțiunilor sale și se mândrește cu un portofoliu diversificat de investiții: piața neagră a vânzării de petrol, grâu și antichități; banii din răscumpărări etc. Donațiile reprezintă și ele o parte însemnată a surselor

[112] General Valery Gerasimov, „Speech at the annual meeting of the Russian Academy of Military Science", *Military-Industrial Courier*, Moscow, 2013, disponibil la http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf, accesat la 17.02.2019.

de finanțare iar IS se asigură prin toate mijloacele că rămâne un grup solvabil din punct de vedere financiar.

- dispreț față de legile internaționale – în baza interpretării extreme a legii Sharia, IS desfăşoară acţiuni violente împotriva femeilor și minorităților, incluzând pedepsirea barbară a acestora cum ar fi amputarea membrelor, bătaia cu pietre, etc. Nu au niciun respect umanitar şi nici norme legale.

Literatura militară de specialitate, în special cea din occident, cuprinde o serie de previziuni privind domeniile mediului global de securitate al viitorului care vor genera ameninţări în mediul operaţional. Sunt menţionate schimbările climatice, creşterea demografică, globalizarea şi impactul ei asupra societăţii, scăderea resurselor energetice şi creşterea necesităţii de a utiliza altele noi, apariţia unor state eşuate, mişcările ideologice bazate pe convingeri religioase sau de identitate, creşterea dezechilibrului economic dintre actori, avansul tehnologic în domeniul militar şi civil etc.

Schimbările climatice sunt un factor relativ nou în configurarea ecuaţiei mediului operaţional. Impactul acestuia se manifestă sub două aspecte. Primul priveşte direct modelarea dimensiunii spaţiale a mediului operaţional, în sensul în care implică necesitatea de a desfăşura operaţii în zone de deşert sau lipsite de apă sau în condiţii meteo extreme, cu temperaturi foarte scăzute sau foarte ridicate pentru o perioadă îndelungată de timp. Un al doilea aspect se referă la impactul asupra populaţiei din zonele afectate de schimbările climatice, în sensul în care aceasta nu va fi în măsură să se adapteze rapid, iar statele respective nu vor fi în măsură să întreprindă la timp acţiuni eficiente pentru eliminarea urmărilor. Aceste situaţii pot duce la creşterea instabilităţii sociale, în special în zonele sensibile, expuse şi la alte tipuri de presiuni.

Creşterea demografică va genera suprapopularea, în special în zonele urbane, situaţie care va duce în mod automat la creşterea cererii de resurse. În condiţiile în care resursele energetice se diminuează în timp, putem considera această situaţie ca pe un factor generator de tensiune. Există posibilitatea ca în viitor, statele care vor considera că securitatea resurselor energetice sau cele de apă şi hrană sunt o problemă

naţională de supravieţuire să acţioneze violent la orice semn de ameninţare. În plus, există riscul apariţiei, chiar şi în statele puternic dezvoltate, a unui fenomen de segregare a societăţii pe criterii etnice sau religioase, care să ducă la manifestarea extremismului sau a altor fenomene sociale ce pot genera instabilitate socială.

Globalizarea şi implicaţiile ei au fost îndelung discutate în rândul specialiştilor militari şi civili, ajungându-se la concluzii contradictorii privind beneficiile aduse de acest fenomen. Privită ca o consecinţă naturală a societăţii dezvoltate, globalizarea creează, pe lângă beneficiile cooperării, şi vulnerabilităţi care pot favoriza apariţia unor situaţii de instabilitate şi conflict. De exemplu, nivelul avansat de conectivitate şi versatilitate în domeniul comunicaţiilor permite acum extremiştilor sau grupurilor teroriste să transmită lumii întregi metodele, convingerile, ideologiile şi mesajele lor, generând tensiune şi instabilitate şi facilitând apariţia conflictului.

Globalizarea presupune cooperarea în ceea ce priveşte comerţul, piaţa de capital, proprietatea intelectuală, resursele şi diverse alte activităţi economice. Cooperarea se realizează pe suportul unei infrastructuri vaste şi complexe, realizată din elemente de naturi diferite, de la unde electromagnetice şi legături de date şi până la linii maritime, drumuri sau căi ferate. Această infrastructură are vulnerabilităţile ei, iar menţinerea controlului asupra întregului sistem devine o provocare extrem de mare. Orice ameninţare la adresa securităţii infrastructurii poate genera riscuri cu consecinţe majore.

Resursele energetice sunt considerate un element de importanţă capitală, iar controlul asupra exploatării şi distribuirii acestora este un permanent generator de tensiuni. Zonele bogate în resurse naturale (Orientul Mijlociu, Asia, Africa, zonele arctice), în special în hidrocarburi, au fost şi vor rămâne un subiect permanent de dispută în contextul geopolitic global. În contextul în care nivelul ridicat de dezvoltare din unele state necesită un consum de resurse pe măsură, este de aşteptat ca şi disputele pentru controlul acestor zone să fie acerb.

Statele eşuate vor constitui permanent o problemă importantă pentru securitatea globală. Ele apar în special din cauza guvernării

deficitare (provocată de cauze interne sau externe) sau problemelor de ordin economic sau social şi sunt prevalente în zone precum Africa, Orientul Mijlociu sau America Centrală. De cele mai multe ori aceste „eşuări" ale statelor sunt însoţite de acte de violenţă care, chiar dacă se manifestă în interiorul graniţelor, generează instabilitate în exterior prin faptul că pun în pericol viaţa cetăţenilor altor state sau înţelegerile de ordin economic, politic sau social cu acestea.

Operaţiile în asemenea zone de conflict au un caracter deosebit de complex întrucât pot include ameninţări de tip hibrid materializate prin combinaţii de luptă armată, acţiuni de gherilă, luare de ostatici, crize umanitare, acţiuni teroriste, uneori îndreptate împotriva populaţiei indigene etc. Faptul că operaţiile în asemenea zone de conflict presupun, de cele mai multe ori, prezenţa populaţiei indigene contribuie la creşterea complexităţii şi a dificultăţii operaţiilor.

Convingerile ideologice, în special pe criterii religioase sau de identitate, constituie un important factor generator de instabilitate şi, în consecinţă, de ameninţări. Grupările politice bazate pe convingerile religioase sau pe extremism naţionalist vor constitui actori foarte prezenţi în mediul operaţional al viitorului. O caracteristică fundamentală a acestui tip de actori este faptul că motivaţia lor ţine de convingeri, de credinţă, iar aceasta nu poate fi limitată de graniţele geografice. Un alt aspect foarte important este faptul că aceste convingeri pot fi uşor de exacerbat, ajungându-se la fanatism.

Creşterea dezechilibrului economic se concretizează, de regulă, între actorii statali şi duce la apariţia unor relaţii de dependenţă pe criterii economice sau tratament preferenţial ce poate genera instabilitate regională. Acest factor, ca şi cel legat de resursele energetice, poate genera ameninţări din partea unor actori cu putere militară convenţională apreciabilă, situaţie care ar putea duce la un conflict armat major.

Avansul tehnologic este cel care „înarmează" ameninţarea şi acţionează ca un catalizator în momentul manifestării ei, în special prin capabilităţile de comunicare. Unul dintre cele mai periculoase tipuri de scenarii presupune întrebuinţarea armamentului convenţional avansat şi a tehnologiei de ultimă generaţie în acţiuni de tip neconvenţional cum ar

fi acţiunile teroriste. Desigur că acest scenariu ar putea fi agravat prin înlocuirea armamentului convenţional avansat cu arme de distrugere în masă, ajungându-se la tipul de ameninţare *catastrofică.* Pe de altă parte, statele puternic dezvoltate îşi pun întrebarea dacă este mai eficient să continue investiţiile şi eforturile în sensul creşterii nivelului de tehnologizare a armatei sau să-şi concentreze eforturile pentru a dezvolta alte direcţii cum ar fi noi metode şi mijloace de instruire a personalului, astfel încât acesta să fie în măsură să contracareze ameninţările „de nişă" caracteristice conflictului de tip hibrid.

Analiza fizionomiei mediului operaţional viitor şi a ameninţărilor ce se pot manifesta în acesta este o condiţie obligatorie pentru determinarea direcţiilor viitoare de dezvoltare a instrumentului militar. Putem deduce necesitatea dezvoltării unei forţe cu multiple specializări, care să fie în măsură, pe de o parte, să contracareze o mare varietate de ameninţări şi, pe de alta, să participe la un efort conjugat desfăşurat în zona de conflict, întrucât este de aşteptat ca rareori instrumentul militar singur să aducă şi mai ales să securizeze victoria. Asigurarea succesului pe o perioadă lungă de timp va solicita, în mod invariabil, o abordare cuprinzătoare a conflictului şi a perioadei postconflict prin integrarea tuturor instrumentelor de putere a unei naţiuni sau coaliţii.

Un alt aspect ce rezultă din această analiză este faptul că în ecuaţia conflictului viitorului, avantajul strategic conferit unui actor de către puterea militară poate fi diminuat prin anumite metode şi mijloace întrebuinţate în aplicarea ameninţării de către un ipotetic adversar ce are capabilităţi militare net inferioare.

Este esenţial să avem în vedere atingerea obiectivelor urmărite şi momentul încheierii conflictului. În condiţiile în care operaţiile militare se desfăşoară într-un mediu cu un profund caracter neregulat, atât prin aspect, cât şi prin compoziţie, ele tind să devină un mozaic cu o complexitate foarte ridicată. În acest sens, este foarte mare probabilitatea ca atingerea obiectivelor militare să fie departe de atingerea obiectivelor politice urmărite. De aceea, este foarte important ca nivelul de decizie politico-militar să fie în măsură să determine tipul de acţiune non-militară care trebuie întreprinsă, precum şi instrumentele şi momentul

declanşării acesteia pentru a înlocui sau completa acţiunea militară în scopul realizării stării finale şi încheierii conflictului.

3.2. Model de configurare a agresiunii de tip hibrid

Conceptul „hibrid” și strategiile aferente vizează vulnerabilitățile ţintei, de la atacurile cibernetice asupra sistemelor de informaţii critice până la dezmembrarea unor servicii esenţiale, cum ar fi aprovizionarea cu energia sau serviciile financiare, pentru a diminua încrederea opiniei publice în instituțiile guvernamentale și coeziunea socială. În acest fel, opinia publică a devenit o țintă atractivă. În mod evident, spațiul cibernetic conţine unele dintre cele mai semnificative vulnerabilităţi. Prin intermediul mediului cibernetic totul este indisolubil interconectat: sistemele, masinile, oamenii. Totul poate fi distrus, alterat sau scos din funcțiune din orice loc, fără a ști când un atac este lansat, unde va lovi și cum. Ambiguitatea care rezultă în urma unor astfel de acțiuni agresive fac contracararea destul de dificilă, în principal pentru societățile sau organizațiile multinaționale care funcționează pe principiul consensului cum ar fi UE și NATO.

„Războiul hibrid” este, fără îndoială, de nivel strategic iar puterea lui derivă din aspectul de variație complexă de acțiuni agresive care implică în mod simultan actori statali și non-statali, cu folosirea unor mijloace convenționale și neconvenționale, acțiuni care nu sunt limitate la un anume câmp de luptă fizic. Trei carateristici ies în evidență:

- ţintele războiului/conflictului trebuie căutate în principal la nivelul centrului de greutate de natură non-militară;
- operațiile desfăşurate împotriva unor vulnerabilități specifice ale oponentului şi în umbra unor interdependențe sunt provocatoare pentru liniile de operații, precum și pentru domeniile şi zonele de responsabilitate tradiționale;
- prin combinarea unor concepte, metode și mijloace diferite, „noile” forme ale războiului și luptei sunt în plină evoluție.

„Războiul hibrid” angajează o gamă variată de instrumente şi acţiuni în întreg spectrul conflictului (tradițional sau neregulat) – forța armată, tehnologia, criminalitatea, terorismul, presiunea economică și

financiară, mijloace umanitare și religioase, informațiile, sabotajul, influenţarea şi dezinformarea. Toate acestea sunt desfăşurate într-un ansamblu realizat într-o abordare ascunsă și cu o capacitate distrugătoare, exercitat în baza unei strategii flexibile care afectează în mod indirect centrul de greutate, fără a fi limitat la un anume câmp de luptă fizic. Mai mult, actorii implicați într-o astfel de confruntare folosesc fiecare oportunitate din orice mediu, în funcție de resursele la dispoziție, inclusiv instrumentele mass-media tradiționale și moderne. Acestora li se adaugă şi implicarea forţei fizice exercitată prin actorilor nestatali intermediari ce pot include milițiile, organizațiile de criminalitate organizată transnaționale sau rețelele teroriste. Dacă în trecut, tactica folosită de grupările neregulate era considerată replica celui slab în faţa celui puternic, în contextul agresiunii de tip hibrid, aceasta devine apanajul celui puternic care o întrebuinţează în mod indirect pentru a desfăşura acţiuni dificil de contracarat prin mijloace şi căi convenţionale.

Ameninţarea de tip hibrid este extrem de complexă, iar modalitatea de contracarare a acesteia trebuie să fie pe măsură. Răspunsul adecvat acestui tip de ameninţare trebuie să fie configurat prin realizarea în mod ingenios şi inteligent a unor conexiuni transdisciplinare reale între domeniile de vârf ale ştiinţei militare.

Este important să precizăm faptul că, în prezent, în mediul internațional ştiinţific, dar şi în cel operaţional, se depune un efort semnificativ în scopul definirii ameninţării de tip hibrid şi modalităţilor în care aceasta se poate pune în aplicare, devenind, astfel, agresiune.

Urmând modelul *Quad chart* al lui Nathan Freier[113], dinamica ameninţării de tip hibrid presupune acţiunea concertată a patru tipuri de ameninţări – *tradiţionale* (convenţionale), *neregulate* (neconvenţionale),

[113] Nathan P. Freier, „Present at the Counterrevolution: An Essay on the 2005 National Defense Strategy and Its Impact on Policy”, *United States Army War College Guide to National Security Issues*, Vol. 2: National Security Policy and Strategy, pp. 120-121, coordonator J. Boone Bartholomees, ediția a 4-a, iulie, 2010.

catastrofice şi *disruptive*[114] – asupra centrului de greutate al actorului ţintă, ceea ce duce la distrugerea acestuia.

Adiţional, se poate desprinde o caracteristică importantă conform căreia, în mediul operaţional de tip hibrid, ponderea acţiunilor, din perspectiva tipologiei, prezintă o puternică migraţie de la cele regulate spre cele neconvenţionale, în special către cele de tip asimetric.

În literatura de specialitate, se utilizează foarte des termenul *ameninţare hibridă* în locul celui de *agresiune hibridă*. Considerăm că motivele ar putea proveni din două situaţii. Pe de o parte, se doreşte evidenţierea caracterului proactiv al acţiunilor de contracarare a agresiunii de tip hibrid, prin eliminarea ameninţării, înainte ca acesta să se manifeste, devenind agresiune (totuşi, nu se ia în consideraţie situaţia în care o ameninţare poate deveni, în sine, agresiune). Pe de altă parte, lipsesc reglementările prin care un complex de acţiuni să poată fi declarat, în mod oficial, agresiune de tip hibrid. În măsura în care, în documentele oficiale din domeniul dreptului internaţional public, agresiunea de tip hibrid nu a fost definită complet, se deduce ideea conform căreia criteriile prin care se poate identifica agresorul şi dovedi agresiunea lipsesc sau sunt neclare. În consecinţă, se preferă termenul *ameninţare*, întrucât acesta oferă cadrul oficial desfăşurării unor măsuri preventive împotriva unor acţiuni potenţiale, considerate agresiuni.

Configurarea agresiunii de tip hibrid presupune un efort considerabil; ea trebuie să fie realizată printr-un proces complex, similar celui de planificare operaţională (produsul se constituie într-o serie de acţiuni în toate domeniile asimilate operaţiilor militare) şi care trebuie desfăşurat de către un actor cel puţin raţional, dacă nu chiar super-raţional. Dacă ţinta percepe acţiunile agresorului ca fiind iraţionale, înseamnă că agresiunea de tip hibrid care le subsumează este bine configurată şi aplicată. Cu cât mai iraţională pare agresiunea, cu atât mai mult aceasta creşte în valoare şi îşi amplifică efectele, iar ţintei îi va fi mai dificil să genereze un răspuns adecvat.

[114] N.A.: termenul *disruptiv* provine din *disruptive* (en.) şi este considerat cu sensul de scoatere din funcţiune, afectare a funcţionării unui sistem, fără a-l distruge.

Considerând un mediu operaţional în care coexistă mai mulţi actori de tip statal sau non-statal, configurarea ameninţărilor pe care le poate genera fiecare dintre aceştia şi, în final, a celor pe care un agresor le poate aplica asupra unei ţinte, necesită o atenţie deosebită, un mare nivel de cunoaştere a posibilităţilor de acţiune ale fiecăruia, o capacitate ridicată de sinteză şi chiar o imaginaţie bogată.

Pentru a oferi un model teoretic complet, în cele ce urmează, considerăm că suntem în afara mediului analizat şi, astfel, excludem posibilitatea plasării noastre în rolul agresorului sau al ţintei. Obiectivele urmărite vizează obţinerea de date eficient structurate pentru a estima impactul pe care îl pot avea acţiunile agresorului în mediul operaţional asupra ţintei, compunerea lor şi modul în care se realizează conexiunile între diferite tipuri de agresiuni (componente) pentru a se obţine configuraţia de tip hibrid. Pentru ca acest proces să se desfăşoare în mod eficient, este necesară parcurgerea a şapte etape, pe care le voi expune în cele ce urmează.[115]

1. Prima etapă constă în identificarea ameninţărilor ce pot apărea în mediul operaţional şi redarea lor într-o formă tabelară, alături de caracteristici specifice acestora, astfel: domeniu, ameninţare, mijloace, efecte, risc, importanţă (impactul asupra ţintei), probabilitate şi frecvenţă de apariţie.

Aceasta se realizează prin analiza mediului operaţional şi de securitate în care se află actorii. Pentru operativitate, se poate utiliza o listă standard care să fie adaptată şi completată corespunzător mediului respectiv şi caracteristicilor actorilor. Se recomandă ca primul criteriu de ordonare descrescătoare a ameninţărilor să fie cel al nivelului de risc, şi anume al produsului dintre impactul şi probabilitatea de apariţie a fiecărei ameninţări. Lista va fi definitivată după parcurgerea etapelor de analiză a actorilor, privind capabilităţile şi vulnerabilităţile lor. În tabelul de mai jos este prezentat câte un exemplu pentru fiecare domeniu: politic, militar, economic, social, informaţii, infrastructură, securitate (PMESII-S).

---

[115] Dan-Lucian Petrescu, „Model avansat de configurare a agresiunii de tip hibrid”, Revista *Impact strategic*, nr. 2[63]/2017, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, pp. 45-52.

Model privind identificarea ameninţărilor ce pot apărea în mediul operaţional

DOMENIU	AMENINŢARE/ AGRESIUNE	MIJLOACE	EFECTE	R	I	PI	FA
POLITIC	Subminarea încrederii populaţiei în autorităţile de guvernare	Formatori de opinie, informaţii, timp	Diminuarea/ pierderea controlului asupra politicii interne şi externe	R	4	0,75	P
MILITAR	Inserţia unor forţe pentru operaţii speciale (FOS) fără însemne care să joace rolul unor miliţii locale	FOS, mercenari	Fabricarea unui motiv pentru intervenţia militară sau destabilizarea ordinii interne	R	4	0,75	M
ECONOMIC	Subminarea relaţiilor economice externe ale ţintei pe domeniile critice ale acesteia (ex. exportul de resurse) prin concurenţă neloială sau alte mijloace	Resurse economice, influenţă	Reducerea veniturilor la bugetul de stat, afectarea procesului de dezvoltare economică	R	4	0,75	P
SOCIAL	Infiltrarea unor formatori de opinie care să polarizeze populaţia din statul ţintă	Personal specializat, informaţii, timp	Afectarea coeziunii sociale	S	2	0,5	P
INFORMAŢII	Promovarea prin formatori de opinie (în mass-media sau mediul virtual) a ineficienţei autorităţilor sau a incompetenţei clasei politice	Formatori de opinie, informaţii, circumstanţe, timp	Diminuarea sprijinului acordat de populaţie autorităţilor şi structurilor de guvernare	M	3	0,75	P
INFRASTRUC-TURĂ	Distrugerea unor elemente de infrastructură critică (centrale electrice, treceri permanente etc.)	FOS, mercenari, informaţii	Distrugeri, victime sau afectarea vieţii societăţii	R	4	0,75	R
SECURITATE	Subminarea autorităţilor statului ţintă (sistemul de securitate internă cel de impunere a legii, sistemul de justiţie etc.	Agenţi infiltraţi, resurse financiare, informaţii, timp	Diminuarea capacităţii statului de a-şi asigura securitatea proprie	R	4	0,75	P

Gradul de risc (R) reprezintă produsul între probabilitatea de apariţie şi impactul asupra ţintei şi poate avea valorile Scăzut (0-1,25), Mediu (1,25-2,75), Ridicat (2,75-4). Impactul (I) poate fi 1=*slab*, 2=*mediu*, 3=*ridicat*, 4=*critic*. Probabilitate independentă (PI) este de forma 0,xx şi se exprimă în multipli de 0,25. Frecvenţa de apariţie (FA) poate avea valorile *Singulară, Redusă, Medie, Mare, Permanentă*.

2. Cea de-a doua etapă presupune *analiza capabilităţilor actorilor* din mediul operaţional (din punctul de vedere al instrumentelor, resurselor, pregătirii, doctrinei, acţiunilor anterioare) de a genera agresiunile ce pot compune o ameninţare de tip hibrid. De aici rezultă (se poate selecta dintr-o listă constituită apriori) setul de agresiuni independente pe care fiecare actor le poate aplica asupra unei ţinte oarecare. Pentru a sprijini etapele următoare, se recomandă consemnarea, în dreptul fiecărei ameninţări, a actorilor ce se pot constitui în potenţiale ţinte.

3. Cea de a treia etapă constă în *identificarea agresorului şi a ţintei*. Considerând cazul general ce implică posibilitatea declanşării confruntării de tip hibrid între oricare dintre actorii existenţi în mediul operaţional, în acest stadiu se realizează analiza relaţiilor dintre actori, pentru care se recomandă utilizarea metodei MACTOR[116] inventată de către analistul francez Michel Godet. Rezultatele obţinute oferă posibilitatea stabilirii argumentate a alianţelor şi conflictelor ce pot apărea între actori şi, în consecinţă, permit identificarea agresorului şi a ţintei. Strategiile determinate pot include realizarea de alianţe între diferiţi actori, caz în care rezultă noi actori cu capacităţi combinate şi care pot genera ameninţări de tip hibrid în configuraţii sau cu ponderi ale elementelor componente specifice acestora. Pentru a avea imaginea corectă, este necesar să se analizeze agresiunile şi efectele compuse

[116] N.A.: MACTOR reprezintă matricea alianţelor şi conflictelor: tactici, obiective, recomandări. Metoda a fost prezentată în original în lucrarea *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994, p. 105. În formă adaptată, a fost prezentată în „The prospective analysis of strategic relations between geopolitical actors in the contemporary security environment - the MACTOR method", în cadrul Conferinţei internaţionale *Strategies XXI – Strategic Changes in Security and International Relations*, organizată de către Facultatea de Securitate şi Apărare şi Şcoala Doctorală din Universitatea Naţională de Apărare „Carol I" în perioada 14-15 aprilie 2016, vol. 1, pp. 62-72, disponibil la https://www.strategii21.ro/index.php/ro/conference-proceedings.

aferente părţilor rezultante implicate în conflict. De asemenea, nu trebuie uitat faptul că structura ameninţării de tip hibrid (din punct de vedere cantitativ şi calitativ) depinde fundamental, în afară de capacităţile generatorului, de vulnerabilităţile, dar şi de punctele tari ale ţintei (se recomandă evitarea/erodarea punctelor tari şi „ochirea" vulnerabilităţilor).

4. În următoarea etapă se realizează *analiza ţintei* (analiza SWOT şi analiza structurală), urmărindu-se identificarea vulnerabilităţilor şi, respectiv, a variabilelor operaţionale cheie ce direcţionează acţiunile agresorului.

Din analiza SWOT, rezultă vulnerabilităţile ţintei care, aşa cum am precizat, vor constitui obiective pentru agresor. Vulnerabilitățile determină o a doua selecţie a acţiunilor pe care agresorul are posibilitatea şi trebuie să le aplice asupra ţintei pentru a-şi atinge scopul. Prin urmare, rezultatul analizei SWOT a ţintei determină în mod decisiv stabilirea setului de agresiuni care se adresează ţintei şi, în plus, alături de rezultatele analizei structurale, contribuie la cristalizarea strategiilor de combinare a acestora pentru maximizarea efectelor (în special rezultatele relaţiilor puncte tari – oportunități și amenințări – puncte slabe).

Analiza structurală[117] a ţintei permite descrierea stării actorului ţintă prin prezentarea caracteristicilor acestuia ca variabile de sistem şi a relaţiilor dintre ele, precum şi prin identificarea aspectelor relevante în măsură să justifice strategii posibile ale agresorului care nu pot fi deduse pe cale intuitivă. Trebuie specificat faptul că variabilele de intrare sunt, în primul rând, vulnerabilităţile ţintei determinate din analiza SWOT. Pe lângă acest produs de natură descriptivă, rezultatele obţinute evidenţiază variabilele cheie prin intermediul cărora agresorul poate influenţa

[117] N.A.: Metoda a fost inventată de către Michel Godet şi J.C. Duperrin în 1973 şi este denumită MICMAC (*Matrice d'Impacts Croisés – Multiplication Appliquée à un Classement*). În formă adaptată, a fost prezentată în „*Structural analysis of hybrid aggression target*", în cadrul Conferinţei internaţionale „*Strategies XXI – Strategic Changes in Security and International Relations*", organizată de către Facultatea de Securitate şi Apărare şi Şcoala Doctorală din Universitatea Naţională de Apărare „Carol I" în perioada 06-07 aprilie 2017, vol. 1, pp. 87-94, disponibil la adresa https://www.strategii21.ro/index.php/ro/conference-proceedings, accesat la 04.04.2019.

dinamica stărilor ţintei astfel încât să o dezechilibreze. Nu trebuie uitat faptul că „unul dintre obiectivele principale urmărite de ameninţările de tip hibrid este destabilizarea guvernării şi instituţiilor principale ale oponentului, prin aceasta creându-se haos şi vacuum de putere”[118]. De asemenea, analiza structurală a actorului ţintă prezintă concluzii privind stabilitatea acestuia, deduse din dispunerea variabilelor de sistem în cadrul *Graficului relaţiilor directe* şi *Graficului relaţiilor directe şi indirecte*. Graficele relaţiilor reprezintă câte o „hartă” a influenţelor şi dependenţelor dintre factorii care definesc actorul ţintă şi îi evidenţiază pe aceia (*variabilele cheie*) pe care agresorul trebuie să îi exploateze pentru a genera perturbaţii semnificative în sistem. Factorii vor desemna, cu prioritate, obiectivele vizate de către acţiunile ce compun agresiunea de tip hibrid, într-o configuraţie bazată pe efecte. Produsele analizei structurale depind calitativ de obiectivitatea cu care se realizează determinarea variabilelor de sistem şi a relaţiilor dintre acestea.

Cu ajutorul produselor rezultate din analiza structurală a ţintei şi din analiza SWOT, agresorul poate determina o „hartă” a efectelor necesare a fi generate asupra ţintei pentru exploatarea vulnerabilităţilor şi destabilizarea acesteia. Mai mult ca orice, agresorul caută să controleze efectele acţiunilor sale pentru a le putea combina şi focaliza asupra ţintei. Agresorul trebuie să aibă în permanenţă în vedere faptul că rezultatul urmărit constituie configurarea setului de acţiuni care, prin integrarea efectelor, să ducă la atingerea scopului, adică impunerea voinţei proprii asupra ţintei fără a o distruge şi fără a fi sancţionat, în conformitate cu dreptul internaţional.

5. În continuare, *analiza de impact încrucişat*[119] *a agresiunilor* oferă o imagine a interdependenţei lor, luând în considerare probabilitatea condiţională dintre acestea. Aplicarea metodei create de către Michel

[118] Valery Gherasimov, „Valoarea ştiinţei în predicţie”, revista *VPK*, nr. 8(476), februarie-martie 2013, disponibil la http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf, accesat la 19.02.2019.

[119] Michel Godet, *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994.

Godet (1974) presupune întocmirea pentru actorul agresor a matricei de impact încrucişat privind agresiunile pe care le poate aplica asupra ţintei, considerând cele două criterii: capabilităţile agresorului şi vulnerabilităţile ţintei. Aceasta este o matrice pătratică de forma ($A_n \times A_n$), unde A_1, …, A_n reprezintă acţiunile agresorului. Elementele matricelor sunt de forma $a_{i/j}/a_{i/\bar{j}}$, unde:

- $a_{i/j}$ reprezintă probabilitatea de manifestare a ameninţării A_i dacă se manifestă A_j
- $a_{i/\bar{j}}$ reprezintă probabilitatea de manifestare a ameninţării A_i dacă nu se manifestă A_j

Considerând agresiunea de tip hibrid ca un complex de acţiuni cu diferite probabilităţi de manifestare, se poate calcula probabilitatea ca agresorul să genereze în mediul operaţional toate combinaţiile posibile. Pentru operativitatea execuţiei, se poate utiliza aplicaţia informatică *Smic*[120], dezvoltată de către *Heurisco*. Interpretarea rezultatelor analizei de impact încrucişat presupune şi identificarea unor concluzii care să completeze rezultatele obţinute în etapa de determinare a strategiilor actorilor prezenţi în mediul operaţional (etapa 3). Mai exact, concluziile rezultate din analiza impactului încrucişat dintre ameninţări oferă informaţii extrem de valoroase în crearea conexiunilor dintre acţiunile ce compun strategia agresorului şi obiectivele pe care acesta le urmăreşte, prin prisma efectelor pe care le generează.

Configuraţiile agresiunilor de tip hibrid se ordonează în ordine descrescătoare a probabilităţii de manifestare. Rezultatul oferă, astfel, variantele cele mai probabile de combinare a acţiunilor pe care agresorul este în măsură să le desfăşoare pentru a genera efecte asupra ţintei. Ţinând cont de definiţia ameninţării de tip hibrid, este evident că aceasta, în forma ei ideală şi completă, conţine, în proporţii corespunzătoare şi într-o manieră de manifestare coerentă, toate tipurile de agresiuni pe care agresorul este în măsură să le aplice asupra ţintei. Arta constă în identificarea strategiei în care agresiunile să fie aplicate

[120] ***, Methods of Prospective, disponibil la http://en.laprospective.fr/methods-of-prospective/softwares/62-smic-prob-expert.html, accesat la 18.06.2019.

astfel încât să producă efectul maxim asupra ţintei. Această activitate se desfăşoară în pasul următor.

6. *Configurarea agresiunii de tip hibrid* (sub aspect temporal şi spaţial) şi *planificarea acţiunilor* care o compun constituie cea mai importantă etapă. După determinarea componentelor agresiunii de tip hibrid, configurarea acesteia presupune stabilirea proporţiilor, resurselor, locului, succesiunii şi momentelor în care agresiunile, ca manifestări ale ameninţărilor, să fie aplicate astfel încât să producă efectul maxim asupra ţintei. Pentru a determina modalitatea cea mai eficientă de acţiune se pot utiliza diferite metode de asistare a procesului de luare a deciziei, cum ar fi aplicaţia informatică *ORANetScenes*[121] în care se consideră ca date de intrare setul instrumente, obiective, strategii, astfel:

- *Instrumente* – instrumentele de care dispune agresorul
- *Obiective* – vulnerabilităţile cheie ale ţintei
- *Strategii* – configuraţiile agresiunii de tip hibrid

Aplicaţia are posibilitatea să realizeze o reprezentare grafică a triadei *instrumente-strategii-obiective* şi să determine care dintre strategii (în acest caz, configuraţii ale agresiunii de tip hibrid) sunt cele mai eficiente (utilizează mai puţine resurse pentru atingerea obiectivelor) şi mai eficace (duc la atingerea a cât mai multe obiective dintre cele propuse). Pe lângă precizarea tuturor instrumentelor, obiectivelor şi strategiilor, utilizatorul trebuie să introducă şi datele referitoare la relaţia *instrumente-strategii* (ce instrumente se utilizează pentru aplicarea fiecărei configuraţii a agresiunii de tip hibrid) şi la relaţia *strategii-obiective* (ce obiective sunt atinse de către fiecare agresiune de tip hibrid).

Fiecare configuraţie poate fi reprezentată sub forma unui graf care să evidenţieze relaţiile cauzale (în strânsă legătură cu efectele pe care le generează fiecare) ce se stabilesc între acţiunile ce le compun. Astfel, pentru o agresiune de tip hibrid analizată, nodurile grafului reprezintă acţiunile, iar legăturile dintre noduri reprezintă existenţa unei relaţii de

[121] ***, ORA-NetScenes-st-iw-32, disponibil la http://ora-netscenes-st-iw-32.updatestar.com/, accesat la 14.01.2019.

tip cauzal dintre ele (elementele matricei pătratice $A_n \times A_n$ din cadrul analizei de impact încrucişat). Prin aceasta, artizanul agresiunii de tip hibrid are posibilitatea de a estima (şi controla) efectul rezultant al fiecărei configuraţii de tip hibrid în urma analizei modului în care se compun efectele fiecărei componente din cadrul acesteia.

Configuraţiile obţinute constituie esenţa planificării agresiunii de tip hibrid. Ele se pot materializa printr-o reprezentare de tip „design operaţional", adică o reprezentare în timp a succesiunii acţiunilor componente (cu resursele necesare şi efectele rezultante ale acestora) şi a atingerii obiectivelor urmărite de către agresor. De asemenea, agresorul poate realiza o selecţie a configuraţiei convenabile utilizând un criteriu oarecare, care poate fi cel al probabilităţii, cel al timpului la dispoziţie pentru pregătirea şi executarea acţiunilor etc. Ulterior, el va dezvolta acest produs într-un plan, realizând conexiunea în dimensiunea temporală şi cea spaţială între resurse şi obiective prin acţiuni (agresiuni) şi efecte.

7. Etapa a şaptea constă în *interpretarea rezultatelor analizei ameninţării*. Trebuie menţionat faptul că metoda elaborată nu oferă un rezultat cuantificat în ceea ce priveşte efectul rezultant al unei agresiuni hibride. Efectul compus al unui set de agresiuni care se manifestă în mod simultan asupra unei ţinte este extrem de imprevizibil, iar aplicarea unor metode matematice care să determine valoarea interferenţelor dintre ele ar putea duce la rezultate înşelătoare. Totuşi, după stabilirea configuraţiilor agresiunii de tip hibrid, prin analiza structurală a acestora, se poate determina o hartă a efectelor, care să fie comparată cu „imaginea" ce prezintă efectele necesare exploatării cu succes a vulnerabilităţilor ţintei şi care a fost realizată în etapele iniţiale. Astfel, luând în considerare instrumentele la dispoziţia agresorului şi acţiunile pe care acesta le poate desfăşura pentru a exploata vulnerabilităţile ţintei, prin adaptarea metodei de analiză structurală MICMAC, se pot determina componentele principale ale agresiunii de tip hibrid (înlocuind variabilele operaţionale cu acţiuni) precum şi modul în care acestea facilitează (influenţează) sau sunt favorizate (dependente) de celelalte componente. De asemenea, rezultatele conduc la concluzii ce pot fi utilizate în identificarea celor mai probabile

componente ale agresiunii de tip hibrid, precum şi în determinarea modului de desfăşurarea în timp a acestora (succesiv/simultan, periodic/permanent). În ceea ce priveşte stabilitatea/instabilitatea agresiunii hibride (considerată ca sistem) metoda MICMAC oferă posibilitatea determinării vulnerabilităţilor acesteia din care derivă modalităţi de contracarare, informaţii extrem de utile în stabilirea acţiunilor ţintei.

Capitolul 4

CONTRACARAREA AMENINŢĂRII DE TIP HIBRID

Cum ar putea cineva să se apere de o himeră atât de complexă, secretă și vicleană, care atacă din întuneric? Cum poate un stat țintă să știe că ceva groaznic este pregătit împotriva sa și vine să atace cele mai de preţ valori care îl definesc: teritoriul, populația și suveranitatea? Contracararea unei amenințări atât de complexe necesită cu siguranță un set de mijloace și acțiuni care să constituie un răspuns corespunzător. Poate un actor statal să dezvolte singur un sistem defensiv suficient de puternic pentru a detecta și contracara o potențială amenințare hibridă? Acestea sunt câteva întrebări fundamentale la care actorii de tip statal și organizațiile internaționale trebuie să găsească răspunsul corect.

4.1. Inițiative regionale

Una dintre organizaţiile cu activitatea cea mai proeminentă în domeniul contracarării amenințării hibride este NATO. Alianţa trebuie să aibă un răspuns la această configurare contemporană a amenințării care se poate manifesta împotriva membrilor săi. De vreme ce complexul de acțiuni care îl compune este orientat împotriva unui actor de tip statal, „responsabilitatea principală de a răspunde amenințărilor hibride sau atacurilor revine națiunii vizate”, dar „NATO este pregătită să ajute orice Aliat împotriva amenințărilor hibride ca parte a apărării colective” [122]. Pentru a îndeplini această sarcină în mod eficient, NATO a început să elaboreze o strategie și să înființeze mai multe organisme pentru adaptarea și implementarea acesteia. Două dintre ele sunt Comprehensive Crisis and Operations Management Centre (CCOMC), destinat „analizei, planificării și acțiunii strategice și cuprinzătoare în multiple crize și operații” [123] și Joint Intelligence and Security Division

[122] ***, NATO’s response to hybrid threats, disponibil la https://www.nato.int/cps/en/natohq/topics 156338.htm, accesat la 10.08.2019.

[123] ***, Comprehensive Crisis and Operations Management Centre, disponibil la https://shape.nato.int/comprehensive-crisis-and-operations-management-centre-

(JISD) care, începând cu anul 2016, are rolul „de a sprijini NAC și MC în probleme de informații și securitate” [124]. În iulie 2018, membrii NATO au convenit să înființeze echipe de sprijin axate pe combaterea amenințărilor hibride. Aceștia vor putea oferi asistență specifică aliaților NATO la cererea lor.”

Strategia NATO de combatere a amenințării hibride este construită pe cei trei piloni ai *pregătirii*, *descurajării* și *apărării* împotriva acesteia. *Pregătirea* înseamnă, pe de o parte, colectarea, partajarea și evaluarea continuă a informațiilor pentru detectarea și atribuirea unei agresiuni în desfășurare și, pe de altă parte, asistarea statelor membre în identificarea vulnerabilităților naționale și consolidarea rezilienței proprii. *Descurajarea* atacatorului reprezintă trimiterea unui semnal puternic că „Alianța își îmbunătățește capacitatea de reacție politică și militară, precum și capacitatea sa de a desfășura forțe adecvate la locul potrivit la momentul potrivit”. *Apărarea* împotriva amenințării hibride are loc în cazul în care descurajarea eșuează, iar NATO își va adapta și va încuraja permanent eforturile „pentru a putea reacționa într-un mod rapid și agil, oricând și oriunde este nevoie.”[125]

Deși amenințarea hibridă vizează însăși supraviețuirea statului țintă, deci contracararea acesteia ar fi o problemă de apărare națională, caracteristicile sale și, în special, dinamica sa complexă și multiplele domenii vizate o transformă într-o problemă de securitate națională, iar contramăsurile trebuie să fie la acest nivel. Mai mult decât atât, modul în care este implementată amenințarea, mai ales în faza pregătitoare (pe care o considerăm critică), împreună cu amplitudinea și intensitatea acesteia din faza de atac fac ca răspunsul la amenințarea hibridă să fie insuportabil de către un singur actor de tip statal. Dacă nu se iau contramăsuri eficiente încă din prima fază, adică dacă statul țintă nu are un sistem eficient de detectare a agresiunii și de combatere a acțiunilor în faza incipientă, apărarea împotriva ei în a doua fază devine extrem de dificilă întrucât o bună parte din țintele prioritare din faza pregătitoare

[124] N.A.: mai multe detalii sunt disponibile la adresa https://www.nato.int/cps/en/natohq/topics 156338.htm, accesat la 10.08.2019.

[125] N.A.: NATO’s response to hybrid threats, disponibil la https://www.nato.int/ cps/en/natohq/topics 156338.htm, accesat la 10.08.2019.

vizează demantelarea instrumentelor de putere pe care statul ar trebui să le folosească în faza a doua. Cooperarea cu alţi actori de tip statal şi suprastatal în acest domeniu reprezintă una dintre componentele cheie în combaterea ameninţării hibride. În această problemă, NATO încearcă să-și consolideze cooperarea și coordonarea cu parteneri, atât actori statali, precum Suedia, Finlanda, Ucraina, cât și organizații, cum ar fi Uniunea Europeană. În plus, Centrele de Excelență ale Alianţei contribuie cu expertiză în domeniu, iar în acest sens putem menționa Centrul European de Excelență pentru combaterea amenințărilor hibride, situat la Helsinki, Finlanda (din octombrie 2017), Centrul de Excelență pentru comunicarea strategică din Riga, Letonia, Centrul de Excelență pentru cooperarea privind apărarea cibernetică din Tallinn, Estonia și Centrul de Excelență pentru securitatea energetică din Vilnius, Lituania. Toate servesc ca hub-uri de expertiză, contribuind la îmbunătățirea rezilienţei și pregătirii membrilor Alianței pentru a contracara amenințarea hibridă.

Este bine înţeles faptul că o amenințare hibridă reprezintă, din perspectiva efectelor produse, mai mult decât suma totală a părților sale constitutive. Contracararea unor astfel de amenințări nu necesită neaparat noi capabilităţi cât necesită noi parteneri, procese noi și, mai ales, un nou mod de gândire. Cooperarea şi forumurile de consultare trebuie să ofere medii propice, lipsite de ostilitate, în care să se desfășoare activități de analiză și informare fără a exista vreo amenințare iminentă. Prin desfăşurarea acestor activități, atât militarii, cât și civilii pot fi încurajați să depășească predispozițiile legate unul de celălalt și să ajungă la înțelegere reciprocă. Comandamentului Aliat pentru Transformare al NATO a efectuat un astfel de experiment în luna mai 2011, denumit „Combaterea amenințărilor hibride”, în timpul căruia au fost abordate multe teme referitoare la definirea amenințării hibride şi dezvoltarea de strategii de apărare şi combatere a accestora. Experimentul de o săptămână a beneficiat de participarea a aproape 100 de profesioniști din sectorul privat, iar fiecare dintre aceştia a petrecut o săptămână completă de lucru în acest cadru de excepţie. Numărul și nivelul participanților și timpul petrecut sugerează că NATO este considerată organizaţie relevantă, inclusiv de către de mediul de afaceri

și că ACT ocupă un loc important comunitatea ştiinţifică internaţională. Această percepție poate prezenta oportunități semnificative dar și câteva provocări. Trebuie menționat faptul că în acest eveniment a fost utilizată o abordare de tip *bottom-up*, care îi conferă caracterul de excepţie. Luarea în considerare a opiniilor experților prezenţi s-a dovedit deosebit de utilă, nu numai datorită cunoştinţelor și experienței lor, ci și pentru acest lucru că ar putea împiedica repetarea greșelilor din trecut.

Experimentul şi consultările pot oferi o atmosferă în care problemele legate de derularea angajamentului NATO cu actorii ce pot furniza *soft power* să fie explorate în colaborare. Deși este normal ca fiecare membru NATO să-şi angajeze propriile instituții guvernamentale și persoane fizice pentru a identifica mijloacele şi capabilităţile necesare contracarării ameninţării hibride, este mai puțin clar cine şi cum ar trebui să abordeze sectorul privat. NATO ar trebui să se adreseze marilor instituții multilaterale, cum ar fi Organizația Națiunilor Unite, Banca Mondială și Consiliul de Cooperare al Golfului, pentru ca acestea să-şi pună la dispoziţie capabilităţile proprii de *hold and build*. Dar, în afară de această abordare instituţională, rămân de explorat posibilităţile de implicare a civililor în faza de prevenire sau în faza incipientă a dislocării forţelor armate, în care NATO ar putea fi interesată de cunoştinţele şi experiența acestora pentru a modela mediul operaţional. În plus, în cadrul operaţiilor expediţionare, interacțiunile cu instituțiile multilaterale neguvernamentale, inclusiv cu cele din țara sau regiunea gazdă, au o importanţă majoră pentru eficienţa dislocării, integrării şi acţiunii forţelor în teatrul de operaţii. La ce nivel ar trebui ca NATO să stabilească relaţii cu asemenea instituţii civile şi să înceapă să planifice cooperarea cu acestea? Când ar trebui să se întâmple? Are sens să se stabilească relații periodice cu instituțiile, în așteptarea unor probleme posibile în a căror rezolvare NATO le-ar putea solicita pentru facilitarea modelării mediului operaţional? Unde ar trebui să se întâmple această angajare? Reprezintă această stabilire a relaţiilor o funcție rezervată comandamentelor de nivel strategic/operativ sau comandanților locali, după cum consideră ei de cuviință? Ar trebui ca NATO să elaboreze o politică generală care să ghideze aceste tipuri de angajamente, precum și

contribuțiile necesare, dacă este cazul, pe care să le aibă actorii statali care nu sunt membri NATO, dar și cei privați?

Una dintre cerințele esențiale în dezvoltarea unui cadru de lucru eficient în contracararea amenințării de tip hibrid o constituie concentrarea eforturilor în sensul îmbunătățirii sinergiei dintre organismele NATO. Acest lucru ar trebui să faciliteze abordări/procese esențiale cum ar fi dezvoltarea unei posturi de apărare şi descurajare ferme, abordarea cuprinzătoare a operaţiilor desfăşurate, planificarea strategică şi procesul de transformare continuă a NATO. Asemenea atitudine ar putea permite NATO, cu acordul statelor membre, să devină proactivă, mai degrabă decât să rămână reactivă. Simultan, demersurile trebuie dezvoltate în sensul stabilirii unor relaţii ferme de cooperare cu alte organizaţii cum ar fi Organizația Națiunilor Unite, Uniunea Europeană, Organizația pentru Securitate și Cooperare în Europa, Uniunea Africană, cu angajarea mai multor experți din domeniul diplomatic.

În contextul în care statele membre NATO trebuie să conducă demersurile privind anticiparea competențelor, practicilor și capabilităților necesare pentru a diminua sau elimina amenințările hibride emergente ori pentru a contracara agresiunile hibride în desfăşurare, ACT are un rol vital în implementarea şi activarea unor mecanisme de tip *soft power* și în inițierea dialogului necesar cu cei mai potriviţi actori non-NATO pentru a sprijini acest demers.

În opinia noastră, contracararea amenințării de tip hibrid trebuie să includă un complex de acțiuni întreprinse pentru a descuraja și, dacă acestea nu au efect, pentru a combate agresiunea hibridă sau cel puţin unele dintre componentele acesteia. Trebuie să luăm în considerare faptul că amenințarea hibridă se manifestă printr-un sistem compus şi adaptabil de agresiuni care afectează grav ținta bazându-se pe efectul sinergic al componentelor sale. Combaterea unora dintre ele poate duce la diminuarea semnificativă a rezultatului final, determinând ca acesta să fie inutil sau, cel puțin, nu atât de eficient precum a fost planificat.

4.2. Modele strategice de contracarare a ameninţării de tip hibrid

Măsuri şi acţiuni de contracarare a ameninţării de tip hibrid

Determinarea condițiilor de succes în contracararea amenințării hibride joacă un rol foarte important în identificarea setului de mijloace și contramăsuri. Ambasadorul Sorin Dumitru Ducaru a creat un cadru conceptual care poate genera etapele posibile pentru dezvoltarea unui sistem de contracarare. Conform studiilor întreprinse[126], condițiile pe care trebuie să le îndeplinească un actor statal pentru a face față cu succes amenințării hibride sunt: să aibă dezvoltat nivelul de reziliență necesar şi suficient pentru a rezista acțiunilor hibride; a fi pregătit să reziste; să aibă un proces care să permită evaluarea rapidă a situaţiei și luarea deciziilor; să fie în măsură să răspundă eficient. La toate acestea, considerăm că este obligatoriu să adăugăm componenta proactivă, în sensul necesității ca un actor statal să dezvolte un sistem eficient şi eficace de detectare a ameninţării, prin creșterea nivelului de conștientizare a situației și prin descurajarea oricărei forme de acțiune care ar putea avea o caracteristică agresivă.

Totuşi, înainte de a detecta, descuraja și combate amenințarea hibridă, mai sunt de făcut câţiva pași. Una dintre cele mai importante direcții este ceea ce pare a fi o adevărată provocare în special pentru mediul științific sau academic, dar şi pentru organizațiile interguvernamentale de securitate. Aceasta este *definirea amenințării*. Apoi, acţiunea presupusă de către ameninţare trebuie *clasificată ca o agresiune*, în termenii sistemului de drept internațional. Acesta este singurul mod de a emite un răspuns legal sub formă de sancțiuni impuse făptuitorului (izolarea politică, sancțiunile economice, limitările legale sau chiar ameninţarea cu intervenţia militară), ca acte menite să-l descurajeze. Adăugăm faptul că agresiunea în sine, dacă cineva i-a demonstrat existența, trebuie să fie *atribuită unui actor* de către organele de drept internațional care, datorită naturii sale, este, de cele mai multe ori, dificil sau chiar imposibil de realizat. Să considerăm, de exemplu,

[126] Sorin Dumitru Ducaru, „The cyber dimension of modern hybrid warfare and its relevance for NATO”, *Europolity*, vol. 10, no. 1, 2016, disponibil la http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf, accesat la 18.01.2019.

componenta sa cibernetică. Globalizarea informațiilor a creat multe oportunități pentru membrii actuali ai societății moderne de a se conecta între ei, dar a creat, de asemenea, mediul perfect pentru a lovi și a dispărea pentru atacatorii cibernetici. Sau, în zona economică, atunci când agresorul poate folosi unele companii intermediare pentru a agresa sau controla relațiile economice ale țintei, cum ar fi comerțul și accesul pe piața internațională, pentru a aplica o politică de preț neloială privind bunurile de care depinde statul țintă sau chiar pentru a-l îndatora la un nivel insuportabil pentru acesta. Acest tip de situații sfârșesc, de obicei, prin crearea unor vulnerabilități ale țintei sau aprofundarea celor existente și facilitarea atacării de către un autor „greu de identificat". Toate acestea sunt posibile, fără să mai vorbim de PSYOPS, o componentă puternică a INFOWAR, care este chiar o componentă fundamentală pentru fiecare agresiune de tip hibrid. Utilizarea, de exemplu, a formatorilor de opinie influenţaţi și sponsorizați de către agresor face ca acesta din urmă să fie aproape imposibil de identificat. Nu trebuie uitat: complexitatea amenințării face extrem de dificilă izolarea, demontarea și combaterea acesteia. Pentru toate acestea, clasificarea acţiunilor specifice amenințării drept agresiuni şi crearea, ca atare, a cadrului judiciar pentru aplicarea sancțiunilor este, prin urmare, imposibilă fără a avea definiția și principalele sale caracteristici. Chiar şi găsirea unor caracteristici comune care ar ajuta judecătorul să formuleze verdictul ar fi o provocare.

Un alt set de măsuri care trebuie luate vizează capacitatea de a detecta dezvoltarea viitoare a unei amenințări hibride. „Războiul hibrid" nu este niciodată declarat. „Războaiele nu mai sunt declarate și, odată începute, se continuă conform unui șablon necunoscut. Un stat perfect înfloritor poate, în câteva luni și chiar zile, să fie transformat într-o arenă a conflictului armat acerb, să devină o victimă a intervenției străine și să se scufunde într-o rețea de haos, catastrofă umanitară și război civil."[127] Valery Gherasimov, citându-l pe Georgy Isserson cu cartea sa „New Forms Of Combat" scrie: „Războiul în general nu este declarat. Pur și simplu începe cu forțe militare deja dezvoltate. Mobilizarea și

[127] Valery Gherasimov, *op. cit*.

concentrarea nu fac parte din perioada de după debutul stării de război așa cum s-a întâmplat în 1914, ci mai degrabă, neobservate, se desfășoară cu mult înainte.” [128] De aceea, fiecare stat, mai întâi singur și apoi prin cooperare, ar trebui să dezvolte un set de indicatori, fiecare dintre ei caracterizaţi de praguri specifice pentru a putea identifica și avertiza timpuriu despre acțiunile cu tendinţe agresive ce se pot desfăşura în faza pregătitoare. Pe baza activării lor, un potenţial stat țintă poate identifica faptul că se pregăteşte o agresiune hibridă împotriva sa, poate declara acest lucru la nivel politic și poate reacționa corespunzător pentru a evita escaladarea campaniei hibridă în faza de atac sau ca aceasta să degenereze într-un conflict militar.

Abordările de tip “whole of government” şi “whole of society” în interiorul frontierelor actorului statal și cea de tip „comprehensive approach” la nivelul organizațiilor internaționale și, de asemenea, între organizații pot focaliza eforturile comune pentru *a dezvolta rezilienţa* împotriva oricărei forme hibride a amenințării sau, mai degrabă, împotriva componentelor sale. Atunci când priveşte securitatea și apărarea, acest concept destul de nou de *rezilienţă* stârneşte foarte mult interes în întreaga comunitate științifică. Deși încă nu este complet definit, este considerat un factor cheie în abordarea apărării împotriva amenințării hibride. O definiție a rezilienţei este „capacitatea oamenilor, a societăților sau a statelor de a supraviețui șocurilor și crizelor majore, de a-și menține funcțiile vitale, de a limita impactul asupra propriei funcționări și de a se perfecţiona în urma acestei experiențe.”[129] Strategia Militară a României (2016) definește rezilienţa drept „abilitatea Sistemului Naţional de Securitate de a rezista unui atac și de a-și reveni în urma acestuia, dezvoltând capabilități suficiente de a anticipa și a contracara o amenințare, de a asigura condițiile de victorie și soluțiile optime de răspuns”. După cum putem vedea, acest concept urmărește o abordare multidimensională a apărării împotriva unei amenințări multidimensionale. Mai mult, creşterea nivelului rezilienţei constă în

[128] *Ibidem.*

[129] Cristina Bogzeanu, „Resilience: concept, approaches and implications”, *Strategic Impact* No. 3-4/2017, „Carol I” National Defence University Publishing House, Bucharest, p. 51, disponibil la https://cssas.unap.ro/en/pdf_periodicals/si64-65.pdf, accesat la 11.01.2019.

dezvoltarea mai multor capabilităţi menite să sporească posibilităţile actorului statal de a rezista, de a gestiona efectele, de a se recupera și de a combate amenințarea hibridă. În consecinţă, principalele măsuri pentru consolidarea rezilienței trebuie luate în toate domeniile specific statului nu numai la nivel militar. Ele trebuie să fie concentrate pe monitorizarea permanentă a mediului de securitate; identificarea vulnerabilităților și riscurilor asociate și luarea măsurilor adecvate pentru diminuarea, eliminarea sau protejarea acestora; dezvoltarea unui proces interinstituţional de luare a deciziilor eficient; educarea societății și furnizarea de sprijin militar și de impunere a legii pentru măsurile luate; dezvoltarea și acordarea resurselor necesare. Eforturile trebuie să fie orientate către aproape toate domeniile care ar putea fi vizate de componentele amenințării hibride: protecția infrastructurii critice, comunicațiile strategice, protecția civililor, apărarea cibernetică, securitatea energetică și contraterorismul.

Cadrul de răspuns la agresiunea hibridă

În situaţia în care măsurile preventive nu au avut succes, este necesară configurarea răspunsului ce poate fi dat agresiunii hibride iar pentru aceasta putem folosi modelul clasic al strategiei şi anume triada *obiective – căi – mijloace*. Înainte de aceasta, prezentăm un sistem de trei aspecte de care considerăm că trebuie să se ţină cont în configurarea răspunsului la o potenţială agresiune de tip hibrid: rezilienţa, stabilirea de măsuri şi voinţa de a acţiona (fermitate).

1. *Rezilienţa*
    a. Scopul strategic – menținerea capacității de acţiune.
    b. Pragul de atins – concentrarea eforturilor pe toate domeniile PMESII în scopul eliminării sau protejării vulnerabilităţilor cu accent pe social, infrastructură și informațional.
    c. Măsuri de descurajare:
        i. prin acţiuni indirecte: identificarea sprijinului și a acțiunii internaționale împotriva intervenţiei străine; introducerea unei legislații de protejarea infrastructurii critice şi informaţionale, concomitent cu creșterea finanțării pentru aceste domenii; desfăşurarea unor campanii de informare și

avertizare a populației și implementarea unor măsuri de educare împotriva dezinformării și a influenţării;

ii. prin acţiuni directe: Inițierea de demersuri pentru impunerea de sancțiuni economice de către comunitatea internaţională.

d. Răspunsul – protejarea vulnerabilităţilor proprii şi implementarea unor sancțiuni economice care să protejeze sectoarele industriale cheie.

2. *Stabilirea de măsuri*

a. Scopul strategic – menținerea capacității de acționa (reziliența) și combaterea agresiunii hibride.

b. Pragul de atins – concentrarea eforturilor pe domeniile militar, economic și infrastructură.

c. Măsuri de descurajare:

i. prin acţiuni indirecte: introducerea unei legislații de protejare a infrastructurii critice; creșterea transparenței financiare și adoptarea unor legi de prevenire a spălării banilor; declarații politice și încheierea de acorduri împotriva violării spațiului aerian și maritim;

ii. prin acţiuni directe: creșterea libertății de acțiune pe mare și în spaţiul aerian; inițierea de acorduri pentru sancțiuni economice; participarea la forumuri politice internaționale și prezentarea agresiunii.

d. Răspunsul:

i. aducerea la cunoștința opiniei publice interne şi internaţionale a acțiunilor agresive;

ii. adaptarea regulilor de angajare pentru a da posibilitatea unor acțiuni de răspuns elocvente;

iii. desfăşurarea unei intense campanii de informare pentru explicarea posturii agresive și a practicilor agresorului.

3. *Voinţa de a acţiona*

a. Scopul strategic – orice scop stabilit.

b. Pragul de atins – concentrarea eforturilor pentru diminuarea efectelor în domeniul militar şi social.

c. Măsuri de descurajare:
   i. prin acţiuni indirecte: reglementarea modului de funcționarea a mass-media; creșterea transparenței deciziilor politice;
   ii. prin acţiuni directe: obținerea şi menţinerea libertății de acțiune în orice mediu (terestru, aerian, maritim şi cibernetic).
d. Răspunsul:
   i. câștigarea şi menţinerea libertății de acțiune;
   ii. expunerea pericolelor la adresa infrastructurii critice.

Având în vedere aceste trei elemente, dezvoltăm în continuare modelul ce poate sta la baza dezvoltării strategiei de combatere a agresiunii de tip hibrid.

Obiectivele. Dilema care există în formularea unei strategii de combatere a agresiunii hibride constă în a identifica setul de acţiuni care să constituie răspunsul adecvat atingerii obiectivului propus. Înainte de a o rezolva, în formularea obiectivelor, guvernul trebuie să ţină cont de faptul că nu poate răspunde la fiecare incident determinat de agresiunea hibridă şi de aceea trebuie să analizeze și să interpreteze în mod responsabil nivelul de ostilitate pe care națiunea îl poate tolera. În plus, cu cât se stabilesc mai multe obiective strategice, cu atât răspunsul, deși mai complex, poate duce la reducerea, dacă nu anihiliharea agresiunii hibride. Tinând cont de cele trei elemente prezentate anterior (reziliența, măsurile și voinţa de a acționa) se poate stabili când, cum și cu ce scop va trebui dat răspunsul pentru a se asigura că acesta este justificat, corespunzător şi eficace.

Căile și mijloacele. Odată ce s-a decis că acordarea răspunsului este potrivită și obiectivele au fost stabilite, următorul pas este acela de a identifica căile și mijloacele ce pot fi întrebuințate pentru atingerea obiectivelor. Se recomandă ca acestea să fie analizate simultan întrucât având în vedere faptul că actorul ţintă dispune de resurse limitate, de regulă mai reduse decât agresorul, primul va trebui să efectueze numeroase ajustări privind corelaţia căi-mijloace pentru a obţine posibilitatea şi, mai mult, eficienţa în implementarea lor. Stabilirea tandemului *căi-mijloace* trbuie realizat prin analiza *opțiunilor politice*, *factorilor cheie* și a *instrumentelor de putere*.

A. Opțiunile politice. Orice răspuns la acțiunile de luptă hibride este profilat în primul rând de obiectivele strategice ale actorului aflat în postura de apărare, la îndeplinirea cărora trebuie să ducă modalitatea de răspuns. Următorul pas poate fi descris prin formularea a patru caracteristici fundamentale ale opțiunii politice. Luate împreună ele trebuie să definească natura şi carateristicile răspunsului. Aceste caracteristici sunt interdependente și elementele din cuprinsul lor trebuie să se regăsească în varianta finală a răspunsului.

a. Angajare vs. dezangajare. Aceste element ia în considerare nivelul la care adversarul poate conştientiza faptul că poate primi un răspuns la atacul iniţiat. O strategie conform căreia actorul care se confruntă cu acțiuni hibride ostile, de exemplu expunerea la atacuri cibernetice, desfăşoară acţiuni de răspuns pe măsură, contraatacând, poate produce o descurajare eficientă. Dezavantajul acestei abordări este acela că poate legitimiza acţiuni ulterioare din partea agresorului și astfel, ţinta s-ar expune şi la alte amenințări care altfel ar fi mai puțin ofensive. Pe de altă parte, strategia de a ignora pur și simplu sau de respinge posibilitatea producerii unui atac ca fiind irelevantă sau inconsecventă poate contribui la recurența acestuia și obținerea de către adversar a efectelor preconizate. Adoptarea de către ţintă a unei strategii care ignoră amenințările poate presupune lipsa pregătirii şi/sau a sprijinului politic pentru acţiunile viitoare.

b. Interior vs. exterior. Această caracteristică ia în considerare dacă răspunsul este concentrat în *interior*, pentru apărarea de către cel atacat a propriei populații și a factorilor de decizie sau în *exterior*, către adversar sau pentru a obţine sprijin de la comunitatea internațională. În unele cazuri răspunsul poate fi în întregime orientat în *interior*, de exemplu prin acţiuni de educare a populației asupra aspectului dezinformării sau de creştere a încrederii acesteia în organele de guvernare. În alte cazuri, atenția poate fi orientată spre adversar, şi este recomandat să conţină acţiuni de tip smart power – de exemplu prin canale diplomatice (soft power) sau prin impunerea de sancţiuni economice (hard power). Impactul uneia sau alteia dintre metode poate avea consecințe neintenționate, sau poate fi folosit în mod constructiv. De exemplu, orientarea spre interior prin adoptarea unor măsuri de

creştere a rezilienței poate avea un efect de descurajare asupra adversarului. De asemenea, măsurile orientate spre adversar, cum ar fi sancțiunile economice, ar putea asigura populația că adversarul este ținut la distanță. În niciun caz nu trebuie ignorat sprijinul actorilor internaţionali ce poate fi atras prin relaţii de cooperare stabilite, de preferat înainte de declanşarea agresiunii.

c. Descoperit vs. sub acoperire. Acțiunile descoperite sunt caracterizate ca fiind publice, evidente și oficiale şi pot fi orientate spre interior și spre exterior. Ele pot fi eficiente în generarea conștientizării pericolului de către populaţie, obţinerea sprijinului opiniei publice internaţionale şi expunerea acțiunii adversarului. Dezavantajul acțiunilor descoperite poate presupune apariţia unor consecințe neintenționate din cauza caracterului lor public care elimină posibilitatea realizării surprinderii adversarului sau pot atrage dezacordul opiniei publice internaţionale. Acțiunile sub acoperire se caracterizează printr-o audiență limitată și pot fi eficiente prin trimiterea de mesaje directe factorilor de decizie ai adversarului și prin generarea de efectele fizice care pot preveni sau împiedica adversarul în a pregăti atacuri viitoare (de exemplu, atacuri cibernetice). Pe de altă parte, acţiunile acoperite pot avea consecinţe împotriva celui ce se apăra care, prin acestea, poate ceda agresorului controlul informării propriei populații.

d. Constrângere vs. convingere. Aceste element determină dacă răspunsul este orientat înspre luarea unor măsuri realiste şi hotărâte pentru a constrânge adversarul sau aplicarea unor măsuri care să-l convingă să recurgă la dialog şi cooperare (*hard power* vs. *soft power*). Dacă se optează pentru implementarea unor măsuri coercitive trebuie să urmărească exploatarea avantajelor generate de escaladarea pe orizontală prin desfăşurarea în mod credibil și creativ a unor acţiuni de nivel redus dar în toate domeniile PMESII, utilizând în mod conjugat şi adaptat toate instrumentele de putere MPECI. Dezavantajele constau în faptul că această abordare a răspunsului poate impune costuri semnificative şi, în plus, poate duce la o escaladare pe verticală a confruntării. Riscul asociat escaladării verticale generate de o abordare coercitivă ar fi crearea unui *casus belli* pentru agresor care să justifice o intervenţie deschisă din partea acestuia. În acest fel, situaţia ar putea deveni

dezastruoasă pentru ţintă, întrucât agresorul ar putea avea ocazia să inducă la nivelul audienţei şi a organizaţiilor internaţionale ideea că actorul ţintă este adevăratul agresor. Pe de altă parte măsurile destinate convingerii agresorului să coopereze şi să renunţe prin aceasta la obiectivele sale se pot dovedi insuficiente, în sensul în care efectele produse să fie neînsemnate în ceea ce priveşte modificarea comportamentului agresorului, ducând din nou la o escaladare pe verticală a agresiunii. Probabil cea mai potrivită abordare este cea specifică *smart power*, în care măsurile de constrângere să fie complementate cu cele de inducere a agresorului spre calea cooperării şi dialogului. Proporţiile exacte în care să fie aplicate cele două seturi de măsuri sunt circumstanţiale, însă este clar că trebuie stabilit echilibrul „carrot and stick" adecvat situaţiei şi actorilor implicaţi.

B.Factorii cheie. Atunci când se analizează opțiunile politice, înainte de alegerea sau formularea măsurilor ce trebuie luate pentru a răspunde unei agresiuni hibride, trebuie să se ţină cont de următorii factori cheie:

1. Riscul. Care sunt riscurile ce pot apărea la executarea unei anumite acțiuni de răspuns și care sunt riscurile dacă nu se ia nicio măsură? Riscul principal al adoptării unei acţiuni este escaladarea agresiunii, în timp ce riscul inacțiunii poate fi continuarea agresiunii hibride. Toate acțiunile au consecințe pe termen lung sau scurt. În schimb în cazul inacţiunii, dacă urmările pe termen scurt pot reprezenta o escaladare minoră, riscul pe termen lung poate fi escaladarea majoră din partea agresorului.

2. Vulnerabilitatăţile. Care din vulnerabilitățile PMESII vor fi atacate? Măsurile interne, cum ar fi cele de creştere a nivelului de reziliență, vizează vulnerabilițile care aparțin actorului ţintă, care exercită răspunsul, iar măsurile de răspuns ce se aplică în exterior ţintesc vulnerabilitățile agresorului.

3. Instrumentele de putere. Care dintre instrumentele de putere MPECI vor fi întrebuințate şi, mai ales care este ponderea acestora în construirea şi implementarea ansamblului de acţiuni care reprezintă răspunsul? Mijloacele specifice instrumentelor de putere folosite trebuie să aibă capacitatea de a influența vulnerabilitățile țintite.

4. Escaladarea orizontală versus escaladarea verticală. Un răspuns la agresiunea hibridă poate exploata avantajele unei escaladării coordonate orizontale și verticale. În timp ce agresorul încearcă să crească nivelul de complexitate, escaladând astfel pe orizontală, apărătorul poate răspunde astfel: să gestioneze escaladarea printr-un răspuns proporţionat, să gestioneze escaladarea printr-un răspuns asimetric, să crească aria de acțiune prin țintirea unei game largi de vulnerabilități sau să dea un răspuns de nivel redus prin escaladare orizontală care este mult mai credibilă și mai ușor de implementat.

5. Acţiuni în cadru naţional sau multinaţional? Un răspuns multinațional poate determina un răspuns variat și mai eficient dar este mult mai dificil de planificat, de generat și implementat.

6. Coordonare. Orice răspuns la o agresiune hibridă trebuie coordonată la nivelul guvernului printr-o structură creată pentru acest scop, la fel ca și răspunsul multinațional care trebuie să aibă un acord cadru de implentare.

7. Constrângeri. Baza legală pentru a răspunde unei agresiuni hibride trebuie să fie foarte clară întrucât una din caracteristicile atacurilor ce compun agresiunea este de a exploata „zonele gri" ale dreptului umanitar internaţional. În acest sens, trebuie să reamintim faptul că agresiunea de tip hibrid exploatează confruntarea asimetrică. Din punct de vedere legal, agresorul exploatează situaţiile care sunt la limita legislaţiei internaționale pentru a împiedica victima agresiunii să dea un răspuns pe măsură şi decisiv. Când este combinată cu măsuri coercitive desfăşurate pentru a împiedica reacţia, agresorul poate realiza o situație de avantaj asimetric. Există totuşi două argumente cheie la care se poate face apel din perspectiva dreptului internațional umanitar.

- Primul se referă la faptul că statele pot răspunde la întrebuinţarea forței armate conform capitolului 7 din Carta ONU în baza dreptului la autoapărare (art. 51) şi a rezoluţiilor Consiliului de Securitate ONU (art. 42). NATO și UE au la bază tratate care garantează apărarea colectivă/comună conform Art. 51 din Cartă. În dorinţa de a se adapta ameninţărilor contemporane, NATO și-a declarat intenția de a considera atacurile cibernetice și agresiunile hibride ca fiind atacuri armate, tocmai pentru a le putea încadra la art. 5 din Tratatul de la Washington şi a

putea aplica principiul apărării colective. Răspunsul trebuie să țină seama de constrângerile implementării acestuia care îi poate afecta atât credibilitatea, cât și impactul, cum ar fi nivelul de conștientizare de către public şi de sprijin a anumitor măsuri, resursele la dispoziție, natura atacului hibrid sau atribuirea atacului unui anumit agresor.

- Al doilea argument ia în considerare faptul că legile internaționale prevăd suficiente măsuri ce pot fi luate pentru a contracara o agresiune hibridă fără a se recurge la folosirea forței. Exemplele includ sancțiuni, protecție financiară, reforma sectorului de securitate, lupta anticorupție, diversificarea resurselor, educația, protecția infrastructurii, apărarea cibernetică sau reglementarea activităţii mass-media. Cu alte cuvinte, există totuși un amplu registru legal pentru o escaladare orizontală a acțiunilor de contracarare a agresiunii hibride.

C. Instrumentele de putere (MPECI)

a. Instrumentul *Militar*. Acțiunile militare trebuie calibrate pentru a asigura proporționalitatea, deşi potențialul coercitiv al instrumentului tinde să fie maximizat pentru a ținti vulnerabilitățile hibride ale agresorului. Poate fi folosită întreaga gamă de opțiuni militare pentru a răspunde atacurilor hibride dar intensitatea acestora trebuie să depindă de obiectivele strategice stabilite. Forța militară poate contribui la toate cele trei elemente: reziliența, stabilirea de măsuri și voinţa de a acționa.

b. Instrumentul *Politic*. Măsurile adoptate din punct de vedere politic pot varia de la restricționarea accesului oficialilor politici, la expulzarea diplomaților, suspendarea calității de membru în diferite organisme sau retragerea dreptului de vot anumitor state membre în organismele internaționale.

c. Instrumentul *Economic*. Eficiența măsurilor economice nu trebuie subestimată. Sancțiunile și penalizările financiare ce țintesc anumite state, corporaţii sau chiar persoane pot fi extrem de eficiente pe termen scurt. Însă pe termen lung, adoptarea unor sancțiuni legate de reducerea schimburilor comerciale poate avea un impact mult mai mare asupra societății în ansamblul ei.

d. Instrumentul *Civil*. Respectarea legii este unul din fundamentele democrației. Acuzaţiile publice, aşa cum s-a întâmplat

după alegerile din 2017 din SUA sau nominalizarea suspecților în cazul otrăvirii fostului agent rus KGB din Anglia pot fi eficiente. Transparența prin blamarea publică crește încrederea societății în instituțiile publice.

e. Instrumentul *Informațional*. Activitatea eficientă a serviciilor de informaţii şi măsurile de sprijin a deschiderii și transparenței mass-media prin reglementarea activităţii acesteia pot duce la creșterea încrederii și accesului la informație în societate. Nu trebuie uitat faptul că dezinformarea poate fi contracarată prin educație.

Mecanismele instituționale pentru descurajarea agresiunii hibride și pentru răspunsul la agresiunea hibridă

Mecanismele instituționale pentru descurajarea agresiunii hibride sunt similare cu cele care generează răspunsul. Ambele necesită o planificare coordonată și implementarea măsurilor în toate domeniile PMESII folosind mijloacele ce compun instrumentele de putere MPECI. Principala diferență dintre cele două o constituie direcţia principală de implementare a măsurilor. De regulă, mecanismele de descurajare presupun aplicarea unor măsuri în interiorul statului pentru a crea efectul de descurajare asupra unui actor extern, în special înainte ca agresiunea să se declanşeze. În schimb acţiunile ce constituie răspunsul sunt direcţionate către agresor pentru a crea efecte în interiorul statului, resimţite prin diminuarea intensităţii sau amplorii agresiunii de tip hibrid, după declanşarea acesteia. Prezentăm mai jos câteva măsuri instituționale care pot crește eficiența acțiunilor de descurajare și a răspunsului prin pregătire, coordonare și implementarea contramăsurilor:

a. Stabilirea unui cadru conceptual şi juridic strategic, la nivel guvernamental, pentru contracararea amenințării hibride, la care părțile implicate să poată contribui.

b. Stabilirea unui grup de decizie și de coordonare, care să aibă autoritatea de a implementa contramăsuri în situații de criză, pentru a asigura răspunsul potrivit în cazul unei agresiuni hibride.

c. Stabilirea unor centre sectoriale cu responsabilitatea de a dezvolta și încuraja luarea măsurilor adecvate pentru contracararea amenințărilor hibride, prin aceasta crescând reziliența PMESII (de

exemplu, un centru național pentru securitatea cibernetică care să prezinte guvernului vulnerabilitățile în situația unui atac cibernetic).

d. Stabilirea unor proceduri de planificare din timp, aplicabile în cadru naţional şi internaţional și pregătirea unor scenarii specifice ameninţării hibride.

e. Elaborarea unei metodologii privind modul de pregătire a contramăsurilor și de implementare a răspunsului la agresiunea hibridă.

f. Dezvoltarea unei culturi de planificare și implementare a politicilor la nivelul departamentelor guvernamentale și chiar între națiuni care să cuprindă procese, comportamente, dezvoltarea unor deprinderi, relaționarea și comunicarea strategică.

g. Educarea periodică, instruirea și antrenarea personalului din instituțiile implicate în contracarea ameninţării hibride pentru stabilirea unei proceduri de comunicare, înțelegerea rolului și a responsabilităților, o cooperarea eficientă, coordonarea planurilor și procedurilor, dezvoltarea unor cunoștințe privind nevoile și capacitățile individuale și instituționale.

În ceea ce privește reziliența, considerată drept principala componentă a descurajării, trebuie avute în vedere următoarele:

a. Stabilirea unei structuri la nivel guvernamental care să monitorizeze reziliența sau nivelul de pregătire pentru contracararea ameninţării de tip hibrid.

b. Întărirea legăturilor cu sectorul privat și societatea civilă pentru conștientizarea atât a existenţei amenințărilor cât și a potențialului lor de a produce efecte.

c. Dezvoltarea unei culturi în cadrul sectorului privat și a societății civile care să sprijine conștientizarea privind existenţa amenințărilor și reziliența de sus în jos (guvernul este lider) și de jos în sus (societatea este lider), precum şi concentrarea eforturilor de creștere a rezilienței și nivelului de pregătire.

4.3. Contracararea ameninţării hibride – implicații pentru domeniul militar

Contracararea ameninţării hibride este responsabilitatea guvernului care se bazează pe întrebuinţarea integrată a instrumentelor de putere MPECI cu ponderi diferite, în funcţie de acţiunile agresorului. Din descrierea caracteristicilor ameninţării de tip hibrid deducem că, de regulă, ponderea cea mai mare o au instrumentele de putere non-militare. Totuși, rolul domeniului militar rămâne unul de primă mână întrucât este un instrument de putere important ce dispune de capabilităţi reale în detecţia componentelor „contondente" ale amenințărilor hibride, poate descuraja un potenţial agresor și poate răspunde la acţiuni cu impact semnificativ din compunerea agresiunii hibride, concomitent cu diminuarea efectelor acestora. Capabilitatea unică a forțelor armate este de a contribui la descurajare și, în situaţia în care aceasta eşuează, la ducerea unor acțiuni de luptă ce pot determina agresorul ca în final să renunţe sau să se demaşte, recurgând la un conflict convențional, amendabil de către organizaţiile internaţionale de securitate. Este nevoie astfel să se realizeze o estimare pertinetă la nivel guvernamental pentru a identifica cele mai probabile și cele mai periculoase amenințări la adresa națiunii. Pentru a veni în sprijinul strategiei de contracarare a ameninţărilor hibride, forțele armate trebuie să fie capabile să contribuie la efortul național și internațional de identificare a acestora, să poată respinge agresorul de tip hibrid și să răspundă la atacurile hibride. Luate împreună, aceste nevoi determină implicații pentru sistemul de apărare în următoarele domenii:

a. *Coordonare* – necesitatea unei coordonări îmbunătățite între utilizarea forței armate și celelalte instrumente de putere în cadrul guvernului și între națiuni pentru a se asigura că rolul apărării în abordarea de tip „whole-of-government" a eforturilor de contracarare a ameninţării de tip hibrid este adecvată și eficientă şi este susținută de un proces de planificare de contingenţă specifică, desfăşurată în mod regulat.

b. *Opţiuni* – evaluarea completă a modului în care forțele armate sunt organizate, dotate şi prevăzute cu resurse pentru a oferi guvernelor cât mai multe opțiuni privind acţiunile acestora sub pragul

conflictului armat în scopul asigurării nivelului de descurajare suficient sau al răspunsului la agresiunea hibridă.

c. *Reziliență* – necesitatea unei abordări moderne atât a contribuției apărării la reziliența națională, cât și a rezilienței proprii a sistemului naţional de apărare la agresiunea de tip hibrid.

Pentru realizarea unui nivel adecvat privind rolul sistemului naţional de apărare în contracararea ameninţării hibride, considerăm că trebuie avute în vedere următoarele puncte cheie:

- contracararea ameninţării hibride necesită „active interinstituționale" guvernamentale adecvate: procese, mecanisme, oameni și abilități pentru implementarea strategiei.
- contracararea ameninţării hibride presupune un set de acţiuni ce trebuie desfăşurate de către fiecare stat într-o configuraţie de tip „whole-of-government", dar necesită o abordare multinațională cuprinzătoare (inclusiv în domeniul militar) și ar trebui să exploateze și să dezvolte instituțiile, procesele și organizațiile existente, acolo unde este posibil.
- pentru detectarea ameninţării hibride, atât „monitorizarea", cât și „descoperirea" necesită o structură de analiză și decizie, care să o includă pe cea similară a instrumentului militar, care să aibă o autoritate instituțională şi o posibilitate de supraveghere largă.
- atât descurajarea, cât și răspunsul la agresiunea de tip hibrid necesită o planificare și o implementare coordonată a măsurilor în domeniile PMESII, folosind toate instrumentele de putere MPECI, pregătite în mod adecvat.

Deși contracararea ameninţărilor/agresiunilor hibride presupune un set de acţiuni ce trebuie desfăşurate în formatul „whole-of-government" şi care se bazează, în principal, pe instrumente non-militare, rolul apărării rămâne unul important datorită contribuțiilor unice pe care le poate aduce la detectarea, descurajarea și răspunsul dat.

Planificarea campaniei de combatere a agresiunii de tip hibrid[130]

De regulă, o campanie militară constă dintr-o serie de bătălii și angajamente concepute pentru a atinge un obiectiv strategic. Această definire este valabilă mai ales în cazul „războiului hibrid" în care o singură luptă nu va rezolva problema, ducând la victoria finală. Diferențele dintre planificarea unei campanii militare convenționale și a unei campanie de contracarare a agresiunii hibride în sprijinul unei națiuni gazdă (HN) pot fi evidenţiate pe cel puţin două planuri:

- ca și în caz de operaţiilor de contrainsurgență, naţiunea gazdă este cea care conduce acţiunile, ajutorul extern completând lipsa capabilităţilor în domeniile în care HN nu are resurse.
- toate elementele de putere (PMECI), atât cele aparţinând actorilor care acordă sprijin, cât și cele ale HN trebuie să fie orientate către niveluri mult mai locale decât în conflictele convenționale generale. Aspectul diplomatic este critic în această situaţie.

Ipoteze

Toate planurile sunt bazate pe presupuneri şi conţin ipoteze, iar planurile de contracarare a agresiunii de tip hibrid nu fac excepție. În acest caz, presupunerea cheie se referă la faptul că agresorul ce întrebuinţează strategia acţiunilor hibride nu dorește să inițieze un conflict convențional nici cu statul ţintă, nici cu actorii care îi acordă acestuia sprijin. Motivele sunt evidente, fie statul agresor ar trebui să pornească un război de agresiune, ceea ce ar atrage asupra sa sancţiuni conform dreptului internaţional umanitar, fie acesta ar trebui să se angajeze într-un conflict cu o forţă superioară, în urma căruia ar fi învins. În consecinţă, agresorul va încerca să păstreze conflictul într-o zonă gri, în special prin utilizarea, pentru acţiunile ce presupun forţa armată, a unor grupuri paramilitare ca actori proxy, de care să se disocieze în cazul apariţiei unor eventale acuzaţii. Pot exista și alte presupuneri, dar negarea plauzibilă a unor incidente grave ce pot apărea

[130] Gary Anderson, „Counter-Hybrid Warfare: Winning in the Gray Zone", *Small Wars Journal*, disponibil la https://smallwarsjournal.com/jrnl/art/counter-hybrid-warfare-winning-gray-zone, accesat la 11.01.2019.

în conflict este esențială pentru o campanie hibridă de succes întreprinsă de un actor de tip statal.

Designul operaţiilor de combatere a agresiunii de tip hibrid

Dacă un actor de tip statal se confruntă cu o agresiune hibridă determinată de manifestarea unei amenințări hibride ce a fost generată de către un stat agresor mai puternic, nu se poate aștepta să câștige războiul rapid, într-o singură luptă decisivă. Statul victimă va trebui să reia teritoriul în litigiu în mod treptat prin acţiuni specifice contrainsurgenței, desfăşurate în cadrul unei strategii de tip *oil-spot*. Este extrem de important să se evite ca un actor de tip statal cu o putere echivalentă sau superioară agresorului să desfăşoare o intervenţie militară cu forţe armate convenţionale întrucât acest act ar conduce la un conflict armat interstatal major. Cu toate acestea, statul care inițiază conflictul hibrid trebuie să înțeleagă că o intervenție militară de amploare este oricând posibilă în situaţia în care este identificat ca stat agresor.

Vulnerabilităţi ale agresiunii hibride

Orice plan de campanie trebuie să ia în considerare vulnerabilitățile cheie ale adversarului și modalitățile de exploatare a acestora. O agresiune hibridă desfăşurată de către un actor de tip statal are, de regulă, trei vulnerabilități cheie:

1. agresiunea hibridă nu funcționează întotdeauna. În conflictele convenționale din secolele XIX și XX, partea care a inițiat conflictul a reuşit să își atingă obiectivele majore doar în jumătate din cazuri. Aceasta nu este o medie mare, însă conflictele hibride moderne au avut rate de succes şi mai mici. Conflictele hibride desfăşurate după perioada Războiului Rece au fost și mai dezamăgitoare pentru actorii inițiatori.[131] Începerea unui conflict prin agresiuni desfăşurate într-o configuraţie hibridă a fost, până în prezent, o opţiune foarte riscantă.

2. actorii nestatali, cum ar fi grupurile paramilitare și mercenarii, sunt foarte greu de controlat. Marea majoritate a atrocităților din războiul din spaţiul ex-Iugoslav au fost comise de miliții de ambele părți, dar în special de cele susținute de Serbia pe teritoriul Bosniei. În Siria,

[131] *Ibidem*, fig. 1÷3, accesat la 11.01.2019.

mercenarii ruși şi-au exprimat public dezacordul faţă de conducerea rusă incompetentă și despre echipamentele slabe, după ce mulți dintre ei au fost măcelăriți într-un atac aerian american desfăşurat în 2018. Acest lucru a fost extrem de jenant pentru sponsorii lor ruși.

3. acțiunile hibride care evoluează în mod eronat pot duce la război convențional dacă actorii cinetici hibrizi pot fi relaţionaţi cu un anumit actor statal agresor și efervescența publică din presa mondială asupra atrocităților comise în numele acestuia determină o terță parte să intervină militar în mod direct, în numele națiunii gazdă victimă sau sub un mandat emis în cadrul juridc internaţional (pentru responsabilitatea de a proteja populaţia civilă, restabilirea păcii etc.). O asemena situaţie a fost cazul în Kosovo în 1999, când o coaliție NATO condusă de SUA a purtat direct o campanie aeriană asupra Serbiei, ceea ce a dus la prăbușirea guvernului sârb și intentarea unor procese de crime de război pentru mai mulți lideri sârbi. Războiul civil sirian și conflictul paralel declanşat de Statul Islamic au determinat mai mulți actori statali să intervină împotriva IS, pentru precum și împotriva guvernului sirian, pentru motivele binecunoscute. Acest lucru nu a dus încă la un conflict convențional generalizat, dar s-a apropiat în mai multe rânduri de o atare situaţie.

Centre de greutate

Un actor de tip statal ce întrebuinţează o strategie a acţiunilor hibride în care componenta de forţă armată are o prezenţă semnificativă trebuie să-și protejeze centrul de greutate, care este reprezentat de capacitatea sa de a susține o mișcare separatistă, fără a declanșa un răspuns cu forța convențională din partea statului victimă și a aliaților săi. Un element cheie în acest sens este negarea plauzibilă împotriva declanșării procesului de sancțiuni internaționale, intervenția ONU sau implicarea directă a unor forţe armate superioare.

Centrul de greutate al statului victimă îl reprezintă capabilitatea forțelor sale de securitate de a gestiona o insurecție desfăşurată cu întrebuinţarea forţei, cu sprijinul aliaților săi. Cu ajutorul forţelor armate și cu sprijin consultativ din partea unor state prietene, Ucraina a reuşit să izoleze conflictul separatist hibrid sprijinit de Rusia în zona granitei sale de est. Totuşi, în acest caz, dificultatea obţinerii unui deznodământ favorabil constă în faptul că nu este membru al NATO și nu are un acord bilateral cu o terță parte care i-ar putea permite să-și recupereze teritoriul deja pierdut.

CONCLUZII

Ameninţarea de tip hibrid se manifestă în mediul operaţional într-o configuraţie de o complexitate deosebită, mereu diferită, adaptată vulnerabilităţilor actorului ţintă şi într-o manieră care, de cele mai multe ori, produce un efect de dezechilibru ce uzează capabilităţile lui în toate domeniile, diminuându-i puterea de a riposta. Contracararea agresiunii de tip hibrid devine, astfel, una dintre cele mai complexe probleme privind asigurarea securităţii actorilor de pe mapamond la început de secol XXI. De aceea, conflictul în care este prezentă agresiunea de tip hibrid nu mai este o problemă de apărare naţională, ci devine una de securitate naţională.

Măsurile şi acţiunile care compun combaterea ameninţării de tip hibrid trebuie să înceapă înainte ca aceasta să se materializeze în agresiune, trebuie să fie gândite şi desfăşurate într-o abordare proactivă. În caz contrar, actorul ţintă va întâmpina dificultăţi majore în configurarea răspunsului, dificultăţi care vor escalada exponenţial, pe măsură cu puterea sa se diminuează. Augmentarea capabilităţilor necesare combaterii ameninţării de tip hibrid se poate face prin previzionarea situaţiilor de criză, prin pregătirea corespunzătoare a forţei şi prin desfăşurarea de acţiuni eficiente şi eficace care să compună răspunsul adecvat. Aceste secvenţe trebuie să fie conectate între ele printr-un proces de planificare eficient, care trebuie desfăşurat în mod conjugat la toate nivelurile părţilor implicate în conflict. Un instrument util este metoda scenariilor, care pune la dispoziţie un cadru flexibil şi controlat, un „laborator” ce permite utilizarea coerentă unei game variate de algoritmi şi proceduri pentru identificarea răspunsului optim, precum şi pentru antrenarea şi verificarea forţelor.

În funcţie de modul de aplicare, metoda scenariilor poate declanşa procesul de planificare sau îl poate sprijini pe parcursul întregii perioade de desfăşurare. Scopul utilizării ei este eliminarea incertitudinii sau, cel puţin, stabilirea unor limite controlabile în jurul incertitudinilor generate de mediul operaţional de tip hibrid şi concentrarea efortului planificatorilor înspre soluţionarea problemei. În plus, întrebuinţarea

metodei scenariilor în cadrul procesului de planificare facilitează utilizarea de procedee avansate de cercetare operaţională care, corelate cu utilizarea modelării şi simulării, contribuie la crearea unor planuri viabile şi valide necesare generării unei capacităţi de ripostă flexibilă şi eficientă.

O alt concluzie ce rezultă din acest studiu se referă la necesitatea de a avea o terminologie clară, atât în lucrările ştiinţifice care tratează acest subiect al hibridizării ameninţărilor şi agresiunilor din mediul operaţional şi de securitate, cât şi în analizele şi documentele realizate la nivel operaţional. Pentru a reduce la minimum ambiguitatea cauzată de terminologia nestandardizată, NATO a lucrat la elaborarea unui vocabular clar în ceea ce privește conflictele hibride. Cu toate că nu există încă o definiție acceptată în unanimitate a „ameninţării hibride” şi a „războiului hibrid”, NATO ia în considerare faptul că termenul esențial şi anume „hibrid”, atunci când caracterizează un conflict, presupune un actor statal sau nestatal ce foloseşte în mod concertat diferite mijloace și metode multimodale (folosește o „strategie hibridă”) într-un mod adaptat la mediul operaţional şi de securitate existent. În accepţiunea NATO, „strategia hibridă” este o strategie bazată pe o combinație largă, complexă, adaptivă și adesea extrem de integrată de mijloace convenționale și/sau neconvenționale, cu participarea unor actori militari, paramilitari și/sau civili şi care presupune acţiuni complexe atât descoperite, cât și sub acoperire, desfășurate în întregul spectru al instrumentelor de putere vizând în mod preponderent procesul de luare a deciziilor. De aici rezultă că „ameninţarea hibridă” este reprezentată de către un actor statal sau nestatal care utilizează o strategie hibridă. Se consideră că, pentru a utiliza o strategie hibridă, un actor nestatal ar avea nevoie de capacitatea de a întrebuinţa multe sau toate instrumentele de putere puterii asociate, în mod normal, unui stat suveran. Manifestarea ameninţării hibride determină o „agresiune hibridă” în sensul în care aceasta presupune întrebuinţarea de către un adversar a unei strategii hibride, care include amenințarea sau utilizarea forței. Forța poate fi folosită la un nivel mai redus decât termenul de conflict armat şi poate presupune o serie de acţiuni de luptă armată cu caracter convenţional sau neconvenţional care au ca efecte exercitarea de

presiune, influență și / sau destabilizare fără a implica neapărat cucerirea teritoriului.

Reunind într-o singură frază toţi aceşti termeni, pentru a evidenţia relaţia dintre ei, putem afirma faptul că *fiecare ameninţare hibridă va avea o configuraţie unică ce va corespunde unui model hibrid care fundamentează strategia hibridă întrebuinţată în cadrul manifestării ameninţării, ceea ce reprezintă agresiunea hibridă desfăşurată de către un agresor hibrid împotriva unui actor ţintă, de regulă statal.* Acesta din urmă va trebui să dezvolte un sistem de tip „whole of government", corespunzător caracteristicilor sale de bază (SWOT), integrat ce cel al partenerilor şi adaptat configuraţiei agresiunii de tip hibrid executată asupra sa, care să permită contracararea acesteia, adică detectarea, prevenirea (descurajarea – eliminarea ameninţării), rezilienţa (apărarea, rezistenţa la impact şi recuperarea în urma agresiunii hibride) şi combaterea (care se desfăşoară concomitent cu prevenirea şi rezilienţa şi presupune implementarea de contramăsuri ce constituie răspunsul la agresiunea hibridă). Sistemul de contracarare a ameninţării de tip hibrid trebuie să implementeze o strategie coerentă, care să întrebuinţeze toate instrumentele de putere (MPECI) în acţiuni desfăşurate în toate domeniile care definesc actorul de tip statal (PMESII) pentru a atinge toate obiectivele de securitate stabilite la nivel naţional în realizarea scopului pentru care a fost creat.

Se poate afirma faptul că atât NATO, cât şi UE au reușit în mare parte utilizarea în mod consecvent a terminologiei propuse în doctrinele, protocoalele, memoriile și declaraţiile lor ulterioare. Cu toate acestea, există documente NATO în care termenul „hibrid" atribuie construcţiei în care este utilizat şi alte conotaţii. De exemplu, termenul „amenințare aeriană hibridă" este utilizat pentru a descrie utilizarea potențială a platformelor aeriene fără pilot (UAV), împreună cu cele tradiţionale, mai ales dacă au dimensiuni mici, evoluează la viteze reduse și, eventual, sunt conectate în rețea prin tehnologii de tip „swarming". În aceste cazuri, eticheta „amenințarea aeriană de tip hibrid" pare să fie aleasă pur și simplu pentru că:

- adversarul utilizează tehnologie modernă (mijloace aeriene fără pilot) în conjuncţie cu cea tradiţională, cu pilot;

- utilizarea acestei tehnologii (UAV) conduce la o posibilă ambiguitate în identificarea și atribuirea acţiunilor agresive, precum și la o amenințare asimetrică dificil de contracarat cu sistemele militare tradiționale de apărare aeriană.

Niciuna dintre aceste caracteristici nu se conformează sensului atribuit termenului „hibrid” adoptat în cadrul Alianței, fie şi pentru faptul că, de regulă, acesta este atribuit unui construct de nivel strategic şi nu unei acţiuni tactice. Nu există nicio îndoială că, în războiul modern, adversarul poate folosi mijloace aeriene inovatoare, cum ar fi cele fără pilot, a căror detectare, identificare și angajare cu sistemele de foc antiaerian și poliție aeriană implică noi capabilităţi tehnice și procedurale ce pot să nu fie la dispoziţia tuturor statelor. Tehnologia modernă și modurile de angajare, şi nu „hibriditatea”, sunt cele care definesc noutatea în această amenințare militară formidabilă. În consecinţă, putem considera faptul că niciun atac izolat singular, cu mijloace militare convenționale şi neconvenționale nu ar putea fi considerat „hibrid” *per se*. Având în vedere aspectului general al „hibridității” descris în capitolele anterioare, considerăm că nu există un tip de atac „hibrid” distinct şi singular, ci acesta va fi întotdeauna un amestec cuprinzător de acţiuni, desfăşurate pe multiple planuri, vizând multiple puncte de aplicare şi care necesită un răspuns complex.

Utilizarea conceptului „Hybrid Warfare” și a celor aferente pentru a exprima un sentiment de urgență poate fi ineficientă sau chiar contraproductivă. Specialiștii militari ar trebui să se abțină de la utilizarea necorespunzătoare a termenului „hibrid”, deoarece caracteristica de incluziune generală a teoriei „Războiului hibrid” poate genera confuzie și estompează aspectele pe care factorii de decizie trebuie să le înțeleagă atunci când configurează soluţia. „Strategul hibrid” din partea adversarului ar putea considera o asemenea lipsă de înțelegere un succes.

Aşa cum am precizat în capitolele 1 şi 2, hibridizarea mijloacelor întrebuinţate în conflict, precum şi a acţiunilor specifice acestuia nu constituie o abordare nouă. Dar configuraţia şi modul de aplicare a mixului de agresiuni s-a schimbat. Globalizarea și complexitatea sporită a mediului geostrategic, permise de progresele tehnologice și accesul la

acesta, au permis agresorilor să îmbine forme asimetrice sofisticate pentru a-și ascunde rolul lor de parte la conflict şi, mai ales, acţiunile acestora şi scopurile urmărite cu scopul de a complica și întârzia luarea deciziilor şi implementarea contramăsurilor de către ţintă. Agresiunea de tip hibrid şi componentele sale sunt rareori în concordanță cu prevederile dreptului conflictelor, iar ambiguitatea sa reprezintă provocări pentru încadrarea legală și conceptuală în normele tradiționale ale crizelor și războiului. Prin urmare, acest nou tip de abordare a agresiunii necesită un nivel mai înalt de conștientizare și cooperare a actorilor de tip statal şi suprastatal (în special privind partajarea de informații), voință și pregătire politică (privind luarea şi implementarea deciziilor), comunicare strategice (combaterea propagandei) și sisteme de apărare care să confere un nivel înalt de rezilienţă (apărare cibernetică, solidaritate economică și socială etc.).

Îmbunătățirea posturii de descurajare și apărare a actorilor de tip statal şi suprastatal față de provocările emergente de securitate trebuie să înceapă prin a evidenţia cu exactitate lacunele privind capabilităţile existente şi vulnerabilităţile către factorii de decizie relevanți. „De fiecare dată când ne confruntăm cu o nouă provocare de securitate, un contractor pe probleme de apărare sau de securitate așteaptă în proximitate să ne ofere o soluție. În cazul amenințării hibride, nu există o soluție unică pentru toate configuraţiile și nici un sistem nou pe care să îl cumpărăm pentru a le atenua. În schimb, tot ce am învățat de la agresiunea Rusiei împotriva Ucrainei în 2014 ne spune că trebuie să ne adaptăm cadrele legale și cultura de lucru și să îmbunătățim conexiunile dintre ministere și organizații pentru a permite propriilor noastre guverne să ne protejeze mai bine societatea.”[132]

În acest context, putem să constatăm faptul că în cele mai multe state din Occident, dependența culturii de securitate la nivel național de cumpărarea de soluții de la contractanți le-a diminuat capacitatea de a face mai multe progrese în abordarea amenințărilor hibride. Unele țări precum Finlanda și Marea Britanie sunt mult avansate în această

[132] Christopher Kremidas-Courtney, „Countering hybrid threats: We can’t just buy a solution”, disponibil la http://www.ekathimerini.com/237701/opinion/ekathimerini/comment/countering-hybrid-threats-we-cant-just-buy-a-solution, accesat la 14.07.2019.

problemă, deoarece au adoptat o abordare procesuală a acestei provocări. Pentru rezolvarea acestei probleme, ar trebui ţinut cont de câteva aspecte de bază cu care trebuie început.

În primul rând, este necesară înțelegerea faptului că agresiunea hibridă este un „joc de acasă”, în sensul în care acţiunile care o presupun şi efectele generate se realizează în interiorul graniţelor propriului stat. Mai mult decât atât, acţiunile ce compun agresiunea hibridă nu presupun în mod preponderent lupta armată, determinând astfel apariţia unei situaţii de apărare naţională, ci generează efecte îndreptate împotriva securităţii naţionale. Combaterea amenințărilor hibride necesită, astfel, o schimbare culturală de la modul de gândire exclusiv expediționar, în care ministerul de afaceri externe și ministerul apărării au întâietate, către unul naţional, orientat către interiorul statului, în care ministerul de interne și ministerul public ocupă adesea un rol principal. Totuşi, în acest context, natura interstatală a abordării amenințărilor hibride există, în special în cadru multilateral, şi presupune faptul că ministerele de externe continuă să joace un rol esențial, într-o abordare de tip *whole-of-government*.

Un al doilea aspect se referă la asigurarea cadrului legal care să permită entităților guvernamentale să contracareze amenințările hibride, care pot avea loc adesea în zonele gri, fie la limitele responsabilităţilor şi autorității diferitelor ministere, fie în domenii în care acestea se suprapun. Mai mulți aliați și parteneri NATO au efectuat analize interne extinse, sprijinite de simulări și exerciții pentru a identifica lacunele și vulnerabilitățile specifice sistemelor juridice. Ulterior, organele legislative, la nivel naţional, au acţionat pentru a reduce orice lacune juridice identificate și pentru a elimina orice posibilă confuzie privind responsabilităţile și autoritățile diferitelor organisme statale.

În al treilea rând, identificarea de soluţii la nivel guvernamental presupune aprofundarea nivelului de cooperare pe plan intern și internațional, pentru a construi un cadru sănătos de încredere și consultare, necesar pentru contracararea amenințării hibride. Până acum, cele mai mari provocări în abordarea amenințărilor hibride au fost atribuirea și luarea deciziilor în situaţii de criză pentru a determina

răspunsuri adecvate. Ambele probleme necesită un nivel ridicat de încredere și coeziune între funcționari, ministere și instituții.

Pe plan intern, soluția în asigurarea descurajării credibile a amenințărilor hibride este simplă: construirea și menținerea unei proces de guvernare rezilient, credibil și capabil, care să ridice efortul necesar desfăşurării agresiunii hibride și să-i reducă șansele de succes. Pentru a realiza acest deziderat în mod eficient, este nevoie de cooperare și colaborare din partea tuturor entităților.

În ceea ce priveşte cooperarea și colaborarea națională și multilaterală, în funcție de nivelul de disponibilitate al diferiților actori, există *trei niveluri*, între care există o relaţie de incluziune şi care permit guvernelor și societăților să abordeze mai eficient amenințările hibride. *Primul* îl reprezintă cadrul pentru o abordare de tip „*whole-of-government*”, în care toate ministerele și agențiile, de la nivel național la nivel local, cooperează, își fixează obiective comune și împărtășesc informații. *Al doilea* presupune o abordare „*whole-of-society*”, care este similară cu nivelul anterior şi care include implicarea sectorului privat, mediului academic și societăţii civile. *Al treilea* nivel se referă la „*comprehensive approach*”, şi anume la abordarea cuprinzătoare şi integratoare a cadrului de cooperare, în care grupuri de organizaţii sau state cu moduri de gândire şi strategii similare lucrează împreună cu organizații și entități internaționale precum NATO, Uniunea Europeană, Organizația pentru Securitate și Cooperare în Europa, Organizaţia Națiunilor Unite, Banca Mondială, Comitetul Internațional al Crucii Roșii, sectorul privat și societatea civilă. Fiecare dintre acestea colaborează și își coordonează eforturile pentru a face față provocărilor împreună, toate respectându-şi reciproc rolurile, responsabilităţile și autonomia decizională.

În fiecare dintre aceste cazuri, colaborarea în discuțiile interinstituţionale, în exercițiile bazate pe scenarii privind amenințările hibride și în discuțiile la nivel înalt sunt vitale pentru crearea nivelului optim al încrederii și interoperabilității dintre ministere, națiuni, societatea civilă, organizații internaționale și sectorul privat.

Concentrarea pe o abordare cooperativă a proceselor specifice determină obţinerea unei perspective care aliniază mai strâns autoritățile

și cadrele juridice proprii ale fiecărei națiuni. Având în vedere natura acestor amenințări, primele care detectează şi răspund sunt cel mai probabil autoritățile civile şi entități private. La rândul său, instrumentul militar pune la dispoziţie diferite capabilităţi necesare pentru a oferi sprijin. Această cooperare este vitală, deoarece niciun guvern nu este în măsură să întreţină mai multe mijloace care oferă capabilităţi similare.

În cazul apariţiei unei situaţii escaladate, este necesară o strânsă cooperare civil-militară, cu un grad înalt de interoperabilitate, pentru a asigura un răspuns adecvat, cu întrebuinţarea tuturor instrumentelor necesare și disponibile în cadru național și internațional.

Din acest motiv, nivelurile doi şi trei sunt esențiale pentru crearea încrederii și interoperabilității, astfel încât orice lacune și vulnerabilități din cadrul juridic și procedural propriu să poată fi identificate și eliminate. Prin consolidarea acţiunii mecanismelor de guvernare în sectorul public și privat și prin realizarea unui cadru de cooperare mai profundă și mai largă între instituții, națiuni, societatea civilă și sectorul privat, se poate transforma nivelul înalt de globalizare și interconectare contemporan dintr-o vulnerabilitate într-un avantaj.

Agresiunea de tip hibrid nu poate fi contracarată uşor şi de aceea, această nouă abordare a impunerii voinţei asupra adversarului este ceva care trebuie prevenit sau descurajat întrucât odată ce sunt create condițiile sociale, politice și economice pentru a permite eficacitatea şi eficienţa implementării strategiei acţiunilor hibride, este probabil prea târziu pentru a fi oprită. „Războaiele hibride” trebuie câștigate înainte ca lupta să înceapă şi pentru a face acest lucru, actorii de tip statal, în special, precum şi cei suprastatali trebuie să creeze condițiile care să interzică unui potenţial agresor utilizarea eficientă a strategiei acţiunilor hibride. Există trei moduri principale de a realiza acest deziderat.

Primul, şi poate cel mai eficient îl reprezintă realizarea unui nivel ridicat de bună guvernare la nivel local și național. Dacă membrii societăţii simt că sunt guvernați corect și bine, atunci devin mai puțin sensibili la acţiunile de dezinformare și propagandă ale agresorului. Existenţa unui nivel ridicat de corupție endemică, lipsa unei guvernări locale puternice și deconectarea guvernului central în rezolvarea

nemulțumirilor de natură politică la nivel local, reprezintă caracteristici ale mediului propice de manifestare a amenințării de tip hibrid.

Al doilea mod presupune realizarea unui nivel ridicat de libertate economică. Oamenii trebuie să simtă că au un nivel acceptabil de stabilitate economică și că generaţiile următoare au un viitor asigurat din punct de vedere economic. Urmărirea politicilor care ajută la creșterea economică şi sporirea prosperității cetăţenilor este o parte importantă a combaterii strategiei acţiunilor hibride. Persoanele care simt ca au oportunități economice rele, într-un mediu stabil sunt mai puțin sensibile la componentele agresiunii de tip hibrid.

În cele din urmă, trebuie creată o legătură de încredere și respect între populaţie și sistemul de impunere a legii și serviciile de informații. Dacă cetăţenii au sentimentul că legea este aplicată corect, în mod echitabil și că serviciile de informații acţionează în slujba lor fără a-şi depăşi limitele, societatea va deveni mai rezistentă împotriva acţiunilor destbilizatoare, extrem de prezente în toate configuraţiile agresiunii de tip hibrid. În plus, impunerea legii şi menţinerea ordinii publice se situează adesea în prima linie de apărare într-un scenariu de manifestare a amenințării hibride. Un asemenea sistem capabil și profesional, alături de cel creat de către serviciile de informații, atenuează semnificativ eficacitatea agenților provocatori care acționează în numele unui potenţial agresor.

Deşi aceste trei măsuri sunt dificil de implementat, dacă sunt urmărite cu adevărat de către guvernele naționale, ele pot descuraja sau afecta semnificativ implementarea strategiilor de tip hibrid de căre un potenţial agresor sau, cel puțin, pot reduce eficacitatea unor acţiuni care le compun.

Se poate considera că un exemplu de actor statal care a implementat cele trei moduri, alături de altele care au contribuit la construirea rezilienţei la agresiunea de tip hibrid este Estonia. Chiar dacă minoritatea rusă reprezintă aproximativ un sfert din populație (totuşi semnificativ mai redusă decât procentul din zona peninsulei Crimeea sau din regiunea Donbas) Moscova nu a reușit să creeze aceleași probleme folosind tactica sa hibridă ca și în Ucraina. S-a constatat că populația din Estonia nu este sensibilă la componentele sociale ale agresiunii de tip

hibrid ale Moscovei manifestate sub forma propagandei sau la cele destabilizatoare aplicate de structuri de tipul „omuleţilor verzi”. Motivul determinat pe baza unor sondaje de opinie publică arată că o mare majoritate a cetăţenilor au un grad ridicat de încredere în instituțiile lor de conducere. Un exemplu în acest sens îl reprezintă cel realizat de Ministerul Apărării din Estonia[133], potrivit căruia 66% dintre estonieni au încredere în președintele țării și 56% în prim-ministru. Potrivit aceluiași sondaj, 87% dintre estonieni au spus că au încredere în poliție. Poate că nu este surprinzător, Indexul Libertății Economice din 2019 realizat de către Fundația Heritage a clasat Estonia a cincisprezecea în lume şi a şaptea în Europa în ceea ce privește libertatea economică[134]. Încrederea în guvern și poliție, combinată cu oportunitățile economice ale Estoniei, interzic capacitatea unui potenţial agresor de a folosi acţiuni specifice strategiei hibride. Estonia a reușit să câștige „războiul hibrid” chiar înainte de începerea acestuia. Comparând situația Estoniei de astăzi cu cea a Ucrainei din 2013 și 2014, ajungem la concluzia că din cauza unei situații economice precare și a perioadei îndelungate de corupție politică și economică în fruntea guvernului, Rusia a putut să exploateze situația din Ucraina. În momentul în care „omuleţii verzi” au apărut în Crimeea, era prea târziu.[135]

În cele din urmă, buna guvernare şi libertatea economică, conjugate cu acţiunile eficiente ale unui sistem corect de impunere a legii și a unor servicii de informaţii şi securitate de încredere reprezintă cea mai bună modalitate de a spori rezilienţa unui actor de tip statal şi de a opri agresiunea hibridă chiar înainte de a începe.

---

[133] ***, *Public opinion and national defence*, disponibil la http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_ and_national_defence_2018_march.pdf, accesat la 12.09.2019.

[134] N.A.: mai multe detalii se pot găsi la adresa https://www.heritage.org/index/country/estonia, accesat la 12.09.2019.

[135] Luke Coffey, „How to Defeat Hybrid Warfare Before It Starts”, disponibil la https://www.defenseone.com/ideas/2019/01/how-defeat-hybrid-warfare-it-starts/154296/, accesat la 14.08.2019.

LISTA CU ABREVIERI ŞI ACRONIME

Termen	Explicaţie în limba română	Explicaţie în limba engleză/franceză
0	**1**	**2**
A2/AD	-	anti-acces, area denial
ACT	Comandamentul aliat pentru transformare	Allied Command Transformation
ADMCBRN	arme de distrugere în masă chimice, biologice, radiologice şi nucleare	-
CCOMC	-	Comprehensive Crisis and Operations Management Centre
INFOOPS	operaţii informaţionale	Information operations
INFOWAR	război informaţional	Information warfare
IS	Stat Islamic	Islamic State
JISD	-	Joint Intelligence and Security Division
FOS	Forţe pentru operaţii speciale	Special operations forces
HN	naţiune gazdă	Host Nation
MACTOR	matricea alianţelor şi conflictelor: tactici, obiective, recomandări	Matrix of Alliances and Conflicts: Tactics, Objectives and Recommendations
MC	Comitetul militar	Military Committee
MENA	Orientul Mijlociu și Nordul Africii	Middle East and North Africa

Termen	Explicaţie în limba română	Explicaţie în limba engleză/franceză
0	**1**	**2**
MICMAC	matricea de impact încrucişat şi multiplicare aplicată clasificării	Matrice d'Impacts Croisés – Multiplication Appliquée à un Classement (fr.)
MPECI	Militar, politic, economic, civil, informaţional	-
NAC	Consiliul Nordatlantic	North Atlantic Council
PMESII-PT	Politic, militar, economic, social, informaţii, infrastructură, mediu înconjurător şi timp	Political, Military, Economic, Social, Infrastructure, Information – Physical Environment and Time
PSYOPS	operaţii psihologice	psychological operations
SACEUR	Comandantul Suprem al Forţelor Aliate	Supreme Alied Commander Europe
SHAPE	Comandamentul suprem al forţelor aliate din Europa	Supreme Headquarters Allied Powers Europe
SWOT	puncte tari, puncte slabe, oportunităţi, ameninţări	Strengths, weaknesses, opportunities, threats
UAV	platformă aeriană fără pilot	unmanned aerial vehicle

BIBLIOGRAFIE

1. ***, *Strategic trends programe. Future character of conflict*, UK Ministery of Defence, 02.02.2010.
2. ***, AAP-6, *NATO glossary of terms and definitions*, NATO Standardization Agency, 2015.
3. ***, ADRP 3-0, *Unified Land Operations*, Washington, noiembrie 2016.
4. ***, *Dicţionarul explicativ al limbii române*, Editura Univers Enciclopedic Gold, 2009.
5. ***, *Doctrina Armatei României*, Bucureşti, 2012.
6. ***, *Doctrina Militară a Federaţiei Ruse*, 2014.
7. ***, FM 100-2-1, *The Soviet Army: Operations and Tactics*, Washington DC: Department of the Army, 1984.
8. ***, JP 1-02, *DOD Dictionary of Military and Associated Terms*, US Department of Defense, mai 2017, URL: http://www.dtic.mil/ doctrine/new_pubs/dictionary.pdf
9. ***, Legea nr. 355/2009 privind regimul stării de mobilizare parţială sau totală a forţelor armate şi al stării de război.
10. ***, Legea nr. 535 din 25 noiembrie 2004 privind prevenirea şi combaterea terorismului.
11. ***, NATO, *Bi-SC Input to a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats*, 2010.
12. ***, *Strategia naţională de apărare a ţării pentru perioada 2015 - 2019*, Bucureşti 2015.
13. ***, *Terms and Definitions of Interest for Counterintelligence Professionals, Public Intelligence*, Department of Defense, 09 iun. 2014.
14. AARONSON, Michael; DIESSEN, Sverre; DE KERMABON, Yves; LONG, Mary Beth; MIKLAUCIC, Michael, „NATO Countering the Hybrid Threat", *Prism*, 2(4), pp. 111-124, 2012, URL: http://mercury.ethz.ch/serviceengine/Files/ISN/133803/ichaptersection_ singledocument/fee9d9be-0d38-4db7-ab4a-31e7c2bfde19/ en/Chapter8.pdf
15. ANDERSON, Gary, „Counter-Hybrid Warfare: Winning in the Gray Zone", *Small Wars Journal*, URL: https://smallwarsjournal.com /jrnl/art/counter-hybrid-warfare-winning-gray-zone
16. BACEVICH, Andrew J., „The Petraeus Doctrine", *The Atlantic*, octombrie 2008, URL: https://www.theatlantic.com/magazine/archive /2008/10/the-petraeus-doctrine/306964/

17. BACHMANN, Sascha-Dominik, „Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats– mapping the new frontier of global risk and security management", *Amicus Curiae*, Vol. 88, 2011, URL: https://papers.ssrn.com/sol3/ papers.cfmabstract_id=1989808
18. BENBOW, Tim, „Talking About Our Questions? Assesing the Concept of Four-Generation Warfare", *Comparative Strategy*, 27:2, 2008.
19. BERZINS, Janis, „A New Generation of Warfare", *Per Concordiam*, 6:3, 2015, URL: www.marshallcenter.org/mcpublicweb/MCDocs/files /College /F_ Publications/perConcordiam/pC_V6N3)en.pdf
20. BLUM, Rebecca, *The future of NATO in the face of hybrid conflict*, Bernard El Ghoul, International Relations, Academic year 2014/2015.
21. BOGZEANU, Cristina, „Resilience: concept, approaches and implications", *Strategic Impact*, No. 3-4/2017, "CAROL I" National Defence University Publishing House, Bucharest, URL https://cssas.unap.ro/en/pdf_ periodicals/si64-65.pdf
22. BRET, Perry, „Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations", în *Small Wars Journal*, 14 oct. 2015, URL: http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera
23. BRYNEN, Rex, *Countering Hybrid Threats AAR, Pax Sims*, 2011, URL: https://paxsims.wordpress.com/2011/05/15/countering-hybrid-threats-aar/
24. CARAYANNIS, Tatiana, „The complex wars of the Congo: towards a new analytic approach", *Journal of Asian and African Studies*, 38(2-3), 2003.
25. CHEKINOV, G. Serghei; BOGDANOV, A. Serghei, T*he Nature and Content of New Generation War*, Voyenna Mysl 4, 2013, URL: http://www.eastviewpress.com/Files/MT_from%20the%20current%20issue_ No.4_2013.pdf
26. COHEN, Ariel; HAMILTON, Robert, „The Russian Military and the Georgia War: Lessons and Implications", *ERAP Monograph*, Fort Leavenworth, Kansas: Strategic Studies Institute, 2011.
27. CROFT, Adrian, „NATO says Russia has big force at Ukraine's border, worries over Transdniestria", *Reuters*, 23 mar. 2014, URL: https://www.reuters.com/article/us-ukraine-crisis-nato-idUSBREA2M0EG 20140323
28. CRUCERU, Valerică, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013.

29. DOUGHERTY, Jill, *Everyone Lies: The Ukraine Conflict and Russia's Media Transformation*, Shorenstein Center on Media, Politics and Public Policy, Harvard Kennedy School, iulie 2014, URL: https://shorensteincenter.org/wp-content/uploads/2014/07/d88-dougherty.pdf.
30. DUCARU, Sorin, "The cyber dimension of modern hybrid warfare and its relevance for NATO", *Europolity*, vol. 10, no. 1, 2016, URL: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf
31. DUŢU, Petre, *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale*, Editura UNAp. „Carol I", Bucureşti, 2013.
32. EXUM, Andrew, „Hizballah at War: A Military Assessment", Policy Focus #63, *Washington Institute for Near East Policy*, Washington DC, Decembrie 2006, URL: http://www.washingtoninstitute.org/uploads/ Documents/pubs/ PolicyFocus63.pdf
33. FLEMING, Brian, *Hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art*, United States Army Command and General Staff College, 2011, URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a545789.pdf
34. FREIER, Nathan, *Present at the Counterrevolution: An Essay on the 2005 National Defense Strategy and Its Impact on Policy*, United States Army War College Guide to National Security Issues, Vol. 2: National Security Policy and Strategy, Editor J. Boone Bartholomees Jr., 4th edition, iulie, 2010.
35. GALEOTTI, Mark, „Hybrid War' and 'Little Green Men': How Does It Works and How It Doesn't", URL: http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/
36. GERASIMOV, Valery, *Speech at the annual meeting of the Russian Academy of Military Science*, ianuarie 2013, Military-Industrial Courier, Moscow, 2013, URL: http://vpk-news.ru/sites/default/files/pdf/VPK_ 08_476.pdf
37. GILLES, K.; MONAGHAM, A., „Russian Military Modernization - Goal in Sight", *The Letort Paper*, 2014.
38. GODET, Michel, *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994.
39. GRAY, S. Colin, *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional*, Strategic Studies Institute, U.S. Army War College, Carlisle, 2012.
40. GUNNERIUSSON, Hâkan, *Nothing is Taken Serious Until It Gets Serious: Countering Hybrid Threats*, Defence Against Terrorism Review (4)1, 2012.

41. HIGGINS, Andrew, „Armed Men Seize Police Station in Eastern Ukraine City", *The New York Times*, 12 apr. 2014, URL: http://www.nytimes.com/2014/04/13/world/europe/ukraine.html
42. HOFFMAN, Frank G., *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.
43. HOFFMAN, Frank G., *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies, National Defense University, Strategic Forum No. 240, Aprilie 2009, URL: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591 =0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=98862
44. HOFMANN, Frank G., *Hybrid vs. Compound war*, 1 octombrie 2009, URL http://www.armedforcesjournal.com/hybrid-vs-compound-war
45. HOFMANN, Frank G., *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies, National Defense University, Strategic Forum No. 240, Aprilie 2009, URL: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots59 1=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=98862
46. KASAPOGLU, Can, *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, Research Paper No. 121, Rome: NATO Defence College, 2015.
47. KEIR, Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, London: The Royal Institute of International Affairs, 2016, URL https://www.chathamhouse.org/publication/russias-new-tools-confronting-west
48. LANDLER, M.; Michael, R. GORDON, „NATO Chief Warn of Duplicity by Putin on Ukaine", *The New York Times*, 08 iul. 2014, URL: www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html
49. MANSOUR, Peter R., „Hybrid War in History", în *Hybrid Warfare*, Fighting Complex Opponents from the Ancient World to the Present, Editura Williamson Murray and Peter R. Mansour, Cambridge University Press, 2012.
50. MONAGHAN, Andrew, *The "War" in Russia's 'Hybrid Warfare*, Parameters 45(4), Winter 2015.
51. NEWNHAM, Randall, „Georgia on my mind? Russian sanctions and the end of the 'Rose Revolution", *Journal of Eurasian Studies*, 6/2015.
52. OLIKER, Olga, *Unpacking Russia's New National Security Strategy*, Center for Strategic and International Studies, 7 ianuarie, 2016, URL:

https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy
53. PETRESCU, Dan-Lucian, „Model avansat de configurare a agresiunii de tip hibrid", *Revista Impact Sstrategic*, nr. 2[63]/2017, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti.
54. PICKAR, Charles, *Tactical Deep Battle: The Missing Link*, Monograph, (Fort Leavenworth, Kansas: School of Advanced Military Studies, 1991.
55. POMERANTSEV, Peter, *How Russia Is Revolutionizing Information warfare*, Defence One, 09 sept. 2014, URL: www.defenseone.com /threats/2014/09/how-russia-revolutionizing-information-warfare/93635
56. QIAO, Liang; WANG, Xiangsui,, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, 1999, URL www.oodalooo.com /documents/unrestricted.pdf
57. ROTH, Andrew, *From Russia, 'Tourists' Stir the Protests*, The New York Times, 03 mar. 2014, URL: https://www.nytimes.com /2014/03/04/world/europe/ russias-hand-can-be-seen-in-the-protests.html
58. SIMON, Luis, *A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy*, 03 mai 2016.
59. SIMPSON, Erin, 2005. *Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims*, URL: http://www.allacademic.com /meta/p84945_index.html
60. STARYKOV, Oleh, *Military expert Starykov: Zapad-2017 war games in Belarus designed to demonstrate Russia's military power*, URL: http://euromaidanpress.com/2017/08/30/military-expert-starykov-zapad-2017-war-games-in-belarus-designed-to-demonstrate-russias-military-power/
61. THIELE, Ralph, „Crisis in Ukraine – The Emergence of Hybrid Warfare*", ISPSW Strategy Series*", 2015.
62. THOMAS, Timothy L., „Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies*, 17: 237–256, 2004.
63. TRIANDAFILLOV, Vladimir, *The Nature of the Operations of Modern Armies*, Ed. Taylor & Francis, 1994.
64. VANDIVER, John, „SACEUR: Allies Must Prepare for „Hybrid Warfare", *Star and Stripes*, 04 sept. 2015, URL: www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464
65. WILSON, Andrew, *Russian Active Measures: Modernized Tradition*, The Institute for Statecraft, 03 ian 2016, URL: http://www.statecraft.org.uk/ research/russian-active-measures-modernised-tradition.

EDITURA
UNIVERSITĂŢII NAŢIONALE DE APĂRARE „CAROL I”

Redactor: Andreea Tudor
Coperta: Liliana ILIE
Lucrarea conţine 128 de pagini.

Universitatea Naţională de Apărare „Carol I”
Centrul de Studii Strategice de Apărare şi Securitate
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
Tel.: +41.021.319.56.49, Fax: +41.021.319.57.80
E-mail: cssas@unap.ro, Website: http://cssas.unap.ro

1996/2019 C.281/2019

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
(Editură cu prestigiu recunoscut de Consiliul Național de Atestare
a Titlurilor, Diplomelor și Certificatelor Universitare)

ISBN 978-606-660-402-4