Nr.2/2023, APRILIE-IUNIE
https://doi.org/10.53477/2065-8281-23-19

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

https://buletinul.unap.ro

Hibrid – concept definitoriu al războaielor, operațiilor și amenințărilor specifice secolului 21

Hybrid – defining the concept of the 21st century warfare, operations and threats

Cpt.drd. Georgiana-Daniela LUPULESCU*

*Ministerul Apărării Naționale
e-mail: geo.lupulescu@yahoo.co.uk

Abstract

Amenințările hibride, precum și războiul hibrid au devenit o constantă a secolului în care trăim, primind de-a lungul timpului numeroase definiții, care clarifică într-o măsură mai mică sau mai mare aceste concepte, caracterizate, în principal, de ambiguitate atât în ceea ce privește mijloacele, cât și forțele implicate sau zona geografică de ducere a luptei. Ideea de a încerca să definești un concept apărut din necesitatea de a îngloba tot ceea ce este cunoscut în materie de tehnici, mijloace, metode și instrumente, dar și ceea ce va apărea în viitorul nu foarte îndepărtat, grație fulminantei evoluții tehnologice, folosite de actori statali și nonstatali în încercarea de a-și atinge scopuri dintre cele mai diverse, militare, politice, sociale sau chiar economice, poate fi cel puțin derizorie. Lucrarea de față își propune să realizeze o scurtă prezentare a literaturii relevante în legătură cu amenințările, operațiile și războaiele hibride, pornind de la prima încercare de a le defini și până la noi atribute, adăugate între timp. Vom analiza caracteristici, tipuri, actori implicați și obiective urmărite de aceștia, rezultate din combinarea mai multor tehnici, metode sau instrumente.

Hybrid threats, as well as hybrid war, have become our century's constant, receiving numerous definitions over time, which clarify to a greater or lesser extent these concepts characterized mainly by ambiguity both in terms of means, as well as the forces involved or the geographical area of combat. It can be deemed at least as derisive to try to define a concept that arose from the need to include everything that is known in terms of techniques, means, methods and tools, but also what will appear in the not-too-distant future, thanks to the rapid technological evolution, used by state actors and non-states in an attempt to achieve their most diverse goals, be they military, political, social or even economic. This paper aims to provide a brief overview of the relevant literature on hybrid threats, operations and warfare, starting from the first attempt to define them and up to new attributes added in the meantime. We will analyze the characteristics, types, actors involved, and objectives pursued by them, resulting from the combination of several techniques, methods or tools.

Cuvinte-cheie:
amenințări hibride; război hibrid; operații psihologice; cyber; terorism; dezinformare; propagandă.

Keywords:
hybrid threats; hybrid warfare; psychological operations; cyber; terrorism; disinformation.

Amenințările hibride au devenit o constantă a secolului 21, fiind nelipsite din majoritatea conflictelor din ultimii ani și manifestându-se, totodată, și în perioadele de aparentă pace. Necesitatea studierii și adaptării atât a legislației, cât și a practicii în ceea ce privește apariția acestor noi tipuri de amenințări a fost, pentru prima dată, enunțată în Strategia Națională de Apărare a SUA, în anul 2005 (Department of Defense 2005). Noile provocări cu care Statele Unite se confruntau la vremea respectivă, care au devenit și mai evidente după atacurile teroriste din 11 septembrie 2001, au accentuat această nevoie de regândire și reorganizare a apărării. Ca urmare, analiștii militari și-au concentrat eforturile asupra teoretizării, dar și descoperirii unor tipare în vederea definirii, înțelegerii și contracarării amenințărilor hibride.

Articolul de față își propune, în primul rând, clarificarea conceptelor de: amenințare hibridă, operație hibridă, conflict hibrid, campanie hibridă și război hibrid, precum și analizarea caracteristicilor, tipurilor, actorilor implicați și obiectivelor urmărite de către aceștia, rezultate din combinarea mai multor tehnici, metode sau instrumente, reieșite din studiul aprofundat al literaturii în domeniu, cu scopul de a spori conștientizarea și înțelegerea conceptelor.

Conceptul de amenințare hibridă este în foarte strânsă legătură cu războiul hibrid, întrucât acestea se constituie în instrumente folosite înainte, în timpul și după finalizarea conflictului. În același timp, unii autori consideră că scopul unei amenințări hibride este de a exploata vulnerabilitățile, fără a declara război (Solik, Graf și Baar 2022).

În același timp, conceptele de operație hibridă, conflict hibrid sau campanie hibridă diferă doar din perspectiva desfășurării în timp, dar și a conștientizării de către toți actorii implicați a situației în care se găsesc. În acest sens, operația hibridă poate presupune folosirea unui număr limitat de instrumente și pentru o perioadă mai scurtă de timp, în vreme ce, din punct de vedere conceptual, campania hibridă tinde să se desfășoare un timp mai îndelungat și cu implicarea unei serii de amenințări de tip hibrid, urmărind un scop bine definit. Pe de altă parte, ambele concepte, atât cel de conflict, cât și cel de război, descriu situația în care părțile nu reușesc rezolvarea diferendelor pe cale amiabilă, folosind instrumente diplomatice sau cu sprijinul comunității internaționale. Diferența dintre cele două concepte poate, de asemenea, consta în încadrarea juridică a acestora. Catalogarea unui conflict drept război acordă părților combatante anumite drepturi și îi obligă pe aceștia la respectarea unor reglementări internaționale.

Conceptul de război hibrid a fost, inițial, folosit pentru a descrie acțiunile unor actori nonstatali și capacitatea acestora de a recurge atât la mijloace militare tot mai sofisticate, cât și la instrumente nonmilitare (Reichborn-Kjennerud și Cullen 2016), fiind, ulterior, atribuit și actorilor statali, datorită utilizării de către aceștia a amenințărilor de tip hibrid. Strategia Națională de Apărare a SUA prevede existența a patru tipuri de capabilități și metode: tradiționale, asimetrice, catastrofice și

disruptive, precum și faptul că acestea se suprapun și că este de așteptat ca actorii să utilizeze concomitent două sau mai multe astfel de metode, așa cum a fost cazul în războaiele din Irak și Afganistan, unde insurgenții au reprezentat atât o forță tradițională, cât și o provocare asimetrică (Department of Defense 2005). Frank Hoffman susține, de asemenea, că, în viitor, este de așteptat să existe combinații aparte sau amenințări hibride care să vizeze vulnerabilitățile Statelor Unite și că actorii vor utiliza, probabil, toate modalitățile de luptă, poate chiar simultan (Hoffman 2007).

Războiul hibrid a început să fie privit cu o atenție deosebită abia după războiul israelian din Liban împotriva Hezbollah, din 2006, când Israelul s-a confruntat cu o forță formată din insurgenți bine pregătiți și echipați, capabili să ducă lupte convenționale, dar care au acționat folosind tehnici și instrumente neconvenționale (Schnaufer 2017, 17-31). Războiul dintre Israel și Hezbollah a fost abordat și de Hoffman care îl consideră „prototipul războiului hibrid modern" (Hoffman 2007). În acest prim război hibrid, regăsim așadar caracteristicile acestui tip de conflict, așa cum a fost el prognozat de Strategia Națională de Apărare a SUA (Department of Defense 2005) și definit pentru prima dată de Hoffman (Hoffman 2007). Caracterul nonliniar al acestui tip de război, precum și implicarea actorilor nonstatali care combină modul convențional de luptă cu capabilități din spectrul asimetric sunt elementele definitorii ale războiului dintre Israel și Hezbollah.

Odată cu anexarea Crimeei de către Federația Rusă în 2014, fenomenul „război hibrid" a început să ia amploare, astfel că nu a mai fost tratat doar ca o noțiune teoretică, ci a devenit un termen, folosit pentru a descrie starea de insecuritate și provocările la adresa securității statelor vestice, totodată continuând să fie un subiect de interes și în rândul teoreticienilor, care și-au concentrat efortul în special pe amenințările de natură hibridă, venite din partea Federației Ruse. Statele au început includerea conceptului în politicile de securitate proprii, recunoscând astfel importanța și realitatea existenței amenințărilor de tip hibrid și a războaielor hibride și creând cadrul legislativ pentru luarea de măsuri defensive împotriva acestora. Câteva exemple în acest sens ar fi: Strategia Militară Națională a Statelor Unite ale Americii (2015), Strategia Națională de Apărare a Țării pentru perioada 2015-2019 (2015), Strategia Națională de Apărare a Țării pentru perioada 2020-2024 (2020), Strategia Națională pentru Combaterea Interferențelor Hibride din Republica Cehă (2021), Strategia Națională de Securitate a Republicii Polone (2020). Mai mult decât atât, Strategia de Securitate Națională a Statelor Unite ale Americii din anul 2015 prevede că „în astfel de conflicte hibride, forțe militare își pot asuma o identitate nonstatală, așa cum a făcut Rusia în Crimeea, sau pot implica o organizație extremistă violentă care dispune de capacități rudimentare de arme combinate, așa după cum a demonstrat Statul Islamic în Irak și Siria. De asemenea, în conflictele hibride, putem întâlni actori statali și nonstatali care lucrează împreună pentru atingerea unor obiective comune, utilizând o gamă largă de arme, așa cum am văzut în estul Ucrainei" (Dempsey 2015), identificând și exemplificând astfel materializarea caracteristicilor conflictului hibrid.

Existența amenințărilor hibride și necesitatea contracarării lor într-un mod unitar și eficace reprezintă unul dintre obiectivele principale atât al statelor vestice, cât și al NATO sau al Uniunii Europene. Aceasta din urmă definește amenințările și campaniile hibride ca fiind „multidimensionale, combinând măsuri coercitive și subversive, utilizând atât instrumente și tactici convenționale, cât și unele neconvenționale (diplomatice, militare, economice și tehnologice) pentru a destabiliza adversarul. Acestea sunt concepute pentru a fi dificil de detectat sau atribuit și pot fi utilizate atât de actori statali, cât și de actori nestatali" (Comisia Europeană 2018). De asemenea, la nivelul NATO, în cadrul ultimului Concept Strategic, elaborat în anul 2022, se face referire la sprijinirea de către Alianță a membrilor și partenerilor acesteia, precum și la coordonarea acțiunilor de combatere a amenințărilor hibride cu alți actori relevanți, cum ar fi Uniunea Europeană (NATO 2022).

Amenințare, operație, conflict sau război hibrid?

Utilizarea alternativă a termenilor *amenințare*, *operație*, *conflict* sau *război*, la care se adaugă calitatea de *hibrid* poate crea confuzie atât în rândul teoreticienilor, cât și al factorilor de decizie. Considerăm că una dintre cauzele acestui fapt se datorează ambiguității caracteristice operațiilor hibride, astfel:

- nu există un spațiu clar delimitat de derulare a luptelor, o zonă de război; în special din cauza instrumentelor informaționale utilizate, conflictul depășește de cele mai multe ori granițele statale;
- actorii implicați, fie că sunt statali sau nonstatali, nu sunt întotdeauna cunoscuți, cum este situația în care un actor statal sponsorizează un actor nonstatal care acționează în favoarea primului;
- existența unei linii foarte fine între război și pace, acea zonă gri, despre care vorbește pe larg Jan Almäng (2019);
- țintirea vulnerabilităților unui stat, folosind instrumente și metode de tip hibrid este o stare constantă a geopoliticii internaționale, astfel de acțiuni nefiind catalogate ca acte de război. Un exemplu în acest sens ar fi folosirea de către Federația Rusă a propagandei și dezinformării (Veebel 2016, 14-19);
- amenințarea presupune o situație ipotetică, potențială, aceasta fiind și ceea ce o deosebește, în principal, de orice formă de eveniment în desfășurare.

În consecință, pentru claritatea termenilor, deși uneori sunt catalogate drept conflicte hibride, iar alteori, ca războaie hibride, vom folosi termenul de *război hibrid*, pentru a numi o confruntare declarată între doi sau mai mulți actori statali sau nonstatali care întrebuințează atât mijloace convenționale, cât și neconvenționale în vederea atingerii obiectivelor strategice. Jan Almäng susține că „în cazul în care un conflict se califică drept război, participanții la conflict dobândesc drepturi și îndatoriri pe care nu le aveau până atunci" (Almäng 2019), ceea ce nu servește mereu intereselor și obiectivelor forțelor combatante, motiv pentru care scopul utilizării amenințărilor și instrumentelor de tip hibrid devine chiar acela de a genera o situație în care este

neclar dacă există sau nu stare de război, și dacă există, cine este combatant și cine nu (Thornton 2015, 40-48). Evitarea folosirii termenului de *război* a dus la utilizarea mai frecvent a altor termeni, cum ar fi: conflict, operație, acțiune, campanie etc. hibride, toate având mai mult sau mai puțin aceleași caracteristici. Diferența poate consta în amploarea acțiunii, dacă forțele combatante se cunosc sau dacă au loc doar atacuri de orice natură din partea unui actor necunoscut etc.

Amenințarea la adresa securității unui stat poate fi văzută ca o combinație între capacitate, intenție și oportunitate. Caracterul hibrid, în situația asta, rezultă din tipul de instrumente folosite. Dacă, de exemplu, un actor deține capacitatea tehnică și intelectuală de a conduce un atac cibernetic, dacă are intenția de a o face, cel mai probabil din necesitatea atingerii anumitor obiective strategice și dacă apare și oportunitatea executării atacului, generată cel mai adesea de identificarea unei vulnerabilități, atunci posibilitatea ca actorul respectiv să execute un atac cibernetic devine o amenințare pentru cei ce prezintă vulnerabilități în acest domeniu și se află în zona de interes a acelui actor. Pentru a exemplifica, amintim atacurile cibernetice, conduse de Federația Rusă asupra Georgiei, din 2008, care au început cu câteva luni înaintea declanșării conflictului, considerat, ulterior, „primul război care a avut loc în aer, pe mare, terestru și în spațiul cibernetic" (Mihai 2022). În exemplul menționat, identificăm capacitatea Federației Ruse de a folosi hackeri pentru a executa atacuri cibernetice (acestea au fost atribuite Federației Ruse abia în anul 2020 (Roguski 2020), intenția, demonstrată prin coordonarea atacurilor cibernetice cu utilizarea forțelor convenționale și prin situația politică din Georgia de la momentul respectiv, care nu servea intereselor Federației Ruse („noul președinte ales, Mihail Saakașvili, s-a angajat în apropierea de structurile occidentale și a încercat să reintegreze provinciile Osetia de Sud și Abhazia." (Mihai 2022) și, nu în ultimul rând, oportunitatea generată de vulnerabilitatea sistemelor informatice georgiene.

Probabil, una dintre întrebările cel mai des întâlnite în rândul cercetătorilor, dar și al factorilor de decizie în ultima decadă a fost „ce este războiul hibrid?". Numeroase lucrări științifice au abordat această temă, în încercarea de a defini și de a statua o serie de caracteristici specifice acestui tip de conflict. Printre primii care s-au evidențiat și au avut o contribuție esențială, se află Frank Hoffman, el fiind chiar cel care a denumit astfel conflictele caracterizate de folosirea concomitentă de instrumente din mai multe domenii: militar, informatic, psihologic, economic, politic de către forțe bine pregătite și flexibile. În concepția lui, războiul hibrid presupune o serie de moduri diferite de ducere a luptei, care includ capabilități convenționale, dar și tehnici și instrumente specifice războiului asimetric, acte teroriste, violență fără discriminare, coerciție și chiar acțiuni criminale (Hoffman 2007). Totodată, Thornton susține că una dintre principalele caracteristici ale războiului hibrid este că „tipurile de conflicte se suprapun și se contopesc. Astfel, spațiul de luptă, așa cum este, poate fi modelat la un nivel prin operații convenționale și activități neregulate și concomitent, la un nivel superior, prin aplicarea presiunilor politice și economice de fond" (Thornton 2015, 40-48). Putem astfel deduce că războiul hibrid presupune utilizarea combinată a mijloacelor

convenționale, forțe și instrumente militare, cu mijloace asimetrice. Pe de altă parte, din definiția războiului hibrid, dată de Giannopoulos, Smith și Theocharidou (2021, 11), și anume „combinarea și sincronizarea în mod deliberat a acțiunilor, de către un actor ostil, vizând în mod specific vulnerabilitățile sistemice din societățile democratice", putem extrage una dintre caracteristicile specifice războiului hibrid, țintirea vulnerabilităților. Așadar, nu mai vorbim doar despre atacuri îndreptate asupra forțelor militare adverse, ci și despre identificarea și exploatarea vulnerabilităților adversarului, inclusiv ale populației civile, necombatante. De asemenea, tipurile de acțiuni folosite, amenințările, lansate la adresa forțelor inamice sau populației civile, sunt foarte variate, de la atacuri cu rachete balistice, la operații psihologice sau atacuri cibernetice, de regulă utilizate concomitent asupra unor ținte diverse, pentru atingerea obiectivelor strategice. Totodată, războiul hibrid are un puternic caracter ambiguu în ceea ce privește atât înțelegerea și utilizarea conceptului în sine (Janičatova și Mlejnková 2021), de unde numeroasele definiții, mai mult sau mai puțin suprapuse, cât și crearea unor politici și lansarea de acțiuni concrete pentru prevenirea sau combaterea riscurilor ori amenințărilor de tip hibrid.

Un alt mare semn de întrebare în legătură cu războiul și amenințările hibride este dacă acestea au apărut de curând sau sunt doar un alt mod de a numi ceea ce deja era cunoscut. Există voci care spun că războaiele hibride sunt la fel de vechi ca războiul însuși (Galeotti 2016, 282-301), dar și că, deși nu sunt noi, sunt diferite (Hoffman 2009b). În același timp, Giannopoulos, Smith și Theocharidou consideră că evoluția războiului către această formă hibridă este dată, în principal, de dinamica mediului de securitate, de noi instrumente, concepte și tehnologii, folosite concomitent pentru exploatarea vulnerabilităților. Războiul hibrid reprezintă așadar un concept relativ nou, dar care înglobează noutatea generată de tehnologie și de folosirea acesteia în scopuri ostile. În același timp, deși conceptul a fost introdus și dezvoltat în urmă cu peste cincisprezece ani, odată cu emiterea Strategiei Naționale de Apărare a SUA, în anul 2005, când a fost pentru prima dată identificată necesitatea adaptării legislației, politicilor și măsurilor defensive împotriva acestor tipuri de amenințări, abia după invadarea Crimeei în 2014, conceptul de „război hibrid" a căpătat o importanță deosebită în rândul teoreticienilor, dar și al factorilor de decizie. Astfel, atât NATO, cât și Uniunea Europeană au început includerea termenului „hibrid" în politicile și strategiile proprii (Mikac 2022).

O altă caracteristică pe care o considerăm definitorie în ceea ce privește catalogarea conflictului drept hibrid este reprezentată de estomparea granițelor statelor și de neclaritate în stabilirea perioadei de desfășurare a conflictului. Ceea ce intenționăm să scoatem în evidență este faptul că instrumentele folosite în cadrul unui conflict hibrid, fie că vorbim despre atacuri cibernetice, propagandă, dezinformare, fie despre atacuri teroriste, nu se manifestă obligatoriu în perioadele de conflict, în cadrul unui război declarat, ci se pot constitui în amenințări de tip hibrid la adresa securității statelor, ceea ce duce și mai departe discuția, dacă într-adevăr este vorba despre război hibrid sau doar despre o competiție naturală între state (Wither 2016, 73-87).

https://doi.org/10.53477/2065-8281-23-19

Tipuri de amenințări hibride

Giannopoulos, Smith și Theocharidou (2021) au realizat un model conceptual al amenințărilor hibride, în funcție de actori, instrumente, domenii afectate, activitate și țintă, unde aceasta din urmă a fost stabilită ca fiind subminarea capabilității de luare a deciziilor. Instrumentele folosite nu sunt neapărat acțiuni ilegale sau hibride. De exemplu, din lista extinsă de amenințări hibride, oferită de Giannopoulos, Smith și Theocharidou, exercițiile militare sau susținerea unor actori politici nu sunt nici activități ilegale, nici nu se constituie în amenințări hibride, de sine stătătoare. În schimb, anumite combinații de astfel de instrumente, folosite concomitent și care vizează destabilizarea societății din punct de vedere politic, economic, social sau militar, fac parte din categoria amenințărilor de tip hibrid.

Ca și în celelalte cazuri legate de războaiele și amenințările hibride, în cazul identificării tipurilor de amenințări hibride, situația este departe de a fi clară. Caracterul hibrid este dat de un cumul de factori; dacă o singură persoană distribuie pe o rețea de socializare o știre falsă, nu se poate vorbi de existența unei amenințări hibride. Întotdeauna se iau în calcul actorii implicați, combinația de mijloace kinetice și nonkinetice, scopul amenințării, interesele și obiectivele strategice și bineînțeles prezența ambiguității în toate aspectele menționate, pentru a putea spune că un război sau o operație hibridă are loc.

Evoluția fulminantă a tehnologiei a dus la apariția unor tipuri de amenințări inovative care au depășit de mult sfera strict militară. Deși o parte dintre ele există de foarte mult timp, cum ar fi operațiile psihologice, din care amintim, în speță, propaganda și dezinformarea, modul în care acestea se folosesc, amploarea lor și subtilitatea caracteristică ridică mari probleme în identificarea, prevenirea și combaterea acestor amenințări de tip hibrid. E. Treyger, J. Cheravitch și R. Cohen, de exemplu, punctează faptul că războiul informațional dus de Federația Rusă amenință să erodeze credința în adevăruri faptice și să provoace daune concrete prin dezinformare.

În același timp, atacurile cibernetice ocupă un loc de cinste în tipurile de instrumente folosite în cadrul unui război hibrid, uneori fiind chiar instrumentul principal de „luptă". De exemplu, este cunoscut faptul că Rusia folosește astfel de tactici prin grupările de hackeri, finanțate de stat, iar exemplele sunt multiple, de la atacurile cibernetice împotriva Estoniei, din 2007, la cele împotriva Georgiei, din 2008 sau cele împotriva Ucrainei, atât din 2014, odată cu anexarea Crimeei (Mihai 2022), cât și cele asociate actualului conflict (Smith 2022).

Actori statali și nonstatali care folosesc amenințări de tip hibrid

Atunci când vorbim despre război hibrid sau amenințări hibride, o parte importantă a discuției este necesar a se focusa pe tipurile de actori implicați, conexiunile dintre

aceştia şi caracteristicile specifice fiecăruia. În primul rând, actorii se împart în două mari categorii: actori statali și actori non-statali.

Fie că vorbim despre actori statali, fie că vorbim despre cei nonstatali, discuţia nu poate fi în termeni de alb și negru, întrucât, la fel ca în cazul tipurilor de acțiuni folosite, graniţe, obiective, linia de demarcaţie dintre cele două categorii este estompată, neclară. Dacă luăm ca exemplu războiul israelian din Liban, amintit și mai devreme în articol, fuziunea dintre un actor nonstatal – Hezbollah – și un actor statal – Liban – este cel puțin evidentă. După cum sugerează Hoffman, „Hezbollah (...) a demonstrat o serie de capabilități militare, asemenea celor întrebuințate de către state, inclusiv mii de rachete și proiectile cu rază scurtă și medie. Acest caz demonstrează abilitatea actorilor nonstatali de a studia și de a neutraliza vulnerabilitățile armatelor de tip occidental" (Hoffman 2007, 35-36). Totodată, Hezbollah a beneficiat de arme și de instruire din partea Libanului, fapt ce demonstrează fără echivoc fuziunea actor nonstatal – actor statal.

Pe de altă parte, Janne Jokinen și Magnus Normark consideră că utilizarea de către state a unor actori nonstatali a avut loc dintotdeauna, dar puterea actorilor nonstatali a crescut odată cu dezvoltarea tehnologiei și serviciilor financiare, domenii în care anumiți actori nonstatali au devenit în timp experți. În consecință, probabilitatea ca aceștia să fie utilizați de către state a crescut considerabil. În același timp, actorii nonstatali se pot regăsi și în postura de adversari ai statelor (Jokinen și Normark 2022).

Un alt aspect de luat în considerare este faptul că, indiferent de forma sub care se prezintă un actor nonstatal, fie că vorbim de indivizi, organizații mai mult sau mai puțin legal constituite, grupuri armate etc., încă nu există legi internaționale care să statueze regimul, rolul sau responsabilitățile actorilor nonstatali într-un mod fără echivoc (Kleckowska 2020). Astfel că atât statele, cât și actorii nonstatali profită de această situație, primii, prin folosirea actorilor nonstatali pentru atingerea obiectivelor, uneori, în circumstanțe dubioase, iar secunzii, prin faptul că dețin, pe de-o parte, libertatea de a colabora sau nu cu statele, iar pe de altă parte, prin faptul că își pot exercita influența asupra politicilor statelor.

Vladimir Rauta sugerează o clasificare a actorilor nonstatali care se constituie în grupuri de luptă, luând în considerare relația dintre aceștia și state, în forțe proxy, auxiliare, surogate și afiliate, astfel:

- forțele proxy sunt grupări armate, nu fac parte din forțele regulate, dar luptă pentru acestea sau în numele lor;
- forțele auxiliare nu sunt parte din forțele regulate, dar colaborează cu acestea, fiind încorporate în structura de forțe;
- forțele surogate sunt folosite de forțele regulate pentru a își completa efectivele sau chiar pentru a le înlocui complet;
-forțele afiliate sunt cele care luptă pentru forțele regulate, rămânând, oficial, în afara conflictului (Rauta 2019).

https://doi.org/10.53477/2065-8281-23-19

O astfel de clasificare rezultă din modul în care statele folosesc actorii nonstatali, de implicarea acestora din urmă și din modalitatea în care aceasta are loc. Cu siguranță, lucrurile, în realitate, nu sunt atât de clare, întrucât războiul hibrid și actorii care folosesc amenințări hibride sunt caracterizați prin ambiguitate, iar implicarea actorilor nonstatali nu este întotdeauna la vedere, ceea ce face să fie dificile, dacă nu chiar imposibile, identificarea și catalogarea tuturor actorilor implicați.

Fie actorii nonstatali pot veni în sprijinul statului din diverse motive, au obiective comune, împărtășesc aceeași ideologie etc., fie statele sunt cele care sprijină, în calitate de sponsori, anumite grupuri sau organizații din aceleași motive, situație în care combatantul oficial este actorul nonstatal, iar statul nu se implică oficial în conflict. Actorii nonstatali pot lua forma oricărei combinații de rețele insurgente sau teroriste, grupări de crimă organizată, grupuri sociale, de tipul clanurilor, triburilor, sau grupurilor etnice, sau organizații motivate ideologic ori religios, toate putând fi sau nu sprijinite la vedere ori pe ascuns de către state sau afaceri legitime (Giannopoulos, Smith și Theocharidou 2021). Numărul mare de tipuri de actori nonstatali, capabilitățile acestora, care, uneori, le ajung sau chiar le depășesc pe cele statale, nu ușurează deloc munca celor care luptă împotriva amenințărilor hibride.

În ceea ce privește actorii implicați în operațiile hibride, cea mai mare provocare în încercarea de a preveni sau contracara o amenințare de tip hibrid este reprezentată, în primul rând, de identificarea acestora (Jokinen și Normark 2022), existând situații în care nu se poate stabili cu exactitate implicarea unui anume actor. Statele pot beneficia de pe urma acestei situații, în sensul că pot oricând nega și respinge orice acuzație de implicare în activități hibride, iar, conform lui Giannopoulos, „statele care dirijează activități prin intermediul entităților nestatale exploatează oportunitatea de a desfășura activități de natură prejudiciabilă împotriva altor țări în mod ascuns. Acest lucru are avantajul de a îngreuna statele vizate să detecteze respectiva activitate și să răspundă, înainte ca aceasta să se producă, dar și de a împiedica capacitatea statului vizat de a atribui operația prejudiciabilă statului străin din spatele evenimentului sau seriei de evenimente" (Giannopoulos, Smith și Theocharidou 2021).

Scopuri, obiective și ținte

Ca orice conflict care a avut, are sau va avea loc, și războaiele hibride au la bază un scop, o motivație și o serie de obiective. De cele mai multe ori, ele se încadrează în sfera politică prin influențarea politicilor unor state, scăderea încrederii populației în instituțiile statului, într-un cuvânt, prin slăbirea guvernării unui stat sau chiar colapsul acestuia. Totodată, orice vulnerabilitate a statului poate fi exploatată în cadrul unei operații hibride, acesta fiind și modul de acțiune al amenințărilor hibride, identificarea și exploatarea vulnerabilităților unui stat sau ale modului de ducere a luptei (Hoffman 2007).

Înainte de declanșarea unei operații hibride, după stabilirea obiectivelor urmărite, următorul pas este selectarea țintelor. Această acțiune este strâns legată de identificarea vulnerabilităților de exploatat. Conform lui Cederberg și Eronen, acestea cuprind toate capabilitățile militare, securitatea internă, zona politică internă, dar și externă, economia, infrastructura, nivelul de trai și de reziliență al populației la operații psihologice (Cederberg și Eronen 2015). Operația hibridă are loc la intersecția vulnerabilității identificate, a capabilității agresorului de a exploata această vulnerabilitate și a obiectivelor urmărite de acesta din urmă. Cederberg și Eronen susțin că „operațiile hibride se bazează pe utilizarea asimetriilor identificate pentru a face operațiile de succes prin confruntarea propriilor puncte forte cu punctele slabe cunoscute ale obiectivelor" (Cederberg și Eronen 2015). În articolul său, Cîrdei, de asemenea, susține că modul de acțiune în operațiile hibride are la bază exploatarea vulnerabilităților, dar și evitarea confruntării directe (Cîrdei 2016, 113-119). În același timp, istoria recentă ne demonstrează faptul că anumite obiective în continuare nu pot fi atinse, fără o componentă militară activă, așa după cum este cazul în prezentul conflict ruso-ucrainean, care include de la agresiune armată, la atacuri cibernetice (Viasat 2022) sau operații psihologice (EU vs DiSiNFO 2022).

Un motiv particular pentru care statele s-ar implica în acțiuni hibride, în special prin intermediul unor actori nonstatali care dețin anumite abilități, ar putea fi obținerea accesului la anumite infrastructuri sau sisteme. O astfel de situație este prezentată de Giannopoulos, Smith și Theocharidou. Este vorba despre Airiston Helmi, o companie imobiliară din Finlanda, care ar fi putut fi folosită ca acoperire pentru a face investiții strategice importante și pentru a pregăti proprietățile pentru utilizare ulterioară. În situația aceasta, cetățeni ruși ar fi cumpărat proprietăți foarte bine securizate, cu echipamente tehnice excepționale pentru a găzdui un număr mare de persoane, fiind amplasate într-o importantă zonă strategică a Finlandei. Autorul consideră acesta un foarte bun exemplu pentru „modul în care statele străine pot acționa prin intermediul terților pentru a influența, a interveni sau a obstrucționa afacerile statelor, pentru a genera consecințe negative sau pentru a stabili capacitatea de a face acest lucru atunci când se dorește" (Giannopoulos, Smith și Theocharidou 2021).

Concluzii

Atributul hibrid, adăugat amenințărilor la adresa securității statelor și războaielor, desfășurate în ultimii ani, a creat polemici și diferențe de concepție atât la nivelul lumii academice, cât și în rândul puterii politice. Războaiele hibride și complexitatea lor au fost și vor fi studiate, probabil, mult timp de acum încolo, în special datorită faptului că dimensiunea informațională, care stă de multe ori la baza manifestării multor altor tipuri de amenințări, se află într-o continuă dezvoltare.

Deși, la nivelul teoreticienilor, nu există un consens în ceea ce privește utilizarea termenilor de amenințare, conflict, operație sau război hibrid, putem afirma că instrumentele folosite și modalitățile de combinare a acestora, implicarea actorilor atât nonstatali, cât și statali, scopurile urmărite și, poate cel mai important, ambiguitatea în ceea ce privește toate aspectele mai sus menționate sunt elemente definitorii și sunt cele care imprimă caracterul hibrid oricărei amenințări, operații, oricărui conflict sau război.

Apariția și evoluția conceptelor de amenințări și războaie hibride nu sunt elemente de noutate. Hibriditatea conflictelor și amenințărilor nu creează un concept cu totul nou, ci unul într-o continuă dinamică, adaptat capabilităților tehnologice ale vremurilor noastre. Deși termenul „hibrid" a intrat în vocabularul academicienilor și al factorilor de decizie politico-militară acum aproape 20 de ani, dar mai pregnant după 2014, această modalitate de ducere a luptei poate fi observată și în cadrul unor conflicte mult mai vechi, în special atunci când ne referim la utilizarea unor instrumente nonmilitare, cum ar fi propaganda sau dezinformarea. Mai mult decât atât, caracterul hibrid, atribuit amenințărilor și conflictelor contemporane, a început să fie tot mai des asociat cu dimensiunea cibernetică a acestora. Aceasta din urmă este un instrument în sine, dar și un mijloc de punere în aplicare a altor tipuri de amenințări, ceea ce generează ambiguitate, dar și estomparea granițelor statale, acțiunile desfășurându-se, deseori, în spațiul cibernetic.

Securitatea și apărarea împotriva războaielor și amenințărilor hibride au fost și vor fi o provocare în continuare, în special datorită ambiguității caracteristice, atât în ceea ce privește instrumentele folosite, combinarea și sincronizarea lor, cât și în ceea ce privește identificarea actorilor implicați.
Evoluția și caracterul dinamic al conceptelor de război hibrid și amenințare hibridă reprezintă o provocare pentru securitatea statelor vestice. Caracteristicile definitorii ale acestora nu mai permit nici o apărare individuală și nici tratarea separat a fiecărei amenințări în parte, ci va fi necesară o abordare comună a statelor, o planificare riguroasă a apărării, incluzând toate domeniile cheie ale societății. În plus, identificarea și diminuarea vulnerabilităților societății, înaintea exploatării de către entitățile ostile, ar trebui să fie unul dintre principalele obiective ale statelor.

Referințe

Administrația Prezidențială. 2015. "Strategia Națională de Apărare a Țării pentru perioada 2015-2019." https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf.

—. 2020. „Strategia Națională de Apărare a Țării pentru perioada 2020-2024."

Almäng, Jan. 2019. "War, vagueness and hybrid war." *Defence Studies* 19 (2): 189-204.

Cederberg, Aapo și Pasi Eronen. 2015. ”How can Societies be Defended against Hybrid Threats.” *Geneva Centre for Security Policy* (9).

Cîrdei, Ionuț Alin. 2016. ”Countering the hybrid threats.” *Revista Academiei Forțelor Terestre* (2): 113-119.

Comisia Europeană. 2018. „Comunicare comună către Parlamentul European, Consiliul European și Consiliu.” https://data.consilium.europa.eu/doc/document/ST-10242-2018-INIT/ro/pdf.

Dempsey, Martin. 2015. ”The National Military Strategy of the United States of America.” https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

Department of Defense. 2005. ”National Defense Strategy of the United States.” https://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=tFA4Qqo94ZB0x_S6uL0QEg%3d%3d.

EU vs DiSiNFO. 2022. ”Key Narratives in Pro-Kremlin Disinformation: «Nazis».” https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation-nazis/#.

Galeotti, Mark. 2016. ”Hybrid, ambiguous, and non-linear? How new is Russia’s new way of war?” *Small Wars & Insurgencies* 27 (2): 282-301.

Giannopoulos, Georgios, Hanna Smith și Marianthi Theocharidou. 2021. *The lanscape of hybrid threats: A conceptual model.* Luxembourg: Publications Office of the European Union.

Hoffman, Frank. 2007. *Conflict in the 21st century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

—. 2009a. ”Further Thoughts on Hybrid Threats.” *Small Wars Journal.*

—. 2009b. ”Hybrid Warfare and Challenges.” *JFQ* (52): 34-48.

Janičatova, Silvie și Petra Mlejnková. 2021. ”The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom’s political–military discourse on Russia’s hostile activities.” *Contemporary Security Policy.*

Jokinen, Janne și Magnus Normark. 2022. ”Hybrid threats from non-state actors: A taxonomy.” *Hybrid CoE Research Report.*

Kleckowska, Agata. 2020. ”States vs. non-state actors – a public international law perspective.” *Hybrid CoE Strategic Analysis.*

Mihai, Paul. 2022. „Provocări hibride de natură cibernetică.” *Infosfera* (2).

Mikac, Robert. 2022. ”Determination and Development of Definitions and Concepts of Hybrid Threats and Hybrid Wars: Comparison of Solutions at the Level of the European Union, NATO and Croatia.” *Politics in Central Europe* 18 (3): 355-374.

Ministry of Defense Czech Republic. 2021. ”The National Strategy for Countering Hybrid Interference of Czech Republic.” https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf.

NATO. 2022. ”NATO 2022 Strategic Concept.” https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

President of the Council of Ministers. 2020. "The National Security Strategy of the Republic of Poland." https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

Rauta, Vladimir. 2019. "Towards a typology of non-state actors in „Hybrid Warfare": Proxy, auxiliary, surrogate and affiliated forces." *Cambridge Review of International Affairs.*

Reichborn-Kjennerud, Erik și Patrick Cullen. 2016. "What is Hybrid Warfare?" *Policy Brief* (Norwegian Institute of International Affairs) (1).

Roguski, Przemyslaw. 2020. "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace." https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Schnaufer, Tad A. 2017. "Redefining Hybrid Warfare: Russia's Non-linear War against the West." *Journal of Strategic Security* 10 (1): 17-31.

Smith, Brad. 2022. "Defending Ukraine: Early Lessons from the Cyber War." https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Solik, Martin, Jan Graf și Vladimir Baar. 2022. "Hybrid Threats in the Western Balkans: A Case Study of Bosnia and Herzegovina." *Romanian Journal of European Affairs* 22 (1).

Tenenbaum, Elie. 2015. "Hybrid Warfare in the Strategic Spectrum an Historical Assessment." In *NATO's response to hybrid threats*, by Guillaume Lasconjarias and Jeffrey A. Larsen, 95-112. Rome: NDC Forum Paper.

Thornton, Rod. 2015. "The Changing Nature of Modern Warfare." *The RUSI Journal* 160 (4): 40-48.

Treyger, Elina, Joe Cheravitch și Raphael S. Cohen. 2022. *Russian disinformation efforts on social media.* Santa Monica: RAND Corporation.

Veebel, Viljar. 2016. "Estonia confronts propaganda: Russia manipulates media in pursuit of psychological warfare." *Per Concordiam* 7 (1): 14-19.

Viasat. 2022. "KA-SAT Network cyber attack overview." https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

Wither, James K. 2016. "Making Sense of Hybrid Warfare." *Connections: The Quarterly Journal* 15 (2): 73-87.