CONCEPTUALIZAREA, OPERAȚIONALIZAREA ȘI CONEXIUNEA DINTRE SINTAGMELE „AMENINȚARE HIBRIDĂ” ȘI „CULTURĂ DE SECURITATE”

Colonel prof.univ.dr. Adrian LESENCIUC
Academia Națională de Informații „Mihai Viteazul”, București
Drd. Corneliu Mugurel COZMANCIUC
Academia Națională de Informații „Mihai Viteazul”, București

Până în prezent, potențialul de a aborda amenințările hibride printr-o cultură de securitate puternică rămâne subdezvoltat, în timp ce răspunsurile la nivel național încă nu au claritatea și complementaritatea necesare.

Articolul prezintă legătura dintre o gamă largă de amenințări emergente care provoacă, deopotrivă, țări și instituții și potențialul de atenuare a acestor probleme prin cultura de securitate, construind și consolidând un sistem național rezilient. Sub pragul de declarare oficială a războiului, amenințările hibride au demonstrat inutilitatea răspunsurilor care implică doar instituții cu responsabilități în domeniul securității și apărării.

Susținem că măsurile, procedurile și bunele practici pentru îmbunătățirea culturii de securitate printr-o abordare guvernamentală integrată vor asigura un cadru util pentru soluționarea acestor provocări, vizând, totodată, un răspuns civil-militar comun. Setul de instrumente hibride trebuie să fie dezarmat prin măsuri active și pasive, capacitatea societăților și a instituțiilor de a-și reveni în urma șocurilor fiind susținută atât de reziliență, cât și de măsuri robuste care ar spori pregătirea civilă și militară.

Evaluând creșterea amenințărilor hibride și poziția lor în gândirea strategică rusă și comparând doctrinele occidentale care reflectă aceste provocări, obținem o imagine de ansamblu asupra diferențelor de concept și operaționalizare, care sunt neclare în prezent.

Având în vedere că vulnerabilitățile naționale au, acum, implicații globale, răspunsurile naționale pentru acestea trebuie completate în mod eficient prin alianțe și parteneriate, ținând cont, de asemenea, de acțiunile hibride cu ținte specifice. Analizând componentele războiului hibrid și informațional, subliniem faptul că este timpul să avem și să folosim un vocabular uniform pentru a construi o cultură comună de securitate, necesară pentru acest peisaj de securitate în continuă schimbare.

Cuvinte-cheie: amenințări hibride, război informațional, cultură de securitate, război hibrid, reziliență națională.

INTRODUCERE

Emergența confruntărilor în mediul online ne aduce în față o nouă formă a războiului. Un război în care nu se mai confruntă soldații, ci indivizii cu competențe tehnice în domeniul IT devin atacatori, iar populația civilă devine țintă – războiul asimetric. Acesta este definit ca *„strategii și tactici neconvenționale adoptate de către un participant la conflict atunci când capacitățile puterilor beligerante nu sunt pur și simplu inegale, ci sunt diferite în mod semnificativ, astfel încât acestea nu pot executa atacuri asemănătoare unul asupra celuilalt".* (Sexton, 2014).

Una dintre particularitățile războiului asimetric este utilizarea puterilor soft și hard în cadrul aceluiași confruntări. Dacă puterea hard reprezintă uzul de forță sau capacitatea de coerciție a unui stat, puterea soft înseamnă cooptarea celorlalți în eforturile unui stat.

Participanți devin atât statele, cât și actorii politici nonstatali (indivizi sau organizații care dețin o influență politică semnificativă, dar nu sunt aliați, în mod particular, ai unui stat).

Gândirea care stă la baza acestui tip de confruntări a evoluat din utilizarea tacticilor de gherilă în mediul online: neutralizarea avantajului tehnico-tactic al adversarului, a susținerii populației pentru forțele militare, aliații tradiționali sau chiar a guvernului statului-țintă.

Una dintre particularitățile războiului asimetric este utilizarea puterilor *soft* și *hard* în cadrul aceluiași confruntări. Dacă puterea *hard* reprezintă uzul de forță sau capacitatea de coerciție a unui stat, puterea *soft* înseamnă cooptarea celorlalți în eforturile unui stat (Nye, 2004, p. 5). Diferența dintre cele două forme ale puterii este descrisă astfel: *„puterea **hard** impune conformarea bazându-se, în principal, pe puterea tangibilă, în timp ce puterea **soft** cultivă conformarea printr-o varietate de politici, calități și acțiuni, în mod indirect și prin măsuri non-coercitive".* (Gallarotti, 2011, pp. 10-11).

Utilizarea integrată a acestor fațete ale conceptului de putere a fost denumită putere *smart.* Este văzută drept *„o abordare ce subliniază necesitatea unei prezențe militare puternice, dar care investește masiv în alianțe, parteneriate și instituții la toate nivelurile, cu scopul de a extinde influența cuiva și de a-i legitima acțiunile".* (Armitage, 2007, p. 7).

DOCTRINA GHERASIMOV

Articolul generalului rus Valeri Gherasimov, *„Valoarea științei este în perspectivă: noile provocări solicită regândirea formelor și metodelor de efectuare a operațiunilor de luptă”,* aduce în prim-planul preocupărilor occidentale *„amenințările hibride*” și este interpretat ca propunerea unui nou mod rusesc de abordare a confruntărilor care îmbină războiul convențional și neconvențional cu aspecte ale puterii naționale, adesea denumit *„război hibrid”.*

Guvernul SUA definește războiul neconvențional ca *„activități conduse cu scopul de a ajuta o mișcare de rezistență sau o insurgență să constrângă, să perturbe sau să răstoarne un guvern sau o forță ocupantă, operând prin sau cu ajutorul unor forțe subterane, auxiliare sau de gherilă într-o zonă interzisă”.* (Public Law 114-92, 2015, Sec. 1097, (d)).

Guvernul SUA definește războiul neconvențional ca „activități conduse cu scopul de a ajuta o mișcare de rezistență sau o insurgență să constrângă, să perturbe sau să răstoarne un guvern sau o forță ocupantă, operând prin sau cu ajutorul unor forțe subterane, auxiliare sau de gherilă într-o zonă interzisă”.

Alte concepte folosite de Gherasimov sunt *„războiul de nouă generație”*, caracterizat de erodarea liniilor de demarcație dintre starea de război și cea de pace, și *„război non-liniar”*: *„un mijloc de a atinge orientarea strategică dorită și rezultatele dorite folosind, în mod primar, abordări non-militare”*. (Morris, 2015).

Gherasimov a ajuns la aceste concluzii cercetând modul în care Occidentul conduce războiul, bazându-se mai puțin pe invaziile tradiționale, precum Irak, în 2003, și mai mult pe intervenția din 2011, în Libia, evenimentele *Primăverii arabe* și *„revoluțiile colorate”*. În opinia sa, Occidentul a fost pionierul în abordările indirecte ale războiului, folosind subversiunea politică, propaganda și rețelele de socializare, alături de măsuri economice precum sancțiunile. Intervențiile umanitare, utilizarea forțelor speciale occidentale, finanțarea pentru mișcările *„democratice”* și desfășurarea de mercenari au fost, toate, trăsăturile unei doctrine americane a războiului indirect, subliniind că există un raport de patru la unu între măsurile non-militare și cele militare în conflictul modern, însă aduceau în discuție modul în care Occidentul modelează câmpul de luptă înainte de intervenție.

Gherasimov nu a fost primul care a observat acest lucru. George F. Kennan a avansat un argument similar în memoriul său din 1948 privind organizarea războiului politic: *„Războiul politic reprezintă angajarea tuturor mijloacelor la comanda națiunii, pentru atingerea obiectivelor sale naționale. (...) Ele variază de la acțiuni atât de abrupte precum alianțe politice, măsuri economice și propagandă ‹albă› până la operațiuni ascunse, precum sprijinul unor elemente străine*

‹prietenoase›, război psihologic ‹negru› și chiar încurajarea rezistenței subterane în statele ostile". (Kennan, 1948, pp. 1-2).

Din perspectivă rusă, se pot identifica trei teorii majore care abordează înțelegerea războiului informațional: *„războiul insurecțional"*, propus de Evgheni Messner, *„războiul net-centric"*, în viziunea lui Aleksandr Dughin, și *„războiul informațional"*, dezvoltat de Igor Panarin.

Viziunea lui Messner asupra contextului politico-militar internațional a fost puternic influențată de conflictul dintre marii câștigători ai celui de-al Doilea Război Mondial, URSS și SUA. El observă că, după 1945, explicația lui Troțki despre Tratatul de la Brest-Litovsk, *„nici război, nici pace"*, se aplică la nivel global. De asemenea, interpreta *„războaiele proxy"*, din timpul Războiului Rece, ca parte a unei imagini mult mai generale. Din aceste considerente, Messner a prevăzut necesitatea unui nou tip de război, în condițiile în care cel *„clasic"* devenea imposibil de dus.

Din perspectivă rusă, se pot identifica trei teorii majore care abordează înțelegerea războiului informațional: „războiul insurecțional", propus de Evgheni Messner, „războiul net-centric", în viziunea lui Aleksandr Dughin, și „războiul informațional", dezvoltat de Igor Panarin.

Una dintre caracteristicile distinctive ale războiului insurecțional îl reprezintă creșterea importanței dimensiunii psihologice/informaționale. Scopul principal al războiului a devenit nu capturarea teritoriul fizic al inamicului, ci modul de influențare a emoțiilor populației unei țări-țintă. Confuzia și disconfortul populației din statele țintă au devenit obiective, iar principalele instrumente pentru a face acest lucru sunt propaganda și agitația.

Messner observă două caracteristici principale ale războiului informațional: *„propaganda prin cuvânt"* și *„propaganda prin faptă"*. Dacă prima cuprinde discursul oficial al autorităților și forme ale manifestărilor cultural-artistice, cea de-a doua cuprinde fapte de succes, realizate în timp util: *„o idee câștigă credibilitate atunci când este susținută de realizări militare, politice, sociale, diplomatice și economice".* Așadar, nu este doar ceea ce se spune, se scrie, se publică, se difuzează, ci și ceea ce se face: *„în vremuri de război psihologic, nici victoria în luptă, nici câștigurile teritoriale nu sunt obiective în sine: valoarea lor principală rezidă în efectele psihologice"*. Se distinge necesitatea unei congruențe între vorbă și faptă: pe de o parte, discursul trebuie secondat de o acțiune concretă, de cealaltă parte, acțiunile trebuie aduse la cunoștința publicului printr-un discurs pe măsură. (Freedman, 2017, p. 68 și urm.).

Propaganda *„nu ar trebui să fie defensivă, justificatoare; în schimb, ar trebui să stimuleze în mod activ emoțiile și gândurile soldaților noștri, combatanți și non-combatanți"* (Freedman, 2017, p. 68).

Astfel de acțiuni vor fi sortite eșecului dacă discursul lor nu se adaptează la context. Studierea atentă a contextului cultural și a specificului național sau regional al populațiilor țintă poate oferi răspunsul acestor probleme. Disimularea propagandei este o condiție esențială: *„atât cea defensivă, cât și propaganda ofensivă sunt sortite eșecului dacă arată ca propagandă”*. (Freedman, 2017, p. 68).

Dughin și Panarin se remarcă prin faptul că au fost, ei înșiși, participanți la războiul informațional, în calitate de lideri de opinie. Panarin oferă instrumentele de bază ale luptei informaționale, pe care le împarte în categoriile secrete și nesecrete. Acestea includ: propagandă, intelligence instituțional, monitorizare și analiză, componenta organizațională (canale de coordonare și direcție), agenți secreți cu influență în mass-media și alte canale combinate, inclusiv forțe speciale de operațiuni (operațiuni de sabotaj, efectuate sub steag străin).

Ceilalți doi teoreticieni ruși, Dughin și Panarin, academicieni și mentori, se remarcă prin faptul că au fost, ei înșiși, participanți la războiul informațional, în calitate de lideri de opinie. Panarin oferă instrumentele de bază ale luptei informaționale, pe care le împarte în categoriile secrete și nesecrete. Acestea includ: propagandă, *intelligence* instituțional, monitorizare și analiză, componenta organizațională (canale de coordonare și direcție), agenți secreți cu influență în mass-media și alte canale combinate, inclusiv forțe speciale de operațiuni (operațiuni de sabotaj, efectuate sub steag străin). Etapele procesului de gestionare a operațiunilor de informații ar fi următoarele: (1) prognoză și planificare, (2) organizare și stimulare, (3) feedback, (4) reglarea funcționării, (5) controlul performanței.

Aleksandr Dughin este teoreticianul conceptului de*„război centrat pe rețea”*, ceea ce înseamnă crearea unei noi infrastructuri militare informaționale, care implică elemente interactive și mijloace de comunicare rapidă. *„Rețeaua eurasiatică”* ar oferi un răspuns simetric la *„provocarea net-centrică din SUA”*. Misiunile vor fi executate de *un „grup special format din oficiali superiori, cel mai bun personal ‹orientat spre misiune› din serviciile secrete rusești, intelectualii, oamenii de știință, oamenii politici și corpul jurnaliștilor și activiștilor culturali orientați spre patriotism trebuie creat în acest scop”*. Modelul *„rețelei eurasiatice”* în opoziție cu *„rețeaua Atlanticului”* este de așteptat să combine elementele de bază ale postmodernismului american și abordarea net-centrică cu realitatea rusă.

Această abordare ar putea avea succes cu condiția ca forțele armate rusești, serviciile secrete, instituțiile politice, sistemele de informare și comunicare etc. să fie *„postmodernizate”.* Un război al internetului poate fi câștigat numai dacă țara folosește mijloace de rețea, iar acestea trebuie adaptate la realitatea și obiectivele proprii ale Federației Ruse și la tehnologii eficiente, conform ideilor lui Dughin.

Războiul informațional și războiul de rețea de sorginte rusă, observate recent, ar trebui privite ca un produs al tehnologiilor politice tradiționale care sunt utilizate de ani de zile și reprezintă moștenirea

URSS. Geopolitica informațională rusă contemporană se bazează în mod vădit pe înțelegerea sovietică asupra războiului psihologic și pe stereotipurile mentale reminiscente. Propaganda rămâne instrumentul cheie al războiului informațional. Trăsăturile sale distinctive sunt limbajul (limbajul emoțiilor și prejudecăților și nu al faptelor), conținutul (respectarea propagandei oficiale a Kremlinului) și funcția (discreditarea adversarului). Însă, nu putem ști dacă instrumentele specific rusești ale războiului informațional vor fi eficiente într-o eventuală cruciadă ideologică îndreptată împotriva Occidentului. Mesajele emise cu acest scop sunt puțin credibile și ușor de verificat în era noilor tehnologii. Mai mult, ideile ofertate nu sunt atrăgătoare. Cu toate acestea, dacă propaganda tinde să dea greș în Vest, știrea ideologică bazată pe dezinformare găsește un teren fertil în Est.

RĂZBOIUL INFORMAȚIONAL

Terminologia specifică a *„războiului informațional"* a apărut la începutul anilor '90, însă pot fi distinse cel puțin două sensuri distincte în înțelegerea acestuia: a) măsuri disruptive pentru sisteme bazate pe fluxuri de informații; b) influențarea percepțiilor prin afectarea conținutului informației. Primul sens este orientat spre aspecte tehnice, iar cel de-al doilea pe cunoștințe. (Freedman, 2019, p. 311).

Există câteva definiții ale războiului informațional propuse de Whitehead, unele dintre ele acceptate de către armata SUA, cea mai complexă fiind: Războiul informațional constă în *„acțiuni desfășurate în mediul informațional cu scopul de a interzice, exploata, altera, distruge sau asigura viabilitatea informației. Scopul este de a asigura avantajul informațional".* (Whitehead 1999, pp. 4-5).

Acest tip de război are următoarele caracteristici principale: costuri reduse, limite tradiționale greu de definit, rol crescut al managementului percepției, o provocare pentru managementul informațiilor strategice, dificultatea de a construi și de a susține coaliții (Molander et. al., 1996, pp. 15-16). Conform acestor caracteristici, devin tot mai grele delimitările propuse de conceptul tradițional de război: Cine este combatant și cine nu? Cine atacă și când? Sunt posibile armistițiile și încetarea, cel puțin temporară, a acțiunilor ostile? Mai mult decât atât, consecințele implicării în conflict ale actorilor politici nonstatali pot avea consecințe grave la adresa întregii societăți: o entitate privată afectată poate genera pierderea încrederii publicului, șomaj și, în cele din urmă, neliniște socială.

Există câteva definiții ale războiului informațional propuse de Whitehead, unele dintre ele acceptate de către armata SUA, cea mai complexă fiind: Războiul informațional constă în „acțiuni desfășurate în mediul informațional cu scopul de a interzice, exploata, altera, distruge sau asigura viabilitatea informației. Scopul este de a asigura avantajul informațional".

Războiul informațional poate lua forme mai mult sau mai puțin subtile. Accesul la internet transformă populația civilă în participanți la acest război, care nu numai că este supusă tirurilor propagandistice, ci, în unele instanțe, devine vector al propagării acestor informații. Dacă, inițial, informațiile false se puteau contracara prin adevăr și dovezi, această metodă funcționează mult mai puțin într-o lume socială populată de *trolli* și roboți (Fukuyama, 2017).

Fenomenele de tip *fake news* sunt instrumentalizate de instituții media achiziționate sau finanțate în mod netransparent. Ascensiunea tehnologiilor de inteligență artificială a dat posibilitatea folosirii *deepfakes*, înregistrări video în care fața unei persoane este înlocuită cu cea a unui lider politic sau social, mesajele emise de aceștia sunt alterate sau chiar *„construite”* din bucăți de discurs aranjate în așa fel încât să susțină poziții pe care liderul prezentat nu le-ar fi exprimat. Propaganda este încărcată emoțional și se bazează pe interesul agresorului, pentru a schimba sentimentul colectiv față de intențiile și scopurile agresorului (Nate, Rațiu, 2017, p. 2).

În războiul informațional, adversarii sunt ascunși și eforturile de a le distruge anonimitatea sunt, de multe ori, sortite eșecului. Un exemplu de atac informațional este reprezentat de Operațiunea „Grizzly Steppe”, în care comunitatea de informații a SUA a aflat că GRU a avut acces la resursele informatice ale Comitetului Național Democrat din iulie 2015 până în iulie 2016.

În războiul informațional, adversarii sunt ascunși și eforturile de a le distruge anonimitatea sunt, de multe ori, sortite eșecului. Un exemplu de atac informațional este reprezentat de Operațiunea *„Grizzly Steppe”*, în care comunitatea de informații a SUA a aflat că GRU (Direcția principală de informații a Rusiei) a avut acces la resursele informatice ale Comitetului Național Democrat din iulie 2015 până în iulie 2016. Serviciile de securitate și informații rusești au reușit să extragă cantități mari de date din calculatoarele Comitetului Național Democrat, transmise, apoi, de utilizatorul *„Guccifer 2.0”* către site-urile Wikileaks.com și DCLeaks.com. Faptele au fost urmate de o operațiune psihologică masivă, cu scopul discreditării lui Hillary Clinton, candidat la alegerile prezidențiale din SUA, și, mai ales, erodarea încrederii în instituțiile SUA (Rugge, 2018, pp. 4-5).

CULTURA DE SECURITATE – INSTRUMENT DE LUPTĂ ÎMPOTRIVA RĂZBOIULUI INFORMAȚIONAL

Cultura de securitate este un model de ipoteze de bază, valori, norme, reguli, simboluri și credințe care influențează percepția provocărilor, oportunităților și/sau amenințărilor și modul de a simți securitatea și de a se gândi la aceasta, comportamentul și activitățile actorilor sociali activi individuali sau colectivi, conectați într-o varietate de moduri (Piwowarski, 2017, pp. 17-19).

Apărut în septembrie 1977, conceptul de *„cultură de securitate"* a evoluat de la o înțelegere limitată în domeniul militar sau strategic către aplicarea sa la nivelul întregii societăți. Kai Roer oferă o definiție incluzivă a culturii de securitate: *„ideile, obiceiurile și comportamentele sociale ale unui individ sau ale unui grup care îi ajută pe aceștia să fie liberi de amenințări și pericole"* (Roer, 2015, p. 14). Conform acestuia, cultura de securitate se compune din trei elemente fundamentale: tehnologii, politici și competențe: tehnologiile sunt tangibile și intangibile (modele mentale, standarde și *know-how*) (Roer, 2015, p. 19).

Dintre cercetătorii români, Lungu (et. al.) oferă o definiție care mărește sfera de aplicabilitate a conceptului: *„Cultura de securitate este rezultatul interacțiunilor sociale care au loc în grupuri, organizații, comunități preocupate de aspectele securității sociale, ale unor procese de învățare și acumulare de cunoștințe, în acord cu nevoile umane de protecție, siguranță, adăpost. Cultura de securitate este adaptivă, se dezvoltă în raport cu evoluția societății și este transmisă între generații prin diferite forme de comunicare scrisă și orală, precum și prin practici de susținere a valorilor de securitate".* (Lungu, 2018).

Barometrul Culturii de Securitate, publicat în 2018, relevă faptul că românii sunt interesați, mai degrabă, de o latură conspirativă a informațiilor pe care și le iau din știri, fapt cauzat de lipsa unei gândiri critice în anumite pături ale societății. Acest lucru poate agrava fenomene de tip *fake news*, care pot ajunge la cât mai multe persoane (INSCOP, 2018, p. 44).

Conform aceluiași studiu, nu există diferențe semnificative între populațiile din mediul de rezidență urban și cel rural, nici între diferite categorii de vârstă, gen sau în funcție de regiunea istorică în care locuiesc, atunci când vine vorba de categoriile sociale sensibile la tendințe conspiraționiste.

Un studiu despre comportamentul digital al românilor, publicat în 2018, arată modul în care aceștia subestimează puterea știrilor false și a informațiilor inexacte. Peste 50% dintre respondenți au declarat că opiniile lor sunt într-un grad mic sau mediu influențat de informații inexacte, însă rata ridicată a celor care nu au răspuns acestei întrebări (18%) duce la concluzia că problema modului în care încrederea față de știri modelează opiniile și acțiunile nu este deloc luată în considerare de mulți români (Bârgăoanu, Radu, 2018).

„Cultura de securitate este rezultatul interacțiunilor sociale care au loc în grupuri, organizații, comunități preocupate de aspectele securității sociale, ale unor procese de învățare și acumulare de cunoștințe, în acord cu nevoile umane de protecție, siguranță, adăpost. Cultura de securitate este adaptivă, se dezvoltă în raport cu evoluția societății și este transmisă între generații prin diferite forme de comunicare scrisă și orală, precum și prin practici de susținere a valorilor de securitate".

Principalele și cele mai eficiente metode de contraatac sunt conștientizarea și educația. Responsabilitatea asupra ambelor îi revine atât cetățeanului, cât și instituțiilor statului. *„Cyber-igiena"* nu va proteja țara de atacuri avansate și persistente, de scenarii hibride sau de un război de ultimă generație, însă constituie o metodă ușoară și relativ ieftină de a aloca puține resurse financiare și tehnologice pentru a face față unor amenințări serioase. Cultivând spiritul critic, o societate va putea construi bariere eficiente împotriva *fake news*, educația reducând efectul de cameră cu ecou al *social media* (Rugge, 2018, pp. 6-7).

Fostul director al CIA, Michael V. Hayden, aprecia că implicarea Federației Ruse în alegerile prezidențiale din SUA reprezintă echivalentul politic al atacurilor teroriste de la 11 septembrie. Din acest motiv, statului îi revine sarcina de a întări guvernanța și mecanismele de răspuns la nivel instituțional, dar și să construiască alianțe împreună cu cei care sunt supuși acelorași amenințări la nivel cultural, politic și militar.

Adeziunea la principiile de bază ale democrației – transparență decizională, deschidere și stat de drept – creează un mediu politic în care ingerința entităților străine în procesele democratice poate fi ușor observată și contracarată. În schimb, un climat de ostilitate publică la adresa oponenților ideologici ai puterii politice va eroda legitimitatea instituțiilor democratice.

Fostul director al CIA, Michael V. Hayden, aprecia că implicarea Federației Ruse în alegerile prezidențiale din SUA reprezintă echivalentul politic al atacurilor teroriste de la 11 septembrie, eveniment care a expus o vulnerabilitate până atunci de neimaginat. Din acest motiv, statului îi revine sarcina de a întări guvernanța și mecanismele de răspuns la nivel instituțional, dar și să construiască alianțe împreună cu cei care sunt supuși acelorași amenințări la nivel cultural, politic și militar. Partenerii vor trebui să participe activ la stabilirea măsurilor de creștere a încrederii, precum și a normelor de comportament al statelor în spațiul cibernetic (Ibid., p. 8).

Eforturile instituționale vor fi zadarnice fără ca cetățenii să dețină un instrumentar adecvat pentru filtrarea informațiilor. Războiul informațional exploatează clivajele sociale, erodând încrederea cetățenilor în instituții, decidenți, organizații internaționale, dar și în măsurile luate de aceștia cu scopul de a le asigura securitatea. Manipularea informației de către actori statali și non-statali ostili poate fi contracarată printr-o cultură de securitate solidă.

Abordarea *whole-of-society* acceptă faptul că riscurile de securitate sunt o amenințare la adresa întregii societăți, iar orice membru al său are capacitatea de a deveni o vulnerabilitate, în lipsa unei culturi de securitate. Instituțiile statului pot dezvolta și promova cultura de securitate în rândul cetățenilor prin transparență și acțiuni de conștientizare. Cetățenii își pot forma deprinderi de *„igienă*

mentală" prin dezvoltarea gândirii critice și prin accesarea resurselor de informații puse la dispoziție de către stat. Implementarea culturii de securitate este un efort comun al cetățeanului și al statului. Numai existând această sinergie între cetățean și stat, valorile societății democratice vor fi apropriate mult mai ușor de către membrii săi, iar reziliența la atacurile informaționale va fi sporită.

La nivel programatic, în România, termenul de *„cultură de securitate"* apare în *„Ghidul Strategiei naționale de apărare a țării pentru perioada 2015-2019"*, adoptat de Consiliul Suprem de Apărare a Țării. Conform acestuia, cultura de securitate reprezintă *„totalitatea valorilor, normelor, atitudinilor sau acțiunilor care determină înțelegerea și asimilarea la nivelul societății a conceptului de securitate și a celor derivate (securitate națională, securitate internațională, securitate colectivă, insecuritate, politică de securitate etc.)"*. (Administrația Prezidențială, 2015, p. 7).

Statul român vede cultura de securitate drept o condiție a normalității sociale, iar pe cetățean în dublu rol: beneficiar și generator de securitate. Modalitățile pentru dezvoltarea culturii de securitate sunt stimularea interesului publicului față de cultura de securitate, plasarea în procesul de educație formală a cursurilor de educație pentru securitate, programe de formare accesibile de către publicul larg, identificarea experților la nivel public ca fiind promotori ai programelor de conștientizare etc. (Ibid., p. 14).

„Strategia Națională de Apărare a Țării 2020-2024" continuă viziunea precedentului document, adoptat în 2015, însă nuanțează unele aspecte și introduce concepte complementare culturii de securitate. Conform documentului, România trebuie să se transforme *„într-un stat rezilient, capabil să se raporteze adecvat la impredictibilitatea și amploarea evoluțiilor din mediul de securitate. Pentru aceasta, este nevoie de un stat puternic, un stat care conștientizează necesitatea dezvoltării unor mecanisme proprii de reacție rapidă și eficientă și, inerent, a unei culturi de securitate solid dimensionate – inclusiv* în rândul cetățenilor săi*"*. (Administrația Prezidențială, 2020, p. 6). Însă, acest deziderat de creare a unui stat rezilient *„se află în interdependență cu nivelul culturii de securitate a cetățenilor săi"*. (Ibid., p. 12).

Documentul citat pune un accent major pe interdependența dintre cultura de securitate și reziliență, dar și pe crearea unei *„culturi a prevenirii, prin pregătirea activă și continuă a populației pentru a reacționa la producerea unei situații de urgență majoră"*. (Ibid., p. 37).

„Strategia Națională de Apărare a Țării 2020-2024" nuanțează unele aspecte și introduce concepte complementare culturii de securitate. Conform documentului, România trebuie să se transforme „într-un stat rezilient, capabil să se raporteze adecvat la impredictibilitatea și amploarea evoluțiilor din mediul de securitate. Pentru aceasta, este nevoie de un stat puternic, un stat care conștientizează necesitatea dezvoltării unor mecanisme proprii de reacție rapidă și eficientă și, inerent, a unei culturi de securitate solid dimensionate – inclusiv în rândul cetățenilor săi".

Efortul realizării acestora va fi *„coordonat la nivel strategic, în baza unui plan unic de implementare”* (Ibid.), în plan orizontal, prin cooperarea instituțiilor reunite în grupuri de lucru.

CONCLUZII

Sub pragul de declarare oficială a războiului, amenințările hibride au demonstrat inutilitatea răspunsurilor care implică doar instituții cu responsabilități în domeniul securității și apărării. Starea continuă de *„asediu”* impune asumarea unei conștiințe alerte a întregii societăți, fiind esențială pregătirea, educația și cultura în domenii care nu se mai regăsesc în tranșeele convenționale, ci în cămine și instituții.

Ca urmare a efectelor amenințărilor hibride asupra coeziunii statale și securității societale, este importantă participarea cetățenilor la securitatea statului prin dezvoltarea unei culturi de securitate individuale solide. Acesta se bazează atât pe promovarea valorilor fundamentale ale societăților democratice, reprezentate de transparență, deschidere și consolidarea statului de drept, cât și pe alianțe între diferite categorii ori entități amenințate, putând fiind realizată prin metode practice, precum și prin dezvoltarea unor soluții de viralizare a informațiilor veridice, ceea ce ar duce la o creștere generală a nivelului de alfabetizare digitală.

Ca urmare a efectelor amenințărilor hibride asupra coeziunii statale și securității societale, este importantă participarea cetățenilor la securitatea statului prin dezvoltarea unei culturi de securitate individuale solide.

BIBLIOGRAFIE:

1. Armitage, R.L. (2007). *How America Can Become a Smarter Power. CSIS Commision on Smart Power. A Smarter, more secure America*. Washington, D.C.: Center for Strategic and International Studies.
2. Bârgăoanu, A., Radu, L. (2018, iunie). *„Fake News or Disinformation 2.0? Some Insights Into Romanians' Digital Behaviour”.* În *Romanian Journal of European Affairs*. Vol. 18, nr. 1.
3. Freedman, L. (2019, noiembrie). *Viitorul războiului*. București: Kronika.
4. Fukuyama, F. (2017, 12 ianuarie). *The Emergence of a Post-Fact World, Project Syndicate*, https://www.project-syndicate.org/onpoint/the-emergence-of-a-post-fact-world-by-francis-fukuyama-2017-01, accesat la 13 mai 2020.
5. Gallarotti, G.M. (2011). *„Soft Power: What it is, Why it's Important, and the Conditions Under Which it Can Be Effectively Used”. În Journal of Political Power*. Middletown.
6. Kennan, George F. (1948, 30 aprilie). *The Inauguration of Organized Political Warfare, Digital Archive, International History Declassified*. Washington D.C.: Wilson Center.

7. Lungu, C., Buluc R., Deac, I. (2018). *Promovarea culturii de securitate*. București: ProSCOP.
8. Molander, R.C., Riddile, A.S., Wilson, P.A. (1996). *Information Warfare. A New Face of War*. California, Santa Monica: RAND.
9. Morris, V.R. (2015). *Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrin*e. În Small Wars Journal, https://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine, accesat la 12 octombrie 2020.
10. Nate, S., Rațiu, A. (2017). *„Defending the Truth and Counter Information Warfare".* În *Europe. Knowledge-Based Organization*. Vol. XXIII, nr. 1.
11. Nye Jr., J.S. (2004). *Soft Power: The means to success in world politics*. New York: Public Affairs.
12. Piwowarski, J. (2017). *„Three Pillars of Security Culture, Security Dimensions".* În International & National Studies, nr. 22.
13. Roer, K. (2015). *Build a Security Culture*. Cambridgeshire: IT Governance Publishing.
14. Rugge, F. (2018, ianuarie). *„Mind Hacking: Information Warfare in the Cyber Age"*. În *Instituto Per GliStudi Di Politica Internazionale*.
15. Sexton, E. (2016). *Asymmetrical Warfare*, https://www.britannica.com/topic/asymmetrical-warfare, accesat la 12 octombrie 2020.
16. Whitehead, Y.G. (1999). *Information as a Weapon. Reality vs. Promises, Air University*. Alabama: Maxwell Air Force Base.
17. Administrația Prezidențială (2015). *Ghidul Strategiei naționale de apărare a țării pentru perioada 2015-2019*. București.
18. Administrația Prezidențială (2015). *Strategia națională de apărare a țării 2015-2019*. București.
19. Administrația Prezidențială (2020). *Strategia Națională de Apărare a Țării 2020-2024*. București.
20. INSCOP (2018). *Barometrul culturii de securitate – februarie 2018*, https://larics.ro/wp-content/uploads/2018/04/Raport-sondaj-INSCOP-barometru-LARICS-partea-1.pdf, accesat la 12 octombrie 2020.