REZILIENȚA NAȚIONALĂ LA AMENINȚĂRILE HIBRIDE ȘI CULTURA DE SECURITATE. UN CADRU DE ANALIZĂ.

***Dr. Teodor FRUNZETI*[*]**
***Cristian BĂRBULESCU*[**]**

Rezumat: *Lucrarea de față prezintă, în prima parte, aspecte referitoare la emergența forme (hibride) de manifestare a amenințărilor de securitate, prin descrierea factorilor care determină și favorizează evoluțiile de acest tip în interiorul sistemului internațional. Ulterior, pornind de la aceste elemente specifice, argumentăm necesitatea unei noi abordări centrate pe reziliență în gestionarea amenințărilor de acest gen. Abordarea pe care o susținem pune în centru statul-națiune – cu diferitele sale elemente constitutive (instituții publice, societatea civilă și infrastructura critică) – și relevă câteva direcții de acțiune care pot fi utile, pe dimensiunea de promovare a culturii de securitate, în proiectarea unui model conceptual al rezilienței naționale la amenințări hibride.*

Cuvinte-cheie*: amenințări hibride, război hibrid, reziliență națională, cultură de securitate, vulnerabilitate, știri false, știri contrafăcute.*

Considerații preliminare

Evenimentele înregistrate în ultimii ani în mediul internațional de securitate, începând cu anexarea Peninsulei Crimeea și destabilizarea situației de securitate din estul Ucrainei și culminând cu proliferarea acțiunilor ostile derulate în domeniul cibernetic și informațional în scopul influențării percepțiilor sociale și proceselor politice din unele state occidentale – cum este cazul SUA și al Franței – intră în categoria provocărilor de securitate emergente care reclamă identificarea unor noi abordări în procesele de gestionare a situațiilor de criză la nivelul actorilor statali și proiectarea unui cadru eficient de cooperare la nivel regional.

Multiplicarea tiparelor hibride din ultima perioadă relevă, pe de o parte, multitudinea combinațiilor de metode și mijloace ale agresorului, care contribuie la atingerea obiectivului strategic al acestuia – reprezentând, de fapt, chintesența războiului hibrid – și, pe de altă parte, necesitatea aprofundării eforturilor conjugate, instituționale și academice, pe problematica răspunsului la noile tipuri de amenințări de securitate. Demersul nostru este corelat acestui din urmă obiectiv și vizează dezvoltarea unui *model conceptual al rezilienței naționale la amenințări hibride care să se bazeze pe promovarea culturii de securitate*. Un astfel de model ar putea contribui la o mai bună înțelegere a conceptelor cu care operăm – *amenințările hibride*, *reziliența națională* și *cultura de securitate* – și a elementelor de interdependență care rezultă din intersectarea acestora.

[*] ***Dr. Teodor FRUNZETI Doctor în ştiinţe militare şi în ştiinţe politice, profesor universitar în cadrul Univesității „Titu Maiorescu”, președintele secției de științe militare din cadrul Academiei Oamenilor de Știință din România, email: tfrunzeti@gmail.com***

[**] ***Drd. Cristian BĂRBULESCU - Doctorand în domeniul informații și securitate națională la Univestitatea Națională de Apărare „Carol I” și asistent de cercetare în cadrul Academiei Oamenilor de Știință din România email: cebarbulescu@gmail.com***

Considerăm că un asemenea demers trebuie să pornească, într-o primă fază, de la identificarea factorilor care determină modul de manifestare a *amenințărilor hibride* precum și a tiparelor cunoscute, derivate din analiza acțiunilor recente din această categorie. Aceste elemente și aspectele rezultate în urma analizei relației care se poate stabili între *amenințările hibride* și *reziliența națională* – ca instrument de răspuns la acestea – pot susține, în final, definirea unui *cadru de analiză pentru gestionarea răspunsului la amenințări hibride*, cu aplicabilitate inclusiv pe dimensiunea de *consolidare a culturii de securitate la nivel național*.

1. Amenințările hibride – o nouă provocare la adresa securității naționale

Pentru prima dată, în luna iulie 2016, pe durata Summitului NATO de la Varșovia, combaterea amenințărilor hibride a fost identificată ca unul dintre domeniile prioritare de cooperare dintre UE și NATO. Cu câteva săptămâni în urmă, raportul comun al Comisiei Europene și al Serviciului European de Acțiune Externă a descris mediul de securitate european ca fiind semnificativ afectat de acțiunile hibride: „activitățile hibride devin o caracteristică frecventă a mediului de securitate european. Intensitatea acestor activități este în creștere, existând motive de îngrijorare tot mai mari legate de influențarea alegerilor, campaniile de dezinformare, activitățile cibernetice ostile și autorii de acte hibride care încearcă să îi radicalizeze pe membrii vulnerabili ai societății pentru a acționa apoi prin intermediul lor. Vulnerabilitățile constatate în raport cu amenințările hibride nu se limitează la frontierele naționale”[1]. În acest fel, se recunoaște, practic, nu doar faptul că impactul amenințărilor hibride excedează teritoriul statelor membre, resimțindu-se la nivel european, ci și că „*securitatea europeană a devenit o chestiune negociată, contestată și combătută*”[2] ca urmare a noilor provocări derivate din acțiunile actorilor statali și non-statali.

Dacă în perioada Războiului Rece evoluțiile de securitate au fost marcate de confruntarea a două superputeri militare dominante în interiorul sistemului internațional, în prezent, mediul de securitate global este mult mai dificil de descris în aceeași termeni, de prevalență a mijloacelor convenționale de descurajare. Această schimbare nu face, însă, ca amenințările de securitate clasice să se resimtă mai puțin intens la nivelul actorilor internaționali. Acestea continuă să se manifeste, dar se suprapun peste formele neconvenționale de manifestare ale amenințărilor de securitate, cele asimetrice și hibride. Amenințările curente sunt multidimensionale, iar legăturile dintre diferitele activități care le definesc sunt neclare și, uneori, foarte dificil, dacă nu chiar imposibil de verificat. Acest gen de amenințări, de natură hibridă, se manifestă la limita escaladării conflictului dintre doi sau mai mulți actori. Dacă interesele și obiectivele agresorului care utilizează astfel de tactici nu sunt atinse și, mai ales, dacă acțiunile acestuia nu sunt detectate la timp, conflictul poate escalada într-un *război hibrid*[3]. *Amenințările hibride* sunt și pot fi utilizate pentru a defini o realitate nouă în care pot fi testate noile tactici militare[4] – cel mai elocvent exemplu, în acest sens, fiind conflictul din Ucraina din anul 2014. De aceea, pentru statele predispuse la *amenințări hibride* un prim efort ar trebui întreprins pentru înțelegerea instrumentarului utilizat în cadrul acestor activități ostile și al principiilor după care se desfășoară aceste activități.

Combinarea diferitelor metode și mijloace este o caracteristică omniprezentă în acțiunile militare clasice. Această particularitate, desprinsă din teoria generală a războiului, face ca teza războiului hibrid să nu poată fi contestată (*pentru că, în esență, războiul a fost dintotdeauna hibrid!*). De asemenea, acest tip de strategie, prin care mai multe instrumente de putere sunt utilizate simultan și complementar pentru a atinge un obiectiv comun, a existat cu mult înaintea anexării ilegale a peninsulei Crimeea și a apariției grupării teroriste Statul Islamic din Irak și Levant. Un

[1] **** Raport comun către Parlamentul European și Consiliu referitor la punerea în aplicare a Cadrului comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene*, 2017, p. 3, disponibil la adresa https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017JC0030&from=RO, accesat la data de 12.08.2018

[2] Matti, Saarelainen, *Hybrid threats – what are we talking about?* Centrul European de Excelență pentru contracararea amenințărilor hibride, Helsinki, 2017, disponibil la adresa https://www.hybridcoe.fi/news/hybrid-threats-what-are-we-talking-about/, accesat la data de 10.07.2018.

[3] Ibidem.

[4] Ibidem.

actor care practică *războiul hibrid* poate opta pentru „*escaladarea pe verticală*" a confruntării cu ținta acestuia, prin intensificarea acțiunilor specifice unuia sau mai multor instrumente de putere, sau pentru „*escaladarea pe orizontală*", prin sincronizarea mai multor instrumente pentru a obține un efect combinat mai mare[5].

Spre deosebire de *războiul hibrid*, ceea ce este esențial de reținut cu privire la *amenințările hibride* are legătură cu interconectarea dintre diferitele activități care se circumscriu acestora și, mai mult, cu dificultatea stabilirii legăturilor existente între aceste activități anterior perioadei de manifestare a acestora, deci, în afara cadrului consacrat al confruntării armate sau al războiului.

În *Cadrul comun privind contracararea amenințărilor hibride*, elaborat de Comisia Europeană în anul 2016, este propusă o primă definiție a amenințărilor hibride, demers care reprezintă, în opinia noastră, un prim punct de plecare în procesele de operaționalizare a conceptului la nivelul statelor membre. *Amenințările hibride* sunt descrise ca un ansamblu 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. De obicei, se pune accentul pe exploatarea vulnerabilităților țintei vizate și pe generarea unei ambiguități în scopul împiedicării proceselor decizionale. Campaniile de dezinformare masive, care utilizează platforme de comunicare socială pentru a controla discursul politic sau pentru a radicaliza, a recruta și coordona actori intermediari pot constitui vectori ai amenințărilor hibride"[6].

Gama de metode și activități circumscrise *amenințărilor hibride* este mult mai extinsă, spre deosebire de celelalte tipuri de amenințări, convenționale și/sau asimetrice, cu care suntem deja familiarizați. Astfel, dacă sunt corelate atingerii aceluiași obiectiv strategic, *acțiunile hibride* pot include acțiuni de influențare prin propagandă și dezinformare, presiuni economice prin exploatarea vulnerabilităților unui anumit actor (ex.: dependența energetică), speculareа limitărilor sau lacunelor din cadrul normativ existent la nivel internațional sau acțiuni care urmăresc amplificarea sentimentului de nesiguranță în proximitatea propriilor frontiere (demonstrații de forță, incidente provocate la frontieră precum încălcările spațiului aerian etc.).

Amenințările hibride se referă, deci, la metodele și instrumentele utilizate de un potențial agresor – care poate fi un actor statal sau non-statal – pentru a-și susține propriile interese, strategii și obiective[7] în raport cu adversarul sau adversarii ii acestora. În actualul sistem internațional, multipolar și puternic globalizat, actorii statali mai slabi sunt cei care dezvoltă tendința de a-și susține propria agendă prin implementarea unor *strategii hibride* în registrul acțional. Acestora li se adaugă actorii non-statali care urmăresc, cu preponderență, popularizarea unor succese operaționale, impunerea propriilor modele ideologice la nivelul unei anumite comunități și/sau construirea unui brand la nivel regional și global. Aceste tendințe constituie provocări pentru statele occidentale și entitățile din care fac parte, precum UE și NATO, care, în mod inevitabil, vor trebui să identifice opțiuni adecvate de cooperare pentru calibrarea răspunsului la noile tipuri de amenințări.

În scenariile de confruntare hibridă, acțiunile neconvenționale sunt din ce în ce mai prezente în vreme ce componenta acțională militară, clasică sau convențională, este utilizată limitat și, de foarte multe ori, în scopul potențării efectelor activităților derulate pe alte palierele acționale subsecvente, precum cel politico-diplomatic, economic, informațional și/sau cibernetic etc. Noile tipuri de amenințări (hibride) se propagă multivectorial, prezintă un grad ridicat de sincronizare și generează efecte neliniare și dificil de evaluat cu rapiditate.

---

[5] Patrick J. Cullen, Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare*, 2017, p. 8, disponibil la adresa https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, accesat la data de 01.09.2018.

[6] *** *Comunicare comună către Parlamentul European şi Consiliu - Cadrul comun privind contracararea amenințărilor hibride Un răspuns al Uniunii Europene*, 2016, p. 2, disponibil la adresa http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52016JC0018, accesat la data de 01.09.2018.

[7] Matti, Saarelainen, *op.cit.*

Într-un studiu recent[8], elaborat cu participarea unor experți ai *Universității Naționale de Apărare, Centrului de studii a amenințărilor asimetrice* din Suedia, și *Centrului European de Excelență pentru contracararea amenințărilor hibride* din Finlanda, sunt prezentați factorii care contribuie la emergența *amenințărilor hibride*[9], respectiv:

- Schimbarea ordinii internaționale post-Război Rece. *În noul sistem internațional „puterea de a schimba convingerile, atitudinile, preferințele, opiniile, așteptările, emoțiile și/sau predispozițiile de a acționa este astăzi mai importantă decât puterea materială"*[10]. În prezent, lumea experimentează „partea întunecată a globalizării"[11], *rolul statului-națiune este pus în discuție,* la fel ca alianțele cu normele și regulile care limitează răspunsurile la acțiuni antagoniste de tip asimetric.
- *Globalizarea, tehnologiile avansate de comunicații și dezvoltările explozive din mediul online contribuie esențial la creșterea potențialului acțional al actorilor statali, dar și al celor non-statali* (cum sunt, de exemplu, corporațiile multinaționale, grupările de hackeri, grupările teroriste etc.) în domenii operaționale mai puțin consacrate, cum este cel cibernetic și informațional.
- *Apariția unor noi domenii de confruntare, cum ar fi cel cibernetic, unde „regulile jocului" nu au fost încă create*. Cu excepția mijloacelor și tehnologiilor cibernetice, cele mai multe dintre instrumentele utilizate în conflictele hibride – cum sunt de exemplu, propaganda și acțiunile în plan politico-diplomatic sau economice – nu sunt noi. Acțiunile derulate în spațiul cibernetic oferă atât instrumente noi de acțiune (*cu sunt, de exemplu, spionajul cibernetic, intoxicarea cu știri contrafăcute*), dar și noi oportunități pentru maximizarea efectului instrumentelor tradiționale de influență (politico-diplomatice, economice, informaționale etc.).
- *Exploatarea potențialului oferit de noile tehnologii media precum și a noilor instrumente de influențare socială.* Viteza ridicată de circulație a informațiilor, felul în care sunt produse informațiile și modul în care comunitățile sociale se pot conecta dincolo de frontierele naționale sunt rezultatul digitalizării și al dezvoltării instrumentelor *social media.* Încrederea, unul dintre pilonii fundamentali ai societăților democratice avansate, se erodează sub influența tehnicilor moderne de manipulare. Internetul a devenit noul „teren de confruntare", iar propaganda, dezinformarea și știrile contrafăcute (*fake news*) sunt noile arme cu care se duce războiul.
- *Delimitarea clară dintre pace și război este tot mai dificil de realizat.* Prevalența pentru utilizarea mijloacelor neconvenționale face ca ținta vizată de noul tip de agresiune să nu conștientizeze starea de război în care se află, până la utilizarea, disimulat sau la scară redusă, a instrumentului militar (*ex.: cazul Ucrainei*).

2. Consolidarea rezilienței naționale – opțiune strategică de gestionare a amenințărilor hibride

În ultimii ani, în mediul academic și în cel instituțional (european și național)[12] se discută din ce în ce mai mult despre *„reziliență*", în afara ariei tradiționale de aplicabilitate a conceptului[13]. Dacă anterior abordările din domeniul studiilor de securitate asupra *„rezilienței*" vizau, cu precădere, reducerea gradului de expunere la șocuri externe a diferitelor elemente ale infrastructurii critice, în prezent, se pune întrebarea dacă nu cumva acestea sunt utile și pot fi extinse și la nivelul unor sisteme complexe adaptative, de tipul celor sociale (organizații private, instituții publice,

[8] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, Madeline McCue, *Addressing Hybrid Threats,* Swedish Defence University, 2018, disponibil la adresa https://www.hybridcoe.fi/wp-content /uploads/2018/05/Treverton-AddressingHybridThreats.pdf, accesat la data de 01.09.2018.

[9] Lars Nicander, Matti Saarelainen, în Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, Madeline McCue, *op.cit.*, p. 1-2.

[10] Ibidem, p. 1.

[11] Ibidem.

[12] Astfel de trimiteri explicite se regăsesc în conținutul unor documente adoptate la nivelul UE și NATO dar și în diversele strategii elaborate la nivel național.

[13] Științele inginerești, ecologie, științele sociale (teoria organizației, psihologie) sau științele economice

comunități sociale sau chiar state-națiune), într-un cadru metodologic care să contribuie la consolidarea dimensiunii sociale a securității naționale.

De cele mai multe ori, politicile instituționale de intervenție în situații de urgență au constituit instrumente de dezvoltare a rezilienței sistemelor complexe, fizice și sociale, în urma expunerii acestora la efectele unor evenimente extreme din categoria calamităților și/sau dezastrelor naturale, ale căror manifestare este aleatorie și nedeterminată (deci foarte dificil de anticipat). Statele au fost și sunt încă preocupate, de exemplu, de minimizarea efectelor negative, în plan ecologic și social, generate de fenomenele meteorologice extreme (cutremure, furtuni tropicale, erupții ale unor vulcani etc.). Pentru realizarea acestui obiectiv, acestea au dezvoltat planuri de contingență care, prin măsurile concrete de răspuns pe care le includ, contribuie la consolidarea rezilienței societății și a elementelor de infrastructură critică la aceste tipuri de amenințări.

Analiza contribuțiilor din literatura de specialitate relevă faptul că *„reziliența*" reprezintă atât o *caracteristică* cât și un *proces* al sistemelor sociale, ambele atribute fie putând fi observabile, fie fiind observabile pe durata sau în urma expunerii la acțiuni externe cu potențial perturbator.

„Reziliența" este o *proprietate a sistemelor sociale* pentru că, în principiu, orice astfel de sistem dispune de funcții autoreglatorii care le mențin funcționale, în pofida *„avariilor*" produse de șocurile externe, și le permit să se adapteze la noile condiții de mediu și să se reorganizeze, mai devreme sau mai târziu, în sensul de a deveni *„antifragile*". Sistemele antifragile sunt acele organizări care au capacitatea de a învăța din propriile experiențe și profită de pe urma incertitudinii și a volatilității[14].

În accepțiune generală[15], *reziliența* reprezintă capacitatea acestor sisteme:

- de *a face față / a rezista* la provocările din mediul extern (rezistența / persistența funcționalității sistemelor – o importantă atenție trebuie acordată elementelor de infrastructură critică);
- de *a se adapta* la schimbările în dinamică din mediul de securitate;
- *de a se transforma* în sensul de a deveni mai puternice în fața noilor provocări de securitate.

Capacitatea de învățare este un atribut esențial al sistemelor sociale reziliente. Lecțiile învățate reprezintă elementele care conduc la sedimentarea și consolidarea culturii de securitate în organizările sociale, de la cele specializate – cum sunt companiile private, instituțiile publice, organizațiile neguvernametale – până la cele înglobante, de mari dimensiuni, cum sunt actorii de tip statal și suprastatal.

Teza conform căreia *reziliența este o caracteristică (predefinită) a sistemelor sociale complexe* generează, inevitabil, întrebări al căror răspuns poate contribui la o mai bună înțelegere asupra conceptului. *Dacă aceste sisteme dispun de un anumit grad de reziliență, de ce este necesar ca acestea să devină mai reziliente? De ce nu este suficientă abordarea rezilienței ca proprietate a sistemelor sociale? De ce este necesară generarea unui proces în cadrul acestor sisteme care să conducă la creşterea rezilienței acestora la amenințările cu care se confruntă?*

Viteza cu care se succed schimbările în mediile integratoare ale diferitelor sisteme sociale determină necesitatea antrenării capacităților de reziliență ale acestora pe fiecare dintre cele trei dimensiuni specificate anterior – *rezistență/continuitate, adaptare/flexibilitate* și *transformare/învățare*. De asemenea, abordarea rezilienței ca *proces* apare ca o necesitate și pe fondul diversificării amenințărilor de securitate neconvenționale (manifestate într-un nou domeniu operațional, cel cibernetic, încă nereglementat la nivel internațional), al rezistenței la schimbare a sistemelor instituționale birocratice și al creșterii gradului de interconectare la nivelul societăților, ca efect al digitalizării în domeniul economic și în industria media.

---

[14] Nicholas Nassim TALEB, *Antifragile*, Random House New York, 2012, p. 17.

[15] Christophe Béné, Rachel Godfrey Wood, Andrew Newsham și Mark Davies, *Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes*, Institute of Development Studies, 2012, p. 21, disponibil la adresa https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.2040-0209.2012.00405.x, accesat la data de 12.08.2018.

Dezvoltarea rezilienței nu se poate realiza altfel decât prin intermediul *proceselor* instituite la nivelul sistemelor. În cazul statelor-națiune, de exemplu, un astfel de proces înglobant ar trebui să includă activitățile susținute la nivelul autorităților publice și participarea societății civile.

Managementul riscurilor, dintr-o perspectivă a *rezilienței*, se bazează, în opinia noastră, pe procesul de analiză integrată a tendințelor identificate în manifestarea amenințărilor de securitate și a vulnerabilităților în raport cu acestea. Această abordare readuce în atenție necesitatea identificării propriilor puncte slabe, exploatabile în registrul acțional hibrid al unui potențial adversar. În această abordare, nevoia acută de cunoaștere a viitorului se menține, dar este mult mai ancorată la prezent, la capacitatea de răspuns a sistemului în raport cu potențialii factori externi care îi determină evoluția. Dintr-o perspectivă a rezilienței, este mult mai facil să stabilim dacă un sistem este fragil în anumite condiții de mediu specifice (în cazul nostru, de manifestare a unor acțiuni în spectrul hibrid), decât să insistăm prin eforturi sortite apriori eșecului să prospectăm evoluțiile viitoare incerte. În abordarea de față, trebuie să acceptăm volatilitatea, să înțelegem factorii stresori care afectează/pot afecta propriul sistem și să identificăm posibilități de reproducere a acestuia.

Într-un astfel de context, o abordare sistemică, orientată pe *procesele* din cadrul organizărilor sociale, este relevantă deoarece multe dintre tipurile de amenințări care afectează societățile, devin acum covariante în sensul că afectează simultan mai multe segmente ale acesteia sau chiar comunități întregi (iar amenințările hibride creează astfel de efecte!). Un astfel de efort trebuie să fie interinstituțional și colaborativ – axat pe consolidarea parteneriatului public-privat și a dialogului dintre stat și societate – pentru a putea contribui la reducerea satisfăcătoare a gradului de expunere a statelor-națiune (și a diferitelor sisteme fizice și sociale din cadrul acestora) la diferitele tipuri de acțiuni externe care atentează la securitatea acestora.

3. Gestionarea răspunsului la amenințări hibride – un posibil cadru de analiză

În opinia noastră, în procesele dedicate gestionării *amenințărilor hibride* nu pot fi obținute rezultate satisfăcătoare dacă nu sunt urmărite eventualele răspunsuri la următoarele întrebări esențiale: *Care sunt vulnerabilitățile naționale cărora trebuie să li se acorde o atenție deosebită? Cum ar putea un adversar să profite de aceste vulnerabilități? Care sunt scenariile relevante ale amenințării? Sunt toate sectoarele societății angajate în eforturile de apărare și au fost ele pregătite în mod adecvat să acționeze în sectoarele lor împotriva amenințărilor probabile?*

Aspectele teoretice, precum și cele desprinse din evoluțiile recente din mediul global și regional de securitate ne permit să avansăm un posibil cadru analitic util în procesul de gestionare a *amenințărilor hibride*. Acest cadru ar putea cuprinde următoarele etape:

1) *Identificarea instrumentelor de putere pe care adversarul le-ar putea folosi în acțiunile asociate războiului hibrid*

În această etapă propunem analizarea diferitelor instrumente de putere pe care un potențial adversar ar putea să le folosească într-un scenariu de confruntare hibridă. Considerăm că această analiză este necesară pentru a putea trece mai ușor, la evaluarea modului în care aceste instrumente pot fi sincronizate în practică și la determinarea avantajelor și a efectelor non-lineare ale angajării simultane a mai multor instrumente în raport cu ținta vizată.

Analiza tiparelor recente de acțiuni hibride indică următoarele tendințe specifice formelor de manifestare a amenințărilor identificate cu predilecție în domeniul informațional și cibernetic şi care se pot regăsi în strategiile integrate ale unui potențial agresor în cadrul unui scenariu de agresiune hibridă, astfel:

- *Utilizarea propagandei ca mijloc prevalent de acțiune.* Asistăm, în prezent, la „o militarizare și transformare a informației în armă de război”[16]. Ceea ce se observă din acțiunile specifice derulate pe acest palier nu are legătură cu obiectivele propagandei care rămân aceleași, asociate intenției de influențare a deciziei politice și a populației statului-țintă precum și a populației

[16] Iulian Chifu, *Pulsul planetei. Militarizarea și transformarea informației în armă de război*, „Evenimentul Zilei”, disponibil la adresa https://evz.ro/pulsul-planetei-militarizarea-si-transformarea-informatiei-in-arma-de-razboi.html, accesat la data de 01.09.2018

proprii în vederea legitimării acțiunilor viitoare ale acestuia (imaginea pe care o livrează agresorul propriei audiențe este cea a unui stat în defensivă nevoit să acționeze în legitimă apărare). Noutatea constă în mijloacele care sunt utilizate în cadrul acțiunilor de propagandă. Tehnologiile *new media* și *rețelele sociale* pot constitui vectori de agresiune informațională. Acestea sunt utilizate pentru maximizarea efectelor unei campanii în cadrul unei confruntări hibride. Costurile aferente exploatării acestor mijloace nu este atât de mare în raport cu obiectivul strategic propus de destabilizare a adversarului dacă ne gândim doar, prin comparație, la limitările (de ordin operațional) de care dispuneau în perioada Războiului Rece statele care încercau să implanteze o știre sau un articol într-o publicație dintr-un alt stat.

Pentru derularea cu succes a operațiilor informaționale trebuie îndeplinite două condiții esențiale[17], respectiv *existența canalului prin care informațiile să poată ajunge la țintele vizate* (cum ar fi organisme de presă interne orientate spre publicul străin, sponsorizate de stat și organizații și platforme de social media) și *cunoașterea în detaliu de către agresor a țintei vizate,* pentru ca acesta să fie în măsură să-și dezvolte acele constructe informaționale care îi aduc avantaje în context hibrid. Aceste constructe pot include, după caz, opinii pe teme sensibile pentru publicul-țintă vizat, date din scurgeri de informații sau publicarea unor *știri contrafăcute*.

- *Controlul asupra unor surse media autohtone aservite și cu audiență pe segmente largi de public, atât din interiorul cât și din exteriorul statului agresor.* Mass-media aservite devin foarte influente atunci când materialele pe care le publică sunt preluate de către sursele media populare străine[18].
- *Social media oferă, într-adevăr, noi posibilități pentru un potențial agresor care intenționează să obțină acces la mass-media și la publicul larg al țintelor vizate.* Acțiunile de dezinformare pot fi deosebit de eficiente având în vedere prevalența ridicată în rândul publicului larg de a accesa știri prin intermediul rețelelor sociale.

Modelele de afaceri pe care funcționează platformele social media, dar și publicațiile media – de asemenea, utilizatori ai rețelelor de socializare – se bazează pe generarea de conținut în funcție de preferințele utilizatorilor captivi în propriile „camere de ecou” [19] – care limitează universul de cunoaștere al acestora la conținutul consumat și la „persoanele” cu care împărtășesc aceleași idei și valori – pentru care platformele social media sunt blamate și criticate.

Platformele social media devin, astfel, adevărate „agregatoare” de știri, putând fi utilizate cu ușurință pentru promovarea unor știri din mass-media ostile sau pentru a publica informații noi – prin conturi sponsorizate de stat, rețele de tip botnet, troli sau anunțuri publicitare – care, în acest mod, ajung direct la publicul-țintă. Aceasta pare să fi fost una dintre particularitățile campaniei de influență în alegerile prezidențiale din SUA din anul 2016, când numeroase știri provenite din surse media ruseşti – care au fost raportate mai întâi în *Russia Today* sau *Sputnik* - au fost apoi preluate și rostogolite în rețelele sociale *Twitter* sau pe *Facebook* prin intermediul botnet-urilor și trolilor, generând algoritmi bazați pe tendințe de consum înșelătoare sau false și riscul preluării și popularizării de către sursele media locale[20].

- *Utilizarea pe scară largă a știrilor contrafăcute* în scopul influențării percepției audiențelor-țintă. *Știrile contrafăcute* sunt mai mult decât *știrile false*. Acestea includ informații care distorsionează deliberat adevărul obiectiv la nivelul publicului consumator și urmăresc un obiectiv specific, de obicei, asociat satisfacerii unor interese ostile ale unui potențial agresor. Spre deosebire de *știrile contrafăcute*, *știrile false* sunt sau pot fi generate de cauze care denotă superficialitate în documentarea jurnalistică sau lipsă de profesionalism dar și de interese derivate din politica editorială care se pot reflecta în maniera de prezentare, tendențioasă sau mai puțin obiectivă, a conținutului informațional.

---

[17] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *op.cit.*, p. 46.
[18] Ibidem, p. 47.
[19] *** *Facebook în era post-adevărului*, articol disponibil la adresa http://intelligence.sri.ro/facebook-era-post-adevarului/, accesat la data de 02.09.2018.
[20] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *op.cit.*, p. 47.

Difuzarea de *știri contrafăcute* se realizează, în mod frecvent, prin intermediul canalelor *social media* din cauza absenței unor „filtre" sau instrumente de verificare a veridicității informațiilor postate. De cele mai multe ori, acest tip de filtru se regăsește exclusiv la nivelul utilizatorului final. Chiar în situația în care platformele de socializare își vor dezvolta instrumente de verificare a postărilor publicate, eliminarea completă a acestora din conținut este dificilă, dacă nu chiar imposibilă, din cauza modelului algoritmic după care funcționează acestea, care permite „*rostogolirea*" informației de la un utilizator la altul. La fel de puțin probabilă este și stoparea distribuirii prin rețelele de socializare a materialelor promovate de sursele media *mainstream* care sunt asociate cu practica *știrilor contrafăcute.* Câtă vreme acestea dispun de un nivel ridicat de popularitate în rândul utilizatorilor, acest demers pare irealizabil. Dincolo de avantajele și oportunitățile oferite de noua era a digitalizării informației, una dintre provocările majore căreia trebuie să îi facem față are legătură cu capacitatea socială de procesare a informației, mai ales dacă *știrile contrafăcute* vor ajunge să genereze trenduri în *social media* sau să fie preluate și raportate de alte mass-media în căutarea „senzaționalului".

• *Existența unor platforme (ex.: Wikileaks, DCleaks.com) care facilitează publicarea unor date din categoria scurgerilor de informații*, obținute prin acțiuni de spionaj cibernetic (acțiuni de acest gen ar fi fost derulate în procesele electorale recente din SUA și Franța)[21]. Este foarte dificilă și rămâne în sarcina structurilor de securitate specializate să identifice legăturile între aceste platforme și actorul interesat de publicarea acestor informații sensibile și cu caracter senzațional, consumatorul final nedispunând decât de măsura precauției și a propriului simț critic ca instrument de apărare în fața manipulării.

2) *Evaluarea propriilor vulnerabilități pornind de la premisa că în acțiunile de tip hibrid, agresorul acționează prin exploatarea sensibilităților din interiorul societăților vizate.* Contribuțiile din literatură ne oferă suficiente repere utile[22] în acest sens. Această etapă ar putea include:

• *Identificarea funcțiilor critice ale societății.* De exemplu, o posibilă direcție de evaluare ar putea viza cum și în ce mod statul este dependent de serviciile digitale și cât de vulnerabile sunt acestea în fața agresiunilor cibernetice. Evaluarea, probabil, ar trebui să includă un set relevant de scenarii ale amenințării care pot fi folosite pentru a susține procesele corelate consolidării rezilienței naționale, pe dimensiunea socială și cibernetică.

• *Evaluarea dimensiunilor de vulnerabilitate*. Una dintre acestea este cea *geografică*. Proximitatea față de sursa potențială de amenințare poate amplifica anumite temeri la nivelul societății reprezentate de iminența unei posibile acțiuni ostile, chiar de natură convențională/militară, care să pună în pericol securitatea națională.

Dimensiunea *socială* și *politică* sunt, în egală măsură, relevante în această etapă. Existența unor linii de falie în societate, generate de diferențele de conflictele de opinii între diferitele comunități etnice, generații, clase sociale, medii de conviețuire (rural - urban) sau modalitatea în care este consumată informația la nivelul societății (presa online, radio/televiziune, rețelele de socializare) sunt elemente exploatabile în cadrul campaniilor informaționale. Totodată, orientarea politicii externe a statului și modificările de percepție la nivelul societății cu privire la aceasta, precum și relația dintre autorități și societate (gradul de încredere al populației în instituții) reprezintă teme care se pot regăsi în acțiunile hibride.

3) *Identificarea obiectivelor pe care adversarul ar putea să le urmărească în raport cu vulnerabilitățile existente.* Se realizează în corelație cu instrumentele de putere disponibile în registrul acțional împotriva unei ținte identificate.

4) *Calibrarea mijloacelor de răspuns la agresiunile hibride, aplicabile pe dimensiunea consolidării culturii de securitate.* Pornind de la premisa conform căreia *amenințările hibride* se manifestă, cu predilecție, în domeniul cognitiv, la nivelul societății civile, cu multiple implicații în

[21] Ibidem.
[22] Ibidem.

planul securității naționale[23], considerăm utilă o abordare care să fie centrată pe dezvoltarea culturii de securitate, ca exponent al rezilienței naționale la amenințări hibride.

Cultura de securitate, definită generic ca „ansamblul ideilor, obiceiurilor și comportamentelor sociale ale unei comunități sociale cu privire la eliminarea amenințării și pericolului”[24], comportă două dimensiuni interconectate:

- *cunoaștere* – se referă la gradul de informare a populației asupra problemelor de securitate și percepția acesteia asupra câtorva direcții strategice de acțiune care derivă din răspunsurile la întrebări fundamentale precum *cine este adversarul?*, *cum ne amenință acesta?* și *cum putem gestiona eficient amenințările din partea acestuia?*[25];
- *comportament* – exprimă valorificarea *cunoașterii* în modul oamenilor de a se raporta la o anumită problemă de securitate cu impact asupra comunității din care fac parte. Se referă la participarea activă a societății în gestionarea problemelor de securitate.

Procesul inițiat în sensul dezvoltării culturii de securitate poate fi proiectat pe trei paliere: *individual* – se referă la cultivarea ideilor și principiilor proprii fiecărei persoane (vizează dimensiunea mentală și spirituală), *social* – se referă la dezvoltarea unor seturi de valori la nivelul organizărilor sociale și a unei conștiințe de acțiune în beneficiul propriei securități și *material* – se referă la resursele existențiale de la nivelul societății.

Concluzii

Interconectarea dintre domeniile fizic, digital și social – ca efect al dezvoltărilor generate de *cea de-a patra revoluție industrială* pe care o experimentăm în prezent – face ca formele hibride de manifestare a agresiunii să devină mult mai accesibile actorilor statali și non-statali, care le utilizează pentru susținerea propriilor interese strategice în relațiile internaționale. Caracterul hibrid al noilor tipuri de amenințări este o reflexie a evoluțiilor înregistrate în crizele din Ucraina și Siria dar și mai recent la nivelul democrațiilor occidentale care reclamă un grad ridicat de expunere la acțiunile ostile derulate în domeniul informațional/cognitiv și cibernetic în scopul influențării percepției populației în context electoral.

Noua eră a *amenințărilor hibride* pune în discuție rolul statului-națiune și, în egală măsură, pe cel al formatelor de cooperare regională și al alianțelor din care acestea fac parte, precum și normele de drept internațional existente care fie limitează, fie nu asigură un cadru adecvat de răspuns la acest gen de acțiuni.

În noul context de securitate definit de manifestări hibride în conduita actorilor internaționali, *reziliența* și *securitatea* nu sunt concepte incompatibile. În acest cadru de analiză, *reziliența* nu trebuie considerată o alternativă la *securitatea națională*, ci, dimpotrivă, un mod inovativ de asigurare a acesteia. Această posibilă nouă perspectivă asupra securității ar trebui să fie mult mai flexibilă și să permită descurajarea și contracararea adversarilor hibrizi cu o gamă largă de instrumente, rezultat al interconectării dintre sectoarele civile (*publice și private*) și sectorul militar.

Complexitatea formelor de manifestare ale *amenințărilor hibride* testează capacitatea de reacție a instituțiilor publice și legătura existentă între societate și autorități. De aceea, în faza de pre-manifestare a amenințării, conștientizarea pericolului și consolidarea parteneriatului dintre instituțiile publice și societatea civilă sunt primordiale pentru creșterea rezilienței sociale. Considerăm că intensificarea efortului pentru identificarea unor soluții inteligente pe dimensiunea

[23] De exemplu, afectarea coeziunii sociale în situațiile de criză pe care le poate traversa la un moment dat statul-țintă, subminarea încrederii populației în instituțiile statului, schimbarea unor percepții la nivelul populației în raport cu anumite teme sensibile de dezbatere publică etc.

[24] Kai Roer, *Build a Security Culture,* IT Governance Publishing, 2015, p. 6, disponibil la adresa https://news.asis.io/sites/default/files/Build%20a%20Secuirty%20Culture%20%28Fundamentals%20Series%29%20by%20Kai%20Roer.pdf, accesat la data de 28.08.2018

[25] Lucian Dumitrescu, *Lansarea barometrului culturii de securitate. Ce este cultura de securitate?* București: Fundația Universitară a Mării Negre, 2018, articol în publicația „Adevărul”, disponibil la adresa https://adevarul.ro/news/eveniment/lansarea-barometrului-culturii-securitate-cultura-securitate-1_5acf1cf9df52022f75bd7153/ index.html, accesat la data de 28.08.2018.

culturii de securitate poate susține dezvoltarea *rezilienței sociale / comunitare* pe termen mediu și lung.

În opinia noastră, dimensiunea socială a securității trebuie să reprezinte – alături de inițiativele de întărire a capacității instituționale de răspuns în planul deciziei strategice, al apărării, ordinii publice și siguranței naționale și la nivelul infrastructurii critice (de transport, comunicații, energie etc.) – o funcție complementară a „bunei guvernări" care să poată susține, pe termen lung, abordarea strategică integratoare (de tip *whole of government*) în formularea măsurilor de răspuns la *amenințările hibride*. Una dintre opțiunile utile pe care o susținem, în acest sens, este relaționată necesității de promovare a politicilor care contribuie la dezvoltarea culturii de securitate, ca una dintre aceste măsuri.

Relația dintre guvern şi populație în context hibrid este esențială. *Reziliența națională* la *amenințări hibride* nu implică doar măsurile specifice de răspuns proiectate la nivel instituțional (cum se pregătesc autoritățile să răspundă în cazul unei agresiuni?) ci este un proces înglobant care include toate elementele componente ale unei națiuni, inclusiv participarea societății. Dezvoltarea culturii de securitate la nivelul societății nu trebuie să vizeze exclusiv palierul consolidării încrederii în instituțiile cu atribuții în domeniul securității naționale ci și măsuri concrete destinate creșterii gradului de cunoaștere/conștientizare a formelor emergente/revoluționare de manifestare a amenințărilor de securitate, precum și politici concrete de combatere a noilor acțiuni din sfera războiului informațional – cum sunt, de exemplu, acțiunile de minimizare a efectelor generate de propagarea la scară globală a fenomenului „știrilor false" – și din domeniul cibernetic.

BIBLIOGRAFIE

1. AARONSON, Michael, DIESSEN, Sverre, KERMABON, Yves de, LONG, Mary Beth, MIKLAUCIC, Michael, *NATO Countering the Hybrid Threat*, Prism 2, nr. 4, 2012, disponibil la adresa http://cco.ndu.edu/Portals/96/Documents/prism/prism_2-4/Prism_111-124_ Aaronson-Diessen.pdf.
2. ALEXANDER, David, *A brief history of resilience*, Institute for Risk and Disaster Reduction, University College London, disponibil la adresa of https://www.slideshare.net/dealexander/a-brief-history-of-resilience.
3. BACH, Robert, KAUFMAN, David, SETTLE, Kathy, DUCKWORTH, Mark, *Policy Leadership Challenges in Supporting Community Resilience, Strategies for Supporting Community Resilience,* Crisis Management Research and Training: Multinational Experiences, Swedish Defence University, Stockholm, 2015, disponibil la adresa http://fhs.diva-portal.org/smash/get/diva2:795117/FULLTEXT01.pdf.
4. BÉNÉ, Christophe, WOOD, Rachel Godfrey, NEWSHAM, Andrew și DAVIES, Mark , *Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programme*s, IDS WORKING PAPER Volume 2012 Number 405 CSP WORKING PAPER Number 006, 2012, disponibil la adresa https://onlinelibrary.wiley.com/doi/abs/10.1111/j.2040-0209.2012.00405.x.
5. BORBEAU, Philipe, *Resilience and International Politics: Premises, debates, agenda*, International Studies review, 2015, disponibil la adresa https://doi.org/10.1111/misr.12226.
6. CEDERBERG, Aapo, ERONEN, Pasi, *How can Societies be Defended against Hybrid Threats?*, Geneva centre for Security policy, Strategic Security Analysis, nr. 9, 2015, disponibil la adresa https://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats.
7. CULLEN, Patrick J., REICHBORN-KJENNERUD, Erik. *Understanding Hybrid Warfare.* London: Multinational Capability Development Campaign (MCDC) 2016-17, 2017.
8. DUMITRESCU, Lucian. *Lansarea barometrului culturii de securitate. Ce este cultura de securitate?* București: Fundația Universitară a Mării Negre, 2018.
9. HAMILTON, Daniel (ed.), *Forward Resilience, Protecting Society in an Interconnected World,* Center for Transatlantic Relations, 2016.

10. PRIOR, Tim, HERZOG, Michel, *The Practical Application of Resilience: Resilience Manifestation and Expression*, Center for Security Studies, ETH Zürich, 2013, disponibil la adresa https://www.files.ethz.ch/isn/173818/Risk_and_Resilience_Report_Practical_Application_of_Resilience_2013.pdf;
11. ROER, Kai. *Build a Security Culture.* IT Governance Publishing, 2015.
12. SAARELAINEN, Matti, *Hybrid threats – what are we talking about?* Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2017.
13. THIELE, Ralph D., *Building Resilience Readiness against Hybrid Threats-A Cooperative European Union / NATO Perspective.* Vol. No. 449. Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), 2016.
14. TALEB, Nicholas Nassim, *Antifragile*, Random House New York, 2012.
15. TREVERTON, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee, și Madeline McCue. *Addressing Hybrid Threats.* Swedish Defence University, 2018.
16. *** *Comunicatul Summit-ului NATO de la Varşovia din iulie 2016*, disponibil la adresa https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummit Communique.pdf
17. *** *Comunicare comună către Parlamentul European şi Consiliu - Cadrul comun privind contracararea ameninţărilor hibride Un răspuns al Uniunii Europene*, 2016, disponibil la adresa http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52016JC0018.
18. *** *Declarația comună adoptată la Summit-ul NATO de la Varşovia*, din 7-8 iulie 2016.
19. *** *Hybrid threats and the EU State of play and future progress*, European Union Institute for Security Studies, 2017, disponibil la adresa https://www.iss.europa.eu/sites /default/files/EUISSFiles/EE%20hybrid%20event%20report.pdf.

Prezentul articol este parte integrantă a proiectului de cercetare științifică intitulat „*Cultura de securitate și reziliența națională la amenințările hibride*”, derulat pe parcursul anului 2018, în cadrul Academiei Oamenilor de Știință din România.