RAPORTUL DE CERCETARE INTERMEDIAR NR.2

(septembrie 2018)

realizat în cadrul proiectului

"Cultura de securitate şi rezilienţa naţională la ameninţări hibride"

REZILIENŢA NAŢIONALĂ LA AMENINŢĂRILE HIBRIDE - UN POSIBIL CADRU DE ANALIZĂ CU UTILITATE ÎN PROMOVAREA CULTURII DE SECURITATE

Drd. Cristian BĂRBULESCU

1. Introducere

Prezentul raport continuă demersul iniţiat în etapa anterioară a documentării derulată în cadrul proiectului de cercetare intitulat „*Cultura de securitate şi rezilienţa naţională la ameninţările hibride*". În această perioadă de raportare, obiectivele de etapă pe care ni le-am propus au constat în:

- identificarea elementelor rezultate din problematizarea relaţiei care se poate stabili între *ameninţările hibride* şi *rezilienţa naţională*, ca instrument de răspuns la acestea;

- şi definirea unui *cadru de analiză pentru gestionarea răspunsului la ameninţări hibride* care să servească, în ultima etapă a cercetării noastre, în conceptualizarea unui *model al rezilienţei naţionale la ameninţări hibride prin eforturi sistematice de promovare a culturii de securitate*.

Analiza întreprinsă conţine, în prima parte, explicaţii ale emergenţei noilor forme (hibride) de manifestare a ameninţărilor de securitate, prin enumerarea şi descrierea principalilor factori care determină şi favorizează evoluţiile de acest tip în interiorul sistemului internaţional.

Pornind de la premisa conform căreia utilizarea simultană şi complementară a multor instrumente de putere pentru atingerea obiectivelor strategice nu mai reprezintă atributul exclusiv al marilor puteri globale argumentăm, ulterior, necesitatea unei noii abordări centrată pe rezilienţă în gestionarea ameninţărilor. Abordarea pe care o susţinem pune în centru *statul-naţiune* (cu diferitele sale elemente constitutive: instituţii publice, societatea - organizaţii / entităţi private, comunităţi sociale - şi infrastructura critică) şi explicitează dimensiunile pe care trebuie intervenit în răspunsul la acţiunile de tip hibrid (*rezistenţă/continuitate, adaptare/flexibilitate* şi *transformare/învăţare*).

2. Factori care determină emergenţa ameninţările hibride

Interconectarea dintre domeniile fizic, digital şi social - ca efect al dezvoltărilor generate de *cea de-a patra revoluţie industrială* pe care o experimentăm în prezent - face ca formele hibride de manifestare a agresiunii să devină mult mai accesibile actorilor statali şi non-statali, care le utilizează pentru susţinerea propriilor interese strategice în relaţiile internaţionale. Caracterul hibrid al noilor tipuri de ameninţări este o reflexie a evoluţiilor înregistrate în crizele din Ucraina şi Siria dar şi mai recent la nivelul democraţiilor occidentale care reclamă un grad ridicat de expunere la acţiunile ostile derulate în domeniul informaţional/cognitiv şi cibernetic în scopul influenţării percepţiei populaţiei în context electoral.

În scenariile de confruntare hibridă acţiunile neconvenţionale devin din ce în ce mai prezente în vreme ce componenta acţională militară, clasică sau convenţională, este utilizată limitat şi, de foarte multe ori, în scopul potenţării efectelor activităţilor derulate pe alte palierele acţionale subsecvente, precum cel politico-diplomatic, economic, informaţional şi/sau cibernetic etc. Noile tipuri de ameninţări (hibride) se propagă multivectorial, prezintă un grad ridicat de sincronizare şi generează efecte neliniare şi dificil de evaluat cu rapiditate.

Într-un studiul recent, „*Adressing Hybrid Threats*”[1], elaborat cu participarea unor experţi ai *Universităţii Naţionale de Apărare, Centrului de studii a ameninţărilor asimetrice* din Suedia, şi *Centrului European de Excelenţă pentru contracararea ameninţărilor hibride* din Finlanda sunt prezentaţi factorii care contribuie la emergenţa *ameninţărilor hibride*, respectiv:

- schimbarea ordinii internaţionale post-Război Rece. *În noul sistem internaţional „puterea de a schimba convingerile, atitudinile, preferinţele, opiniile, aşteptările, emoţiile şi/sau predispoziţiile de a acţiona este astăzi mai importantă decât puterea materială”*[2]. În prezent, lumea experimentează „partea întunecată a globalizării”[3], *rolul statului-naţiune este pus în discuţie*, la fel ca alianţele cu normele şi regulile care limitează răspunsurile la acţiuni antagoniste de tip asimetric. Globalizarea, tehnologiile avansate de comunicaţii şi dezvoltările explozive din mediul online contribuie esenţial la creşterea rolului şi al potenţialului acţional al statelor mici (cu referire la cele care nu aveau un cuvânt de spus în perioada bipolarismului) şi, mai cu seamă, al actorilor non-statali (cum

[1] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats,* Swedish Defence University, 2018

[2] Lars Nicander, Matti Saarelainen în Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats,* Swedish Defence University, 2018, p. 1-2

[3] Ibidem

sunt, de exemplu, corporaţiile multinaţionale, grupările de hackeri, grupările teroriste etc.).

- a*pariţia unor noi domenii de confruntare, cum ar fi cel cibernetic, unde „regulile jocului" nu au fost încă create*;

- *noile tehnologii media oferă noi instrumente de influenţare în societate.* Viteza ridicată de circulaţie a informaţiilor, felul în care sunt produse informaţiile şi modul în care oamenii sunt conectaţi peste graniţele naţionale sunt rezultatul digitalizării şi al dezvoltării social media. Încrederea, unul dintre pilonii fundamentali ai societăţilor democratice avansate se erodează. Internetul a devenit noul „câmp de luptă", iar propaganda, dezinformarea şi *ştirile contrafăcute* (*fake news*) sunt noile arme cu care se duce războiul;

- *delimitarea dintre război şi pace este tot mai dificil de realizat.* Prevalenţa pentru utilizarea mijloacelor neconvenţionale face ca statul vizat de noul tip de agresiune să nu conştientizeze că se află în război până la utilizarea la scară redusă şi disimulată a instrumentului militar;

- *la nivel global experimentăm o fază de tranziţie la nivelul generaţiilor şi, odată cu aceasta schimbarea memoriei istorice* care lasă spaţiu pentru manipularea politică a evenimentelor istorice. Generaţia care a trăit perioada Războiului Rece (dominată de lupta ideologică dintre comunism şi capitalism şi de teama războiului nuclear) este substituită de generaţia post-Război Rece care experimentează o lume post-globalizare, a societăţilor digitalizate în care se manifestă două tendinţe contradictorii - cosmopolitanismul (rezultat al interconectivităţii societăţilor) şi neo-naţionalismul (ca efect al insatisfacţiei faţă de beneficiile globalizării).

Multe dintre instrumentele utilizate în conflictele hibride - de exemplu, propaganda sau pârghiile de constrângere politice şi economice - nu sunt noi. Principala excepţie este reprezentată de acţiunile derulate în spaţiul cibernetic, care oferă atât instrumente noi de acţiune (cu sunt, de exemplu, spionajul cibernetic, intoxicarea cu ştiri contrafăcute), dar şi noi oportunităţi pentru maximizarea efectului instrumentelor tradiţionale de influenţă. Ameninţările hibride ale secolului XXI[4] constau în utilizarea simultană şi complementară a multor instrumente de putere pentru a atinge un obiectiv comun.

În afara complementarităţii, o altă caracteristică definitorie a acţiunilor asociate războiului hibrid este utilizarea *strategică* a acestor instrumente de putere atât pe verticală, cât şi pe orizontală. Aceasta înseamnă că acestea vizează şi exploatează *vulnerabilităţile* unui alt stat şi sunt utilizate pentru a atinge *obiective specifice*, care pot sau nu să se schimbe pe durata campaniei iniţiate de agresor[5].

[4] precizarea merită făcută deoarece caracterul hibrid al mijloacelor utilizate în confruntările între actorii internaţionali a existat dintotdeauna, nereprezentând o noutate a conflictelor din prezent.

[5] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *op.cit.*, p. 45

Un actor care practică războiul hibrid poate opta pentru „*escaladarea pe verticală*” a confruntării cu ţinta acestuia, prin intensificarea acţiunilor corelate unuia sau mai multor instrumente de putere, sau pentru „*escaladarea pe orizontală*”, prin sincronizarea mai multor instrumente pentru a obţine un efect combinat mai mare[6].

3. Consolidarea rezilienţei - opţiune strategică de gestionare a ameninţărilor hibride

În ultimii ani, în mediul academic şi în cel instituţional (european şi naţional)[7] se discută, din ce în ce mai mult, despre *„rezilienţă*” în afara ariei tradiţionale de aplicabilitate a conceptului. Dacă anterior abordările din domeniul studiilor de securitate asupra *„rezilienţei*” vizau, cu precădere, reducerea gradului de expunere la şocuri externe a diferitelor elemente ale infrastructurii critice, în prezent, se pune întrebarea dacă nu cumva acestea sunt utile şi pot fi extinse şi la nivelul unor sisteme complexe adaptative de tipul celor sociale (ex.: organizaţii private, instituţii publice, comunităţi sociale şi state-naţiune), într-un cadru metodologic care să contribuie la consolidarea dimensiunii sociale a securităţii naţionale.

De cele mai multe ori, politicile instituţionale de intervenţie în situaţii de urgenţă au constituit instrumente de dezvoltare a rezilienţei sistemelor complexe, fizice şi sociale, în urma expunerii acestora la efectele unor evenimente extreme din categoria calamităţilor şi/sau dezastrelor naturale, ale căror manifestare este aleatorie şi non-determinată (sau foarte dificil de anticipat). Statele au fost şi sunt încă preocupate, de exemplu, de minimizarea efectelor negative, în plan ecologic şi social, generate de fenomenele meteorologice extreme (ex.: cutremure, furtuni tropicale, erupţii ale unor vulcani etc.). Pentru realizarea acestui obiectiv, acestea au dezvoltat planuri de contingenţă care, prin măsurile concrete de răspuns pe care le includ, contribuie la consolidarea rezilienţei sociale şi a elementelor de infrastructură critică la aceste tipuri de ameninţări.

Analiza contribuţiilor din literatura de specialitate relevă faptul că *„rezilienţa*” reprezintă atât o *caracteristică* cât şi un *proces* al sistemelor sociale, ambele atribute putând fi observabile pe durata sau în urma expunerii la acţiuni externe cu potenţial perturbator.

„Rezilienţa” este o *proprietate a sistemelor sociale* pentru că, în principiu, orice astfel de sistem dispune de funcţii autoreglatorii care le menţin funcţionale, în pofida *„avariilor*” produse de şocurile externe, şi le permit să se adapteze la noile condiţii de mediu şi să se reorganizeze, mai devreme sau mai târziu, în sensul de a

[6] 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

[7] astfel de trimiteri explicite se regăsesc în conţinutul unor documente adoptate la nivelul UE şi NATO dar şi în diversele strategii elaborate la nivel naţional.

deveni *„antifragile*". Sistemele antifragile sunt acele organizări care au capacitatea de a învăţa din propriile experienţe şi profită de pe urma incertitudinii şi a volatilităţii[8].

În accepţiune generală[9], *reziliența* reprezintă capacitatea acestor sisteme:

- de *a face faţă / a rezista* la provocările din mediul extern (rezistenţa / persistenţa funcţionalităţii sistemelor - o importantă atenţie trebuie acordată elementelor de infrastructură critică);

- de *a se adapta* la schimbările în dinamică din mediul de securitate;

- şi *de a se transforma* în sensul de a deveni mai puternice în faţa noilor provocări de securitate. Capacitatea de învăţare este un atribut esenţial al sistemelor sociale reziliente. Lecţiile învăţate reprezintă elementele care conduc la sedimentarea şi consolidarea culturii de securitate în organizările sociale, de la cele specializate - cum sunt companiile private, instituţiile publice, organizaţiile neguvernametale - până la cele înglobante, de mari dimensiuni, cum sunt statele-naţiune şi alianţele şi uniunile de state.

Teza conform căreia *reziliența este o caracteristică (predefinită) a sistemelor sociale complexe* generează, inevitabil, întrebări a căror răspuns poate contribui la o mai bună înţelegere 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 ameninţările cu care se confruntă?*

Viteza cu care se succed schimbările în mediile integratoare ale diferitelor sisteme sociale determină necesitatea antrenării capacităţilor de reziliență ale acestora pe fiecare dintre cele trei dimensiuni specificate anterior - *rezistență/continuitate, adaptare/flexibilitate* şi *transformare/învăţare*. De asemenea, abordarea rezilienței ca *proces* apare ca o necesitate şi pe fondul diversificării ameninţărilor de securitate neconvenţionale (manifeste într-un nou domeniu operaţional, cel cibernetic, încă nereglementat la nivel internaţional), al rezistenței la schimbare a sistemelor instituţionale birocratice şi al creşterii gradului de interconectare la nivelul societăţilor ca efect al digitalizării în economie şi în industria media.

Dezvoltarea rezilienței nu se poate realiza altfel decât prin intermediul *proceselor* instituite la nivelul sistemelor. În cazul statelor-naţiune, de exemplu, un

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

[9] Christophe Béné, Rachel Godfrey Wood, Andrew Newsham şi 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

astfel de proces înglobant ar trebui să includă activităţile susţinute la nivelul autorităţilor publice şi participarea societăţii civile.

Managementul riscurilor, dintr-o perspectivă a rezilienţei, se bazează, în opinia noastră, pe procesul de analiză integrată a tendinţelor identificate în manifestarea ameninţărilor de securitate şi a vulnerabilităţilor în raport cu acestea. Această abordare readuce în atenţie necesitatea identificării propriilor puncte slabe exploatabile în registrul acţional hibrid al unui potenţial adversar. În această abordare, nevoia acută de cunoaştere a viitorului se menţine, dar este mult mai ancorată la prezent, la capacitatea de răspuns a sistemului în raport cu potenţialii factori externi care îi determină evoluţia. Dintr-o perspectivă a rezilienţei, este mult mai facil să stabilim dacă un sistem este fragil în anumite condiţii de mediu specifice (în cazul nostru, de manifestare a unor acţiuni în spectrul hibrid), decât să insistăm prin eforturi sortite apriori eşecului să prospectăm evoluţiile viitoare incerte. În această abordare, trebuie să acceptăm volatilitatea, să înţelgem factorii stresori care afectează/pot afecta propriul sistem şi să identificăm posibilităţi 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 ameninţări care afectează societăţile, devin acum covariante în sensul că afectează simultan mai multe segmente ale acesteia sau chiar comunităţi întregi (iar ameninţările hibride creează astfel de efecte!). Un astfel de efort trebuie să fie interinstituţional şi colaborativ - axat pe consolidarea parteneriatului public-privat şi a dialogului dintre stat şi societate - pentru a putea contribui la reducerea satisfăcătoare a gradului de expunere a statelor-naţiune (şi a diferitelor sisteme fizice şi sociale din cadrul acestora) la diferitele tipuri de acţiuni externe care atentează la securitatea acestora.

4. Gestionarea răspunsului la ameninţări hibride - un posibil cadru de analiză

Elementele teoretice şi practice identificate ne permit să avansăm un posibil cadru analitic util în procesul de gestionarea ameninţărilor hibride. Acest cadru ar putea cuprinde următoarele etape:

- *Pasul 1: Identificarea instrumentelor de putere pe care adversarul le-ar putea folosi în acţiunile asociate războiului hibrid;*

În această etapă a cercetării urmărim analizarea diferitelor instrumente de putere pe care un adversar ar putea să le folosească într-un registru de confruntare hibridă. Considerăm că această analiză este necesară pentru a putea trece mai uşor, ulterior, la evaluarea modului în care aceste instrumente pot fi sincronizate în practică şi descrierea avantajelor şi a efectelor non-lineare ale angajării simultane a mai multor instrumente în raport cu ţinta vizată.

Analiza tiparelor recente de acţiuni hibride - având la bază datele sintetizate în studiul „*Adressing Hybrid Threats*" elaborat cu participarea unor experţi ai *Universităţii Naţionale de Apărare, Centrului de studii a ameninţărilor asimetrice* din Suedia, şi *Centrului European de Excelenţă pentru contracararea ameninţărilor hibride* din Finlanda (studiu la care vom face trimitere în repetate rânduri în continuare) - indică următoarele *tendinţe specifice formelor de manifestare a ameninţărilor din domeniul informaţional şi cibernetic*[10] care se pot regăsi în strategiile integrate ale unui potenţial agresor în cadrul unui scenariu de confruntare hibridă, astfel:

- *utilizarea propagandei ca mijloc prevalent de acţiune.* Asistăm, în prezent, la „o militarizare şi transformare a informaţiei în armă de război"[11]. Ceea ce se observă din acţiunile specifice derulate pe acest palier nu are o legătură cu obiectivele propagandei care, în general, rămân neschimbate şi asociate intenţiei de influenţare a deciziei politice şi a populaţiei statului-ţintă - *centrul de greutate principal al acţiunilor agresorului* - precum şi a populaţiei proprii în vederea legitimării acţiunilor viitoare în raport acesta (imaginea pe care o livrează agresorul propriei audienţe este cea a unui stat în defensivă nevoit să acţioneze în legitimă apărare). Noutatea constă în mijloacele care sunt utilizate în cadrul acţiunilor de propagandă. Tehnologiile *new media* şi *reţelele sociale* reprezintă vectori purtători de agresiuni informaţionale. Acestea sunt utilizabile pentru maximizarea efectelor unei campanii în cadrul unei confruntări hibride. Costul cu exploatarea acestor mijloace nu este atât de mare în raport cu obiectivul strategic propus de destabilizare a adversarului dacă ne gândim doar, prin comparaţie, la limitările (de ordin operaţional) de care dispuneau în perioada Războiului Rece statele care încercau să implanteze o ştire sau un articol într-o publicaţie dintr-un alt stat.

Pentru derularea cu succes a operaţiilor informaţionale trebuie îndeplinite două condiţii:

i. existenţa canalului prin care informaţiile să poată ajunge la ţintele vizate (ex. organisme de presă interne orientate spre publicul străin, sponsorizate de stat şi organizaţii şi platforme de social media);

---

[10] facem precizarea că pentru obiectul de studiu al proiectului nostru de cercetare - care are pune în centru cultura de securitate ca exponent al rezilienţei naţionale la ameninţări hibride - prezintă relevanţă acţiunile în spectru hibrid care ţintesc în primul rând societatea, în ansamblul ei, cu posibile multiple implicaţii în planul securităţii naţionale (ex.: afectarea coeziunii sociale în situaţii de criză pe care le poate traversa la un moment dat statul-şintă, subminarea încrederii populaţiei în instituţiile statului, schimbarea unor percepţii la nivelul populaţiei în raport cu anumite teme sensibile de dezbatere publică etc.)

[11] Iulian Chifu, *PULSUL PLANETEI. Militarizarea şi transformarea informaţiei în armă de război*, articol publicat în publicaţia „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

ii. şi *cunoaşterea în detaliu de către agresor a ţintei vizate*, pentru ca acesta să fie în măsură să-şi dezvolte acele constructe informaţionale care îi aduc avantaje în context hibrid. Aceste constructe pot include, după caz, opinii pe teme sensibile pentru publicul-ţintă vizat, date din scurgeri de informaţii sau publicarea unor *ştiri contrafăcute*[12].

- *controlul asupra unor surse media autohtone aservite şi cu priză la audienţele largi de public, din interiorul şi exteriorul statului cu potenţial agresor.* Mass-media aservite devin foarte influente atunci când materialele pe care le publică sunt preluate de către sursele media populare străine. În studiul la care am făcut trimitere anterior este exemplificat cazul Russia Today şi Sputnik care promovează atât ştiri din actualitatea internaţională cât şi din cea internă dintr-o perspectivă a statului sponsor - în speţă, Federaţia Rusă - servind drept platformă pentru promovarea ideilor şi preferinţele acestuia din urmă, concomitent cu prezentarea într-un registru distorsionat şi tendenţions a politicilor statelor occidentale[13];

- *social media oferă, într-adevăr, noi posibilităţi pentru un potenţial agresor care intenţionează să obţină acces la mass-media şi la publicul larg al ţintelor vizate.* Acţiunile de dezinformare pot fi deosebit de eficiente având în vedere prevalenţa ridicată în rândul publicului larg de a accesa ştiri prin intermediul reţelelor sociale.

Modelele de afaceri pe care funcţionează platformele social media, dar şi publicaţiile media - de asemenea, utilizatori ai reţelelor de socializare - se bazează pe generarea de conţinut în funcţie de preferinţele utilizatorului captiv în „camerele de ecou" - termen folosit pentru a descrie starea de izolare care cuprinde utilizatorul al cărui univers este delimitat de conţinutul consumat şi „persoanele" cu care aceştia împărtăşesc aceleaşi idei şi valori - pentru care platformele social media sunt blamate şi criticate[14]. Platformele social media devin, astfel, adevărate „agregatoare" de ştiri, putând fi utilizate cu uşurinţă pentru promovarea unor ştiri din mass-media ostile sau pentru a publica informaţii noi - prin conturi sponsorizate de stat, reţele de tip bootnet[15], troli sau anunţuri publicitare - care, în acest mod, ajung direct la publicul-ţintă[16]. Aceasta pare să fi fost o trăsătură proeminentă a campaniei de provenienţă rusă în alegerile prezidenţiale din SUA

---

[12] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *op.cit.*, p. 46

[13] Ibidem, p. 47

[14] *** *Facebook în era post-adevărului*, articol disponibil la adresa http://intelligence.sri.ro/facebook-era-post-adevarului/, accesat la data de 02.09.2018

[15] Un botnet reprezintă o reţea de calculatoare infectate (prin exploatarea unor vulnerabilităţi sau prin inginerie socială) cu o aplicaţie malware care permite infractorilor cibernetici să le poată controla de la distanţă, fără ca proprietarii de drept să fie conştienţi de acest lucru.

[16] Ibidem

din anul 2016, când numeroase povestiri provenite din surse media ruse - care au fost raportate mai întâi în Russia Today sau Sputnik - au fost apoi reiterate şi amplificate pe Twitter sau pe Facebook prin intermediul bootnet-urilor şi trolilor, generând algoritmi bazaţi pe tendinţe de consum înşelătoare sau false şi riscul preluării şi popularizării de către sursele media locale[17];

- *utilizarea pe scară largă a ştirilor contrafăcute* în scopul influenţării percepţiei audienţelor-ţintă. *Ştirile contrafăcute* sunt mai mult decât *ştirile false*. Acestea includ informaţii care distorsionează deliberat adevărul obiectiv la nivelul publicului consumator şi urmăresc un obiectiv specific (de obicei, asociat satisfacerii unor interese ostile ale unui actor cu potenţial agresor), spre deosebire de cele din urmă, unde eroarea „involuntară", rezultată din insuficienta documentare jurnalistică, sau maniera de prezentare a conţinutului informaţional atribuie circumstanţe sursei care le-a promovat (care pot varia de la lipsa de profesionalism până la promovarea unor interese derivate din politica editorială).

Difuzarea de *ştiri contrafăcute* se realizează încă prin intermediul canalelor *social media*. Chiar în situaţia în care platformele de socializare îşi vor dezvolta instrumente de verificare a postărilor publicate, eliminarea completă a acestora din conţinut este dificilă, dacă nu chiar imposibilă, din cauza modelului algoritmic după care funcţionează acestea (care permite rostogolirea informaţiei de la un utilizator la altul în funcţie de liberul arbitru al utilizatorului). La fel de puţin probabilă este şi stoparea distribuirii prin reţelele de socializare a materialelor promovate de sursele media mainstream care sunt asociate cu practica ştirilor contrafăcute, câtă vreme acestea dispun de un nivel ridicat de popularitate în rândul utilizatorilor. Devine, astfel, deosebit de problematic dacă *ştirile contrafăcute* vor ajunge să genereze trenduri în *social media* sau să fie preluate şi raportate de alte mass-media în căutarea „senzaţionalului".

- *existenţa unor platforme (ex.: Wikileaks, DCleaks.com) care facilitează publicarea unor date din categoria scurgerilor de informaţii*, obţinute prin acţiuni de spionaj cibernetic (acţiuni de acest gen ar fi fost derulate în procesele electorale recente din SUA şi Franţa)[18]. Este foarte dificilă şi rămâne în sarcina structurilor de securitate specializate să identifice legăturile între aceste platforme şi actorul interesat de publicarea acestor informaţii sensibile şi cu caracter senzaţional, consumatorului final nedispunând decât de măsura precauţiei şi a propriului simţ critic ca instrument de apărare în faţa manipulării.

- *<u>Pasul 2:</u> Evaluarea vulnerabilităţilor;*

[17] Ibidem
[18] Ibidem

În această etapă a cercetării, pornim de la premisa că *în acţiunile de tip hibrid, agresorul nu crează vulnerabilităţile pe care le exploatează.* Prin prezentul raport nu ne propunem să identificăm vulnerabilităţi naţionale la ameninţările hibride (nici n-am avea cum, având în vedere posibilităţile limitate de care dispunem şi faptul că acest exerciţiu cade în sarcina instituţiilor abilitate) ci, mai degrabă, să sugerăm câteva repere, bazate pe contribuţiile din literatură, care ar putea fi utile în acest scop:

- *identificarea funcţiilor critice ale societăţii.* O dimensiune critică este cum şi în ce mod statul este dependent de serviciile digitale şi cât de vulnerabile sunt acestea în faţa agresiunilor cibernetice. Evaluarea, probabil, ar trebui să includă un set relevant de scenarii de ameninţare care pot fi folosite pentru a susţine planificarea pentru apărare. O altă dimensiune poate viza funcţia informativă ;
- *evaluarea dimensiunilor de vulnerabilitate*:
    - *geografică* - proximitatea faţă de sursa potenţială de ameninţare poate amplifica anumite temeri la nivelul societăţii reprezentate de iminenţa unei posibile acţiuni ostile, chiar de natură convenţională/militară, care să pună în pericol securitatea naţională;
    - *socială* - existenţa unor linii de falie în societate, generate de diferenţele de conflictele de opinii între diferitele comunităţi etnice, generaţii, clase sociale, mediu de convieţuire (rural - urban), exploatabile în cadrul campaniilor informaţionale. Un posibil punct de plecare în analiza vulnerabilităţilor naţionale la acţiunile de dezinformare de provenienţă rusă poate fi studiul *„Disinformation Resilience in Central and Eastern Europe”*, realizat cu concursul mai multor centre regionale de analiză[19] şi publicat, la începutul anului 2018, de centrul *The Foreign Policy Council “Ukrainian Prism”*[20].
    - *politică* - orientarea politicii externe a statului şi modificările de percepţie la nivelul electoratului pe acest subiect (europenism - naţionalism); legătura dintre autorităţi şi societate (gradul de încredere al populaţiei în instituţii);
    - *mass-media:* modalitatea în care este consumată informaţia la nivelul societăţii (presa online - radio/televiziune) etc.

- *<u>Pasul 3:</u> identificarea obiectivelor pe care adversarul ar putea să le caute în raport cu vulnerabilităţile existente;*

[19] din România a participat Centrul pentru Studii Europene din cadrul Facultăţii de Drept a Universităţii Alexandru Ioan Cuza din Iaşi.

[20] Studiul este disponibil la adresa http://prismua.org/en/dri/, accesat la data de 23.08.2018

Se realizează în corelaţie cu instrumentele de putere disponibile în registrul acţional împotriva unei ţintei identificate (Acţiunea nu face obiectul prezentului raport. Aceste aspecte pot fi evidenţiate separat, eventual, în conţinutul unui studiul de caz).

- *<u>Pasul 4:</u> calibrarea mijloacelor de răspuns la agresiunile hibride - aplicabilitate pe cultura de securitate*[21]

Relaţia dintre guvern - populaţie în context hibrid este esenţială. Rezilienţa naţională la ameninţări hibride nu implică doar măsurile specifice de răspuns proiectate la nivel instituţional (cum se pregătesc autorităţile să răspundă în cazul unei agresiuni?) ci este un proces înglobant care include toate elementele componente ale unei naţiuni, inclusiv participarea societăţii. Un posibil instrument util pe această dimensiune (un prim model este prezentat în **Tabelul nr. 1**) ar putea fi construirea unei matrici cu acţiunile de promovare sistematică a culturii de securitate ca instrument de consolidare a rezilienţei la ameninţări hibride pornind, eventual, de la ideile cuprinse în *Ghidul de implementare a Strategiei Naţionale de Apărare pentru perioada 2015 - 2019*.

[21] Etapele 3 şi 4 vor fi detaliate în următoarea etapă de cercetare.

Tabelul nr. 1 - *Matricea cu acţiunile de promovare a culturii de securitate ca instrument de consolidare a rezilienţei la ameninţări hibride - MODEL*

	Dimensiunile rezilienţei ***(registrul acţional hibrid)***			
		Rezistenţă	**Adaptare**	**Transformare**
Unitatea de analiză (*nivelul rezilienţei*)	**Instituţii publice**	*Exemplu:* „dezvoltarea unor atitudini şi comportamente necesare apărării şi protecției personale, de grup şi statale față de vulnerabilități, factori de risc, amenințări, stări de pericol sau agresiuni potențiale, precum şi promovarea lor în mediul intern şi internațional de securitate”[22];	*Exemplu:* introducerea conceptului de securitate cibernetică în şcoli elaborarea unui ghid privind ameninţările hibride	*Exemplu:* promovarea ideii şi importanței (asigurării) securității naționale;
	Organizaţii private			
	Comunităţi sociale	- creşterea gradului de cunoaştere asupra particularităţilor ameninţărilor hibride;		

[22] *** *Cum ne apără cultura de securitate*, articol disponibil online la adresa http://intelligence.sri.ro/cum-ne-apara-cultura-de-securitate/, accesat la data de 02.09.2018

BILIOGRAFIE

I. LUCRĂRI DE AUTORI STRĂINI

1. HAMILTON, Daniel (ed.), Forward Resilience, Protecting Society in an Interconnected World, Center for Transatlantic Relations, 2016;

2. McMANUS, Sonia T., Organisational resilience in New Zealand, University of Canterbury, 2008, disponibil la adresa https://resorgs.org.nz/wp-content/uploads/2017/07/organisational-resilience-in-new-zealand.pdf;

3. TALEB, Nicholas Nassim, Antifragile, Random House New York, 2012.

4. WILDAVSKY, Aaron B., Searching for Safety, Piscataway, N.J.: Transaction Publishers, 1988;

II. REVISTE

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 şi DAVIES, Mark , Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes, 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. BONANNO, George A., Clarifying and Extending the Construct of Adult Resilience, American Psychologist, 2005, disponibil la adresa ttps://www.researchgate.net/publication/232434008;

7. 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;

8 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;

III. DOCUMENTE DE REFERINŢĂ

1. *** Comunicatul Summit-ului NATO de la Varşovia din iulie 2016, disponibil la adresa https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf

2. *** 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;

3. *** Declaraţia comună adoptată la Summit-ul NATO de la Varşovia, din 7-8 iulie 2016;

4. *** 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

5. *** National Preparedness Goal, Second Edition, 2015, https://www.fema.gov/national-preparedness-goal;

6. *** Strategic National Framework on Community Resilience, Cabinet office, Marea Britanie, 2011

Autor:

drd. Cristian BĂRBULESCU