RAPORTUL FINAL

privind activitatea de cercetare desfășurată în cadrul Proiectului de cercetare

„Cultura de securitate și reziliența națională la amenințări hibride”

Drd. Cristian BĂRBULESCU

Prezentul raport integrează aspectele rezultate în urma activității de documentare derulată în proiectul intitulat „*Cultura de securitate şi reziliența națională la amenințările hibride*”, în perioada mai - decembrie 2018.

1. Obiective

Obiectivul general pe care l-am asumat în proiectul de cercetare a constat în dezvoltarea unui *cadrul de analiză pentru gestionarea răspunsului la amenințări hibride* care să servească, în ultima etapă a cercetării noastre - prin integrarea tuturor contribuțiilor științifice subsecvente - la definirea unui *model al rezilienței naționale la amenințări hibride prin eforturi sistematice de promovare a culturii de securitate*.

Pe parcursul desfășurării activității de cercetare științifică am urmărit îndeplinirea următoarelor *obiective intermediare*:

- identificarea determinaților de manifestare a *amenințărilor hibride* precum și a particularităților și tiparelor cunoscute utilizate în acțiunile recente de acest tip;
- evaluarea elementelor care descriu relația de complementaritate dintre *reziliență* și *securitatea națională*;
- identificarea unor modele de dezvoltare a *rezilienței* pe diferite dimensiuni (materială, socială, organizațională) și investigarea modalităților în care poate fi abordată teoretic relația dintre *reziliență* și *amenințările hibride*;
- identificarea atributelor esențiale ale *culturii de securitate* în perspectiva integrării acestora *modelul analitic al dezvoltării rezilienței naționale la amenințări hibride*;

Considerăm că aceste obiective au fost atinse, rezultatele întreprinse fiind consemnate în Rapoartele intermediare nr. 1 (iunie) și 2 (septembrie).

2. Livrabile

Rezultatele cercetării întreprinse au fost diseminate în conținutul articolului intitulat *„Reziliența națională la amenințările hibride și cultura de securitate. un cadru de analiză”* (*prezentat în **Anexa nr. 1** la prezentul raport*), elaborat în

coautorat de prof.univ.dr. Teodor Frunzeti și drd. Cristian Bărbulescu, evaluat și acceptat pentru publicare în revista „Impact Startegic”, nr. 1-2 / 2018, a Universității Naționale de Apărare „Carol I”, publicație indexată în BDI (Index Copernicus, Ebsco, Proquest, Ceeol, Road, Oclc WorldCat) și NATO Multimedia Library.

3. Sinteza rezultatelor științifice obținute

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.

Aplicarea noțiunilor de teorie a relațiilor internaționale și teorie generală a războiului pe evoluțiile recente din mediul global și regional de securitate ne permite avansarea unui 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” a informației. 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 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.

Pentru derularea cu succes a operațiilor informaționale trebuie îndeplinite două condiții esențiale[1], 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 parțiale adevărate / false și/sau 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.

- *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. 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.

- *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.

- *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).

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

2) *Evaluarea propriilor vulnerabilități pornind de la premisa că în acțiunile de tip hibrid, agresorul acționează prin exploatarea sensibilităților din interiorul societăților vizate.* 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 planul securității naționale (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.), 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”[2], comportă două dimensiuni interconectate:

- *cunoaștere* – se referă la gradul de informare a populației asupra problemelor de securitate și percepția acesteia asupra amenințării;
- *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.

4. Concluzii și recomandări

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. De aceea abordarea pe care o susținem în gestionarea amenințărilor hibride pune în centru *statul-națiune* cu diferitele sale elemente constitutive - instituții publice, societatea (organizații / entități private, comunități sociale) și infrastructura critică și explicitează dimensiunile pe care trebuie intervenit în proiectarea rezilienței la acțiunile de tip hibrid (*rezistență/continuitate, adaptare/flexibilitate* și *transformare/învățare*).

În noul context de securitate definit de manifestări hibride în conduita actorilor internaționali, *reziliența* și *securitatea* nu sunt concepte incompatibile. În cadrul de analiză pe care îl propunem, *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, într-o abordare „*whole of nation*”.

Complexitatea formelor de manifestare ale *amenințărilor hibride* testează capacitatea de reacție a instituțiilor publice și legătura existentă între societate și autorități. De aceea, în perioada anterioară manifestării amenințării, conștientizarea

[2] 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

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 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 nation*) în formularea măsurilor de răspuns la *amenințările hibride*.

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. 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.

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.

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.

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 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 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 REFERINȚĂ

1. *** Comunicatul Summit-ului NATO de la Varșovia 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 amenințărilor hibride Un răspuns al Uniunii Europene, 2016, disponibil la adresa http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52016JC0018;

3. *** Declarația comună adoptată la Summit-ul NATO de la Varșovia, 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