IMPORTANŢA STRUCTURILOR MILITARE ÎN CONTRACARAREA EFECTELOR RĂZBOIULUI HIBRID

THE IMPORTANCE OF MILITARY STRUCTURES TO COUNTER HIBRID WAR EFFECTS

Lt.col.instr.av. asociat Dragoş Alexandru NECULA*

Mediul de securitate global şi regional este marcat de dificultăţile în contracararea riscurilor şi a ameninţărilor clasice, asimetrice şi hibride. În acest sens, este necesar a se acorda o atenţie deosebită tendinţelor de reconfigurare, pe termen mediu şi lung, a jocurilor geostrategice datorită evenimentelor ce se succed cu repreziciune şi care aduc în faţa noastră provocări ce pleacă de la resurgenţa naţionalismului şi a extremismului, precum şi cele care duc la fragmentarea etnico-religioasă şi la radicalizarea ideologică. Dezvoltarea rapidă a tehnologiei informaţiei a dus la apariţia unor noi riscuri şi ameninţări greu de identificat şi de combătut. Acestea pot duce rapid la atacuri cibernetice ce pot afecta infrastructurile critice, dar pot duce şi la crize energetice.

The global and regional security environment is marked by difficulties în countering classical, asymmetric and hybrid risks and threats. It is necessary to pay a particular attention to the medium and long-term tendencies of the geostrategic games reconfiguration. These successive events bring în front of us challenges that arise from the resurgence of nationalism and extremism ethnic-religious fragmentation and ideological radicalization. The rapid development of information technology led to new risks and threats that are hard to identify and counter. They can quickly lead to cyber attacks that can affect critical infrastructure which can lead to regional and global energy crises.

Cuvinte-cheie: riscuri; ameninţări; vulnerabilităţi; securitate; război hibrid.
***Keywords**: risks; threats; vulnerabilities; security; hybrid war.*

Mediul de securitate din spaţiul Uniunii Europene s-a schimbat în ultimii ani în mod dramatic datorită provocărilor la adresa păcii şi a stabilităţii din vecinătatea estică şi sudică a UE. Aceste ameninţări suscită din partea Uniunii necesitatea de adaptare a capabilităţilor de apărare existente sau crearea unora noi pentru a deveni un furnizor de securitate atât în exteriorul graniţelor cât şi în interiorul acestora. În acest sens, în orientările politice din anul 2014, Comisiei Europene, Jean-Claude Juncker, afirma că trebuie „să depunem eforturi pentru ca Europa să fie mai puternică în materie de securitate şi de apărare”[1].

În acest context, observăm cum incertitudinea mediului de securitate global cumulată cu fluiditatea mediului politic intern şi extern al spaţiului european pot afecta pe termen scurt parcursul României în integrarea deplină a acesteia în Uniunea Europeană şi NATO. Din această cauză se impune identificarea unor noi modalităţi de acţiune care să genereze răspunsuri pe termen mediu şi lung la posibilele turbulenţe interne, regionale şi internaţionale ale mediului de securitate care pot afecta România.

În aceste zile, se observă cum anumiţi actori statali trimit semnale de contestare a prevederilor tratatelor şi înţelegerilor semnate şi asumate anterior ce privesc ordinea internaţională, statutul armelor şi muniţiilor sau desfăşurarea şi staţionarea de forţe şi capacităţi militare. „Punerea sub semnul întrebării a sistemului de valori liberale, derapajele de la normele statului de drept, tendinţele autoritare în exercitarea puterii, exacerbarea discursului naţionalist şi populist determină creşterea instabilităţii regionale şi diminuarea sentimentului de securitate în zonă”[2]. Aceste acţiuni au ca scop final fragmentarea opiniei publice şi pot duce la turbulenţe în anumite spaţii.

Universitatea Naţională de Apărare „Carol I”
e-mail: *gabinec2002@yahoo.com*

Relevant pentru securitatea zonei europene este declaraţia Înaltului Reprezentant al Uniunii pentru Afaceri Externe şi Politică de Securitate, Federica Mogherini, care afirma că: „În ultimii ani, mediul de securitate s-a schimbat dramatic. Am observat intensificarea ameninţărilor hibride la graniţa Uniunii Europene. A existat o solicitare puternică pentru ca Uniunea Europeană să se adapteze şi să-şi consolideze capacităţile de furnizor de securitate. Relaţia dintre securitatea externă şi cea internă trebuie în continuare consolidată. Cu aceste noi propuneri, vrem să intensificăm capacitatea noastră de a contracara ameninţări de natură hibridă. În acest efort, vom face paşi concreţi în cooperarea şi coordonarea noastră cu NATO”[3].

Securitatea naţională se confruntă, în prezent, cu presiunea exercitată de riscurile şi meninţările generate şi/sau alimentate de globalizare, de fenomenele demografice mondiale şi naţionale, de schimbările climatice, de conflictualitatea actorilor statali şi nonstatali din estul şi sudul graniţelor pentru a-şi impune zona de influenţă sau de a avea acces la resursele naturale.

Deşi, la nivel global, un rol important în anticiparea şi prevenirea riscurilor majore de securitate îi revine Organizaţiei Naţiunilor Unite evenimentele ce au loc în prezent ne reliefează faptul că pentru România, Alianţa Nord-Atlantică reprezintă garantul principal al securităţii în contextul în care prin poziţionarea ei pe flancul estic al Alianţei Nord-Atlantice şi al Uniunii Europene este supusă unor riscuri şi ameninţări ce depăşesc posibilităţile proprii de apărare. Avem în vedere aici acţiunile Federaţiei Ruse în regiunea Mării Negre, acţiuni ce au încălcat normele de drept internaţional datorită anexării Crimeii şi conservării conflictelor îngheţate.

În consecinţă, evoluţiile din Vecinătatea Estică a spaţiului european, precum şi cele din Orientul Mijlociul şi Nordul Africii afectează arhitectura europeană de securitate cu implicaţii directe asupra intereselor naţionale de securitate ale României. În acest context, România are obligaţia de a deveni sursa de echilibru strategic din această zonă, dar şi motorul care să genereze un proces de europenizare în spaţiile din afara graniţelor prin exportul de libertate şi securitate care să ducă, în final, la prosperitate şi justiţie socială.

Obligaţiile României în domeniul securităţii pot fi afectate de distorsiunile de pe pieţele energetice, precum şi iniţiativele concurente ale unor potenţiali adversari ce pot fi actori statali sau nonstatali. Aceste acţiuni pot afecta eforturile României de a-şi asigura securitatea energetică.

Este necesar să se acorde o atenţie deosebită ameninţărilor cibernetice ce pot afecta infrastructura informaţională de interes strategic. Ameninţarea teroristă este din ce în ce mai greu de contracarat datorită formelor de manifestare, dar şi din prisma imposibilităţii structurilor responsabile de a identifica şi a destructura reţelele de recrutare şi de finanţare a acestor activităţi. Pentru a putea fi capabilă să îşi asigure apărarea, România este obligată să îşi dezvolte capabilităţi de răspuns eficiente ce pot gestiona provocările de securitate, dar şi să ajute la respectarea angajamentelor asumate prin tratatele internaţionale.

„O Românie puternică în Europa şi în lume înseamnă, în primul rând, un stat care asigură securitatea cetăţenilor săi oriunde s-ar afla ei. Această declaraţie include o multitudine de aspecte. A asigura securitatea cetăţenilor începe cu a-i respecta la ei acasă, a le proteja drepturile şi libertăţile în ţară şi în străinătate, a pune efectiv instituţiile în serviciul cetăţeanului, aşa cum le este menirea, şi continuă cu o dimensiune cât se poate de practică – a le oferi securitate în comunităţile lor, precum şi garanţii juridice şi protecţie diplomatică în afara graniţelor”[4].

Acest deziderat se poate realiza prin ancorarea la realitate şi evaluarea continuă a riscurilor, ameninţărilor şi provocărilor la care este supusă securitatea acestui spaţiu. În *Strategia naţională de apărare a ţării pentru perioada 2015 - 2019 – O Românie puternică în Europa şi în lume* se precizează faptul că securitatea naţională are în componenţa ei dimensiunile apărare, ordine publică, informaţii şi contrainformaţii, educaţie, sănătate, economic, energetic, financiar, mediu şi infrastructuri critice.

Observăm că în securitatea României sunt implicate, pe lângă Ministerul Apărării Naţionale (care este responsabil de dimensiunea de apărare), şi alte structuri. Apărarea Naţională *cuprinde ansamblul de măsuri şi activităţi adoptate şi desfăşurate de statul român în scopul de a garanta suveranitatea naţională, independenţa şi unitatea statului, integritatea teritorială a ţării şi democraţia constituţională.*[5] Prin acest lucru se respectă prevederile din Constituţie, şi anume că: „Armata

este subordonată exclusiv voinţei poporului pentru garantarea suveranităţii, a independenţei şi a unităţii statului, a integrităţii teritoriale a ţării şi a democraţiei constituţionale”[6].

Vom avea în vedere faptul că obiectivul strategic al politicii de apărare îl reprezintă creşterea capacităţii operaţionale a Armatei României, inclusiv prin creşterea capacităţii de decizie şi acţiune a organismului militar prin adaptarea cadrului legislativ, în vederea afirmării intereselor României şi valorificării oportunităţilor la nivel european, euroatlantic şi internaţional[7].

Ministerul Apărării Naţionale este structura de specialitate a administraţiei centrale, care conduce activităţi în domeniul apărării ţării conform legislaţiei în vigoare. Acesta are responsabilitatea să elaboreze concepţia de apărare a ţării şi de a răspunde de punerea ei în aplicare. În interiorul statului român se impune, în cadrul dimensiunii de apărare, derularea unui proces de revizuire al strategiei de apărare care să asigure capabilităţile necesare pentru promovarea şi protejarea intereselor în faţa riscurilor şi ameninţărilor de o mare diversitate ca natură, forme de manifestare, dimensiuni şi caracteristici[8].

Criza din Ucraina este un exemplu care trebuie analizat pentru a identifica lecţiile învăţate şi a lua măsuri în consecinţă. O lecţie învăţată din această criză o reprezintă faptul că formele de manifestare a războiului hibrid sunt multiple şi eficiente. Aşa cum arăta Yevhen Magda[9], într-un interviu la Radio Europa Liberă, pe 17 mai 2016: „Specificul unui război hibrid este că lupta se dă nu pentru teritorii, ci pentru minţile şi atitudinile cetăţenilor altor state, iar mijloacele de luptă sunt foarte sofisticate. De aceea, un război hibrid e o confruntare între state, în care unul din aceste state încearcă să şi-l subordoneze pe celălalt prin diverse mijloace: economice, informaţionale, memoria istorică. Adică este un război în care acţiunile militare nu sunt prioritare, ci doar au rolul de catalizator”.

În consecinţă, războiul hibrid poate fi definit ca o formă de conflict interstatal nedeclarat, care încorporează capabilităţi convenţionale şi neconvenţionale, militare şi nonmilitare, tactici combinate şi acţiuni teroriste, în care actorul statal şi nonstatal agresor urmăreşte explorarea vulnerabilităţilor actorului statal supus agresiunii.

Observăm astfel de ce identificarea riscurilor şi ameninţărilor este foarte importantă şi de aceea se impune o definire clară a acestor noţiuni. În acest sens, noţiunea de risc exprimă, în general, o posibilitate de a te găsi într-o primejdie, de a avea de gestionat un necaz sau de a suporta o pagubă: pericol posibil; termenul derivând din franţuzescul *risque*[10].

Riscul este definit în *Dicţionarul explicativ al limbii române (DEX)* drept un pericol posibil. De asemenea, în acelaşi dicţionar, pericolul este considerat ca fiind o ameninţare [11]. Încercările de determinare matematică a potenţialităţii riscurilor în domeniul securităţii se lovesc de starea anarhică a sistemului relaţiilor interumane şi a relaţiilor internaţionale.

Riscul de securitate poate apărea din cauza unui pericol cunoscut sau bănuit şi care are ca origine fenomene naturale, tehnologice sau umane ce au posibilitatea de a aduce atingere: oamenilor sau colectivităţilor umane şi bunurilor acestora; funcţionării normale a instituţiilor statului şi organizaţiilor statale şi din structura societăţii civile. Toate aceste atingeri au efecte negative asupra securităţii cetăţenilor şi mediului ambiant ducând în cele din urmă la o afectare a indivizilor sau a unor întregi comunităţi umane.

Fiecare risc de securitate are propriile caracteristici şi condiţii de manifestare. În *Ghidul* strategiei naţionale de apărare a ţării pentru perioada 2015-2019 este definită noţiunea de „risc la adresa securităţii naţionale” ca fiind: probabilitatea de producere/manifestare a oricărui eveniment, situaţie, condiţie cu potenţial de manifestare incert, a cărui concretizare ar conduce la afectarea în orice mod a funcţionării normale a instituţiilor statului, a organizării şi funcţionării comunităţilor umane, precum şi a vieţii şi integrităţii fizice a cetăţenilor, într-o împrejurare dată sau context determinat[12].

Ameninţarea poate fi explicată ca fiind un pericol potenţial ce poate fi evidenţiat prin cuvinte sau gesturi prin care autorul are în vedere un scop, obiectiv şi o ţintă. Astfel, ameninţarea are indicatori concreţi prin care se declară intenţia de a răni sau admonesta o persoană, un grup de persoane, o colectivitate sau ţară. În acest sens, ameninţarea de securitate este definită ca un ansamblu de activităţi coerente şi acţiuni importante de origine umană şi/sau naturală ce aduc atingere lipsei de pericol a unei persoane sau a unui grup uman.

Din punct de vedere juridic, *ameninţarea* este definită ca: *infracţiune care constă în alarmarea*

unei persoane, prin manifestarea intenţiei de a săvârşi, faţă de ea sau faţă de o rudă apropiată, o infracţiune sau o faptă păgubitoare[13].

Ameninţările la adresa securităţii pot fi faptele sau stările de fapt în care intră capacităţile, strategiile și intenţiile ce pot aduce atingere valorilor, intereselor și obiectivelor securităţii naţionale ce sunt de natură a afecta direct sau indirect siguranţa naţională prin incapacitatea instituţiilor statului de a funcţiona normal sau afectează viaţa și integritatea fizică a cetăţenilor și a organizării comunităţilor umane[14].

Ameninţarea poate reprezenta o declarare a unei intenţii de a pedepsi sau a aduce atingere integrităţii fizice a unei persoane datorită faptului că aceasta ignoră semnalele transmise privind un posibil necaz, pericol etc.[15]

Apar din ce în ce mai mult, în spaţiul public, informaţii cu privire la riscurile și la ameninţările asimetrice și hibride care sunt greu de contracarat.

Riscurile și ameninţările asimetrice se folosesc cu precădere de către actorii nonstatali de tipul grupărilor teroriste, de gherilă, insurgenţă, sau organizaţii criminalitate organizată pentru a atinge obiectivele propuse folosind metode și proceduri convenţionale, dar mai ales neconvenţionale pentru a-şi maximiza reuşita. Ameninţările asimetrice urmăresc o maximizare a rezultatelor prin valorificarea vulnerabilităţilor unui adversar mai puternic, dar, în acelaşi timp, evitând contactul direct cu acesta.

Atunci când aducem în discuţie noţiunea de *ameninţare hibridă* trebuie avut în vedere faptul că definirea acesteia este flexibilă datorită caracterului evolutiv al proceselor şi al metodelor. Acest concept urmăreşte să aibă ca arie de cuprindere un amestec de activităţi coercitive ce sunt declarate, subversive sau nedeclarate, de instrumente ale puterii ce pot fi convenţionale și neconvenţionale care pot fi utilizate la nivel strategic de actori statali sau coordonat de actori nonstatali pentru a atinge obiectivele propuse dar care rămâne ca nivel de intensitate sub limita declarării oficiale a stării de război.

După cum afirmam anterior, exploatarea vulnerabilităţilor reprezintă pentru actorii statali sau nonstatali obiectivul principal, deoarece se doreşte generarea de distorsiuni în procesul de luare a deciziilor[16]. Noţiunea de ameninţare hibridă fiind foarte volatilă, ea poate îngloba în interiorul ei atacurile cibernetice la adresa sistemelor de informaţii, punerea în pericol a serviciilor financiare şi de furnizare energiei, subminarea încrederii publice în instituţiile guvernamentale prin exploatarea vulnerabilităţilor sociale. De asemenea, ameninţările hibride vizează să lovească adversarul folosind în principal acţiunile neconvenţionale şi într-o mică măsură acţiunile convenţionale.

Diferenţa faţă de ameninţările asimetrice constă în faptul că ameninţările hibride includ pe lângă acţiunile asimetrice şi o combinare a instrumentelor de putere pentru realizarea obiectivelor propuse. Actorii nonstatali ce utilizează astfel de ameninţări apelează, în principal, la metode neconvenţionale, deoarece sunt greu de contracarat de către instituţiile responsabile în domeniul securităţii.

Lumea globală este puternic dependentă de comunicaţiile electronice, iar statele se confruntă din ce în ce mai mult cu vulnerabilităţi ale infrastructurilor critice şi sistemelor informatice. Evenimentele internaţionale în domeniul securităţii ce s-au derulat în ultimii ani au fost reliefate şi în spaţiul virtual. Pe teritoriul naţional, evenimentele pot afecta infrastructurile critice prin acţiuni de criminalitate organizată ce pot escalada datorită creşterii rolului statului român ca generator de securitate regional. Hazardele naturale sunt un alt tip de eveniment şi pot fi datorate fenomenelor sau defecţiunilor tehnice neprevăzute. Aceste defecţiuni pot apărea din cauzapecial uzurii morale a echipamentelor şi neplanificării corecte a activităţilor de mentenanţă. Erorile sau acţiunile umane ce duc la o exploatare deficitară sau la o intruziune neautorizată pot afecta infrastructura critică a statului.

Resursele de care dispun diversele entităţi agresoare în spaţiul cibernetic creează dificultăţi statului român în gestionarea ofensivelor cibernetice. Se observă o intensificare a atacurilor la adresa sistemelor informatice ce au avut un impact major asupra naţiunilor, comunităţilor sau grupurilor din cadrul societăţii.

Recrudescenţa, începând cu anul 2015, a fenomenului terorist din Europa a dus şi la creşterea numărului de atacuri în spaţiul cibernetic pe motive religioase şi de criminalitate organizată. Grupările hacktiviste nu au ocolit România şi astfel s-a semnalat o frecvenţă crescută a atacurilor cibernetice asupra unor sisteme informatice aparţinând unor entităţi publice sau private, precum

instituţii de învăţământ superior şi de administraţie publică care avut drept scop promovarea unor mesaje de propagandă islamistă. Actorii statali sau nonstatali care derulează astfel de acţiuni urmăresc să identifice vulnerabilităţile de securitate pe care nu ezită să le exploateze.

„Un eveniment, aflat şi în atenţia mass-media, s-a derulat în luna ianuarie 2015 şi a avut ca actori principali gruparea de hackeri SECURITY CREWZ ce au lansat atacuri de tip defacement împotriva unor site-uri web ale instituţiilor publice, asociaţii şi societăţi comerciale din România ce au afectat integritatea şi disponibilitatea acestora. Mesajele lansate au fost ideologice pentru susţinerea Califatului. Această grupare de hackeri a lansat 300 de atacuri similare la siturile diferitelor instituţii din Europa, Statele Unite ale Americii şi Emiratele Arabe Unite până în anul 2015”[17].

Acest exemplu ne reliefează faptul că România nu este scutită de astfel de atacuri. Acetea sunt motivele pentru care statele occidentale şi-au sporit considerabil capabilităţile apărării cibernetice pentru a preveni şi combate eficient agresiunile în mediul virtual la adresa infrastructurilor critice, sistemelor de comunicaţii sau organismelor guvernamentale, precum şi la adresa cetăţenilor. În acest sens, dezvoltarea unei strategii pe termen lung vizând dezvoltarea capacităţii defensive a României în acest domeniu devine de o importanţă critică. Până atunci se impune implementarea unor politici de securitate minime pentru sistemele informatice deţinute de autorităţile şi instituţiile publice, dar şi de cele private, precum şi executarea regulată de verificări asupra respectării normelor şi politicilor de securitate din acest domeniu.

Spaţiul media european a fost supus în ultimul timp unor campanii masive de dezinformare. Putem da ca exemplu reportajul prezentat de postul britanic de televiziune Sky News prin care se sugera că România este scena unui trafic intens de armament lucru ce s-a dovedit neadevărat. Modalitatea de transmitere a informaţiilor este diversă, iar în ultimul timp se utilizează platformele de comunicare socială on-line pentru controlul discursului politic sau radicalizare, recrutare şi coordonarea unor actori intermediari ce pot acţiona ca vectori ai ameninţărilor hibride. Un exemplu de radicalizare şi de recrutare de pe platformele social media îl reprezintă cazul lui Luigi Constantin Boicea, elev la Liceul Tehnologic Auto din Craiova, care într-o postare pe un blog, povestea că s-a convertit la Islam şi şi-a luat numele Omar al-Faruq, după ce l-a cunoscut pe un anume Omar Hamadi.

Omar al-Faruq este numele unui fost terorist al-Qaeda, unul dintre locotenenţii lui Osama Bin Laden, care a fost ucis de trupele britanice la Basra, în Irak. De reţinut este faptul că elevul plănuia să îşi ia bacalaureatul şi carnetul de conducere pentru a studia Islamul la Universitatea din Medina, Arabia Saudită. Este important să menţionăm că şi protestele din Piaţa Victoriei de la sfârşitul lunii ianuarie şi începutul lunii februarie 2017 împotriva promulgării Ordonanţei de Urgenţă a Guvernului României nr. 13/2017 pentru modificarea şi completarea Legii nr. 286/2009 privind Codul penal şi a Legii nr. 135/2010 privind Codul de procedura penală poate fi încadrată în aceeaşi categorie a dezinformării şi manipulării.

Platformele de socializare on-line ce au determinat ieşirea în stradă a unui număr mare de manifestanţi au folosit texte manipulatoare alimentând starea de frustrare a populaţiei. Interviurile luate de presă manifestanţilor a demonstrat faptul că aceştia nu cunoşteau ce măsuri anume a luat Guvernul pentru ca populaţia să iasă în stradă în număr atât de mare.

Observăm cum platformele media pot constitui surse de pericol la adresa securităţii statului cu efecte greu de anticipat pe termen lung. Se pune întrebarea: Cum pot fi contracarate aceste pericole fără să fie afectate drepturile şi libertăţile cetăţeneşti stipulate în Constituţia României?

Un alt tip de ameninţare hibridă este şi cel din domeniul economic prin care firme mari în special din ramurile industriale metalurgice şi energetice aparţinând unui actor statal cu interese geostrategice într-o anumită zonă pătrund pe piaţa locală, utilizând mecanismele economiei de piaţă şi cumpără întreprinderile locale ce activează în aceste domenii pe care apoi le falimentează folosind cu bună ştiinţă politici manageriale defectuoase.

Aceste acţiuni pot fi posibile prin exploatarea de către grupuri de influenţă bine pregătite a vulnerabilităţilor din instituţiile responsabile cu activitatea de control şi reglementare. Zonele în care sunt dispuse aceste întreprinderi sunt, de obicei, monoindustriale, iar falimentarea lor aduce pe lângă şomaj şi instabilitate socială din cauza scăderii încrederii populaţiei în instituţiile statului. Spaţiul românesc a fost martorul în ultimii 26 de ani la multe astfel de falimente.

Din multitudinea de exemple doresc să îl supun atenţiei pe cel al rafinăriei RAFO Oneşti care după ce a fost cumpărată de compania rusă Petrochemical Holding a ajuns în situaţia de a fi vândută la fiare vechi.

În spaţiul diplomatic se observă cum ambasadori acreditaţi într-un anumit stat derulează cu intenţie sau fără intenţie acţiuni ce servesc intereselor altui stat în acea zonă. Este cazul ambasadorului american acreditat în Republica Moldova care afirma că unirea Moldovei cu România „nu este o alegere practică şi aceasta nu ar face lucrurile mai bune. (...) Moldova nu e România, are propria istorie şi este o ţară multietnică cu oameni care vorbesc limbi diferite şi, desigur, mai este şi problema transnistreană, care nici măcar nu este sub controlul guvernului central, dar care are nevoie de un statut special...”.

Acest tip de abordare diplomatică chiar dacă a fost combătut de ambele state româneşti se aseamănă foarte mult cu discursul diplomaţiei Federaţiei Ruse privitor la această zonă. Harta Moldovei „istorice” rezultată în urma Păcii de la Bucureşti din 1812 a fost cadoul primit de preşedintele Republicii Moldova, Igor Dodon, de la omologul său din Federaţia Rusă, Vladimir Putin, în cadrul vizitei oficiale din ianuarie 2017, la Kremlin, reprezentând un exemplu al modului de acţiune al Federaţiei Ruse.

Se pune întrebarea: Cum pot fi contracarate astfel de ameninţări hibride în spaţiul naţional şi european?

În opinia mea, un prim pas ar fi elaborarea unor noi politici publice[18] naţionale de securitate şi apărare, precum şi respectul faţă de lege. Responsabilitatea pentru măsurile de contracarare revin în totalitate instituţiilor naţionale cu responsabilităţi în domeniile de securitate şi apărare. Aceste instituţii au resursele umane, tehnice şi financiare care să le permită identificarea vulnerabilităţilor cu care se confruntă România în acest domeniu şi uneltele care să le permită luarea măsurilor de contracarare necesare. România este obligată să elaboreze politici pentru contracararea ameninţărilor hibride şi de a ameliora rezilienţa lor atunci când se confruntă cu aceste ameninţări, corelând instrumentele puse la dispoziţie de instituţiile europene cu cele naţionale.

O privire retrospectivă a spaţiului european scoate în evidenţă faptul că multe dintre statele membre se confruntă cu ameninţări comune la adresa reţelelor şi a infrastructurilor critice naţionale dar care sunt interconectate şi pot avea efecte distructive transnaţionale. Din această cauză se impune ca ameninţările să fie abordate integrat în cadrul instituţiilor europene pentru a se stabili politici comune eficiente de contracarare. Solidaritatea europeană la care se face referire în Tratatului de la Lisabona are rolul definitoriu, iar asistenţa reciprocă maximizează şansele de reuşită.

În România se impune realizarea unor cercetări care să identifice domeniile vulnerabile la ameninţările hibride şi să creioneze mecanismele de avertizare timpurie. Acest lucru ar permite statului prin instituţiile specializate să identifice ameninţările hibride şi să ia măsuri în consecinţă.

Comisia Europeană sprijină statele membre în realizarea studiilor privind ameninţările hibride şi vulnerabilităţile la aceste ameninţări prin stabilirea unor indicatori specifici ce pot afecta structurile şi reţelele naţionale sau paneuropene. S-a convenit de asemenea realizarea unei cooperări între UE şi NATO pentru a contracara ameninţările hibride. Cele două entităţi vor conlucra în domeniul analizei, prevenţiei şi detectării situaţiilor de iminent pericol. Ameninţările hibride vor fi preîntâmpinate prin intermediul schimbului de informaţii şi intelligence între staffuri şi prin cooperarea în dimensiunea comunicării strategice ce se vor face prin proceduri de coordonare.

La nivelul factorilor de decizie din România este necesară o conştientizare a situaţiei astfel încât orice schimare a mediului de securitate să fie atent monitorizată pentru a identifica eventualele acţiuni hibride derulate de diverşi actori statali sau nonstatali. Orice inflamare a opiniei publice naţionale poate degenera şi duce la o stare de instabilitate a acestei regiuni de care ar putea beneficia entităţi ostile statului român. În acest sens este important a se îmbunătăţi schimburile de informaţii dintre instituţiile publice cu atribuţii în domeniul securităţii şi apărării, dar şi cu instituţiile internaţionale ale UE şi NATO.

Informaţiile obţinute vor trebui distribuite factorilor politici decidenţi pentru a lua măsuri eficiente de contracarare şi de ce nu de contraofensivă care să îndepărteze pericolul de spaţiul românesc şi european. Liderii europeni au înţeles gravitatea acestor ameninţări ce planează asupra spaţiului demarând procedurile de înfiinţare a unei celule

de fuziune împotriva ameninţărilor hibride[19], care să îşi desfăşoare activitatea în cadrul Centrului de analiză a informaţiilor al UE (INTCEN UE). Acest centru urmează să fie parte a Serviciului European de Acţiune Externă (SEAE) cu atribuţii în analiza ameninţărilor hibride. Analiza informaţiilor privind ameninţările hibride se va realiza prin schimb de informaţii între structurile naţionale şi din surse deschise.

La nivel naţional se impune înfiinţarea unei astfel de celule de fuziune care să aibă ca principală misiune analiza ameninţărilor hibride interne şi externe care pot afecta spaţiul naţional şi european.

Această celulă de fuziune este foarte importantă, deoarece contribuie prin produsele pe care le furnizează la fundamentarea deciziilor strategice la nivel naţional, precum şi a celor la nivelul NATO şi UE.

Observăm cum pe diverse platforme media sunt lansate campanii de presă despre un anumit subiect şi care se dovedesc în final false. Aceste campanii de presă au menirea de a radicaliza societatea în vederea destabilizării acesteia şi de a controla discursul public. Apare nevoia la nivelul structurilor de decizie din societatea românească de operaţionalizare a unor capabilităţi responsabile de comunicarea strategică.

În cadrul instituţiilor, comunicarea strategică poate oferi informaţiile oficiale cu privire la unele activităţi menţinând opinia publică informată. „Comunicarea strategică implică existenţa relaţiei cauză-efect între activitatea de comunicare şi obiectivele de îndeplinit ale instituţiei publice. Putem afirma că programele de comunicare sunt o parte importantă în realizarea activităţilor la nivel strategic într-o manieră cuantificabilă”[20].

Este esenţial în acest moment să utilizăm diferite modalităţi de comunicare strategică pentru a răspunde ameninţărilor hibride. Acţiunile de răspuns implică teme concrete de informare şi conştientizare a opiniei publice în ceea ce priveşte pericolul ameninţărilor hibride.

Comunicarea ce se derulează în acest mod contribuie la consolidarea rezilienţei la diverşi factori perturbatori. Mijloacele de transmitere a mesajelor vor trebui să ia în calcul platformele de comunicare socială pe lângă cele deja consacrate precum cele vizuale, audio şi on-line. Instituţiile statului român au obligaţia să dezvolte proceduri de comunicare strategică necesare în operaţiile de contracarare a dezinformării şi pentru identificarea codului sursă al acesteia. Pentru realizarea acestui deziderat este necesar a se optimiza serviciile oferite de către specialiştii în domeniul monitorizării mass-media şi în domeniul lingvistic.

Experienţa fiecărui stat membru NATO şi UE în domeniul ameninţărilor hibride poate fi fructificată prin crearea la nivelul celor două structuri a unor centre de excelenţă pentru „contracararea ameninţărilor hibride”, iar fiecare stat membru să creeze la nivel naţional propriile centre care să înglobeze analizele ce provin de la structurile cu responsabilităţi în domeniul securităţii şi apărării. Un astfel de centru ar fi util în România deoarece ar putea cerceta modul cum s-au aplicat diferitele strategii hibride în anumite spaţii şi ar putea dezvolta reziliența statului la astfel acţiuni. Este important ca acest centru să fie în permanenţă în contact cu societatea civilă și să încurajeze dezvoltarea de noi concepte şi tehnologii care să poată fi utilizate cu succes. Cercetarea în acest domeniu nu ar trebui uitată şi de aceea este necesar a fi cooptat în această activitate personal specializat din mediul civil şi militar, precum şi din mediul academic şi al diverselor sectoare de activitate.

Acest lucru este important, deoarece poate contribui la corelarea politicilor, doctrinelor şi conceptelor naţionale şi internaţionale într-o concepţie unitară. Aşa cum afirmam anterior definirea noţiunii de ameninţare hibridă este flexibilă şi datorită complexităţii şi ambiguităţii specifice. În acest sens, procesul de luare a deciziilor este necesar a ţine seama de aceste realităţi. Programele de cercetare în zona ameninţărilor hibride pot conduce la identificare soluţiilor şi la dezvoltarea unor capabilităţi cu dublă aplicabilitate civilă şi militară. Punerea în aplicare a acestor programe va asigura creşterea rezilienţei sociale şi instituţionale.

Reziliența socială este definită ca abilitatea unui grup sau comunităţi de a face faţă tensiunilor interne și externe generate ca urmare a schimbărilor de ordin social, economic, politic sau ale mediului[21]. În acest sens, apare nevoia ca și instituţiile statului să fie reziliente.

Reziliența instituţională reprezintă capacitatea instituţiei de a se pregăti să reziste și să își revină după producerea unor dezastre majore sau din alte circumstanţe şi care, în mod excepţional, o împiedică parţial sau total să-şi deruleze activităţile curente[22].

În acest sens, apare nevoia ca și instituțiile statului să fie reziliente.

Contracararea eficientă a amenințărilor hibride nu se poate face decât prin identificarea vulnerabilităţilor și implementarea politicilor care să permită înlăturarea acestora sau cel puţin de reducere ca intensitate.

În *Dicţionarul explicativ al limbii române*, noţiunea de „vulnerabil” este definită ca ceva ce poate fi rănit, care poate fi atacat uşor, care are părţi slabe defectuoase, criticabile.[23]

„Vulnerabilităţile sunt consecinţe ale unor disfuncţii ori deficienţe sistemice, care pot fi exploatate sau pot contribui la materializarea unei ameninţări sau a unui risc” [24].

În *Strategia naţională de apărare „Pentru o Românie care garantează securitatea și prosperitatea generaţiilor viitoare”*, din 2010, vulnerabilităţile sunt definite ca factori din interiorul societăţii ce potenţează acţiunea ameninţărilor[25].

Vulnerabilitatea la adresa securităţii naţionale se caracterizează printr-o deficienţă funcţională sau sistemică. Această deficienţă poate fi utilizată pentru crearea unei ameninţări sau risc fapt ce poate conduce la o slăbire a capacităţii instituţiilor statului de a diminua impactul unor evenimente ce pot afecta funcţionarea normală a societăţii[26].

Vulnerabilitatea poate fi definită ca*: o slăbiciune sau o breșă într-un sistem de securitate ce poate fi exploatată prin ameninţări pentru a obţine acces neautorizat la o anumită instituţie*[27].

România are posibilitatea să valorifice instrumentele și politicile UE și NATO în acest domeniu pentru a deveni mai rezilientă la amenințările hibride. Vom avea în vedere ca o primă măsură să fie protejarea infrastructurilor critice, deoarece orice atac neconvenţional al unor actori statali sau nonstatali asupra acestora duc la efecte greu de cuantificat în plan economic și social.

„Programul european pentru protecţia infrastructurilor critice (PEPIC)” oferă pentru protecţia infrastructurilor critice o abordare intersectorială ce vizează pericolele din cadrul diverselor sisteme în totalitatea lor axându-se pe interdependenţele instituţionale. O atenţie deosebită se acordă pregătirii, prevenirii și răspunsului eficient. În *Directiva privind infrastructurile critice europene* este stabilită procedura care permite identificarea infrastructurilor critice la nivel european (ICE), dar și modalitatea de evaluare a nevoilor de îmbunătăţire a protejării acestora”[28].

La nivel naţional apare necesitatea intensificării acţiunilor în ceea ce priveşte protecţia infrastructurilor critice. Acest deziderat se poate realiza printr-o cooperare și diseminare de informaţii între instituţiile statului român și cele europene.

În ceea ce priveşte informaţiile sensibile ce se vor disemina către operatorii economici şi populaţie, acest lucru se poate face numai după o analiză aprofundată a impactului.

Domeniul managementului situaţiilor de criză impune ca la nivel instituţional să se optimizeze cooperarea pentru ca în final să ducă la un parteneriat eficient între sectorul public și cel privat pentru protecţia infrastructurilor critice.

Este necesar a fi elaborate studii care să analizeze impactul acţiunilor hibride asupra infrastructurilor critice. Aceste studii vor fi dezvoltate pe direcţiile ce vor viza elaborarea unor instrumente comune ce permit identificarea şi monitorizarea permanentă a riscurilor, a ameninţărilor şi a vulnerabilităţilor infrastructurilor critice.

Se impune dezvoltarea cooperării dintre autorităţile cu atribuţii în administrarea infrastructurilor critice naţionale şi europene prin operaţionalizarea unor puncte de contact permanent.

Calitatea de membru cu drepturi depline în UE reclamă din partea statului român elaborarea procedurilor pentru realizarea fluxului informaţional de expertiză, care să aibă ca finalitate schimburi de informaţii, în timp real, cu instituţiile responsabile la nivel european, dar și cu statele membre și partenere ale UE și NATO. Procedurile necesare realizării fluxurilor informaţionale se elaborează pe baza unei legislaţii adaptate la noile condiţii de securitate.

Reţelele de distribuţie a energiei sunt de o importanţă deosebită pentru fiecare stat, iar întreruperile alimentării cu energie cauzează pagube greu de cuantificat. UE este obligată ca prin structurile sale să dezvolte strategia privind uniunea energetică prin care să identifice noi furnizori de energie, noi rute de transport și de distribuţie a acesteia.

S-au făcut paşi importanţi în această direcţie, un exemplu în acest sens îl reprezintă proiectul de operaţionalizare a coridorului sudic prin care sursele de energie din Marea Caspică sunt transportate în spaţiul european evitând, în acest mod, dependenţa de Federaţia Rusă. Cunoaştem faptul că acest stat

nu ezită să folosească şantajul energetic atunci când doreşte să-şi impună voinţa în anumite dosare.

Materialele şi instalaţiile nucleare sunt infrastructuri critice obligatoriu a fi protejate în vederea creşterii rezilienţei. Sunt luate, la nivel naţional şi internaţional, măsuri de siguranţă suplimentară pentru prevenirea şi diminuarea consecinţelor accidentelor de natură nucleară. Au fost elaborate, la nivel european, norme ce trebuie aplicate şi urmate în domeniul situaţiilor de urgenţă de către toate statele membre ce au scopul de a îmbunătăţi cooperarea şi a eficientiza răspunsul. Infrastructura de transport este esenţială pentru funcţionarea statului, iar atacurile hibride pot perturba grav lanţurile de aprovizionare şi transporturile de persoane.

Înfiinţarea unor capabilităţi comune în cadrul UE este o preocupare permanentă a factorilor politici. În acest sens, pentru îmbunătăţirea infrastructurii de transport europene au fost alocate pentru perioada 2014-2020 resurse financiare în valoare de 26 de miliarde de euro pentru dezvoltarea unei reţele centrale de transport ce va elimina blocajele din sistem. Prin această infrastructură se doreşte o simplificare a operaţiunilor transfrontaliere de transport europene (avem în vedere atât transportul de marfă, cât şi cel de călători).

În cadrul reţelei centrale de transport vor fi dezvoltate nouă coridoare de transport care au ca obiectiv interconectarea statelor membre pentru gestionarea eficientă a resurselor limitate. Se doreşte ca până în 2050, toţi cetăţenii spaţiului european şi societăţile comerciale să fie dispuşi la cel mult 30 de minute de reţeaua centrală[29].

Politicile la nivelul UE în domeniul infrastructurii de transport pot fi influenţate de ameninţările hibride ale actorilor statali şi nonstatali ce nu au interese ca această infrastructură să devină operaţională. Se impune astfel o abordare întrunită a domeniului securităţii infrastructurilor de transport pentru a contracara eficient ameninţările şi riscurile hibride. Acest deziderat se poate realiza prin creşterea disponibilităţii instituţiilor din statele membre la cooperare intersectorială atât între actorii civili, cât şi cu cei militari. Finalitatea dorită fiind protejarea infrastructurii.

Strategia şi planul de acţiune pentru aprovizionare abordează problemele ce ţin de securitatea lanţului de aprovizionare şi de gestionare a riscurilor vamale în spaţiul european.

La nivel european, politicile în domeniul infrastructurii de transport prevăd realizarea unei reţele europene integrate la nivelul tuturor statelor membre. Aceste politici au scopul de a promova creşterea economică şi competitivitatea prin realizarea legăturilor între vest şi est.

Dezvoltarea acestei reţele este prevăzută a se realiza corelat, pe două paliere: o reţea centrală, formată din cele mai importante rute şi noduri de transport ce va constitui elementul central al infrastructurii de transport în cadrul pieţei unice a Europei, având termen de finalizare anul 2030 şi o reţea extinsă/globală care va susţine reţeaua centrală, având termen de finalizare 2050[30].

Concluzionând, se poate afirma că această reţea de transport oferă soluţii viabile în ceea ce priveşte siguranţa şi durata călătoriilor.

Avem în vedere faptul că ameninţările hibride pot viza şi infrastructurile spaţiale, iar orice disfuncţionalitate în aceste infrastructuri poate genera efecte în multe sectoare. În acest sens, pentru protejarea acestor infrastructuri este necesar a se implementa politicile de supraveghere şi de urmărire spaţială prin care utilizatorii să fie uşor de identificat. Prin utilizatori avem în vedere statele membre, instituţiile internaţionale, proprietarii şi utilizatorii de sateliţi şi nave spaţiale precum şi autorităţile de protecţie civilă. În acest moment, comunicaţiile prin satelit reprezintă o parte importantă din gestionarea situaţiilor de criză şi a celor de urgenţă, precum şi pentru supravegherea frontierelor. Observăm cum această infrastructură este o parte importantă a transporturilor spaţiale viitoare a aeronavelor pilotate de la distanţă.

În concluzie, pentru a ne proteja împotriva ameninţărilor hibride este necesar ca pe lângă instituţiile abilitate ale statului cu responsabilităţi în domeniul securităţii să fie implicat şi sectorul privat sau societatea civilă. Sectorul privat poate fi stimulat să dezvolte activităţile sociale şi economice prin asigurarea locurilor de muncă bine plătite pentru cetăţeni care astfel scapă de grija zilei de mâine şi pot duce la o dezvoltare a societăţii pe baze solide. Pe de altă parte, societatea civilă, prin organizaţiile sale cu vocaţie securizară au obligaţia de a atrage cetăţenii şi de a-i implica la „construcţia” securităţii naţionale.

Fără o implicare a tuturor actorilor naţionali în contracararea ameninţărilor hibride nu se va putea realiza o dezvoltare sustenabilă a societăţilor din spaţiul euroatlantic.

NOTE:

1 Jean-Claude Juncker, *Un nou început pentru Europa: Agenda mea pentru locuri de muncă, creştere, echitate şi schimbări democratice*, Strasbourg, 15 iulie 2014, http://ec.europa.eu/priorities/sites/beta-political/files/pg_ro. pdf, accesat la 12.09.2016.

2 Administraţia prezidenţială, *Strategia naţională de apărare a ţării pentru perioada 2015 - 2019. O Românie puternică în Europa şi în lume*, Bucureşti, 2015, http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf, accesat la 12.09.2016.

3 Robert Lupitu, *Comisia Europeană şi Înaltul Reprezentant UE vor aplicarea clauzei de apărare reciprocă în cazul unor atacuri hibride puternice. Cum vrea UE să devină un furnizor de securitate şi să coopereze cu NATO,* http://www.caleaeuropeana.ro, accesat la 15.09.2016.

4 Administraţia prezidenţială, *Strategia naţională de apărare a ţării pentru perioada 2015 - 2019. O Românie puternică în Europa şi în lume*, Bucureşti, 2015, http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf, accesat la 12.09.2016.

5 *Legea apărării naţionale a României nr. 45/1994*, http://lege5.ro/Gratuit/he2tgmy/legea-apararii-nationale-a-romaniei-nr-45-1994, accesat la 12.09.2016.

6 *Constituţia României*, Art. 118, http://www.ucv.ro/pdf/site/constitutia_romaniei.pdf accesat la12.09.2016.

7 *Document sinteză privind politicile şi programele bugetare pe termen mediu pentru anul 2016 şi perspectivă 2017-2019*, http://www.cdep.ro/pdfs/buget/2016/Anexa%203/ Ministerul%20Apararii%20Nationale.pdf, accesat la 12.09.2016.

8 *Carta albă a apărării* din 11.04.2016, http://lege5.ro/Gratuit/geydkojqgiza/carta-alba-a-apararii-din-11042016, accesat la 12.09.2016.

9 Magda Yevhen, profesor universitar şi analist politic ucrainean, autor al cărţii „Războiul Hibrid”.

10 Aron Liviu Deac, Ion Irimia, *Securitatea României la răscruce de milenii – aspecte politico-militare,* Editura AISM, Bucureşti, 2000, p. 21.

11 *Definiţia riscului*, http://dexonline.ro/definitie/risc, accesat la 12.04.2017.

12 Administraţia Prezidenţială, *Ghidul strategiei naţionale de apărare a ţării pentru perioada 2015-2019,* Bucureşti, 2015, p. 9.

13 *Ibidem.*

14 Administraţia Prezidenţială, *Ghidul strategiei naţionale de apărare a ţării pentru perioada 2015-2019,* Bucureşti, 2015, p. 7.

15 *OXFORD Dictionary of Current English,* Oxford University Press, 1988, Second Edition by Christina Ruse.

16 European Commission – Fact Sheet, http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm, accesat la 12.09.2016.

17 http://www.sri.ro/romania-a-fost-tinta-unor-atacuri-cibernetice.html, accesat la 14.09.2016.

18 „O politică publică este o reţea de decizii legate între ele privind alegerea obiectivelor, a mijloacelor şi resurselor alocate pentru atingerea lor (n.n. – a obiectivelor) în situaţii specifice”, A. Miroiu, *Introducere în analiza politicilor publice*, Editura Paideia, Bucureşti, 2001, p. 9.

19 European Commission – Fact Sheet, http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm, accesat la 14.09.2016.

20 L.R. Potter, *The Ten-Step Strategic Communication Plan*, 1999 Yearbook of Global Communication, Madrid, Spain, October, 1998, p. 14.

21 http://rezilienta.ro/rezilienta, accesat la 15.09.2016.

22 *Ibidem*.

23 https://dexonline.ro/definitie/vulnerabil

24 *Strategia de apărare a ţării pentru perioada 2015-2019 – O Românie puternică în Europa şi în lume*, Bucureşti, 2015, p. 14.

25 *Strategia naţională de apărare „Pentru o Românie care garantează securitatea şi prosperitatea generaţiilor viitoare”*, Bucureşti, 2010, p. 13.

26 Administraţia Prezidenţială, *Ghidul strategiei naţionale de apărare a ţării pentru perioada 2015-2019,* Bucureşti, 2015, p. 10.

27 http://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/ accesat la 15.09.2016.

28 European Commission, *Joint communication to the European Parliament and the council, Joint framework on countering hybrid threats a European Union response*, Brussels, 2016, p. 6.

29 http://ec.europa.eu/romania/news/11092014 _politica_ue_privind_infrastructura_de_transport_ro.htm, accesat la 19.09.2016.

30 *Programul Operaţional Infrastructură Mare 2014-2020*, http://www.mmediu.ro/app/webroot/uploads/files/2014-11-28_Anexa9.pdf, accesat la 19.09.2016.

BIBLIOGRAFIE

*** *Legea apărării naţionale a României nr. 45/1994*.

*** *Carta albă a apărării* din 11.04.2016, http://lege5.ro/Gratuit/geydkojqgiza/carta-alba-a-apararii-din-11042016.

*** *OXFORD Dictionary of Current English,* Oxford University Press, 1988, Second Edition by Christina Ruse.

Administraţia Prezidenţială, *Ghidul strategiei naţionale de apărare a ţării pentru perioada 2015-2019,* Bucureşti, 2015.

Deac Aron Liviu, Irimia Ion, *Securitatea României la răscruce de milenii – aspecte politico-militare,* Editura AISM, Bucureşti, 2000.

Lupitu Robert, *Comisia Europeană şi Înaltul Reprezentant UE vor aplicarea clauzei de apărare reciprocă în cazul unor atacuri hibride puternice. Cum vrea UE să devină un furnizor de securitate şi să coopereze cu NATO*, http://www.caleaeuropeana.ro

Miroiu A., *Introducere în analiza politicilor publice*, Editura Paideia, Bucureşti, 2001.

Potter L.R., *The Ten-Step Strategic Communication Plan*, 1999 Yearbook of Global Communication, Madrid, Spain, October, 1998.

http://www.caleaeuropeana.ro

http://ec.europa.eu/priorities/sites/beta-political/files/pg_ro. pdf

http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf

http://lege5.ro/Gratuit/he2tgmy/legea-apararii-nationale-a-romaniei-nr-45-1994

http://www.ucv.ro/pdf/site/constitutia_romaniei.pdf accesat la:12.09.2016

http://www.cdep.ro/pdfs/buget/2016/Anexa%203/Ministerul%20Apararii%20Nationale.pdf

http://dexonline.ro

http://rezilienta.ro/rezilienta

http://www.mmediu.ro/app/webroot/uploads/files/2014-11-28_Anexa9.pdf