Miruna-Maria COCOLAN[*]
Cristina-Georgiana IVAN[**]

TRANSFORMAREA SECURITĂȚII ÎN SECOLUL XXI. IMPACTUL ASUPRA INFRASTRUCTURILOR CRITICE

Security Transformation in the 21st century. The Impact on Critical Infrastructures

***Abstract**: The 21st century can be defined by the increase in asymmetric threats to global security, in direct relationship with the technological progress and the development of virtual networks. The unprecedented level of technological evolution has led to a society change. The virtual space has an important influence on human behaviour, but it also generates a shift in the area of risks and vulnerabilities. Can we say that nowadays the threats to security have changed deeply or should we say that they have evolved? In the knowledge society, security suffers a continuous development. Due to technological advances, the traditional threats have gained new faces. Conflicts have become asymmetric, and threats have become transnational. Modernity, through integrated technological systems, leads to more efficient social processes. The problem is that the dependency on information systems increases the probability of an attack on critical infrastructures.*

***Keywords:** security, traditional threats, asymmetric threats, technological progress, modernity, critical infrastructures, vulnerabilities.*

* * *

Introducere

Statul națiune a fost, pentru mult timp, unicul subiect al conceptului de *securitate*. În prezent însă, contextul internațional s-a modificat, frontierele excedând granițele statelor. De la amenințările tradiționale, care afectau statul-națiune, accentul s-a deplasat spre amenințările transnaționale. Extinderea amenințărilor se datorează caracterului

[*] Ph.D. Candidate, Doctoral School of Sociology, University of Bucharest, Romania; cocolan.miruna@yahoo.com.
[**] Ph.D. Candidate, Doctoral School of Sociology, University of Bucharest, Romania; Research Assistant, Institute of Political Sciences and International Relations, Romanian Academy; cristinaivan9@yahoo.com.

Date submitted: 23 May 2015
Revised version submitted: 18 June 2015
Accepted: 16 August 2015

asimetric al conflictelor din secolul XXI, caracter care este conferit atât de asimetria resurselor utilizate, de caracteristicile valorilor atacate, cât şi de tipologia atacatorilor.

Lucrarea de faţă realizează o analiză succintă a mediului de securitate, respectiv relaţia ameninţări tradiţionale - ameninţări transnaţionale în contextul asimetriei conflictelor, punând însă accent pe implicaţiile acestui proces pentru un element strategic al statului: infrastructurile critice naţionale. Dezvoltarea tehnologică, pe lângă multitudinea de beneficii aduse progresului naţiunilor, include o serie de dezavantaje, facilitând complexitatea atacurilor cibernetice şi făcând infrastructurile critice ale unui stat din ce în ce mai vulnerabile.

Pentru a înţelege rolul infrastructurilor în cadrul statului, precum şi raţiunea în virtutea căreia acestea sunt considerate un element critic, în prezentul studiu va fi reliefată emergenţa acestora şi importanţa lor din punct de vedere al securităţii naţionale. În acest sens, considerăm utilă trecerea în revistă atât a abordărilor NATO şi UE, cât şi perspectiva României asupra problematicii analizate.

Scopul lucrării este ca, în final, să fie înţeles impactul conflictelor asimetrice, respectiv al dezvoltării tehnologice, asupra infrastructurilor critice. Astfel, în urma analizei legislaţiei în domeniu, vor fi reliefate principalele ameninţări asupra infrastructurilor critice, precum şi necesitatea existenţei unui cadru legislativ funcţional de prevenire şi anticipare a acestora. Nu în ultimul rând, vor fi avute în vedere o serie de modalităţi de protecţie a elementului strategic pe care infrastructurile critice îl reprezintă în societatea globalizată.

1. De la ameninţări tradiţionale la ameninţări asimetrice

Conform lui Arnold Wolfers „securitatea, în sens obiectiv, măsoară absenţa ameninţărilor la adresa valorilor dobândite, iar într-un sens subiectiv, absenţa temerii că asemenea valori vor fi atacate”[1]. Întrucât ameninţările la adresa securităţii naţionale sunt diversificate, când vorbim de subiectul conceptului de *securitate* nu mai putem lua în calcul doar statul-naţiune.

În prezent, provocarea majoră este dată de diversificarea pericolelor la adresa securităţii naţionale. Nu putem vorbi despre o modificare a ameninţărilor în esenţa lor, ci mai precis despre o extindere a acestora. La ameninţările clasice, fundamentale în luarea unei decizii de politică internaţională, se adaugă noi domenii de interes strategic, precum ameninţări cibernetice, securitatea mediului, crize economice, activităţi teroriste ori siguranţă alimentară.

[1] Vezi date suplimentare la: Institutul de Politici Publice, *Informational brief for journalists.Concept of security. Security sector*: 1; http://www.ipp.md/public/files/Proiecte/Info_Brief_no._1_-_Concept_of_Security._Security_Sector.pdf, [Accesat la data de 20.03.2015].

Globalizarea aduce cu sine un flux abundent de informaţii, disponibile în timp real, ceea ce face greu de identificat într-o perioadă scurtă de timp informaţiile relevante din prisma securităţii naţionale. În era cunoaşterii, accesul la mijloacele de comunicare este neîngrădit. Astfel, intenţiile adversarilor sunt mult mai greu de identificat, acţiunile potrivnice statului pot fi puse la cale în timp real, într-o manieră conspirată, atacatorii aflându-se sub protecţia anonimatului ori a identităţilor false. Totodată, accesul neîngrădit la mediile de comunicare diversificate presupune şi posibilitatea desfăşurării unor activităţi de propagandă, de intoxicare ori de atragere la înfăptuirea unor activităţi contrare principiilor securităţii naţionale.

Activitatea de spionaj se realizează din ce în ce mai des prin mijloace tehnologice, fiind mult mai greu de identificat şi de probat. Atacurile cibernetice sunt tot mai frecvente, în spaţiul virtual fiind realizate şi activităţi de terorism ori conexe acestora.

Dezvoltarea mijloacelor de comunicare şi constituirea unor comunităţi virtuale într-un spaţiu cibernetic lipsit de frontiere, a generat o nouă dimensiune de putere şi un nou câmp de luptă. Odată cu evoluţia noilor mijloace media, platformele de socializare online au permis facilitarea interacţiunilor între oameni. Revoluţiile Twitter şi Facebook şi-au pus amprenta asupra modului în care se pot coagula grupuri de indivizi, prin intermediul internetului, în scopul planificării unor acţiuni de destabilizare a puterii de stat.

În acest context, putem menţiona importanţa infrastructurilor critice ale unui stat, necesar a fi protejate, întrucât orice ameninţare la adresa acestora, dacă este materializată, aduce atingere desfăşurării în condiţii de funcţionalitate a vieţii sociale. Odată cu dezvoltarea criminalităţii informatice, care influenţează toate domeniile relevante pentru securitatea cetăţenilor şi statului, orice atac la adresa infrastructurilor critice poate fi efectuat mult mai rapid şi poate avea consecinţe catastrofale.

Datorită dinamicii mediului actual de securitate, instituţiile responsabile ale statului vor fi nevoite să pună accentul pe prevenirea şi anticiparea ameninţărilor la adresa securităţii, în detrimentul acţiunilor întreprinse în urma materializărilor ameninţărilor în cauză. Acestea trebuie să se adapteze constant la noile evoluţii sociale şi economice, revoluţia tehnologică la care asistăm în prezent fiind una dintre ele. Odată cu aceste schimbări cresc vulnerabilităţile şi riscurile la adresa securităţii naţionale, din cauza modificării modului în care instituţiile statului trebuie să răspundă noilor provocări.

Pentru a înţelege complexitatea mediului de securitate, este esenţială extragerea informaţiilor relevante din fluxul informaţional abundent şi analiza corectă a acestor informaţii. Însă, de vreme ce paradigma tradiţională are ca obiect de activitate ameninţările statale, trebuie ţinut cont de faptul că, în prezent, ameninţările au atins o nouă

dimensiune, cea transnaţională. Totuşi, atât garantarea propriei securităţi, cât şi atingerea obiectivelor diplomatice se realizează în mod individual de către fiecare naţiune în parte, excedând cadrul alianţelor din care face parte[2].

2. Revoluţia tehnologică

Globalizarea, în esenţă, nu reprezintă un pericol la adresa securităţii naţiunilor. Acest pericol este dat de implicaţiile globalizării. Astfel, „globalizarea comunicaţiilor şi dezvoltarea exponenţială a tehnologiilor au generat manifestarea unor riscuri „clasice" de securitate într-un mediu nou, cel virtual: de la criminalitate organizată la crimă informatică, la spionajul electronic sau multiplicarea capacităţilor de acţiune teroristă, prin utilizarea Internetului ca vehicul de radicalizare sau pregătire a grupurilor extremiste"[3].

În acest context, prezintă relevanţă emergenţa dimensiunii cibernetice a securităţii, cu precădere în domeniul protejării infrastructurilor critice. Securitatea cibernetică reprezintă „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi ne-repudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private din spaţiul cibernetic. Măsurile proactive şi reactive pot include: politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor"[4].

În spaţiul cibernetic, rapiditatea evoluţiilor este un element cheie. Totuşi, trăim într-o societate a cunoaşterii, iar avantajele conferite de tehnologie nu pot fi neglijate. Din ce în ce mai mult vor fi evidenţiate beneficiile serviciilor digitale în orice domeniu al vieţii sociale. Revoluţia tehnologică, pe lângă beneficii, implică şi dezavantaje. Dependenţa crescută de sistemele informatice şi utilizarea din ce în ce mai frecventă a internetului au condus la definirea problematicii securităţii cibernetice ca fiind prioritară.

În prezent, putem afirma că spaţiul cibernetic constituie o valoare critică pentru orice element al societăţii contemporane. Astfel, ameninţările generate prin mijloace tehnologice pot fi efectuate asupra unor domenii cu valoare strategică.

Spaţiul cibernetic, conform articolului 2 din Hotărârea nr. 494 din 11.05.2011 privind înfiinţarea *Centrului Naţional de Răspuns la Incidente*

---

[2] Mihaela Matei 2013: 40.
[3] Mihaela Matei 2013: 41.
[4] *Hotărârea nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO*, art. 2, alin. e).

de Securitate Cibernetică - CERT-RO reprezintă „mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta”[5].

Spaţiul cibernetic a devenit frontul dezvoltării unui nou tip de război, asimetric. Accentul s-a deplasat de la actorii statali la cei non-statali. Caracterul asimetric al conflictelor derulate prin mijloace tehnologice este dat atât de disproporţionalitatea resurselor utilizate, cât şi de impactul generat. Totodată, vorbind despre asimetrie, este necesar să ne referim la gradul scăzut de predictibilitate al conflictelor derulate în spaţiul virtual, precum şi la dificultatea existentă în ceea ce priveşte modalitatea de atribuire a incidentelor.

Întrucât infrastructurile critice constituie o valoare strategică a unui stat, contribuind la desfăşurarea vieţii în condiţii de funcţionalitate, apărarea acestora devine obligatorie. Acţiunile ostile trebuie prevenite ori efectele lor limitate.

Atacul cibernetic reprezintă acţiunea ostilă derulată în spaţiul cibernetic de natură să afecteze „disponibilitatea, integritatea, autenticitatea, ne-repudierea şi confidenţialitatea sistemelor informatice”[6]. Atacurile cibernetice se pot manifesta în mai multe moduri, de la obţinerea informaţiilor personale ale utilizatorilor la obţinerea informaţiilor deţinute de companii private ori atacurile asupra infrastructurilor critice naţionale.

Ameninţările pot lua forme diverse, inclusiv accesul neautorizat la date cu intenţia de a comite fraude asupra unor indivizi ori companii. În situaţii critice, există riscul unor întreruperi sistematice în cadrul reţelelor şi serviciilor virtuale, în aşa manieră încât ameninţarea cibernetică poate fi încadrată în aceeaşi categorie cu terorismul. Noi ameninţări sunt descoperite constant, iar acestea pot afecta orice sistem de operare[7].

În vederea limitării impactului ameninţărilor generate de spaţiul virtual în România, este necesară consolidarea cadrului legislativ şi instituţional în domeniul de referinţă. Totodată, este indicată responsabilizarea structurilor guvernamentale şi a societăţii civile, interconectarea structurilor statale cu organizaţiile non-guvernamentale, cu entităţile private şi cu cetăţenii statului[8].

Întrucât evoluţia contextului internaţional a dus la un proces de modernizare rapidă a activităţii instituţiilor cu rol în asigurarea securităţii naţionale, prin ralierea la standardele europene şi internaţionale în domeniu, provocările de securitate s-au intensificat, iar rolul interdependenţelor între stat şi societatea civilă devine din ce în ce mai important. Astfel, cultura de securitate existentă la nivelul cetăţenilor statului trebuie să atingă un nivel din ce în ce mai ridicat, iar înţelegerea

---

[5] *Hotărârea nr.494 din 11.05.2011* art. 2, alin. d).
[6] Curculescu & Ştefan 2013: 98.
[7] Shanker 2007.
[8] Maior *et alii* 2010: 8.

corectă a noţiunilor de *risc* şi *securitate* reprezintă punctul de plecare al acestui proces.

3. Infrastructurile critice în contextul modernităţii

3.1. Delimitări conceptuale

În momentul iniţierii unei discuţii despre *securitate*, este necesar să clarificăm contextul la care facem referire, întrucât acest concept este folosit şi în limbajul uzual şi trebuie înlăturate confuziile, deoarece în relaţiile internaţionale acesta capătă o nuanţă cu totul diferită. Astfel, când facem referire la o *problemă de securitate*, aceasta este prezentată „ca o ameninţare la adresa obiectului de referinţă (în mod tradiţional, dar nu necesar, statul, guvernarea, teritoriul, societatea)[9]", *securitatea* fiind sentimentul de încredere prezent în lipsa ameninţărilor, respectiv certificarea ţinerii acelor pericole sub control[10]. Însă în contextul dinamicii mediului de securitate, este dificil să trecem cu vederea complexitatea noilor ameninţări, respectiv valenţa pe care o câştigă infrastructurile critice în această confruntare.

Iar când discutăm despre securitatea statelor, respectiv dinamica politicilor internaţionale, trebuie să luăm în calcul şi ceea ce Buzan consideră ca fiind important de punctat în acest sens. Acesta pune accent pe teoria construită de John Hertz încă din anii '50, o „dilemă a securităţii" conform căreia, statul, în încercarea asigurării nevoilor de securitate, tinde să conducă la creşterea insecurităţii celorlalte state, în cazul nostru, la slăbirea infrastructurilor vitale ale potenţialilor adversari de pe scena relaţiilor internaţionale.

În urma Războiului Rece şi mai curând, în urma atacurilor teroriste de la 11 septembrie 2001, precum şi a celor din Londra şi Madrid (2004), dar şi după Octombrie Roşu şi revoluţia informaţională, modalităţile de gestionare a elementelor vitale din toate aspectele socialului, sau ale mediilor militar, economic sau politic, suferă transformări majore. Restructurările pe aceste planuri aduc cu ele şi vulnerabilităţi care expun securitatea unui stat şi îl fac susceptibil ameninţărilor venite din exterior. Astfel, putem spune că modernitatea vine odată cu o serie de ameninţări asimetrice.

În linii mari, atunci când discutăm despre *infrastructuri*, ne referim la ansamblul elementelor care susţin legăturile necesare ale unui sistem, iar în cazul *infrastructurilor critice*, la cele care au o importanţă majoră pentru securitatea unui stat, destabilizarea lor conducând la incapacitatea asigurării securităţii statului, cu daune considerabile pe diferite paliere.

Definim *infrastructurile* ca având rolul de „verigă strategică în procesul care reuneşte funcţional două domenii vitale ale vieţii economico-

[9] Buzan *et alii* 2011: 42.
[10] Bădălan 2001: 39.

sociale, producţia şi consumul[11]" şi precizăm că, din punct de vedere comunicaţional şi informaţional, o privim ca fiind „influenţată de idei, dar, mai mult decât atât şi alcătuită din idei[12]", fapt care reprezintă „consecinţa revoluţionară a inventării calculatorului şi a expansiunii reţelelor informatice[13]".

Dat fiind că multiplicarea ameninţărilor asimetrice la adresa securităţii globale, facilitată de progresul tehnologic, conduce la multiple atacuri cibernetice, trebuie analizat impactul noilor tehnologii informatice asupra securităţii infrastructurilor critice. În acest sens, vom lua în calcul legile şi strategiile formulate, cu precădere *Programul European pentru Protecţia Infrastructurilor Critice, Directiva 114/08/EC*, *Ordonanţa de urgenţă nr. 98 din 3 noiembrie 2010* privind identificarea, desemnarea şi protecţia infrastructurilor critice, precum şi *Strategia Naţională privind Protecţia Infrastructurilor Critice*, în vigoare de la 04.08.2011 din *Hotărârea nr. 718/2011*, însă nu înainte de prezentarea evoluţiei conceptului de infrastructură critică.

3.2. Caracteristici ale infrastructurilor critice

3.2.1. Evoluţia conceptului de infrastructură critică

Într-o primă clasificare a infrastructurilor, le putem împărţi în obişnuite, speciale şi critice. Cele obişnuite sunt definite ca „o structură, un cadru, care asigură construcţia şi funcţionarea sistemului[14]", fără caracteristici deosebite. Când discutăm despre cele speciale ne vom referi la cele care „au un rol deosebit în funcţionarea sistemelor şi proceselor, asigurându-le acestora o eficienţă sporită, calitate, confort, performanţă[15]", iar pe cele critice le încadrăm în categoria celor „de care depind stabilitatea, siguranţa şi securitatea sistemelor şi proceselor[16]".

Iniţial (încă din anii '80), s-a pornit de la încadrarea unor obiective considerate vitale ale statelor sau organismelor internaţionale ca fiind critice, însă conceptul de infrastructură critică a fost introdus în 1996 prin *Ordinul Executiv pentru Protecţia Infrastructurilor Critice*[17], acestea semnificând elemente ce ţin de infrastructura naţională având o funcţie atât de vitală „încât distrugerea sau punerea lor în incapacitate de funcţionare poate să diminueze grav apărarea sau economia SUA[18]". Acelaşi ordin încadra în această categorie telecomunicaţiile, sistemele de energie electrică, depozitele de gaze şi petrol, băncile şi finanţele, transportul, aprovizionarea cu apă, serviciile de urgenţă şi guvernarea.

---

[11] Victor Matei 2012: 83.
[12] Victor Matei 2012: 86.
[13] Victor Matei 2012: 86.
[14] Alexandrescu & Văduva 2006: 6.
[15] Alexandrescu & Văduva 2006: 6.
[16] Alexandrescu & Văduva 2006: 6.
[17] *Executive Order Critical Infrastructure Protection*.
[18] *Executive Order Critical Infrastructure Protection*.

Ulterior atentatului din 11 septembrie 2001 şi fixării unor noi preocupări în privinţa vulnerabilităţilor naţionale, Casa Albă a formulat un nou *Ordin Executiv pentru Protecţia Infrastructurilor Critice* ce viza elementele „de natură umană, economică, informaţională, din cadrul serviciilor guvernamentale principale şi a securităţii naţionale a SUA[19]", iar elementele au continuat să fie revizuite.

3.2.2. Abordări ale problematicii infrastructurilor critice la nivelul Uniunii Europene şi NATO

Proliferarea ameninţărilor asimetrice conduce la nevoia unor măsuri concrete în planul gestionării riscurilor, respectiv al protecţiei infrastructurilor critice. Astfel, cu scopul evitării periclitării securităţii statelor, s-a recurs la mai multe interpretări ale acestor riscuri, care au condus la raportări specifice ale acestei problematici în funcţie de profilul statelor, respectiv, în faza aceasta, a organizaţiilor internaţionale.

Aducând în discuţie problematica *infrastructurilor critice* de la nivelul Alianţei Nord-Atlantice, acestea se vor caracteriza prin acele „facilităţi, servicii şi sisteme informatice care sunt atât de vitale pentru naţiuni, încât scoaterea lor din funcţiune sau distrugerea lor poate avea efecte de destabilizare a securităţii naţionale, economiei naţionale, stării de sănătate a populaţiei şi asupra funcţionării eficiente a guvernului[20]".

În încercarea realizării unei uniformităţi la nivelul statelor membre ale Uniunii Europene, s-a recurs la *Directiva 114/08/EC*, care privea identificarea infrastructurilor critice ale UE şi evaluarea necesităţii îmbunătăţirii protecţiei acestora, folosind o metodă comună. Aceasta clarifica şi concepte precum infrastructura critică, infrastructura critică a UE, analiza riscului, şi încadra în *infrastructura critică a Europei*, „infrastructura critică localizată în cadrul statelor membre a cărei întrerupere sau distrugere ar avea un impact semnificativ asupra a cel puţin două state membre. Evoluţia acestui impact va trebui evaluată după criterii transversale"[21]. În continuare, oferea o serie de abordări care urmăreau să furnizeze soluţii împotriva unor atacuri similare celor din Madrid şi Londra, dar şi în cazurile unor calamităţi naturale sau a destabilizării sistemelor informatice.

Protecţia infrastructurilor critice în faţa ameninţărilor cibernetice a devenit o prioritate influenţată şi de cazul Estoniei din 2007, care a „afectat sistemele de comunicaţii, site-urile de internet, sectorul bancar şi integritatea sistemelor informatice ale cetăţenilor, pagubele financiare suferite fiind estimate la zeci de milioane de euro[22]" paralizând aproape

[19] Victor Matei 2012: 87.
[20] Victor Matei 2012: 88.
[21] *Council Directive 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.*
[22] *Atacurile cibernetice din Estonia 2007.*

întreaga infrastructură informaţională a ţării şi a continuat şi cu faimosul „Octombrie Roşu". În acest context, pentru protecţia infrastructurii critice care utilizează sisteme tehnologice, s-a iniţiat şi în România *Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO*, iar din 2013 a fost adoptată *Strategia de Securitate Cibernetică a României*. Existenţa acestora însă, nu este suficientă pentru asigurarea unui mediu virtual sigur.

3.2.3. Abordări ale problematicii infrastructurilor critice în cazul României

Dat fiind că securitatea naţională este dependentă de infrastructurile sale strategice, respectiv tot mai vulnerabilă din cauza evoluţiei tehnologice, analiştii acordă o importanţă din ce în ce mai accentuată protecţiei infrastructurilor critice, respectiv instituţionalizării unor aspecte ce ţin de aceasta, chiar dacă nu fac posibilă ajungerea la o soluţie universală care să reuşească în proporţie de 100% protecţia lor.

Relevante în acest sens sunt demersurile luate în formularea unor acte legislative, respectiv a unei *Strategii Naţionale privind Protecţia Infrastructurilor Critice*, însă vom începe cu introducerea *Ordonanţei de Urgenţă nr. 98 din 3 noiembrie 2010* privind identificarea, desemnarea si protecţia infrastructurilor critice, publicată în *Monitorul Oficial Nr. 757 din 12 noiembrie 2010*. Aceasta venea ca urmare a iniţiativei de la nivelul Uniunii Europene, *Directiva 114/08/EC*. Pe acest palier, în încercarea de a schiţa elementele din cadrul *OUG98/2010*, Alessandro Lazari transpune principalele idei in figura de mai jos:

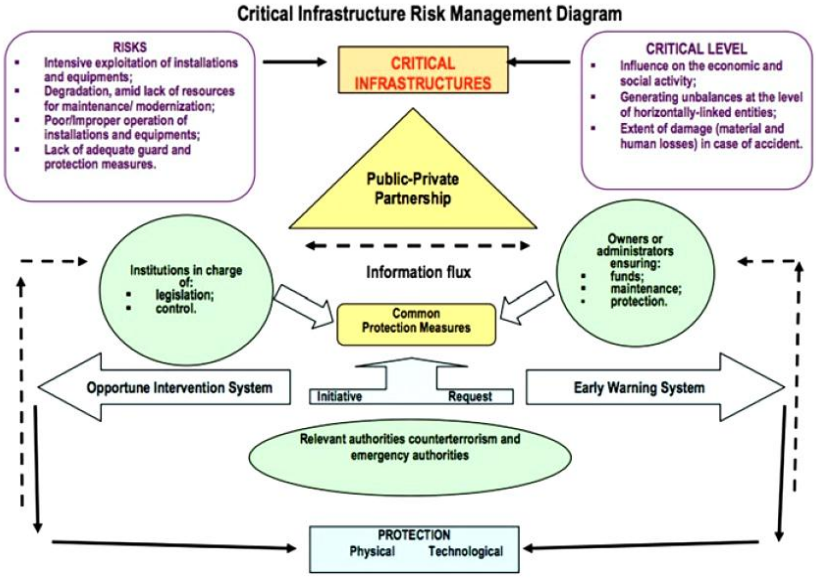

Fig. 1 – Diagrama managementului infrastructurilor critice în cazul României
Sursa: Lazari 2014: 79.

În imaginea de mai sus, Alessandro Lazari urmăreşte şi managementul riscului, respectiv necesitatea unor sisteme de avertizare timpurie care trebuie monitorizate constant. În acelaşi plan, autorul schemei[23] face şi o paralelă cu Marea Britanie, despre care consideră că poate fi luată drept exemplu de măsuri minore de conformitate, pe când România e privită ca un exemplu pozitiv care nu numai că îndeplineşte cerinţele minimale ale *Directivei 114/08/EC*, ci le şi introduce cu succes[24].

Întrucât s-a considerat necesar să se introducă şi un cadru strategic care să faciliteze dezvoltarea măsurilor precizate în *Directiva 2008/114/CE* din 8 decembrie 2008, a fost elaborată şi *Strategia Naţională privind Protecţia Infrastructurilor Critice* „în concordanţă cu prevederile Strategiei Naţionale de Apărare a României, ale Cartei Albe a Securităţii şi Apărării Naţionale şi cu delimitările conceptuale instituţionale în domeniu, atât de la nivel naţional, cât şi internaţional, stabilind astfel politicile şi direcţiile de acţiune din domeniu, necesare dezvoltării şi completării cadrului normativ naţional[25]".

3.3. Protecţia infrastructurilor critice

Pentru asigurarea funcţionalităţii infrastructurilor critice, respectiv pentru diminuarea riscurilor, sunt necesare demersuri corespunzătoare întreprinse în vederea protecţiei acestora. Însă ce trebuie luat în calcul atunci când discutăm despre această activitate şi ce semnifică ea?

Pe lângă identificarea acestui tip de infrastructuri, în concordanţă cu legislaţiile naţionale şi europene în vigoare, trebuie abordate o serie de dimensiuni, evaluarea riscului constituind un element fundamental în dezvoltarea unui program de protecţie al infrastructurilor critice. De asemenea, este important să se acorde atenţie principiilor *Programului european pentru protecţia infrastructurilor critice (PEPIC),* între care amintim necesitatea unor proceduri specifice de identificare şi clasificare a infrastructurilor critice europene, asigurarea protecţiei informaţiilor clasificate din acest domeniu, identificarea interdependenţelor de la acest nivel, sprijin financiar între statele membre UE, formarea unei reţele de alertă şi elaborarea unor studii de caz care să vizeze identificarea dependenţelor şi reducerea vulnerabilităţilor, iar acest lucru în funcţie de o serie de indicatori de performanţă[26], la care se adaugă şi parteneriatul public-privat. Programul european pentru protecţia infrastructurilor critice însă, vizează acele sisteme ale căror atingere produce daune în cel puţin două state membre. Acest program are ca instrument *Directiva 114/2008*, care momentan ia în calcul doar sectorul de transporturi şi pe cel energetic,

[23] Alessandro Lazari este responsabil pe proiecte in domeniul protecţiei infrastructurilor critice la Comisia Europeană.
[24] Lazari 2014: 76.
[25] *Hotărârea nr. 718/2011.*
[26] Vezi *Communication from the Commission on a European Programme for Critical Infrastructure Protection COM/2006.*

necuprinzând nici aspecte importante precum evaluarea riscului sau alocarea clară a responsabilităţilor între părţile implicate.

Pentru ca aceste măsuri de protecţie să fie direcţionate corespunzător, este necesară o analiză a ameninţărilor la adresa infrastructurilor critice, indiferent dacă vorbim despre ameninţarea teroristă, vulnerabilităţile tehnologice sau diversitatea dezastrelor naturale, prin protecţia lor înţelegând măsurile considerate necesare pentru a reduce riscul de distrugere sau de trecere în incapacitate de funcţionare a acestora. Protecţia infrastructurilor critice este mult mai importantă chiar şi decât furnizarea de servicii sociale eficiente, întrucât fără prima, nu există speranţe pentru cea din urmă. În zilele noastre, protecţia infrastructurilor critice nu mai vizează doar reacţia defensivă împotriva pericolelor iminente, ci şi măsuri preventive, deoarece societăţile au devenit din ce în ce mai vulnerabile, cauzele crizelor fiind mai extinse şi mai difuze.

La aceste dimensiuni se adaugă şi aspectul că, dacă în mod tradiţional securitatea naţională era preocupată de ameninţările din exterior, în prezent este nevoită să dezvolte rezilienţa în infrastructura naţională, iar acest lucru printr-o multitudine de măsuri printre care şi cele care ţin de securitatea cibernetică[27]. Protecţia infrastructurilor critice este încă bazată pe interesul naţional, iar acesta devine tot mai dificil de definit. Este necesară cooperarea internaţională, întrucât ca şi în cazul Uniunii Europene, deteriorarea sau pierderea unei părţi din infrastructura unui stat membru poate avea repercusiuni şi asupra economiei Europei în ansamblul ei. Pe fondul dezvoltării tehnologiei, acest aspect devine din ce în ce mai probabil, infrastructura fiind parte dintr-o reţea mai largă.

Maitland Hyslop face o sinteză a principiilor protecţiei infrastructurilor critice elaborate de G8 (Grupul celor 8)[28], enumerând următoarele[29]:

- Crearea unor reţele de avertizare
- Promovarea parteneriatelor
- Menţinerea unor reţele de comunicare pe timp de criză
- Facilitarea detectării urmelor atacurilor
- Formarea şi antrenarea
- Dezvoltarea unui cadru legislativ corespunzător şi a unui personal instruit
- Cooperarea internaţională
- Dezvoltarea cercetării în domeniu

Parte din acestea au fost incluse şi în *Strategia Naţională privind Protecţia Infrastructurilor Critice*, unde mai regăsim şi aspecte precum *Principiul confidenţialităţii* care vizează că diseminarea informaţiilor care

[27] Cavelty & Suter 2012: 16.
[28] Vezi date suplimentare pe: http://www.cfr.org/international-organizations-and-alliances/group-eight-g8-industrialized-nations/p10647.
[29] Hyslop 2007: 186.

privesc protecţia infrastructurilor critice „se va realiza într-un cadru care să asigure protejarea acelor informaţii specifice a căror divulgare ar putea genera vulnerabilităţi de securitate la nivelul respectivelor infrastructuri[30]", sau *Principiul proporţionalităţii*, caracterizat prin faptul că „măsurile de protecţie vor fi proporţionale cu nivelul de risc acceptat". În această direcţie şi pentru că în *Strategie* este menţionat şi *Principiul securizării funcţiilor vitale*, considerăm necesară dezvoltarea evaluării şi analizei riscurilor, demers început în partea următoare a lucrării de faţă.

3.3.1. Evaluarea riscurilor la adresa infrastructurilor critice

Pentru ca programele de protecţie ale infrastructurilor critice să se dovedească eficace, un rol important îl joacă procesul de evaluare a riscului, fapt ce reiese prin existenţa multitudinii de metodologii ale evaluării de risc dedicate acestui segment. Acest lucru se datorează caracterului nesigur şi transnaţional al vulnerabilităţilor şi ameninţărilor aferente domeniului, care generează o preocupare permanentă atât pe plan local, cât şi naţional ori internaţional de gestionare promptă şi corectă a riscului la adresa infrastructurilor critice.

Procesul evaluării riscului este înţeles ca posibilitatea producerii unor rezultate pozitive ori negative, precum şi probabilitatea ca acestea să aibă loc într-un interval de timp determinat. Această definiţie se raportează la conceptul de risc ca având atât elemente pozitive cât şi negative şi introduce limita temporală a estimării riscului.

În mediul privat, evaluarea riscului reprezintă doar o parte dintr-un set complex de factori pentru înţelegerea cărora este necesar a se aloca timp şi resurse[31].

Evaluarea riscului este indispensabilă în vederea identificării ameninţărilor, estimării vulnerabilităţilor şi impactului asupra componentelor individuale, infrastructurilor ori sistemelor, luând în calcul probabilitatea materializării ameninţărilor în cauză. Acesta este un element esenţial în ceea ce priveşte diferenţierea unei metodologii clasice de evaluare a impactului de metodologiile specific evaluării riscului.

În prezent există un număr mare de metodologii pentru evaluarea riscului la adresa infrastructurilor critice. La nivel global, excluzând anumite segmente precum băncile sau societăţile de asigurări, nu a fost creată o metodologie comună după care riscurile pot fi evaluate. În general însă, metodologiile au în comun o serie de elemente: identificarea şi clasificarea ameninţărilor, identificarea vulnerabilităţilor, evaluarea impactului. Referitor la diferenţele dintre aceste metodologii, ele constau, în principal, în scopul acestora, publicul ţintă (factori de decizie, politicieni, institute de cercetare etc.), ori domeniul de aplicare (nivelul componentelor, nivelul infrastructurii, nivelul sistemului).

---

[30] *Strategia Naţională privind Protecţia Infrastructurilor Critice*.
[31] Fischhoff 1995: 139.

Metodologiile care privesc doar componente strategice individuale includ, cu precădere, elementele comune enumerate anterior. Totodată, ele se bucură de un anumit grad de stabilitate, sunt bine definite, testate şi validate. Pe de altă parte, cele care au ca obiectiv evaluarea riscului la un nivel mai înalt, respectiv în cadrul unui sistem, au un nivel de complexitate sporit[32].

Dintre caracteristicile esenţiale ale infrastructurilor critice regăsim interdependenţa acestora şi caracterul lor transnaţional. Plecând de la această afirmaţie, Rinaldi consideră că un element esenţial în procesul de evaluare a riscului îl reprezintă rolul interdependenţelor infrastructurilor critice, respectiv faptul că funcţionarea unei infrastructuri are o influenţă directă asupra alteia. În acest sens, autorul enunţă 4 tipuri de interdependenţe[33] pe care le consideră esenţiale:

- Interdependenţa fizică: Funcţionarea unei infrastructuri depinde de rezultatele materiale ale alteia;
- Interdependenţa cibernetică: Funcţionarea unei infrastructuri este dependentă de informaţiile transmise alteia prin infrastructurile informatice;
- Interdependenţa geografică: Funcţionarea unei infrastructuri este influenţată de efectele produse de un eveniment local;
- Interdependenţa logică: Reprezintă orice fel de interdependenţă între componentele infrastructurilor care nu face parte din categoriile enumerate anterior, fiind determinată de factorul uman.

Pe parcursul timpului, abordarea infrastructurilor critice şi a metodelor de protecţie ale acestora s-a realizat în diferite moduri, în funcţie de specificul fiecărui domeniu, stat ori organizaţie. Datorită importanţei dobândite de acest segment în ultimul timp, buna funcţionare şi eficacitatea procesului de evaluare a riscului depind de existenţa unui cadru legislativ adecvat, de o organizare unitară şi de elaborarea unor strategii convergente. Totodată, din cauza necesităţii de a ţine cont de riscurile şi ameninţările la adresa securităţii naţionale cu impact asupra infrastructurilor critice, a fost reliefată necesitatea implicării factorilor de decizie din acest domeniu în realizarea activităţilor conexe domeniului. În vederea gestionării eficiente însă, este esenţială cunoaşterea adecvată a conceptului şi caracteristicilor infrastructurilor critice, a tipurilor de interdependenţe dintre acestea, a cadrului legislativ aferent domeniului precum şi a modalităţilor de implementare a acestuia, scopul urmărit constând în întreprinderea unor măsuri preventive şi proactive, nu numai de reacţie.

[32] Giannopoulos *et alii* 2012: 3.
[33] Giannopoulos *et alii* 2012: 4.

Concluzii

În contextul globalizării, respectiv în urma trecerii de la ameninţările tradiţionale la cele asimetrice şi la un flux complex de informaţii, intenţiile adversarilor devin din ce în ce mai greu de identificat, iar dezvoltarea mijloacelor de comunicare facilitează complexitatea atacurilor cibernetice, făcând infrastructurile critice ale unui stat tot mai vulnerabile.

De asemenea, este important ca instituţiile responsabile să urmărească prevenirea şi anticiparea ameninţărilor la adresa securităţii statului, să extragă acele informaţii relevante şi verificate, cu accent pe dimensiunea cibernetică a securităţii în domeniul protejării infrastructurilor critice, întrucât revoluţia tehnologică a dus la o dependenţă crescută de sistemele informatice. Acest lucru conduce la un grad mai scăzut de predictibilitate a riscurilor, aspect care le face vulnerabile. Pentru a contracara implicaţiile negative ale globalizării, respectiv faptul că în vederea asigurării securităţii lor, statele ajung să crească insecuritatea altor state, considerăm că este necesară responsabilizarea structurilor guvernamentale şi a societăţii civile, precum şi cooperarea acestora.

Scopul acestei lucrări a fost să reliefeze impactul noilor tehnologii informatice asupra securităţii infrastructurilor critice, întrucât dependenţa de sistemele informatice sporeşte un atac asupra infrastructurilor acestora şi le face mai vulnerabile şi în cazul dezastrelor naturale. Cu toate că în planul legislativ, măsurile abordate de România sunt considerate un exemplu şi pe plan internaţional, respectiv măsurile preventive indicate în *OUG 98/2010*, nu putem spune acelaşi lucru şi despre acţiunile de implementare în scopul diminuării daunelor produse după un eveniment sau gestionarea unui posibil dezastru, respectiv capacitatea sistemului de a redeveni funcţional într-un timp cât mai scurt, aspecte aflate într-o stare incipientă.

În scopul protejării infrastructurilor critice, este necesar ca România să-şi dezvolte nivelul de reziliență şi să se adapteze permanent avansului tehnologic, respectiv să încurajeze conştientizarea riscurilor şi cooperarea societăţii civile cu instituţiile abilitate, cu atât mai mult cu cât o vulnerabilitate se transformă în ameninţare tocmai din cauza „porţilor” lăsate deschise. În acest caz, vulnerabilităţile care survin din cauza interconectării infrastructurilor, facilitează atacuri cibernetice care sunt capabile să destabilizeze sistemul chiar şi de la distanţă. În continuare, considerăm necesar a se pune accent pe îmbunătăţirea procesului de evaluare a riscurilor la adresa infrastructurilor critice, pe managementul eficient al crizelor, parteneriatul public-privat, cercetare-dezvoltare în domeniu şi pregătirea persoanelor cu expertiză în realizarea analizelor prospective, respectiv în elaborarea de sisteme de avertizare timpurie şi monitorizarea permanentă a indicatorilor acestor sisteme.

BIBLIOGRAFIE

Alexandrescu, Grigore; Văduva, Gheorghe (2006). *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*. Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I".

Bădălan, Eugen (2001). *Securitatea României: Actualitate şi perspectivă,* Bucureşti, Editura Militară.

Buzan, Barry; Waever, Ole; Wilde, Jaap de; Jilău, George (Trad.) (2011). *Securitatea: un nou cadru de analiză,* Cluj-Napoca, Editura CA Publishing.

Cavelty, Dunn & Suter, M, in Lopez, Javier, Setola, Roberto, Wolthusen Stephen (2012). *Critical Infrastructure Protection.Information Infrastructure Models, Analysis, and Defense*. Berlin Heidelberg, Springer-Verlag.

Centrul de la Sibiu pentru Studii de Pace, *Atacurile cibernetice din Estonia(2007)*. Disponibil la http://www.cssp.ro/analize/2012/10/01/atacurile-cibernetice-din-estonia-2007/.

Council Directive 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Disponibil la http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

Communication from the Commission on a European Programme for Critical Infrastructure Protection /* COM/2006/0786 final, Disponibil la http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:52006DC0786.

Curculescu, Gabriel; Ştefan Mircea (2013). *Capabilitatea CERT vs. agresiunea cibernetică în spaţiul euro-atlantic* în *Intelligence - număr aniversar - 5 ani*, Bucureşti, pp. 96-109.

Executive Order Critical Infrastructure Protection, Disponibil la http://fas.org/irp/offdocs/eo13010.htm.

Fischhoff, Baruch (1995). „Risk Perception and Communication Unplugged: Twenty Years of Process" în *Risk Analysis*, XV/2.

Giannopoulos, Georgios; Filippini, Roberto; Schimmer, Muriel (2012). „Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, European Comission", *Joint Research Center Technical Notes*, Disponibil la http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf.

Hyslop, Maitland (2007). *Critical information infrastructures. Resilience and protection,* Springer.

Hotărârea nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.

Hotărârea nr.718 din 2011 pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice, Disponibil la http://lege5.ro/Gratuit/gi2tsnjtgu/hotararea-nr-718-2011-pentru-aprobarea-strategiei-nationale-privind-protectia-infrastructurilor-critice?pId=178186180#p-178186180.

Institutul de Politici Publice, *Informational brief for journalists.Concept of security. Security sector*, Disponibil la http://www.ipp.md/public/files/Proiecte/Info_Brief_no._1_-_Concept_of_Security._Security_Sector.pdf.

Lazari, Alessandro (2014). *European Critical Infrastructure Protection*. Switzerland, Springer International Publishing.

Maior, George Cristian *et alii*. (2010), *Un război al minții – intelligence, servicii de informații și cunoaștere strategică în secolul XXI*. București, RAO.

Matei, Mihaela (2013). „Transformarea sistemelor de intelligence şi procesul de modernizare a Serviciului Român de Informaţii" în *Intelligence - număr aniversar - 5 ani*, București, pp. 38-45.

MATEI, Victor (2012), *Importanța strategică a infrastructurii naționale*, București, Editura Institutului de Ştiinţe Politice şi Relaţii Internaţionale.

Shanker, Thom (2007). *Defense Secretary Urges More Spending for U.S. Diplomacy*, New York Times, 27 Noiembrie 2007, Disponibil la http://www.nytimes.com/2007/11/27/washington/27gates.html?_r=0.