# Capitolul II. Trăsături ale mediului de securitate actual

Evenimentele şi schimbările care au avut loc în ultimul deceniu al secolului trecut şi la începutul secolului al XXI-lea au produs efecte multiple pe termen lung în societatea internațională. Contextul strategic internațional actual creat de efectele pozitive şi negative ale acestor evenimente are în prim-plan adaptarea constantă a mediului de securitate internațional, pentru a rezista noilor provocări şi factori de risc.

Sfârşitul Războiului Rece, cu implicațiile sale la nivel regional şi internațional (căderea comunismului, dizolvarea Uniunii Republicilor Sovietice Socialiste – URSS şi a Republicii Socialiste Federative Iugoslavia, reunificarea Germaniei ş.a.), a determinat restructurarea raportului de forțe la nivel global, prin desființarea cadrului de securitate bipolar (constituit în est de URSS, prin Tratatul de la Varşovia şi în vest de Statele Unite ale Americii, prin Organizația Tratatului Nord-Atlantic – NATO). Evoluția interacțiunilor dintre state a determinat reconfigurarea raportului de forțe la nivel global către multipolaritate[1].

În perioada imediat următoare încheierii Războiului Rece, mediul internațional a fost caracterizat de incertitudine şi instabilitate, cu precădere din perspectiva fragmentării URSS, a Iugoslaviei şi a Cehoslovaciei, precum şi din perspectiva creării de noi state independente. Peisajul strategic mondial a fost caracterizat de conflicte interne, în fața cărora mecanismele organizațiilor internaționale au eşuat din cauza incapacității de definire a zonei de responsabilitate şi de acțiune a societății internaționale. Operațiunile militare desfăşurate de NATO în Bosnia-Herțegovina şi în Kosovo au făcut dovada eşecului ONU de a oferi un mecanism de salvgardare a păcii şi securității internaționale la noile provocări de securitate. Politica atacului preventiv, experiențele războiului umanitar, precum cel din Kosovo, şi ale războiului de eliberare, precum cel din Irak lansat în anul 2003, au evidențiat necesitatea reconfigurării sistemului de securitate la realitățile internaționale actuale[2].

Dacă în perioada Războiului Rece adversarii militari ai marilor puteri erau cunoscuți, începând cu ultimul deceniu al secolului al XX-lea, natura adversarilor se diversifică, motiv pentru care cercetătorii au formulat noi perspective ale relațiilor internaționale, ce au depăşit dimensiunea armată de conflictualitate.

---

[1] A. Năstase, C. Jura, Fl. Coman, *14 prelegeri de Drept Internațional Public,* Ed. C.H. Beck, Bucureşti, 2012, p. 19-20.

[2] C.-Gh. Balaban, *Securitatea şi dreptul internațional: provocări la început de secol XXI,* Ed. C.H. Beck, Bucureşti, 2006, p. 50-51.

Apreciem că lupta împotriva terorismului internațional şi globalizarea rămân principalele fenomene care au influențat arhitectura globală de securitate contemporană[1]. Cu precădere, după atacurile teroriste din 11 septembrie 2001, actorii internaționali au identificat terorismul în strategiile, politicile de securitate dar şi în acțiunile de politică externă, fiind una dintre principalele amenințări la adresa securității naționale şi mondiale. Atacurile teroriste ulterioare care au avut loc în Europa, la Madrid (11 martie 2004) şi Londra (7 iulie 2005), au marcat o nouă etapă de reglementare în domeniul securității internaționale.

Rezoluția Consiliului de Securitate ONU nr. 1373 din 12 septembrie 2001[2] defineşte actul terorist ca o amenințare la adresa păcii şi securității internaționale, legitimând răspunsul la atacurile teroriste, în conformitate cu prevederile Cartei ONU, inclusiv în privința responsabilităților în temeiul Capitolului VII. Cu atât mai mult, în contextul proliferării globalizării, consecințele terorismului au luat amploare, din perspectiva facilitării libertății de circulație şi a mecanismelor de finanțare a grupărilor teroriste. În războiul contra terorismului liniile de front nu pot fi definite, combatanții sunt greu de identificat, pagubele produse pot fi mari, iar sentimentul de teamă insecurizează, devenind astfel o provocare actuală a actorilor internaționali.

Multiplele consecințe ale globalizării au în principal efecte pozitive asupra prosperității societății contemporane, prin favorizarea liberei circulații şi a dezvoltării economice. Cu toate acestea, efectele globalizării într-un context irațional pot crea premise pentru vulnerabilizarea mediului de securitate, cu impact negativ asupra societății internaționale, prin creşterea criminalității transnaționale, perpetuarea crizelor economice, permeabilizarea granițelor naționale, respectiv, diluarea distincției intern-extern[3].

Fenomenul globalizării generează, de asemenea, noi contexte de securitate în care se intensifică interdependența actorilor la nivelul societății internaționale, implicit în sectorul de securitate. Caracterul indivizibil al securității la nivel internațional înseamnă că securitatea națională a statelor se corelează cu contextul securității internaționale, întrucât efectele unui eveniment politico-militar poate depăşi frontierele unui singur stat. Altfel spus, interdependența în funcționarea sistemului internațional face ca securitatea națională individuală să fie relativă şi mai puțin eficientă în anumite contexte.

Globalizarea modifică mediul politic contemporan, prin prisma diversității spectrului amenințărilor la adresa valorilor şi intereselor internaționale, cu precădere a celor neconvenționale, securitatea devenind o preocupare

[1] C.G. Gîrleanu, *Terorismul şi securitatea statelor în epoca globalizării,* Ed. Rovimed, Bacău, 2011, p. 107-114.

[2] Rezoluția nr. 1373/2001 a fost publicată în M. Of. nr. 769 din 3 decembrie 2001 [United Nations, Security Council, Resolution 1368 (2001) Adopted by the Security Council at its 4370th meeting, on 12 September 2001, *Threats to international peace and security caused by terrorist acts*, S/RES/1368 (2001)].

[3] R.O. Keohane , J.S. Nye, *Putere şi interdependență*, Ed. Polirom, Iaşi, 2009, p. 290-299.

globală, mai ales într-un context internațional caracterizat de conflictualitate şi instabilitate.

Mediul internațional actual este totodată definit de complexitate, datorită varietății amenințărilor, şi de dinamism, în contextul diversificării şi creşterii numărului de actori internaționali de securitate. Aşadar, în abordarea globalistă a începutului de secol XXI, nu numai statele amenință sau sunt amenințate, ci şi alți actori de securitate, precum mişcările religioase şi etnice, grupările teroriste, organizațiile neguvernamentale sau grupurile subnaționale.

În prezent, în ciuda existenței unor mecanisme de prevenire a războiului, pacea şi securitatea rămân deziderate destul de controversate. Cu atât mai mult, cu cât se constată în situațiile de criză o incapacitate de aplicare a principiilor fundamentale de drept internațional public, mai ales în privința principiilor nerecurgerii la forță sau la amenințarea cu forța, egalității suverane, integrității teritoriale şi inviolabilității frontierelor[1]. Un exemplu recent în acest sens priveşte anexarea ilegală a peninsulei Crimeea de către Federația Rusă în anul 2014, astfel cum este evidențiat în documentele şi pozițiile oficiale ale statelor şi ale unor organizații internaționale[2].

Raportul dintre conceptele de pace şi securitate este acela dintre parte şi întreg; dacă pacea priveşte lipsa conflictualității şi măsura în care un stat are capacitatea de a împiedica un război, de a câştiga sau de a rezista unui război, securitatea are un sens mai larg de lipsă a amenințărilor de orice natură, inclusiv a conflictelor militare.

Putem aprecia că, în general, starea de conflictualitate la nivel internațional este cauzată de lupta pentru accederea la resurse de natură diversă (fizică, ideologică, religioasă, informațională), rivalitatea reprezentând un factor favorizant al securizării naționale.

Provocările şi amenințările specifice arhitecturii de securitate contemporană reclamă necesitatea adaptării reglementărilor de drept internațional public – chiar şi prin inițiativa de redefinire a unor noțiuni fundamentale, precum război, agresiune, atac –, precum şi adoptării la nivel național de acțiuni complexe la problemele interne ale statelor care ar putea să influențeze mediul de securitate internațional.

---

[1] I. Gâlea, *Folosirea forței în dreptul internațional*, Ed. Universul Juridic, Bucureşti, 2009, p. 5-7.

[2] Ch. Marxsen, *The Crimea Crisis: An International Law Perspective*, ZaöRV 74, 2014, p. 367-391.

## Subcapitolul 1. Definirea unui nou cadru de analiză a securității internaționale

Securitatea reprezintă un concept care provine din ştiințele sociale, fiind o condiție esențială a vieții şi o nevoie primară a individului de protecție, apărare şi echilibru[1].

Din perspectiva relațiilor internaționale, nu există o definiție clară şi universal acceptată a conceptului, deoarece securitatea este un concept cu geometrie variabilă, conturat de o anumită percepție statală sau supranațională a decidenților politici şi de contextul istoric, politic, economic şi militar, la un moment dat.

Teoria relațiilor internaționale, prin subdomeniul studiilor de securitate, propune un periplu în procesul de stabilire a unei definiții complexe şi general acceptate a securității, prin operaționalizarea conceptului în cadrul principalelor şcoli de gândire, între care dezbaterea realism – liberalism ocupă un rol principal[2].

În cadrul prezentei lucrări, propunem o definiție a securității care include principalele concepte-cheie regăsite în definițiile propuse în doctrină şi în reglementări specifice. Astfel, securitatea națională/internațională reprezintă constructul social care exprimă sentimentul sau starea de fapt caracterizată de încredere, stabilitate, siguranță, protecție prin lipsa amenințărilor şi riscurilor la adresa intereselor şi valorilor definite de către decidenți, fiind garantată de către entitatea politică responsabilă, prin capacitatea de prevenire şi apărare împotriva pericolelor şi de contracarare a vulnerabilităților.

Din definiția redată, se pot evidenția câteva aspecte-cheie privind conceptul de securitate. Apreciem că starea de securitate sau insecuritate este relativă şi dinamică, fiind legitimată de liderii politici într-o anumită perioadă de timp, de aceea şi strategiile de securitate sunt actualizate periodic în privința conținutului şi structurii. Din perspectivă națională, problematica securității unui stat este o chestiune de percepție şi prin prisma faptului că valorile şi interesele naționale esențiale sunt identificate tot de către decidenții politici, într-un anumit context istoric, ținându-se seama de sistemul de valori acceptat de societate la un moment dat. Relativitatea securității este determinată atât de această componentă temporară de decizie a liderilor, cât şi de interdependența dintre sistemele de securitate naționale, din perspectivă sistemică securitatea ca şi concept relațional având o componentă internă şi una externă.

Logica social-politică a securității permite identificarea şi interpretarea sensului conceptelor de risc, amenințare şi vulnerabilitate la adresa securității.

---

[1] B. Buzan, O. Waever, J. De Wilde, *Securitatea: un nou cadru de analiză*, CA Publishing, Cluj-Napoca, 2010, p. 54-65 (lucrarea va fi citată în continuare „B. Buzan, O. Waever, J. De Wilde, p…").

[2] J.S. Goldstein, J.C. Pevehouse, *Relații internaționale,* Ed. Polirom, Iaşi, 2008, p. 149-151.

Evenimentele ce produc modificări în percepția asupra securității devin factori favorizanți pentru procesul de securizare.

Studiile de specialitate exprimă pericolul la adresa securității prin noțiunile de risc, amenințare şi vulnerabilitate, nuanțarea acestor noțiuni fiind utilă cercetătorului în vederea creării unei perspective teoretice cât mai complexe a modelelor de securitate, în funcție de obiectul studiului său.

Din perspectiva securității şi apărării naționale, definim riscul ca şi probabilitatea de a se produce o deteriorare semnificativă a stării de normalitate a intereselor, valorilor sau obiectivelor naționale de securitate. Riscurile şi provocările pot deveni amenințări dacă nu sunt bine gestionate, generând astfel pericole la adresa valorilor sau intereselor naționale.

Noțiunea de amenințări cuprinde factorii care reprezintă pericol potențial de lezare gravă a intereselor, valorilor, drepturilor sau obiectivelor fundamentale ale statului. Conform teoriei amenințării existențiale propuse în doctrină[1], doar amenințările existențiale, cu caracter important sunt catalogate drept probleme de securitate. În privința amenințărilor existențiale, actorii politici identifică rațiuni şi motivații publice, cu impact social, în vederea prioritizării şi contracarării acestora. Existența unei probleme de securitate legitimează luarea unor măsuri normative, acțiuni, sau poate permite chiar încălcarea unor reguli[2], fapt care ne face să reflectăm asupra echilibrului dintre normă şi securitate. Amenințările pot fi potențiale, nu trebuie să se fi produs, fiind suficient ca o amenințare să fie prezentată de către liderii politici ca pericol la adresa securității, pentru a justifica o anumită conduită.

Vulnerabilitățile reprezintă factorii interni, procese sau fenomene diverse, care diminuează capacitatea de reacție la acțiunea amenințărilor sau riscurilor[3]. Deşi nu se poate trasa o graniță precisă între conceptele de amenințare şi vulnerabilitate, se poate afirma că vulnerabilitățile pot exista chiar în lipsa unei amenințări precise, evidente. Vulnerabilitățile sunt amenințări potențiale, în situația eşecului de reducere a efectelor negative potențiale pe care vulnerabilitatea le poate produce, riscul crescând cu cât vulnerabilitatea este mai mare.

Legiuitorul român consideră astfel că problemele de securitate pot fi în egală măsură vulnerabilități sau amenințări, în funcție de posibilitatea factorului politic de gestionare internă a aspectelor care să le reducă impactul[4].

Amenințările, riscurile şi vulnerabilitățile la securitatea națională şi internațională sunt privite de analişti şi de către decidenții politici ca oportunități

[1] B. Buzan, O. Waever, J. De Wilde, p. 48-49.

[2] *Idem*, p. 291.

[3] A se vedea *Strategia Națională de Apărare. Pentru o Românie care garantează securitatea şi prosperitatea generațiilor viitoare*, Bucureşti, 2010, accesată la http://ccpic.mai.gov.ro/docs/Strategia_nationala_de_aparare.pdf, ultima vizualizare la 17 iulie 2017 (în continuare „*Strategia Națională de Apărare*, 2010").

[4] A se vedea *Strategia Națională de Apărare,* 2010*,* p. 5.

strategice de acțiune, dar şi ca responsabilități în sarcina deținătorilor puterii de stat care realizează identificarea, evaluarea şi ierarhizarea riscurilor, amenințărilor şi vulnerabilităților. Astfel, statele au percepții şi praguri diferite pentru definirea amenințărilor.

Criteriul în funcție de care se realizează încadrarea conceptuală într-unul dintre modelele de securitate propuse de analiştii studiilor de securitate este reprezentat de natura riscului sau a amenințării de securitate. Amenințarea convențională la adresa securității naționale şi internaționale este de natură militară, conflictul militar având încă în mediul internațional actual un rol determinant în definirea securității. Perspectiva militară a securității corespunde modelului de securitate tradițional, realist, care a atins punctul culminant în timpul Războiului Rece, când amenințarea în confruntarea nucleară globală era de natură militară. Conform teoriei realiste, cu precădere specifice acestei perioade, securitatea cuprinde dimensiunea militară şi politică, în condițiile în care raporturile dintre state sunt caracterizate de anarhie.

În teoria tradițională realistă, studiile de securitate definesc perpetuarea suveranității de tip statal ca obiectiv primordial al securității naționale, prin posibilitatea atacării unui stat de altul, în scopul apărării integrității teritoriale şi independenței naționale. Din acest punct de vedere, obiectul de referință al securității, care este amenințat şi care trebuie să supraviețuiască, este statul, ca entitate politică[1]. Instrumentele de realizare a acestui deziderat sunt politicile de confruntare, războiul şi armata, în competiția interstatală statele exercitându-şi influența națională în vederea obținerii unui avantaj sau a unei poziții favorabile în societatea internațională. Securitatea este privită astfel în termeni militari, deoarece mediul de securitate este creat de raportul de forțe interstatal, în procesul de impunere şi maximizare a propriilor interese în plan internațional.

Constrângerile securității tradiționale de natură politico-militară, progresul general al societății internaționale şi modificările constante în mediul de securitate internațional au determinat o lărgire a sferei de definire a securității din perspectiva teoriei relațiilor internaționale, amenințarea încetând să mai fie un concept pur militar.

Momentul culminant al extinderii conceptului, prin crearea unor noi modele de securitate, l-a reprezentat sfârşitul Războiului Rece, în ciuda faptului că populația şi resursele începuseră să aibă rezonanță în studiul securității încă din anii 1940.

Cadrul de analiză extins al securității priveşte lărgirea spectrului amenințărilor la adresa securității, a obiectelor de referință ale securității, a nivelelor de analiză şi a actorilor de securitate.

---

[1] C. Jura, *Securitatea internațională: Privire specială asupra minorităților*, Ed. C.H. Beck, Bucureşti, 2013, p. 8-10.

Amenințările cu care se confruntă mediul de securitate actual reclamă necesitatea reinterpretării perspectivei tradițional-militariste a securității, prin includerea unor factori neconvenționali precum terorismul, instabilitatea statală, criminalitatea organizată transfrontalieră, conflictele etnice din anumite zone ale lumii, problemele economice, demografice, de mediu, discrepanțele sociale, catastrofele, dezastrele umanitare, drepturile omului, migrația, atacurile cibernetice îndreptate împotriva sistemelor de comunicații şi informații.

Cunoaşterea acestor amenințări şi riscuri permite securizarea, dezvoltarea unor politici de securitate sectoriale adecvate şi prioritizarea în implementarea acestora.

Diversitatea naturii amenințărilor evidențiază nevoia elaborării unei agende de securitate multisectoriale cu rol analitic, în care sectorul clasic militar este completat de alte sectoare de securitate. Întrucât întocmirea agendei multisectoriale este un proces subiectiv, dinamic şi contextual, părțile interesate conturează agendele de securitate în mod diferit. Abordarea cea mai frecventă priveşte agenda de securitate propusă de Şcoala de la Copenhaga a teoreticianului post-Război Rece Barry Buzan, constituită din cinci domenii: militar, de mediu, economic, societal şi politic.

Statele abordează securitatea în mod agregat, raportându-se la dimensiunile securității ca la un întreg, în care legăturile dintre sectoare determină interdependența acestora. Alături de dimensiunea militară de apărare, obiectivul securității devine prosperitatea în privința condițiilor economice, sociale sau politice, realizată de autoritatea politică la toate nivelele de organizare socială – individ, grup, stat sau alianțe.

Constatăm, aşadar, în cadrul teoriilor de securitate moderne, o limitare a dimensiunii militare de securitate, în favoarea introducerii unor noi dimensiuni care privesc toate domeniile vieții şi suveranității statale.

Un al doilea element de analiză a modelelor de securitate priveşte obiectele de referință ale securității. Prin prisma faptului că statul are drept de utilizare a forței armate, în conformitate cu dreptul internațional public, modelul tradițional identifică statul ca unic obiect al securității, pe când în modelul extins al securității obiectele de referință se diversifică, integrând şi actori neconvenționali precum grupările teroriste sau grupurile subnaționale.

Totodată, nivelele de analiză a securității se diversifică, abordarea securității nefiind doar statală sau sistemică, ci poate pleca chiar de la indivizi, prin prisma necesității protejării drepturilor şi libertăților fundamentale în vederea asigurării calității vieții[1].

Amenințările şi riscurile la adresa securității, inclusiv cele de natură cibernetică, sunt diferite ca intensitate, probabilitate de producere, formă de acțiune şi apariție (în plan intern sau extern), asigurarea securității cibernetice devenind în ultimul deceniu o prioritate a liderilor politici.

[1] Al. Sarcinschi, *Vulnerabilitate, risc, amenințare,* Ed. Militară, Bucureşti, 2007, p. 8-10.

# Capitolul III. Delimitări conceptuale privind securitatea cibernetică

Utilizarea infrastructurilor informatice şi a internetului, pe lângă beneficiile de ordin economic, social şi politic, poate determina şi apariția unor tensiuni politice sau militare, percepții greşite sau chiar a unor conflicte între actorii societății internaționale, devenind din această perspectivă o nouă provocare de securitate națională şi internațională.

În contextul dezvoltării tehnologice, rolul infrastructurilor informatice s-a modificat din instrumente de facilitare a activităților zilnice, în instrumente strategice de politică externă, argumentându-se chiar ideea că războiul cibernetic ar fi una dintre cele mai importante aspecte de ordin militar dezvoltate în istoria recentă[1]. Creşterea dependenței de internet şi a interdependenței actorilor utilizatori de sisteme informatice, a determinat un proces de intensificare a insecurității pentru state, prin prisma creşterii vulnerabilităților în fața amenințării neconvenționale de natură cibernetică.

În ultimele două decenii, cu scopul de a facilita interacțiunea, internetul a schimbat societatea în mod semnificativ, inclusiv în materia dreptului şi a relațiilor internaționale, deşi, în general asociat cu internetul, spațiul cibernetic reprezintă un concept mai larg, fiind avut în vedere de doctrina specializată în dreptul internațional public. Dacă internetul reprezintă sistemul global de rețele informatice interconectate, spațiul cibernetic include şi rețelele informatice care se presupune că nu sunt conectate la internet (precum rețele private, rețele tranzacționale sau sisteme informatice de control)[2].

Strategia de securitate cibernetică a României defineşte securitate cibernetică, ca fiind: *„starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informațiilor în format electronic, a resurselor şi serviciilor publice sau private, din spațiul cibernetic*"[3].

O definiție a securității cibernetice, mai precisă şi mai complexă, este prevăzută de Uniunea Europeană, în Strategia de securitate cibernetică a UE, precizându-se că acest concept se referă la „*măsurile de protecție şi acțiunile*

---

[1] P. Rosenzweig, *Cyber Warfare: how conflicts in cyberspace are challenging America and changing the world,* Ed.Praeger, 2012, p. 14-15.

[2] R.A. Clarke, R.K. Knake, *Cyberwar. The Next Threat to National Security and What To Do About It,* HarperCollins Publishers, New York, 2010, p. 70.

[3] Potrivit anexei 1 a H.G. nr. 271/2013 din 15 mai 2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, publicată în M. Of. nr. 296 din 23 mai 2013.

*care pot fi utilizate pentru a proteja domeniul cibernetic, atât în domeniul civil, cât şi militar, de acele amenințări care sunt asociate cu, sau care pot afecta, rețelele sale interdependente sau infrastructura de informații. Prin asigurarea securității cibernetice se urmăreşte păstrarea disponibilității şi integrității rețelelor şi a infrastructurii, precum şi confidențialitatea informațiilor conținute de acestea"*[1].

Întrucât ponderea amenințărilor neconvenționale a crescut în ultimul deceniu, atacurile cibernetice reprezintă o amenințare tot mai mare la adresa securității naționale şi internaționale, atât din punct de vedere cantitativ, cât mai ales calitativ, atacurile cibernetice fiind mai sofisticate şi mai complexe. Aşadar, noua viziune asupra securității trebuie să surprindă şi aspectele dezvoltării masive a tehnologiei informației şi comunicațiilor, fapt care determină lărgirea agendei de securitate prin includerea dimensiunii cibernetice a securității naționale şi internaționale. Alături de terorism şi de neproliferarea armelor nucleare sau de distrugere în masă, spațiul cibernetic reprezintă unul dintre domeniile neconvenționale de interes pentru securitatea internațională[2].

Interdependența în relațiile internaționale, în general, şi în spațiul cibernetic, în mod special, determină responsabilizarea societății internaționale, prin cooperarea internațională în vederea identificării unei abordării cuprinzătoare a securității cibernetice. Particularitățile spațiului cibernetic şi impactul multinațional al atacurilor cibernetice reclamă necesitatea adoptării unei politici publice cu o pregnantă componentă internațională. Din cauza naturii spațiului cibernetic, dar şi a caracterului asimetric şi transnațional, considerăm că amenințarea cibernetică reprezintă pentru liderii politici o provocare similară terorismului în privința necesității efortului diplomatic de reglementare a domeniului.

Dezvoltarea cooperării internaționale presupune ca prim pas convenirea unor definiții universal acceptate ale termenilor circumscrişi spațiului cibernetic, în momentul actual neexistând un consens la nivelul societății internaționale cu privire la terminologia specifică.

Problematica securității cibernetice poate fi abordată prin procesul de echilibrare intern, care presupune creşterea propriilor capacități tehnice şi a competenței resurselor umane pentru a reduce vulnerabilitățile, dar şi prin echilibrul sistemic extern, prin promovarea intereselor naționale de securitate cibernetică în formatele de alianțe internaționale care împărtăşesc percepția asupra problemei.

Asigurarea securității cibernetice are valențe internaționale, prin prisma trăsăturilor spațiului cibernetic, care face ca această amenințare neconvențională,

---

[1] Comunicare comună către Parlamentul European, Consiliu, Comitetul economic şi social european şi Comitetul Regiunilor, *Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur şi securizat,* JOIN(2013) 1 final, Bruxelles, 7 februarie 2013, accesată la http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001, ultima vizualizare la 1 august 2017 (în continuare „*Strategia de securitate cibernetică a Uniunii Europene*, 2013").

[2] A se vedea *Strategia Națională de Apărare*, 2010.

să nu aibă limite de distanță sau de frontiere în privința spațiului operativ sau al efectelor produse, necesitând securizarea atât la nivel statal, cât şi internațional.

Noutatea relativă a domeniului face ca amenințarea cibernetică să fie la începutul procesului de securizare. Necesitatea creării unui context instituțional şi normativ comprehensiv, determină oportunitatea plasării securității cibernetice sub controlul factorului politic, prin implicarea statului în elaborarea unei politici publice coerente de securitate cibernetică. Întrucât securitatea cibernetică este importantă pentru toate domeniile de securitate definite prin noul concept de securitate extins, cuprinzând sectoarele în materie economică, socială, politică şi de mediu, iar incidentele cibernetice pot avea impact major asupra stabilității din multiple sectoare de securitate, apreciem necesitatea securizării transsectoriale[1].

Responsabilitatea acestui demers aparține părților interesate *(stakeholders)* de la nivel guvernamental şi din mediul privat specializat în Tehnologia Informației şi Comunicațiilor (TIC), şi presupune interzicerea limitării drepturilor cetățenilor prin conferirea de puteri excesive serviciilor de informații. Conceptul de *stakeholder* a fost preluat în literatura de specialitate ca atare din limba engleză, în cadrul prezentei cercetări conceptul fiind folosit alternativ cu sintagma *părți interesate*[2].

Implicarea statelor şi a organizațiilor internaționale interguvernamentale este esențială, fiind consolidată de o colaborare strânsă cu sectorul privat. În procesul de minimizare a riscurilor de securitate cibernetică statul are doar rol de coordonare şi asistență, prin crearea unui cadru legislativ corespunzător, prin participarea la definirea şi implementarea de politici, prin elaborarea unor instrumente juridice şi prin întreprinderea unor acțiuni şi măsuri specifice.

Nu toate incidentele cibernetice, fie ele intenționate sau accidentale, interesează din punct de vedere al securității naționale. Caracterul de urgență existențială pentru stat are în vedere amenințarea cibernetică la adresa infrastructurilor critice, astfel încât determină prioritizarea acesteia în fața politicilor statale curente. Depindem de spațiul cibernetic pentru transport, telecomunicații, servicii de urgență, alimentarea cu energie şi apă, iar multe aspecte privind dezvoltarea economică la nivel național şi internațional vizează sistemele şi rețelele informatice. Totodată, operațiunile cibernetice pot fi considerate probleme de securitate militară sau non-militară, în funcție de motivația atacului, de actorii implicați şi de efectele produse, delimitarea domeniului militar realizându-se în baza criteriului folosirii forței. Astfel, riscurile în spațiul cibernetic sunt atât de mari, încât sunt de interes pentru stat şi prin prisma reglementărilor de drept internațional public, nu doar ca efect economic pentru mediul de afaceri.

---

[1] B. Buzan, O. Waever, J. De Wilde, p. 267-268.

[2] N. Voiculescu, M.I. Neagu, *Responsabilitatea socială a întreprinderilor: de la concept la normativizare*, Ed. Universitară, Bucureşti, 2016, p. 113-114.

Literatura de specialitate evidențiază valențele complexe ale securității cibernetice, spațiul cibernetic putând fi folosit ca o amenințare din perspectivă teroristă, infracțională sau politico-militară, în funcție de scopul pe care îl urmăreşte atacatorul, dar şi de efectele de care le produce un atac cibernetic. Din acest punct de vedere, doctrina identifică următoarele dimensiuni ale securității cibernetice, fiecare cu implicații juridice diferite: criminalitatea cibernetică, războiul cibernetic, spionajul cibernetic şi terorismul cibernetic.

## Subcapitolul 1. Criminalitatea cibernetică

În prezent, nu există o definiție a criminalității informatice universal acceptată de actorii interesați. În limba engleză, în literatura de specialitate şi în legislație sau în documente oficiale, sunt folosite alternativ sintagme precum *cybercrime*, *computer crime*, *computer-related crime*, *advanced crime, high-technology crime*[1].

Dificultatea în a defini acest concept rezidă în variabilitatea mediului infracțional specific şi în spectrul larg de activități ilegale care se circumscriu sferei criminalității informatice. Apreciem că definiția termenului de criminalitate informatică nu trebuie să fie limitativă, în înțelesul prezentei lucrări optând pentru o definiție mai generală, care să reflecte consecințele dezvoltării tehnologice asupra fenomenului infracțional.

Pornind chiar de la înțelesul noțiunii de criminalitate în general, ca şi *ansamblul faptelor penale comise într-un spațiu şi într-o perioadă de timp determinate*[2], prin raportare la criteriul naturii specifice a faptelor penale, ca element de referință, criminalitatea informatică este definită ca *ansamblul infracțiunilor comise, prin intermediul sau în legătură cu utilizarea sistemelor informatice sau rețelelor de comunicații, într-un interval temporal şi spațial determinat. Sistemele informatice şi rețelele de comunicații putând fi instrumentul, ținta sau locația acestor infracțiuni*[3]. Aşadar, adoptăm clasificarea criminalității informatice propuse în literatura de specialitate, care evidențiază funcția sistemelor şi rețelelor informatice, de obiect/țintă al infracțiunii (spre exemplu, în situația accesului ilegal la un sistem informatic) sau de instrument/mijloc material folosit la săvârşirea infracțiunilor. În această ultimă accepțiune, infracțiuni precum frauda, încălcarea dreptului de proprietate intelectuală sau pornografia infantilă sunt săvârşite prin intermediul sistemelor şi rețelelor informatice.

---

[1] I. Vasiu, L. Vasiu, *Criminalitatea în ciberspațiu,* Ed. Universul Juridic, Bucureşti, 2011, p. 119-121.

[2] V. Cioclei, *Manual de criminologie,* ed. a 5-a, Ed. C.H. Beck, Bucureşti, 2011, p. 25-26.

[3] G.I. Ioniță, *Criminalitatea informatică şi investigarea criminalistică digitală – controverse terminologice şi de conținut*, în revista Criminalistica nr. 3, iunie 2010, vol. XI, Bucureşti, 2010, p. 395-398.