ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII/1, ŞTIINŢE JURIDICE, 2021
DOI: 10.47743/jss-2021-67-1-16

Dimensiunea cibernetică a securității naționale în raport de dreptul european

The Cybernetic Dimension of National Security with Regards to the European Union Law

Ioan Dumitru Apachiței[1]

Rezumat: Dimensiunea securității cibernetice prezintă acea parte componentă a securității naționale care se raportează la oportunitățile, amenințările și mijloacele de apărare ale infrastructurii cibernetice și informațiilor. Globalizarea spațiului cibernetic a trasformat modalitatea prin care înțelegem și reacționăm la potențialele amenințări, poziția geografică ne mai reprezentând din acest punct de vedere un criteriu relevant. Scopul acestei secțiuni este să ofere o perspectivă asupra dimensiunii securității cibernetice în acord cu dreptul intern și european astfel încât să poată constitui o bază de raportare analitică la cadrul legal național și la posibilitățile de îmbunătățire a acestuia. Prezenta analiză a securității cibernetice este structurată în trei părți. Prima parte oferă reperele doctrinare de referință în înțelegerea conceptului și dimensiunilor securității cibernetice, a doua parte trece în revistă principalele strategii europene de asigurare a securității cibernetice, care printr-o analiză compartativă să releve principalele orientări și direcția evoluției la nivelul statelor membre ale Uniunii Europene, atât individual, cât și colectiv, iar cea de a treia secțiune prezintă cadrul legal național, analizat și prin prisma interferențelor legislației europene.

Cuvinte-cheie: securitate cibernetică, strategie de securitate cibernetică, infrastructură critică, securitatea informațiilor

Abstract: The cybersecurity dimension regards that element of the national security which relates to the opportunities, threats and means of defense of the cyber infrastructure and information. The globalization of the cyberspace has shaped the way we understand and react to potential threats, our geographical position being a relevant criterion. The purpose of this section is to provide an insight into the cybersecurity dimension in accordance with the national and the European law so that it could constitute a basis for analytical reporting to the national legal framework and the possibilities of improving it. This cyber security analysis is structured in three parts. The first part provides the doctrinal benchmarks in understanding the concept and dimensions of cybersecurity; in the second part we review the main European strategies for ensuring cybersecurity, which through a comparative analysis should reveal the main orientations and the evolution in the

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, avocat în cadrul Baroului Iași, email : ioandumitruapachitei@gmail.com.

Member States of the European Union, both individually and collectively; and in the third section we shall focus on the national legal framework, analysed also in the light of the interferences of the European legislation.

Keywords: cybersecurity, cybersecurity strategy, critical infrastructure, information security

1. Preliminarii

Securitatea cibernetică împrumută unele dintre trăsăturile securității naționale, prin raportare la noțiunile de risc, amenințări, vulnerabilități particularizate prin intermediul canalului de transmitere, în fapt efectele atacurilor cibernetice având repercusiuni directe asupra spațiului fizic[2]. Securitatea cibernetică este definită în cuprinsul Strategiei de securitate cibernetică a României ca fiind „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private din spațiul cibernetic. Măsurile proactive și reactive pot include: politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor”[3].

2. Conceptul şi dimensiunile securităţii cibernetice

Conectivitatea la nivel global și apariția spațiului cibernetic[4] a determinat o redefinire a conceptului de securitate națională și o reinterpretare a mecanismului de determinare a provenienței riscului. Într-o lume interconectată și cu o mobilitate crescută o clasificare a surselor de risc în funcție de tiparul clasic de riscuri interne și riscuri externe apare ca fiind perimată[5]. Securitatea națională se califică în prezent ca fiind o stare de încredere din partea publicului că riscurile sunt anticipate, iar evoluția societății este ferită de pericole imprevizibile. S-a arătat că menținerea cu succes a securității naționale este un indicator al faptului că

---

2 D. Panc, *Securitatea cibernetică la nivel naţional şi internaţional. Instrumente normative şi instituţionale*, Ed. Hamangiu, București, 2017, p. 9.

3 Definiție preluată *ad literam* și în cuprinsul art. 2 lit. e) din H.G. nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO, publicată în Monitorul Oficial al României, Partea I nr. 388 din 02 iunie 2011.

4 Noțiunea de spațiu spațiu cibernetic (în engleză cyberspace) se consideră că a apărut prima oară în literatura de ficțiune, printre pionierii acesteia numărându-se William Gibson prin nuvela *Burning Chrome* publicată în revista Omni, în anul 1984. În acest sens, a se vedea F. Delerue, *Cyber operations and international law*, Ed. Chambridge University Press, Chambridge, United Kingdom, 2020, p. 10.

5 A se vedea și D.C. Mâță, *Securitatea națională. Concept. Reglementare. Mijloace de ocrotire*, Ed. Hamangiu, București, 2016, pp. 29-30.

națiunea este protejată fără ca drepturile și libertățile să fie erodate[6]. Din cele expuse se poate deduce o simetrie calitativă și cantitativă, astfel încât cu cât avem mai multă siguranță, cu atât drepturile și libertățile sunt mai protejate. Spațiul cibernetic a dus la o redefinire a participanților care pot acționa în sensul protejării sau amenințării securității. Securitatea națională, în sensul său originar, era influențată doar de către state, însă privitor la securitatea cibernetică se constată că pot fi participanți atât persoanele juridice private deținătoare ale sistemului informatic, cât și persoane private, capabile să obțină, să sustragă sau să altereze date informatice[7].

Printre avantajele spațiului cibernetic se numără și confidențialitatea[8], atât a datelor, cât și a utilizatorilor. Cu toate acestea s-a susținut că nici securitatea și nici confidențialitatea nu se pot concretiza în drepturi absolute, în susținerea acestor considerente s-a arătat pe de o parte că și anterior digitalizării anonimatul nu era acceptat, iar pe de altă parte că nu se poate concilia cu actul de justiție și, implicit, cu respectarea legii[9]. O abordare similară o regăsim și în cuprinsul art. 29 paragraful 2 din Declarația Universală a Drepturilor Omului[10], respectiv în art. 10 paragraful 2 din Convenția Europeană a Drepturilor Omului[11].

---

6 D. Omand, *Understanding Digital Intelligence: A British View* în E. De Silva (coord.), *National Security and Counterintelligence in the Era of Cyber Espionage*, Ed. IGI Global, Hershey, 2016, p. 114.

7 În acest context apare ca fiind depășită concepția neorealistă care își fundamenta existența prin identificarea securității cu autoritatea statală, statul fiind considerat exponentul securității și al autorității, iar securitatea sa coincizând cu cea a cetățenilor. În acest sens, a se vedea K. Krause, M. C. Williams, *Broadening the Agenda of Security Studies: Politics and Methods*, în Mershon International Studies Review, vol. 40, nr. 2/1996, p. 232 și P. Rosenzweig, *Cyber Warfare. How conflicts in cyberspace are challenging America and changing the* word, Ed. Praeger, Santa Barbara, California, 2013, p. 21.

8 Cu titlu de notă informativă precizăm că trebuie realizată o distincție între spațiul virtual public și *Dark Web*, acesta din urmă constituind principalul canal de comunicare în vederea ascuderii infracționalității cibernetice, fie că vorbim de infracțiuni la adresa securității naționale sau orice alt tip de infracționalitate. Principala caracteristică a *Dark Web-ului* este reprezentată de anonimizarea utlilizatorilor prin imposibilitatea detectării adresei IP a site-ului accesat. A se vedea P. L. Dordal, *Dark Web*, în H. Jahankhani (coord.), *Cyber Criminology*, Ed. Springer, Switzerland, 2018, p. 95.

9 D. Omand, *op. cit.*, p. 104.

10 „În exercitarea drepturilor şi libertăţilor sale, fiecare om nu este supus decît numai îngrădirilor stabilite prin lege, exclusiv în scopul de a asigura cuvenita recunoaştere şi respectare a drepturilor şi libertaţilor altora şi ca să fie satisfăcute justele cerinţe ale moralei, ordinii publice şi bunăstării generale într-o societate democratică".

11 „Exercitarea acestor libertăţi ce comportă îndatoriri şi responsabilităţi poate fi supusă unor formalităţi, condiţii, restrângeri sau sancţiuni prevăzute de lege care, într-o societate democratică, constituie măsuri necesare pentru securitatea naţională, integritatea teritorială sau siguranţa publică, apărarea ordinii şi prevenirea infracţiunilor, protecţia sănătăţii, a moralei, a reputaţiei sau a drepturilor altora, pentru

Digitalizarea a fost înțeleasă de doctrina britanică sub reperele privitoare la etică și drepturilor omului, clasificând-o sub aspectul său juridic în trei structuri referitoare la securitatea cibernetică, acestea privind: asigurarea fiabilității internetului în vederea îndeplinirii obiectivelor economico-sociale, politice sau militare, adaptarea legislației la tipologia faptelor relevante penal săvârșite prin intermediul internetului și activitatea agențiilor de informații în exploatarea canalelor de comunicații cibernetice astfel încât să poată obține informațiile specifice în vederea asigurării securității[12].

Diferențele dintre capabilitățile naționale și relațiile socio-politice determină statele lumii să adopte o poziție diferită față de prioritizarea amenințărilor la adresa securității cibernetice, diferențele de perspectivă putând conduce la abordări diferite ale tehnicilor de apărare cibernetică[13] și implicit la impedimente cu privire la consensualitatea unor acțiuni comune. Armonizarea perspectivelor asupra surselor de pericol reprezintă un prim pas în direcția obținerii unor planuri comune de acțiune[14].

Menținerea securității cibernetice presupune acceptarea ca statele, prin agențiile de informații, să își exercite competențele în acest domeniu, dar cu respectarea condițiilor de necesitate și proporționalitate raportate la ingerințele aduse vieții private a persoanelor. Pornind de la teoriile formulate ca urmare a experienței conflictelor armate, doctrina a fundamentat o serie de condiții bazate pe *jus ad bellum*[15] și *jus in bello*[16] transpuse în perspectiva securității cibernetice. Operațiunile cibernetice ostile pot fi supuse legilor războiului sau dreptului internațional (calificată sub o perspectivă generală a non-intervenției) în funcție de

a împiedica divulgarea informaţiilor confidenţiale sau pentru a garanta autoritatea şi imparţialitatea puterii judecătoreşti".

12 D. Omand, *op. cit.*, p. 99.

13 Apărarea cibernetică a fost înțeleasă a acel complex de mijloace destinate „prevenirii, detectării și oferirii de răspunsuri la timp la atacuri sau amenințări, astfel încât să nu fie afectată nicio infrastructură sau informație", a se vedea D. Galinec, D. Možnik, B. Guberina, *Cybersecurity and cyber defence: national level strategic approach*, în Automatika, vol. 58, nr. 3/2017, p. 274, disponibil pe https://doi.org/10.1080/00051144.2017.1407022, accesat la data de 24 iulie 2020.

14 F. Hare, *The cyber threat to national security: why can't we agree?*, în C. Czosseck & Podins (Eds), *Proceedings of the Conference on Cyber Conflict,* Tallinn, Estonia: CCD COE Publications, 2010, p. 212.

15 Termen ce definește ansamblul condițiilor de a căror îndeplinire este motivată necesitatea intrării într-un conflict armat. O normativizare actuală a *Jus ad bellum* în legislația internațională este dată de dispozițiile art. 2 paragraful 4 și art. 51 din Carta Națiunilor Unite.

16 Noțiune prin care denumește ansamblul reglementărilor ce devin incidente odată cu începerea unui conflict armat. În mod complementar mai arătăm că se consideră că în ipoteza unui război cibernetic statele au posibilitatea (dreptul) de a răspunde prin utilizarea oricăror alte instrumente militare, în acest sens, a se vedea P. Rosenzweig, *op. cit.*, p. 32.

gravitatea atacului exercitat asupra sistemelor informatice[17]. Depășirea acestor inconveniente de ordin juridic se consideră că s-ar putea realiza prin elaborarea unui tratat privind securitatea cibernetică, un astfel de proiect a fost inițiat fără succes în anul 2012 de către Rusia, ulterior acest stat încheind un pact, sub aceeași sferă de incidență, cu Republica Populară Chineză. S-a susținut că în vederea elaborării unui tratat privind spațiul cibernetic poate fi utilizată Convenția din anul 1997 privind armele chimice[18].

Agențiile (serviciile) de informații trebuie să aibă în vedere existența unor motive temeinice corespondente intereselor naționale, este necesar să fie asigurată integritatea informațiilor de la obținere și până la analizarea rezultatelor, astfel încât obținerea informațiilor să fie realizată de către o autoritate competentă din punct de vedere legal și cu posibilitatea de a fi supravegheată[19], să existe un raționament solid al investigației și de selectare a subiecților investigați și, în final, informațiile să nu poată fi obținute pe alte căi oficiale[20].

Includerea securității cibernetice în cadrul mai larg al securității naționale se realizează prin sincronizarea factorilor generatori de amenințare și punctele de vulnerabilitate dintre cele două. Suprapunerea parțială a celor două domenii de securitate ne arată condițiile în funcție de care putem califica o amenințare ca fiind de natură cibernetică și cu potențial de a afecta granițele securității naționale. Sursele de amenințare pot viza atât statul ca entitate de drept internațional, cât și organizații internaționale sau persoane fizice și juridice. Amenințarea poate lua forma spionajului industrial[21], poate viza identitatea personală în vederea săvârșirii

---

17 A se vedea și M.N. Schmitt (general editor), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Ed. Cambrindge University Press, Cambridge, 2017, pp. 375 – 376.

18 A se vedea și I. Mann, *Towards a Cyber-Security Treaty* (Just Security, 03 august 2016), disponibil pe https://www.justsecurity.org/32268/cyber-security-treaty, accesat la data de 15 iulie 2020. Într-un sens apropiat, se face referire și în cuprinsul Strategidei de securitate cibernetică a Germaniei, document ce afirmă necesitatea existenței unui cod care să stabilească conduita statelor în spațiul cibernetic, a se vedea Strategia de securitate cibernetică a Germaniei, p. 11. Pe de altă parte, prin Strategiei de securitate cibernetică a Uniunii Europene, se stabilește faptul că Uniunea „nu cheamă la crearea de noi instrumente juridice internaționale pentru aspectele cibernetice", caz în care în situația unor conflicte armate în spațiul cibernetic „se vor aplica dreptul umanitar internațional și, după caz, legea drepturilor omului", a se vedea Strategia de securitate cibernetică a Uniunii Europene (2013), p. 17.

19 Supravegherea serviciilor de informații ridică din această perspectivă problema loialității autorității chemate să realizeze supravegherea, aceasta trebuind să ofere suficiente garanții.

20 D. Omand, *op. cit.*, p. 104.

21 Pentru un studiu de caz privitor la sesizarea din anul 2007 a autorităților germane conform căreia aproximativ 40% dintre companiile din această țară au fost victime ale spionajului industrial provenit din Rusia și China a se vedea M.C. Libicki, *Cyberdeterrence and cyberwar*, RAND Corporation, 2009, p. 25, nota 38, disponibil pe https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

unor fapte relevante din perspectiva securității naționale, în fine, un atac cibernetic poate viza chiar instituțiile statului și forma de organizare a statului[22].

Totodată, includerea securității cibernetice în domeniul mai larg al securității naționale se află în opoziție cu teoriile neorealiste care considerau că securitatea națională poate fi afectată doar prin acțiuni de natură militară îndreptate împotriva statului[23]. În opoziție, exponenții Școlii de la Copenhaga Barry Buzan și Ole Waever au extins conceptul de securitate națională de la contextul militar și politic la cel economic, social, ecologic. În aceste două perspective conceptuale observăm că securitatea cibernetică are o structură complexă căreia îi pot fi asociate atât repere de natură militară[24], politică, cât și economică[25], fapt justificat de digitalizarea tuturor acestor domenii[26]. Mai mult decât atât, unii autori consideră că digitalizarea accelerată în mai toate domeniile determină concomitent și incidența unor potențiale riscuri de natură cibernetică, fapt care se consideră ca va determina ca la un moment dat conceptul de securitate națională să se identifice cu cel de securitate cibernetică[27]. *Cu toate acestea, considerăm că asocierea securității cibernetice, ca ramură a securității naționale, cu domeniul economic trebuie să fie analizată cu prudență pentru că securitatea economică, spionajul cibernetic sau furtul de proprietate intelectuală în scop economic pot avea valențe în sfera securității naționale doar în măsura în care se constituie într-un risc la adresa acesteia[28].*

---

[22] F. Hare, *op. cit.*, p. 213.

[23] S-a mai arătat și faptul că esența neorealismului este reprezentată de respingerea oricăror noi abordări asupra problemelor de securitate, în fapt acceptând un sens restrâns al noțiunii, a se vedea K. Krause, M. C. Williams, *op. cit.*, p. 233. Autorii citați mai arată că ceea ce a condus la abandonarea teoriilor neorealiste sunt problemele legate de degradarea mediului, acestea transced granițele convenționale reprezentând o reală problemă asupra tuturor actorilor statali. Mai menționăm cu această ocazie că o serie dintre elementele caracteristice securității de mediu sunt similare și în cazul securității cibernetice.

[24] Pentru o perspectivă asupra securității cibernetice a forțelor militare aeriene, a se vedea M.C. Libicki, *op. cit.*, p. 6. În doctrină se mai opinează că spațiul cibernetic nu ar trebui să constituie al cincilea domeniu în care se pot exercita operațiuni militare, alături de spațiul terestru, maritim, aerian și extraatmosferic, fiind doar un canal de comunicare digital al celor deja existente, în acest sens, a se vedea F. Delerue, *op. cit.*, p. 12.

[25] Cu toate acestea s-a mai arătat faptul că s-au utilizat argumente privind securitatea națională (în fapt securitatea cibernetică) ca pretext pentru protejarea intereselor comerciale, cel mai elocvent exemplu fiind reprezentat de restricțiile impuse Huawei (China) de către Guvernul Statelor Unite ale Americii. Pentru mai multe detalii, a se vedea Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, în Journal of International Economic Law, Ed. Oxford University Press, vol. 18, nr. 2/2015, pp. 10-11.

[26] În același sens, a se vedea F. Hare, *op. cit.*, p. 215.

[27] S. Topor, *Education in the cyber security field and implications for national security*, în Annals – Series on Military Sciences, nr. 1/2020, p. 82.

[28] A se vedea și C. Wilson, N. Drumhiller, *US – China Relations: Cyber Espionage and Cultural Bias* în E. De Silva (coord.), *National Security and Counterintelligence in the Era of Cyber Espionage*, Ed. IGI Global, Hershey, 2016, p. 29.

Pornind de la aceste repere literatura de specialitate a identificat o serie de dimensiuni proprii securității cibernetice, prin raportare la sfera factorilor de risc și sfera efectelor asociate; acestea făcând referire la „criminalitatea cibernetică, războiul cibernetic, spionajul cibernetic și terorismul cibernetic”[29].

Mai trebuie realizată o distincție între conceptele de *securitate a informațiilor*, *securitate cibernetică* și noțiunea mai largă a *securității naționale*. Securitatea informațiilor face referire la confidențialitatea datelor, mai mult decât atât, securitatea cibernetică face trimitere la protejarea infrastructurilor critice, iar nu doar acelora privitoare la informațiilor cu caracter privat sau de natură publică, argument pentru care securitatea cibernetică excede securității informațiilor și se include în conceptul de securitate națională[30].

Pe bună dreptate s-a sesizat în doctrină faptul că asistăm la un fenomen de diluare a noțiunii de securitate națională, în general, și a securității cibernetice în special[31]. În opinia noastră este necesară păstrarea caracteristicilor proprii securității cibernetice și raporturilor de incidență cu securitatea națională, altfel spus să existe o corespondență calitativă la factorii de amenințare și la riscurile incidente. Fundamentarea unei astfel de ideei privitoare la o diluare a conceptului de securitate, are la baza o serie de discordanțe ale studiilor de securitate, acestea fiind determinate pe de o parte de faptul că statele, în funcție de agenda politică adoptată la un moment dat, pot avea o percepție diferită asupra amenințărilor, pe de altă parte s-a mai arătat că diversele studii de securitate abordează domeniul dintr-o perspectivă politică proprie statului în care s-au format[32].

Amenințarea cibernetică are capacitatea de a afecta toate nivelurile securității într-un timp foarte scurt, având ca factor favorizant interconectarea structurilor strategice, comerciale, sanitare etc[33]. În cadrul legislativ român amenințarea cibernetică este înțeleasă ca o „circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice”[34]. Amenințările pot proveni din variate surse atât individuale, cât și colective, privite ca grupări de hackeri, grupări teroriste, crima organizată sau state ostile[35]. Se consideră că tehnologiile bazate pe web cunosc o aplicabilitate diversă privitor la planificarea și executarea actelor teroriste, acestea fiind împărțite în cinci categorii: utilizarea internetului în vederea furnizării de informații, finanțarea și obținerea de fonduri, construirea de rețele interconectate între grupările teroriste, recrutarea și

[29] D. Panc, *op. cit.*, p. 20.

[30] Shin-yi Peng, *op. cit.*, p. 34. Arătăm că există și opinii care consideră că securitatea cibernetică se fundamentează pe securitatea informațională, în acest sens, a se vedea D.C. Mâță, *op. cit.*, p. 30.

[31] D. C. Mâță, *Cybersecurity – Dimensions of national security*, în Journal of Law and Administrative Sciences, Special Issue, 2015, p. 134.

[32] În același sens, a se vedea K. Krause, M. C. Williams, *op. cit.*, p. 245 și 249.

[33] F. Hare, *op. cit.*, p. 215.

[34] Strategia de securitate cibernetică a României (2013), p. 7.

[35] M. E. Hathaway, *Cyber Security. An economic and national security crisis*, în Intelligencer Journal, vol 16, nr. 2/2008, p. 31.

instruirea adepților, obținerea și distribuirea informațiilor[36]. Digitalizarea activităților determină o vulnerabilitate în fața eventualelor atacuri cibernetice, sens în care afectarea sistemului financiar, sistemului medical, sistemului de control al traficului aerian, a sistemului feroviar poate reprezenta o reală amenințare la adresa securității naționale[37].

Potențialitatea unor prejudicii aduse componentelor securității naționale prin utilizarea spațiului cibernetic este una actuală. De exemplu, în anul 2008 utilizarea sistemelor computerizate în vederea transmiterii de e-mail-uri false concomitent cu accesarea sistemelor bancare franceze în vederea depășirii limitelor de tranzacționare, fapt ce a condus la tranzacționarea neautorizată de poziții pe bursă în cuantum de 73 de miliarde de dolari[38]. De referință mai este și cazul Estoniei din 2007 când atacul împotriva sistemelor informatice a avut ca urmare blocarea accesului utilizatorilor la instituții de stat, sisteme bancare rețele de comunucații interinstituționale[39]. Într-o manieră similară poate fi privit și războiul cibernetic[40] dintre Rusia și Georgia din anul 2008, context în care președinta Consiliului Național de Securitate a Georgiei, în cadrul Conferinței GovSec din 2009, a declarat că informaticienii statului atacator sunt asemenea soldaților[41]. Un alt exemplu poate fi reprezentat de atacul din anul 2007 împotriva site-ului Bursei de valori din Londra, fapt ce a cauzat disfuncționalități pentru aproximativ 48 de ore[42].

Pentru ca o acțiune exercitată în spațiul cibernetic să atenteze la securitatea națională, de regulă sunt avute în vedere infrastructurile critice[43], acestea fiind

---

36 S. Virkar, *The mirror has two faces: Terrorist use of the internet and the challenges of Governing Cyberspace*, în E. De Silva, *op. cit.*, p. 10.

37 M. E. Hathaway, *op. cit.*, p. 35.

38 *Idem*, p. 34.

39 În sensul că atacul cibernetic asupra Estoniei din anul 2007 este considerat un act de război, a se vedea M.C. Libicki, *Cyberdeterrence and cyberwar*, RAND Corporation, 2009, p. 179 și M.N. Schmitt (general editor), *Tallinn Manual 2.0, op. cit.*, p. 376. Complementar mai arătăm și faptul că din anul 2014 există un parteneriat între Guvernul Estoniei și NATO, precum și un acord privind securitatea încheiat cu Guvernul Statelor Unite ale Americii în anul 2017, disponibil pe https://www.riigiteataja.ee/aktilisa/2160/6201/7002/Est_USA_agreement.pdf, accesat la 09 iulie 2020.

40 Noțiunea de război cibernetic este privită în literatura de specialitate ca un conflict care tranzitează aceleași paliere ale războiului convențional. Chiar dacă conflictul este purtat prin intermediul spațiului cibernetic, urmările sunt incidente și în spațiul fizic, pentru o serie elocventă de exemple și ipoteze ale urmărilor posibile ale unui război cibernetic, a se vedea P. Rosenzweig, *op. cit.*, pp. 31-34.

41 F. Hare, *op. cit.*, p. 218 și P. Rosenzweig, *op. cit.*, p. 28 și 32. Acest ultim autor citat mai oferă un exemplu privtor la virusul „Gh0stNet", programat să înregistreze datele obținute prin camera video și microfonul computerului, virus ce a infectat calculatoarele a ambasadelor Indiei, Malaeziei, Indoneziei și din sediul central al NATO.

42 M. E. Hathaway, *op. cit.*, p. 35.

43 Noțiunea are o semnificație dual, iar prin referirea la infrastructurile critice înțelegem atât echipamentele fizice utilizate pentru a facilita funcționarea și securitatea societății

reprezentate de serviciile de bază care satisfac o societate și includ resurse, consumabile, bunuri industriale și servicii generale. În literatura de specialitate infrastructurile critice au fost definite ca fiind „coloana vertebrală a socetății”[44]. Relevanța acestora în materia securității cibernetice este dată de repercusiunile potențiale la adresa unui grup de cetățeni sau a întregii societăți. Autorii anterior citați indică cu titlu de exemplu atacul cibernetic care a avut loc în Ucraina în anul 2015 prin care a fost oprită distribuția energiei electrice pentru aproximativ 6 ore, provocând pagube majore la nivelul întregului stat[45]. Având în vedere contextul conflictelor cibernetice internaționale s-a concluzionat că există o cursă a înarmării cibernetice[46].

Distincția dintre atacul cibernetic și spionajul cibernetic privește atât modalitatea de abordare a atacatorului, cât și consecințele și probabilitatea de detectare a acestuia. În cazul atacului cibernetic vorbim despre un atacator și o țintă[47], care spre deosebire de spionajul cibernetic blochează funcționalitatea *sistemului*. Pe de altă parte spionajul cibernetic nu are ca scop alterarea sistemului, ci doar obținerea de date, fapt ce determină o dificultate mai mare în depistarea acestuia[48]. Scopul sionajului cibernetic poate avea două destinații distincte, sub aspectul reprercusiunilor în realitatea fizică, fie în scopul obținerii de informații industriale pentru câștigarea unui avantaj comercial, fie asupra instituțiilor guvernamentale, în vederea obținerii de informații clasificate. Trebuie admis faptul că poate exista și o destinație mixtă între cele amintite anterior[49].

Faptul că guvernele stochează o cantitate mare de informații care mai apoi este transmisă între instituțiile statului sau către alte instituții străine sau persoane private creează premisele ca aceste informații să fie sustrase sau alterate. Un atac de natură cibernetică asupra acestui tip de informații poate determina „destabilizarea economiei, subminarea suveranității și perturbarea serviciilor vitale, constituind astfel o amenințare directă pentru securitatea națională”[50], în fapt devenind o chestiune de politică națională prin prisma implicațiilor generate.

și a economiei, cât și programele informatice prin care infrastructura critică a unui stat devine operațională. În acest sens, a se vedea *Guide to developing a national cybersecurity strategy. Strategic engagement in cibersecurity*, International Telecommunication Union, Geneva, 2018, p. 14, disponibil pe https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf, accesat la data de 23 iulie 2020.

44 S. Rass, S. Schauer, S. König, Q. Zhu, *Cyber-Security in Critical Infrastructures. A game-theoretic approach*, Ed. Springer, Switzerland, 2020, p. 3.

45 *Idem.*, p. 14.

46 F. Hare, *op. cit.*, p. 212.

47 S-a reținut că atacul cibernetic poate fi asemănat cu un act de război, în acest sens M.C. Libicki, *op. cit.*, p. 23 și 179.

48 Pentru referințe privitoare la confluența dintre spionajul cibernetic și raporturile de drept comercial internațional dintre Statele Unite ale Americii și compania chineză Huawei, a se vedea Shin-yi Peng, *op. cit.*, pp. 3-13 și 37.

49 P. Rosenzweig, *op. cit.*, p. 23.

50 Shin-yi Peng, *op. cit.*, p. 35 și 47.

Apărarea împotriva atacurilor cibernetice poate fi adoptată dintr-o perspectivă individuală sau colectivă, în lipsa unei armonizări asupra perspectivelor referitoare la factorii de risc, statele vor fi nevoite să adopte o strategie individuală de apărare. Cu toate acestea avem în vedere lipsa de relevanță geo-strategică, dat fiind faptul că atacurile cibernetice depășesc granițele convenționale, acesta poat determina o serie de puncte nevralgice la adresa securității de grup, fie că avem în vedere Uniunea Europeană sau NATO. În esență, găsirea unei strategii intermediare între apărarea individuală și cea de grup poate reprezenta atât o variantă de compromis, cât și una eficientă[51].

Asigurarea securității cibernetice depășește granițele convenționale și reprezintă o chestiune aflată pe agenda de securitate a tuturor statelor. În acest context s-a pus problema incidenței dreptului internațional în spațiul cibernetic. Adoptarea la nivelul Națiunilor Unite a două rezoluții[52] privind aplicabilitatea dreptului internațional și a Cartei ONU este de natură să clarifice cadrul juridic aplicabil, însă fără a fi stabilită și o modalitate de aplicare. Sub acest aspect s-a reținut faptul că sunt state care contestă aplicabilitatea dreptului internațional asupra spațiului cibernetic, în special în domeniile de incidență ale cadrului normativ ce reglementează conflictele armate, apărarea și luarea contramăsurilor, aspecte care creează potențialitatea unor riscuri de fragmentare geografică a aplicabilității normelor de drept internațional[53]. În procesul de emulare a dreptului intrnațional pe specificul spațiului cibernetic nu sunt implicați doar actori statali, ci devine un domeniu în care sectorul privat devine unul foarte activ[54], dat fiind faptul că interesele ce țin de asigurarea securității naționale interferează cu interesele economice.

Reglulile de drept internațional pot conferi repere de anticipare a mijloacelor legale de prevenire și soluționare a incidentelor ce ar privi spațiul cibernetic. O opinie doctrinară care pornește de la cauzele *Barcelona Traction*[55] și *Corfu Channel*[56] instrumentate de Curtea Internațională de Justiție relevă faptul că statele sunt responsabile de obligațiile *erga omnes*, implicit și de asigurare a surselor de pericol care ar putea atenta la siguranța altor state, în măsura în care acestea le

[51] F. Hare, *op. cit.*, p. 223.

[52] A se vedea rezoluția A/68/98* din anul 2013, respectiv rezoluția A/70/174 din anul 2015.

[53] F. Delerue, *op. cit.*, p. 5 și 14.

[54] În acest moment ne rezumăm doar la a da două exemple de propuneri ale Microsoft: setul de norme privind conduita statelor în spațiu cibernetic și normele de conduită pentru comportamentul statelor și industria cibernetică globală, disponibile pe https://www.microsoft.com/en-us/cybersecurity/content-hub/reducing-conflict-in-lnternet-dependent-world și https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms, accesate la 15 iulie 2020.

[55] Disponibil pe https://www.icj-cij.org/files/case-related/50/050-19700205-JUD-01-00-EN.pdf, accesat la 16 iulie 2020.

[56] Disponibil pe https://www.icj-cij.org/files/case-related/1/001-19491215-JUD-01-00-EN.pdf, accesat la 16 iulie 2020.

sunt cunoscute[57]. Astfel, se realizează o transpunere a principiilor dreptului internațional în vederea identificării unor repre de soliționare a conflictelor în cadrul unui război cibernetic care ar crea posibilitatea tragerii la răspundere a statului sau statelor implicate. Opinie pe care o considerăm relevantă cu atât mai mult în ipoteza infracționalității cibernetice unde securitatea națională a unui stat poate fi amenințată și de persoane private, acestea acționând independent sau la coordonarea unui stat. Astfel, statele au atât o obligație pozitivă de a se asigura că pe teritoriul lor nu există grupări care prin atacuri cibernetice să provoace pagube unui alt stat, cât și o obligație negativă de a se abține ele însele de la a întreprinde astfel de acțiuni.

3. Strategii europene de asigurare a securității cibernetice

Strategia de securitate cibernetică este relevantă în vederea stabilirii cadrului general de acțiune și trebuie să se afle într-o permanentă adaptare atât la ritmul evoluției tehnologice, cât și la natura factorilor generatori de vulnerabilitate. În acest sens, poate cel mai elocvent exemplu în oferă preambulul Strategiei de securitate cibernetică franceze care afirmă că ulterior adoprării precedentei Strategii, în anul 2011, rețelele informatice ale ministerelor franceze au fost victime ale atacurilor cibernetice, consecințele fiind reprezentate de sustragerea informațiilor economice, politice și financiare; aceste consecințe au determinat autoritățile publice franceze ca în anul 2015 să elaboreze o nouă Strategie privind securitatea cibernetică[58]. Atât Strategia privind securitatea cibernetică a Franței, Germaniei, cât și cea a Spaniei, aceasta din urmă adoptată de dată recentă, au semnalat necesitatea reajustării obiectivelor de securitate în spațiul cibernetic, demers justificat de schimbările fundamentale pe care tehnologia le provoacă suveranității, conceptului de aplicabilitate normativă teritorială, mijloacelor de schimb monetar.

Un punct de referință în elaborarea strategiilor de securitate cibernetică din statele membre ale Uniunii Europene este reprezentat de Convenția de la Budapesta privind criminalitatea informatică[59] care cuprinde o serie de incriminări și dispoziții privind cooperarea internațională în materia infracțiunilor cibernetice. Ca și consecință, armonizarea și consolidarea bazelor normative și a instrumentelor de cooperare simplificată au devenit priorități cheie ale statelor. Mai mult decât atât, s-a exprimat chiar perspectiva implementării prevederilor din Convenția privind criminalitatea informatică la nivelul ONU[60].

---

57 D. Delibasis, *Cybersecurity and state responsibility: Identifyng a due diligence standard for prevention of transboundary threats* în J. Kulesza, R. Balleste (editori), *Cybersecurity and human rights in the age of vyberveillance,* Ed. Rowman & Littlefield, Lanham, 2016, pp. 23-24.

58 Strategia de securitate cibernetică a Franței, 2015, p. 7.

59 Ratificată de România prin Legea nr. 64 din 24 martie 2004, publicată în Monitorul Oficial al României nr. 343 din 20 aprilie 2004.

60 Strategia de securitate cibernetică a Germaniei, 2016, p. 10.

În continuarea expunerii inițiale privind reconceptualizarea securității prin distanțarea de teoriile neorealiste, constatăm că strategiile de securitate cibernetică a statelor membre ale Uniunii Europene consacră printre obiectivele asumate importanța protejării persoanelor private de atacurile cibernetice, în deosebi când acestea sunt practicate pe scară largă. Într-o manieră foarte clară, Strategia de securitate cibernetică a Franței reclamă faptul că Agenția Națională de Securitate Cibernetică (ANSSI) este destinată identificării incidentelor de securitate cibernetică ce afectează instituțiile publice, infrastructuri critice, fapt ce o distanțează de atacurile cibernetice îndreptate împotriva persoanelor private. Cu toate acestea, Strategia Franceză semnalează necesitatea ca victimele unor astfel de atacuri să aibă la dispoziție un serviciu public competent; în contextul extinderii rolului rețelelor de socializare și a platformelor digitale, acestea pot fi utilizate în vederea dezinformării, iar o astfel de ipoteză contravine intereselor fundamentale, constituind un atac la securitatea națională[61]. Într-o manieră similară, dar incompletă prin raportare la amplitudinea fenomenului cibernetic asupra persoanelor fizice, Strategia de securitate cibernetică a României se rezumă la a constata faptul că amenințările din spațiul cibernetic pot conduce la „cauzarea unui prejudiciu patrimonial, hărțuirea și șantajul persoanelor fizice și juridice, de drept public și privat".

Stabilirea unei legături între datele personale și securitatea cibernetică, ca partea a securității naționale, necesită identificarea coordonatelor și implicațiilor strategice. Pentru început semnalăm faptul că Strategia privind securitatea cibernetică a României[62] nu cuprinde obiective și direcții de acțiune în privința protejării datelor personale. Pe de altă parte Strategia franceză arată că la baza îmbunătățirii serviciilor publice stă și prelucrarea datelor personale, iar utilizarea rău-intenționată a acestora poate provoca destabilizări economice, propagandă ori inducerea în eroare, considerându-se că aceste amenințări prezintă un potențial risc la adresa securității naționale, date fiind implicațiile sale extinse la nivelul statului.

Asumarea de către România a unei strategii privind securitatea cibernetică are loc în contextul mai larg al dezvoltării tehnologiilor de transmitere a informațiilor la distanță și a pericolelor asociate. Scopul strategiilor de apărare vizează o creștere a nivelului de protecție a infrastructurilor cibernetice[63], iar din perspectiva securității naționale se face referire în special la infrastructurile critice naționale. În mod regretabil Strategia de securitate cibernetică a României a omis

---

61 Strategia de securitate cibernetică a Franței, 2015, p. 20. În același sens s-a abordat și preambulul Strategiei de securitate cibernetică a Spaniei, 2019, p. 15.

62 H.G. nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, publicată în Monitorul Oficial al României, Partea I nr. 296 din 23 mai 2013.

63 În literatura de specialitate se mai uzitează și ideea de scădere a nivelului de vulnerabilitate. În acest sens, a se vedea D. Galinec, D. Možnik, B. Guberina, *op. cit.*, p. 276.

să ofere o definiție noțiunii de „infrastructuri critice" sau să facă trimitere la legislația națională incidentă în materie - H.G. nr. 718/2011 privind aprobarea Strategiei naționale privind protecția infrastructurilor critice - rezumându-se doar la a sublinia importanța acesteia în asigurarea securității cibernetice[64], însă utilizează și definește noțiunea de „infrastructuri cibernetice"[65], fără a preciza dacă există o relație de echivalență între cele două[66]. Spre comparație, Strategia de securitate cibernetică a Germaniei definește infrastructura critică prin acele organizații sau instituții cu importanță majoră pentru bunăstarea publică, a căror disfuncționalități sau deteriorări pot conduce la blocaje, perturbări ale securității publice, fiind considerate ca domenii ce fac parte din categoria infrastructurii critice: energia, transportul, sănătatea, aprovizionarea cu apă și alimente, sectorul financiar, precum și administrația publică[67].

Strategia de securitate cibernetică a României[68] este justificată prin necesitatea combaterii criminalității informatice pe plan național, european și internațional, aceasta are la bază o serie de măsuri destinate creșterii cooperării și coordonării dintre autoritățile competente, elaborarea unui cadru de reglementare coerent și armonizat la nivelul Uniunii Europene și conștientizarea pericolelor și a pagubelor care ar putea surveni în urma criminalității informatice[69].

Scopul vizat prin Strategia de securitate cibernetică a României se constituie pe de o parte în definirea conceptului de securitate cibernetică, iar pe de altă parte în stabilirea obiectivelor și direcțiilor de acțiune care să asigure un spațiu

---

64 Asigurarea securității infrastructurii critice este privită ca una dintre prioritățile de baza ale oricărei strategii de securitate cibernetică, aceasta se asigură prin identificarea riscurilor, stabilirea autorităților competente, fixarea unor standarde minime de siguranță, precum și consolidarea parteneriatelor public-privat. În acest sens, a se vedea *Guide to developing a national cybersecurity strategy. Strategic engagement in cibersecurity*, International Telecommunication Union, Geneva, 2018, p. 14, disponibil pe https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf, accesat la 23 iulie 2020.

65 Noțiunea de infrastructuri cibernetice este definită prin art. 2 lit. c) din H.G. nr. 494/2011 ca fiind „infrastructuri de tehnologia informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice". Cu toate acestea, actul normativ anterior amintit precizează că termenii și definițiile date sunt proprii acestei hotărâri, argument pentru care nu am putea extinde înțelesul noțiunii de infrastructură cibernetică și la nivelul Strategiei de securitate cibernetică a României.

66 D. Panc, *op. cit.*, p. 180.

67 A se vedea Strategia de securitate cibernetică a Germaniei, 2016, p. 15.

68 Hotărârea nr. 271/2013, publicată în Monitorul Oficial al României, Partea I nr. 296 din 23.05.2013.

69 Strategia de securitate cibernetică a Spaniei, 2019, p. 36, a împărțit măsurile de combatere a criminalității informatice în trei domenii: în primul rând, întâlnim o ipoteză în care spațiul cibernetic este ținta atacului cibernetic, o a doua ipoteză vizează spațiul cibernetic din perspectiva unui mijloc prin care se pot săvârși atacurile cibernetice și, în final, o ipoteză care privește spațiul cibernetic ca mijloc direct sau indirect pentru investigarea oricărui tip de comportament ilicit.

virtual sigur, atât sub aspectul capabilității sistemelor de a rezista unor atacuri informatice, cât și sub aspectul oferirii unor garanții de funcționare și confidențialitate.

Obiectivele Strategiei de securitate cibernetică a României vizează îmbunătățirea și completarea cadrului legislativ și instituțional, stabilirea și aplicarea unor standarde minime de securitate, direcțiile de cooperare, îmbunătățirea infrastructurii cibernetice astfel încât să fie capabilă să reziste acțiunilor și evenimentelor cibernetice îndreptate împotriva acesteia[70], valorificarea oportunităților oferite de sapțiul cibernetic[71], îmbunătățirea expertizei asupra riscurilor și mijloacelor de protecție și îmbunătățirea culturii de securitate a populației, participarea la inițiativele de cooperare internațională. Pe bună dreptate, doctrina națională a adus o serie de critici modalității de implementare a obiectivelor enunțate de Strategia de sencuritate cibernetică a României, lipsa prevederii unor termene de implementare și a unei prioritizări în cadrul obiectivelor asumate fiind de natură a creea o stare de incertitudine și neclaritate, sens în care la elaborarea unei noi strategii aceste mențiuni ar putea fi avute în vedere[72].

Printre obiectivele Strategiei de securitate cibernetică a României am amintit și cooperarea dintre mediul privat și insituțiile publice, însă fără a stabili direcții clare de acțiune și de identificare a potențialelor riscuri asociate dependenței statelor de deținerea infrastructurilor cibernetice de către actori privați, chiar localizați în afara teritoriului național sau european. Considerăm că problema trebuie tratată cu multă atenție, dat fiind faptul că are implicații asupra suveranității statelor și strâns legate de securitatea națională a acestora. Pe de altă parte, Strategia de securitate cibernetică franceză identifică o serie de potențiale riscuri pe care le vom expune succint. Dezvoltarea economică se bazează pe utilizarea sistemelor informatice, adesea acestea fiind proiectate și localizate în afara sferei de influență juridică a statelor sau chiar a Uniunii Europene, iar lipsa controlului asupra acestora, complementar cu utilizarea la scară largă determină o problemă de suveranitate. La rezolvarea unui astfel de impediment contribuie

[70] Din acest punct de vedere Strategia de Securitate cibernetică a României tratează într-o manieră extinsă importanța consolidării rețelelor informatice aflate la dispoziția autorităților publice. Ca repere comparative, considerăm că Strategia de Securitate cibernetică a Franței prezintă o abordare mai pragmatică, sens în care în acord cu Politica de Securitate a sistemelor informaționale de stat (PSSIE) sunt abordate o serie de măsuri destinate securizării comunicării electronice inter-instituționale, considerând că securitatea acestora asigură independența, suveranitatea și autonomia Franței în luarea deciziilor și implementarea măsurilor.

[71] Într-o manieră mai concretă Strategia de securitate cibernetică a Austriei din 2013 face referire la digitalizarea administrației publice într-o modalitate care să satisfacă standardele de securitate. Tot o diferență notabilă în categoria obiectivelor asumate este reprezentată de faptul că întreprinderile austriece au îndatorirea de a proteja atât propriile sisteme informatice, cât și datele personale ale clienților. În mod regretabil Strategia privind securitatea cibernetică a României nu face o astfel de diferențiere.

[72] D. Panc, *op. cit.*, p. 181.

dezvoltarea și consolidarea unor servicii digitale locale sau/și regionale. O optică similară este adoptată și de Strategia de securitate cibernetică a Uniunii Europene[73]. Se remarcă riscul ca Europa să devindă dependentă de tehnologiile informatice de provinienţă străină, sens în care cercetarea și dezvoltarea tehnologică în interiorul Uniunii Europene, complementar cu stabilirea unor standarde de securitate la nivelul producătorilor și furnizorilor de echipamente și secvicii informatice ar fi de natură să reducă această dependenţă[74].

Amenințările ce vizează securitatea cibernetică a României sunt caracterizate prin asimetrie, dinamică și caracter global, iar din perspectiva provenienței amenințării acestea sunt de natură umană, tehnică sau naturală.

Amenințările se pot concretiza printr-un atac împotriva serviciilor de utilitate publica sau ale societății informaționale, Strategia de securitate cibernetică a României facând, de asemenea, referire și la spionajul cibernetic, accesarea neautorizată a sistemelor informatice în vederea modificării, ștergerii sau deteriorării datelor informatice, precum și la cauzarea de prejudicii patrimoniale ori hărțuirea sau șantajul prin intermediul sistemelor informatice. Prin comparație, Strategia de securitate națională a Spaniei din 2017 stabilește o diferențiere între amenințările cibernetice (cyberthreats) și acțiuni care utilizează spațiul cibernetic ca mijloc pentru înfăptuirea acțiunilor imputabile. Această distincție este preluată și de Strategia de securitate cibernetică adoptată în 2019, iar diferența constă în aceea că amenințările cibernetice afectează în mod direct, depășind granițele convenționale ale statului, toate domeniile securității naționale[75], exemplificate de apărarea națională, securitatea economică, infrastructurile critice, în timp ce acțiunile care utilizează spațiul cibernetic provocând pagube sunt reprezentate de spionajul cibernetic și infracțiunile informatice[76].

Strategia de securitate cibernetică a României propune patru direcții de acțiune, privind: *stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice*; *dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui program national*; *promovarea şi consolidarea culturii de securitate în domeniul cybernetic* și *dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice*.

Elaborarea strategiilor de securitate cibernetică trebuie să reflecte prioritățile, disponibilitățile statelor, precum și avantajele specifice statului, acestea

---

73 JOIN(2013) 1 final.

74 A se vedea Strategia de securitate cibernetică a Uniunii Europene, 2013, pp. 13-15.

75 Într-o analiză comparativă s-a arătat că strategiile de securitate cibernetică europene menționează importanța atacurilor cibernetice asupra securității naționale, abia după cele privitoare la securitatea economică și a infrastructurile critice. În acest sens, a se vedea M. Gehem, A. Usanov, E. Frinking, M. Rademaker, *Assessing cyber secyrity. A meta-analysus of threats, trends, and resonses to cyber attacks*, The Hague Centre for Strategic Studies, Haga, 2015, p. 59, disponibil pe https://www.jstor.org/stable/pdf/resrep12567.1.pdf, accesat la 23 iulie 2020.

76 Strategia de securitate cibernetică a Spaniei, 2019, pp. 23-25.

putând varia ca nivel de detaliu[77]. Viziunea statelor transpusă prin strategiile de securitate cibernetică reflectă prioritățile majore ale acestora, care pot varia ca și ierarhizare, abordând problematica infrastructurilor critice, protecția proprietății intelectuale, cooperarea cu mediul privat, reziliența sistemelor informatice din administrația publică. În mod complementar, o strategie națională de securitate cibernetică trebuie să vizeze deopotrivă avantajele și neajunsurile domeniilor cu implicații în securitatea cibernetică, într-o manieră adaptabilă evoluției tehnologice. Nu în ultimul rând, considerăm importantă și tehnica de structurare a strategiei aceasta trebuind să reflecte părțile implicate, formele de cooperare, ariile strategice vizate, respectiv planul de implementare și evaluare. În sensul celor precizate, considerăm că este de referință Strategia de securitate cibernetică a Republicii Croația (2015), document sistematizat în funcție de sectoarele societății, formele de cooperare dintre acestea, zonele de securitate cibernetică, precum și obiectivele specifice fiecărei zone, continuând cu obiectivele generale și specifice legăturilor dintre zonele de securitate cibernetică[78].

Din analiza strategiilor de securitate cibernetică a statelor Uniunii Europene, precum și Strategia de securitate cibernetică a Uniunii Europene, s-a constatat faptul că statele pun accent pe prezervarea securității cibernetice în domeniile strategice, sens în care dacă se face vorbire de statele dezvoltate economic, accentul v-a fi pus pe cooperarea cu mediul privat, securitatea proprietății intelectuale; cum de alt fel, Strategia de securitate cibernetică a Uniunii Europene reclamă importanța cooperării dintre statele membre, dezvoltarea tehnologiilor informaționale proprii și implicațiile instituțiilor comune în asigurarea securității ecosistemului cibernetic intern și extern[79].

La nivelul Uniunii Europene, securitatea cibernetică a pornit ca un interes economic în vederea realizării pieței unice digitale, conducând către o cooperare politică. Începând cu anul 1990 politica de securitate cibernetică a devenit un instrument articulat la nivel european, fenomen favorizat de criminalitatea informatică; fapt ce i-a permis să devină un domeniu prioritar de acțiune[80]. Ulterior, la nivelul Uniunii Europene au apărut o serie de instrumente juridice, acestea treptat au devenit obligatorii pentru statele membre. Strategia de securitate cibernetică are rolul de a crea, la nivelul Uniunii Europene, o coordonare între protecția infrastructurilor critice, combaterea criminalității informatice și apărarea

77 D. Galinec, D. Možnik, B. Guberina, *op. cit.*, p. 278.

78 Pentru o prezentare detaliată a Strategiei de securitate cibernetică a Republicii Croația, a se vedea D. Galinec, D. Možnik, B. Guberina, op. cit., pp. 279-283.

79 A se vedea *Guide to developing a national cybersecurity strategy. Strategic engagement in cibersecurity*, International Telecommunication Union, Geneva, 2018, p. 14, disponibil pe https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf, accesat la 23 iulie 2020.

80 În acest sens, securitatea cibernetică a fost inclusă în *Strategia europeană de securitate* (2016).

cibernetică[81]. Elementul de suport în vederea creșterii gradului de securitate la nivel european este reprezentat de cooperarea instituțională, aceasta privind atât instituțiile și grupurile europene, precum și cooperarea cu mediul privat[82]. Concretizarea acestor obiective s-a realizat cel mai recent prin adoptarea Directivei (UE) 2016/1148, aceasta având ca scop armonizarea capacităților și instrumentelor statelor membre în vederea alinierii la un standard minim de siguranță a mediului privat[83].

4. Evoluția normativă în cadrul național de reglementare. Influențe ale dreptului european

4.1. Cadrul legislativ național privind protecția infrastructurilor critice

În funcție de dimensiunile securității naționale observăm incidența unor categorii de riscuri particulare care pot sau nu să fie comune mai multor state. Cu cât riscul la care statele se raportează are implicații orizontale mai largi cu atât măsurile destinate protejării securității tind să devină comune. Caracterul integrator al legislației europene a fost facilitat nu doar de obiectivele comune ale statelor membre, ci și de interdependența acestor obiective. Rețelele de comunicații informatice au ca principal avantaj comunicarea rapidă a informațiilor pe distanțe considerabile, excedând granițile statale convenționale, acestea reprezentând un nod informațional de interes, atât la nivel interguvernamental, cât și la nivel privat.

Legislația națională definește noțiunea de infrastructură critică prin intermediul dispozițiilor art. 3 lit. a) și b) din O.U.G. nr. 98/2010[84], textul ordonanței operând o defalcare semantică între infrastructurile critice naționale și europene. Astfel, infrastructura critică națională reprezentă „atât un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a

---

81 H. Carrapico, A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, în JCMS: Journal of Common Market Studies, Vol. 55, nr. 6/2017, pp. 1260, disponibil pe https://onlinelibrary.wiley.com/doi/pdf/10.1111/jcms.12575, accesat la 24 iulie 2020.

82 S-a arătat că nivelul de cooperare în mdiul privat variază în funcție de sectorul de activitate, a se vedea H. Carrapico, A. Barrinha, *op. cit.*, p. 1265.

83 *Idem.*, p. 1261.

84 O.U.G. nr. 98 din 03 noiembrie 2010 privind identificarea, desemnarea și protecția infrastructurilor critice, publicată în Monitorul Oficial al României nr. 757 din 12 noiembrie 2010, act normativ ce reprezintă transpunerea în legislația internă a Directivei 2008/114/CE privind identificarea și desemnarea ifrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L 345 din 23 decembrie 2008. O.U.G. nr. 98/2010 a fost aprobată cu modificări prin Legea nr. 18/2011, publicată în Monitorul Oficial al României, Partea I nr. 183 din 16 martie 2011.

menține respectivele funcții, cât și proiectul unui obiectiv strategic de interes național a cărui construcție este imperios necesară pentru salvgardarea interesului național", pe de altă parte noțiunea de infrastructură critică europeană, pornește de la sensul celei naționale complinindu-i caracterul transnațional condiționat de implicațiile unei *perturbări sau distrugeri care ar avea un impact semnificativ la nivelul a cel puțin două state membre ale Uniunii Europene.*

Relevanța protejării infrastructurilor critice fie ele naționale sau europene rezidă în implicațiile cauzale, acestea privind atât persoanele juridice de drept public, cât și pe cele de drept privat care activează în cadrul serviciilor de interes național, acestea din urmă constituindu-se fie în funcții vitale ale statului, fie în obiective strategice de interes național. Noțiunea de funcții vitale este exemplificată prin „managementul afacerilor guvernamentale; activitățile internaționale; apărarea națională; securitatea internă; funcționarea economiei și a infrastructurii; securitatea veniturilor populației și nivelul de trai", iar cea de obiectiv strategic de interes național prin „element, sistem sau rețea din infrastructura teritorială de orice tip sau de suport tehnic decizional necesar managementului politico-militar al Sistemului securității naționale și menținerii echilibrului societal în ansamblul general al statului român". Complementar, trebuie avut în vedere și faptul că Anexa nr. 1 la OUG nr. 98/2010 exemplifică sectoarele și subsectoarele ce constituie infrastructuri critice, urmând ca în Anexa nr. 2 a aceluiași act normativ să fie indicate criteriile în funcție de care un sector poate fi considerat ca făcând parte din infrastructura critică.

Stabilirea unui sector ca aparținând categoriei infrastructurilor critice naționale sau europene presupune stabilirea unor nivele de gravitate a *impactului, perturbării sau al distrugerii unei infrastructuri*, astfel cum se stabilește prin prevederile art. 9 alin. (4) din O.U.G. nr. 98/2010, dispoziții ce satau la baza H.G. nr. 1154/2011 pentru aprobarea pragurilor critice aferente criteriilor intersectoriale ce fundamentează identificarea potențialelor infrastructuri critice naționale și privind aprobarea Metodologiei pentru aplicarea pragurilor critice aferente criteriilor intersectoriale și stabilirea nivelului de citicitate[85].

Sub aspectul temei analizate este important să revenim asupra stabilirii criteriilor în funcție de care considerăm securitatea cibernetică o dimensiune a securității naționale. În acest moment avem în vedere punctul 6 din Anexa nr. 1 a OUG nr. 98/2010 care identifică securitatea națională ca și infrastructură critică, în cadrul acesteia având în vedere următoarele: apărarea țării, ordinea publică și siguranța națională; frontiere, migrație și azil; industria națională de securitate, capacități și instalații de producție; situații de urgență; justiție și penitenciare. Considerăm această clasificare ca o înțelegere *stricto sensu* a dimensiunii cibernetice în cadrul securității naționale; astfel cum precizam și în secțiunile anterioare, elementele infrastructurii critice pot avea relevanță în materia securității naționale atunci când satisfac condițiile atât sub aspectul naturii amenințărilor, cât și sub aspectul urmărilor relevante.

[85] Publicată în Monitorul Oficial al României nr. 849 din 30 noiembrie 2011.

În vederea optimizării activităților de protejare a infrastructurilor critice funcționează un grup de lucru interinstituțional stabilit prin H.G. nr. 1110/2010[86]. Grupul de lucru este coordonat de un consilier de stat desemnat de primul-ministru și are printre atribuții evaluarea riscurilor, amenințărilor și evoluției infrastructurilor critice, formularea de puncte de vedere pentru acte normative incidente, formularea de propuneri privind sistemul de avertizare în domeniul infrastructurii critice etc.

La nivel guvernamental a fost adoptată Strategia națională privind protecția infrastructurilor critice, H.G. nr. 718/2011 reprezintând documentul-cadru care vine să sigure coerența și direcția de implementare a măsurilor destinate protejării infrastructurilor critice. Strategia definește noțiuni ca factori de risc, amenințări, stare de pericol, pe lângă acestea se consideră ca fiind o amenințare la adresa infrastructurii critice și afectarea echipamentelor tehnice privitoare la dimensiunea cibernetică prin „producerea de sincope în funcționarea sistemelor informatizate ale infrastructurilor critice, ca urmare a unor acte criminale, erori sau disfuncții tehnice/umane, dezastre naturale sau deficiențe manageriale". Strategia mai enumeră principiile, scopurile și obiectivele avute în vedere pentru protejarea infrastructurii critice naționale și europene.

4.2. Cadrul legislativ național privind securitatea cibernetică și protejarea rețelelor și sistemelor informatice

Prin adoptarea Strategiei de securitate cibernetică a României s-a asumat responsabilitatea Guvernului în vederea elaborării unui proiect de lege privind securitatea cibernetică, acesta urmând a fi supus aprobării Parlamentului. Un astfel de proiect de lege a dost adoptat de ambele Camere ale Parlamentului[87], în expunerea de motive reținându-se că „prin adoptarea acestui act normativ, România va continua să transmită semnale puternice de racordare la realitățile internaționale, fiind pe deplin conștientă de necesitatea armonizării cu demersurile similare ale statelor europene". Legea a fost trimisă spre promulgare Președintelui României, cu toate acestea, în cursul termenului de promulgare, la data de 23 decembrie 2014, a fost sesizată Curtea Constituțională a României (CCR) în vederea efectuării unui control de constituționalitate *a priori*.

Legea privind securitatea cibernetică avea în vedere, printre altele, instituirea unui cadru legal și instituțional armonizat, totodată instituind o serie de obligații și responsabilități în sarcina celor ce dețin infrastructuri cibernetice, astfel încât să fie asigurate infrastructurile critice. În acest sens, dispozițiile actului normativ amintit indicau destinatarii prevederilor instituite, limitele conceptului de securitate cibernetică, o serie de definiții ale noțiunilor utilizate, constituirea și organizarea Sistemului Național de Securitate Cibernetică (SNSC).

---

[86] H.G. 1110/2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I nr. 757 din 12 noiembrie 2010.

[87] Disponibil pe http://www.cdep.ro/pls/proiecte/docs/2014/cd263_14.pdf, accesat la 26 iulie 2020.

Față de aspectele avute în vedere anterior, Curtea și-a fundamentat decizia[88] de admitere a excepției de neconstituționalitate pe o serie de argumente pe care le vom expune succint în cele ce urmează.

La elaborarea proiectului de lege privind securitatea cibernetică a României Guvernul a omis ca în baza dispozițiilor art. 4 lit. d) pct. 1 din Legea nr. 415/2002 să solicite avizul Consiliului Suprem de Apărare a Țării, autoritate competentă să avizeze „proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională", astfel încălcându-se dispozițiile art. 1 alin. (5) din Constituție privitor la principiul legalității, respectiv art. 119 din Constituție care consacră atribuțiile Consiliului Suprem de Apărare a Țării.

Prin dispozițiile art. 10 alin. (1) din Legea privind securitatea cibernetică a României s-a desemnat Serviciul Român de Informații (SRI) ca autoritate națională competentă în domeniul securității cibernetice, urmând ca Centrul Național de Securitate Cibernetică să funcționeze în structura SRI. Față de aceste dispoziții s-a reținută că autoritatea competentă în domeniul securității cibernetice trebuie să fie una civilă, soluție justficată prin prisma faptului că existența competenței în sarcina unei structuri de informații militarizate ar creea premisele unei lipse de proporționalitate și a unor riscuri de depășire a limitelor de ingerință în viața privată. Aceste argumente au fundamentat constatarea încălcării prevederilor constituționale de la art. 1 alin. (3) și (5) privitor la statul de drept și principiul legalității, respectiv art. 26 și art. 28 privind viața intimă, familială și privată, respectiv secretul corespondenței.

O altă problemă de neconstituționalitate a vizat prevederile art. 2 din Lege, acestea indicând destinatarii normei, aceștia fiind deținătorii de infrastructuri critice: proprietari, administratori, operatori sau utilizatori de infrastructuri critice, sub această ultimă categorie fiind incluse toate persoanele care utilizează infrastructuri critice. Față de aceste prevederi sintetice Curtea a stabilit că legea nu are un caracter precis și previzibil, motiv pentru care contravine dispozițiilor art. 1 alin. (5) din Constituție.

Analiza Curții a vizat, de asemenea, și conținutul dispozițiilor art. 17 alin. (1) lit. a) din Legea privind securitatea cibernetică a României, prevederi care enunțau responsabilitățile deținătorilor de infrastructuri critice, printre acestea fiind inclusă și acordarea sprijinului necesar Serviciului Român de Informații, Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Oficiului Registrului Național al Informațiilor Secrete de Stat, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, CERT-RO și ANCOM. Curtea realizează o contrapondere între interesele colective și cele personale, statuând că trebuie să existe un just echilibru, precum și garanții care să asigure o protecție eficientă împotriva eventualelor abuzuri. Dat fiind faptul

[88] Decizia Curții Constituționale a României nr. 17 din 21 ianuarie 2015, publicată în Monitorul Oficial al României nr. 79 din 30 ianuarie 2015.

că dispozițiile legale nu satisfăceau aceste exigențe, s-a reținut încălcarea art. 1 alin. (5), art. 26, art. 28 și art. 53 din Constituție[89].

Prin dispozițiile art. 19 din Legea avută în vedere se menționează că prin hotărâre a Guvernului este aprobat catalogul deținătorilor de infrastructuri cibernetice de interes național (ICIN). Față de acestea, Curtea arată pe de o parte că O.U.G nr. 98/2010 stabilește criteriile intersectoriale de identificare a structurilor infrastructurii critice naționale, iar pe de altă parte că o astfel de modalitate de stabilire nu se poate realiza prin legislația infralegală. Față de aceste argumente s-a reținut că nu sunt respectate cerințele de previzibilitate, stabilitate și certitudine, corespondente art. 1 alin. (5) din Constituție.

Sunt avute în vedere și prevederile art. 20 din lege, acestea stabilind la lit. c) că persoanele juridice de drept public sau privat ce dețin sau au în răspundere infrastructuri critice au obligația de a permite efectuatea de auditări din partea SRI, în materia securității cibernetice. Curtea mai arată că există posibilitatea ca SRI ocupe, în cadrul acestei proceduri, atât calitatea de solicitant, cât și pe cea de instituție responsabilă cu efectuarea auditului. De asemenea, Curtea a analizat și dispozițiile de la lit. h), din cuprinsul aceluiași articol, prevederi care stabilesc *obligația de a notifica imediat, după caz, CNSC, CERT-RO, ANCOM sau autoritățile desemnate*, însă fără a stabili în mod exact condițiile în care se realizează notificarea și conținutul acesteia. Față de aceste inconsecvențe legislative, s-a conchis că sunt încălcate prevederile constituționale ale art. 1 alin. (3) și (5), respectiv art. 26 și art. 28.

În fine, Curtea mai arată faptul că dispozițiile Legii privind securitatea cibernetică a României nu reglementează posibilitatea persoanelor ale căror drepturi, libertăți sau interese legitime au fost încălcate să se adreseze unei instanțe jurecătorești, de asemenea, au mai fost reținute deficiențe de constituționalitate și în raport de stabilirea instituțiilor ce au competențe în monitorizarea și controlul aplicării legii, precum și referirea la instituții și autorități înființate prin acte normative infralegale anterioare. Față de toate aceste considerente, Curtea a stabilit faptul că Legea privind securitatea cibernetică a României este neconstituțională în ansamblul său.

Ulterior pronunțării Deciziei CCR nr. 17/2015 a fost pus în dezbatere un nou proiect de lege care să privească securitatea cibernetică a României[90]. Ulterior, la nivelul Uniunii Europene, a fost adoptată Directiva (UE) 2016/1148 privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune[91], transpusă în legislația internă prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice[92].

Directiva (UE) 2016/1148 are scopul de a reglementa la nivelul legislației Uniunii Europene, precum și la nivelul statelor membre măsurile de securitate ale

---

89 A se vedea și D. Panc, *op. cit.*, p. 202.

90 Disponibil pe https://cert.ro/vezi/document/proiect-de-lege-securitate-cibernetica, accesat la 28 iulie 2020. A se vedea și D.C. Mâță, *op. cit.*, p. 42.

91 Publicată în Jurnalul Oficial al Uniunii Europene L 194/1 din 19 iulie 2016.

92 Publicată în Monitorul Oficial al României nr. 21 din 09 ianuarie 2019.

rețelelor informatice, în corespondență cu obiectivele NIS stabilite prin Strategia Europeană de securitate cibernetică, acesta fiind considerată „componenta principală a Strategiei de securitate cibernetică a Uniunii Europene”[93]. Justificarea măsurilor impuse rezidă în necesitatea asigurării rețelelor și sistemelor informatice, acestea stând la baza tranzacțiilor naționale și intracomunitare, și în consecință, eventualele atacuri sau disfuncționalități ale rețelelor informatice putând avea repercusiuni transnaționale sau asupra întregii Uniuni Europene[94].

Complementar cadrului legal privind securitatea cibernetică din România, în expunerea de motive a Legii nr. 362/2018 se arată că „nu există prevederi unitare în legislația națională privitor la notificarea în sensul Directivei NIS a incidentelor de securitate a rețelelor și sistemelor informatice”.

Atât directiva, cât și norma națională de transpunere delimitează conținutul acesteia de domeniul mai larg al securității cibernetice, art. 2 alin. (2) din Legea nr. 362/2018 stabilind că prevederile actului normativ nu se aplică în domeniul securității naționale, abordând expres domeniul securității rețelelor și sistemelor informatice. De asemenea, prevederile art. 7 din Directiva NIS impun în sarcina statelor obligația elaborării unei strategii naționale privind securitatea rețelelor și a sistemelor informatice, acestea urmând a fi comunicate Comisiei Europene, cu mențiunea că statele membre au posibilitatea de a nu comunica și acele elemente ale strategiei care au legătură cu securitatea națională.

Conținutul Directivei NIS relevă o abordare pe patru paliere, corespondente capitolelor actului normativ.

Primul palier face referire la cadrele naționale de securitate a rețelelor și a sistemelor informatice. Sunt avute în vedere o serie de obligații instituite în sarcina statelor: elaborarea unei strategii naționale privind securitatea rețelelor informatice, desemnarea unei autorități naționale responsabile cu securitatea rețelelor și sistemelor informatice, respectiv constituirea uneia sau mai multor echipe de intervenție (CERT[95]/CSIRT[96]) care să administreze riscurile și incidentele de securitate a rețelelor informatice. Menționăm că dispozițiile art. 8 Directiva NIS nu menționează calitatea autorității naționale competente în materia asigurării securității rețelelor și sistemelor informatice, însă într-o formă anterioară se preciza necesitatea ca autoritățile naționale să fie civile, iar nu militarizate, aspect care ar conferi independență și garanții ale respectării drepturilor și libertăților cetățenilor, pe un astfel de raționament s-a bazat și Curtea Constituțională în pronunțarea Deciziei nr. 17/2015, la care am făcut trimitere anterior[97]. Cu toate acestea, unele opinii doctrinare și-au exprimat preferința pentru necesitatea instituirii unor autorități civile[98], aspect care s-a și concretizat prin art. 15 alin. (1) din Legea nr. 362/2018 care stabilește că „CERT-RO este autoritate competentă la

93 D. Panc, *op. cit.*, p. 86.
94 *Idem.*, p. 85.
95 Acronim de la *Centrul Național de Răspuns la Incidente de Securitate Cibernetică.*
96 Acronim de la *Computer Security Incident Response Team.*
97 A se vedea paragraful 27 din decizia amintită.
98 A se vedea și D. Panc, *op. cit.*, p. 201.

nivel național pentru securitatea rețelelor și a sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale".

Un al doilea palier privește relațiile de cooperare în vederea asigurării securității rețelelor informatice. Instrumentele de cooperare sunt reprezentate de stabilirea unui grup de cooperare compus din reprezentanți ai statelor membre, respectiv ai Comisiei Europene și ai ENISA, acesta urmând a avea ca scop facilitarea schimbului de informații și creșterea coeziunii dintre statele membre. Având același obiectiv de consolidare a cooperării, se are în vedere constituirea unei rețele CSIRT europene compusă din echipele CSIRT/CERT naționale, la care se alătură Comisia Europeană în calitate de observator și ENISA, asigurând secretariatul rețelei. În final, se are în vedere posibilitatea Uniunii ca în baza art. 218 din TFUE să stabilească acorduri de cooperare și cu state terțe.

Al treilea palier privește asigurarea securității rețelelor și sistemelor informatice deținute de operatorii de servicii informatice esențiale. Demersurile ce trebuiesc efectuate de către state sunt reprezentate de asigurarea existenței unor măsuri tehnice și organizatorice luate de către operatori astfel încât să fie asigurate rețelele, implementarea sistemului de notificare de către operatori spre echipele CSIRT în caz de incidente asupra serviciilor esențiale pe care le furnizează, respectiv existența mijloacelor tehnice și de competență a autorităților naționale chemate să evalueze gradul în care operatorii de servicii esențiale își îndeplinesc obligațiile de asigurare a securității serviciilor furnizate.

Ultimul palier este reprezentate de cerințele de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii digitale. Directiva pune în sarcina statelor obligația de a se asigura că furnizorii de servicii digitale iau măsurile necesare în vederea gestionării riscurilor de securitate, precum și că aceștia notifică autoritățile sau echipele CSIRT în situația unui incident ce ar putea afecta furnizarea unui serviciu informatic esențial.

Pornind de la conținutul Directivei NIS, legiuitorul național, prin expunerea de motive a Legii nr. 362/2018, abordează sfera de reglementare prin prisma a trei principii: responsabilitate și conștientizare, proporționalitate, respectiv cooperare și coordonare, corespondente palierelor de structurare normativă prezentate anterior.

Autoritatea competentă la nivel național în vederea asigurării respectării nivelului de securitate a rețelelor și sistemelor informatice este CERT-RO, aceasta cooperând cu Serviciul Român de Informații pentru aspectele ce implică securitatea națională, Ministerul Apărării Naționale privitor la aspectele ce presupun apărarea națională, respectiv cu Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază în legătură cu sistemele informatice prin care aceste instituții își desfășoară activitatea sau pe care le au în răspundere. De asemenea, CERT-RO prin personalul de specialitate desemnat de directorul general al Centrului exercită controlul asupra respectării obligațiilor impuse operatorilor de servicii esențiale și furnizorilor de servicii digitale, iar în ipoteza încălcării obligațiilor legale pot aplica sancțiuni contravenționale. Dacă

neregula identificată de personalul de control prezintă un pericol grav și iminent la adresa securității naționale, apărării naționale, ordinii sau sănătății publice, în baza dispozițiilor art. 41 alin. (3) din Legea nr. 362/1018 „CERT-RO va informa organele judiciare și va notifica instituțiile competente din domeniul apărării și securității naționale, ordinii publice sau sănătății publice".

Prevederile Legii nr. 362/2018 mai stabilesc obligația operatorilor și furnizorilor de servicii digitale[99] de a respecta normele tehnice elaborate de CERT-RO în vederea stabilirii unui nivel minim de securitate a rețelelor și sistemelor informatice, precum și obligativitatea notificării autorităților în cazul unor incidente de secutitate.

De asemenea, este reglementat și auditul de securitate, acesta putând fi realizat de persoane fizice sau juridice și presupunând „o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora". Constatăm o diferență majoră față de ceea ce reprezenta auditul în forma adoptată a Legii privind securitatea cibernetică a României unde se reglementa faptul că auditările trebuiau realizate de Serviciul Român de Informații sau de către furnizori de servicii în materia securității cibernetice, aspecte care au fost abordate în controlul de constituționalitate *a priori* concretizat prin Decizia C.C.R. nr. 17/2015.

O altă deficiență a Legii privind securitatea cibernetică a României a fost reprezentată de lipsa unor prevederi care să asigure cadrul legal persoanelor a căror drepturi, libertăți sau interese legitime au fost vătămate de a se adresa unei instanțe[100] în vederea contestării actelor administrative prin care s-a luat act de neîndeplinirea unor obligații. În această ordine de idei, dispozițiile Legii nr. 362/2018 consacră în cuprinsul art. 24 alin. (1) lit. b), respectiv art. 42 alin. (2) posibilitatea persoanelor care au fost vătămate printr-o decizie a CERT-RO, prin refuzul nejustificat de procesare a unei cereri, respectiv în vederea contestării unei sancțiuni contravenționale de a se adresa instanței de contencios administrativ.

5. Concluzii

Analiza domeniului securității cibernetice reprezintă un demers supus în permanență actualizării, motivat de faptul că dinamica evolutivă a factorilor de risc și a mijloacelor de apărare este în continuă schimbare. În cuprinsul prezentei

[99] Operatorii de servicii esențiale sunt reprezentați de persoane fizice sau juridice de drept public care efectuează activități în: sectorul energetic, transport, sectorul bancar, infrastructuri ale pieței financiare, sectorul sănătății, furnizarea și distribuirea de apă potabilă, respectiv infrastructură digitală. Detalierea pe subsectoare și tipuri de activitate este inclusă în anexa la Legea nr. 362/2018. Constatăm că legiuitorul a avut în vedere criticele de neconstituționalitate pe care s-a bazat Decizia nr. 17/2015 a Curții Constituționale a României (para. 54 - 56), când s-a constatat că Legea privind securitatea cibernetică a României nu stabilea în mod clar și neechivoc categoriile destinatarilor normei.

[100] Aspecte reținute și în cuprinsul paragrafelor 77 – 81 din Decizia CCR nr. 17/2015.

lucrări am avut în vedere prezentarea cadrului general de raportare la securitatea cibernetică în contextul mai larg al securității naționale, continuând cu primul nivel de contextualizare, prin strategiile de securitate cibernetică și finalizând cu legislația-cadru în materie. Prin parcurgerea temei pe cele două planuri ale cadrului normativ european și național am conturat principalele deosebiri și neajunsuri ale prevederilor naționale.

Referințe

Carrapico H., Barrinha A., *The EU as a Coherent (Cyber)Security Actor?*, în JCMS: Journal of Common Market Studies, Vol. 55, nr. 6/2017, https://doi.org/10.1111/jcms.12575

Delerue F., *Cyber operations and international law*, Editura Chambridge University Press, Chambridge, United Kingdom, 2020

Delibasis D., *Cybersecurity and state responsibility: Identifyng a due diligence standard for prevention of transboundary threats* în J. Kulesza, R. Balleste (editori), *Cybersecurity and human rights in the age of vyberveillance*, Editura Rowman & Littlefield, Lanham, 2016

Dordal P.L., *Dark Web*, în H. Jahankhani (coord.), *Cyber Criminology*, Editura Springer, Switzerland, 2018

Galinec D., Možnik D., Guberina B., *Cybersecurity and cyber defence: national level strategic approach*, în Automatika, vol. 58, nr. 3/2017, pp. 273-286, https://doi.org/10.1080/00051144.2017.1407022

Gehem M., Usanov A., Frinking E., Rademaker M., *Assessing cyber secyrity. A meta-analysus of threats, trends, and resonses to cyber attacks*, The Hague Centre for Strategic Studies, Haga, 2015

***, *Guide to developing a national cybersecurity strategy. Strategic engagement in cibersecurity*, International Telecommunication Union, Geneva, 2018

Hare F., *The cyber threat to national security: why can't we agree?*, în C. Czosseck & Podins (Eds), *Proceedings of the Conference on Cyber Conflict,* Tallinn, Estonia: CCD COE Publications, 2010

Hathaway M.E., *Cyber Security. An economic and national security crisis*, în Intelligencer Journal, vol 16, nr. 2/2008, pp. 31-36

Krause K., Williams M.C., *Broadening the Agenda of Security Studies: Politics and Methods*, în Mershon International Studies Review, vol. 40, nr. 2/1996, pp. 229-254, https://doi.org/10.2307/222776

Libicki M.C., *Cyberdeterrence and cyberwar*, Editura RAND Corporation, Santa Monica, 2009

Mann I., *Towards a Cyber-Security Treaty*, Just Security, 2016 [on-line]

Mâță D.C., *Cybersecurity – Dimensions of national security*, în Journal of Law and Administrative Sciences, Special Issue, 2015, pp. 132-142

Mâță D.C., *Securitatea națională. Concept. Reglementare. Mijloace de ocrotire*, Editura Hamangiu, București, 2016

Omand D., *Understanding Digital Intelligence: A British View* în E. De Silva (coord.), *National Security and Counterintelligence in the Era of Cyber Espionage*, Editura IGI Global, Hershey, 2016, pp. 97-121, https://doi.org/10.4018/978-1-4666-9661-7.ch006

Panc D, *Securitatea cibernetică la nivel național și internațional. Instrumente normative și instituționale*, Editura Hamangiu, București, 2017

Peng Shin-yi, *Cybersecurity Threats and the WTO National Security Exceptions*, în Journal of International Economic Law, Editura Oxford University Press, vol. 18, nr. 2/2015, https://doi.org/10.1093/jiel/jgv025

Rass S., Schauer S., König S., Zhu Q., *Cyber-Security in Critical Infrastructures. A game-theoretic approach*, Editura Springer, Switzerland, 2020, https://doi.org/10.1007/978-3-030-46908-5

Rosenzweig P., *Cyber Warfare. How conflicts in cyberspace are challenging America and changing the* word, Editura Praeger, Santa Barbara, 2013

Schmitt, M.N., *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Editura Cambrindge University Press, Cambridge, 2017, https://doi.org/10.1017/9781316822524

Topor S., *Education in the cyber security field and implications for national security*, în Annals – Series on Military Sciences, nr. 1/2020, pp. 81-98

Virkar S., *The mirror has two faces: Terrorist use of the internet and the challenges of Governing Cyberspace*, în E. De Silva (coord.), *National Security and Counterintelligence in the Era of Cyber Espionage*, Editura IGI Global, Hershey, 2016, pp. 7-27, https://doi.org/10.4018/978-1-4666-9661-7.ch001

Wilson C., Drumhiller N., *US – China Relations: Cyber Espionage and Cultural Bias* în E. De Silva (coord.), *National Security and Counterintelligence in the Era of Cyber Espionage*, Editura IGI Global, Hershey, 2016, pp. 28-46, https://doi.org/10.4018/978-1-4666-9661-7.ch002