SECURITATEA CIBERNETICĂ.

LIBERTATE VS. SECURITATE ÎN MEDIUL ONLINE

Rezumat

Evenimentele de la 11 septembrie 2001 au influențat strategiile de securitate națională ale statelor, în care terorismul era definit drept amenințare principală, sprijinind astfel procesul de globalizare, care a depășit natura sa economică, în momentul în care întreaga lume s-a unit împotriva unui singur inamic, în mod solidar. Însă, în perioada recentă, se constată o estompare a acestei solidarități[1], căpătând o mai mare importanță „competiția și competitivitatea între state”[2].

Totodată, unul dintre pilonii globalizării îl constituie evoluția tehnologiei și, implicit, utilizarea internetului la scară largă, ceea ce a dus la înlăturarea unor bariere majore de comunicare, de cunoaștere și explorare a lumii și a creat noi oportunități de dezvoltare și cooperare, în diverse domenii, accelerând procesul. Din această perspectivă, utilizarea internetului și facilitarea accesului la informație a dus, în perioada recentă, la reconfigurarea relațiilor dintre state, pornind de la nevoia de consolidare a rolului și locului lor în relațiile internaționale. Informația este putere, iar internetul și tehnologia oferă acces la informație. Însă, acest mediu este dominat de amenințări, aflate într-o evoluție continuă și rapidă, ceea ce a generat nevoia de securitate a utilizatorilor de internet – fie simpli utilizatori, fie companii, organizații sau state, iar măsurile de securitate trebuie adoptate la toate nivelurile și de către toți actorii implicați.

Lucrarea de față are ca element central conceptul de securitate cibernetică și percepția utilizatorilor asupra acestuia, din perspectiva analizei raportului dintre libertate și securitate.

Securitatea cibernetică este un domeniu complex și în continuă evoluție, fiind direct influențat de dezvoltarea și diversificarea amenințărilor în mediul online, care trebuie abordat în mod diferit în funcție de efectul pe care amenințările îl pot produce asupra securității sistemelor.

[1] Monitorul Apărării și Securității, gl. Sergiu Medar, în cadrul Conferinței *Cum răspundem la crizele de securitate națională*?, 2021, video la https://www.facebook.com/monitorulapararii/videos/1136156286802705/?__so__=permalink&__rv__=related_videos, ultima accesare, februarie 2021

[2] Ibid.

Dacă la nivel de individ securitatea cibernetică presupune măsuri minime de protecție în fața amenințărilor care pot afecta sistemele la un nivel scăzut, în cazul instituțiilor, organizațiilor sau al statelor, impactul poate fi unul extins, întrucât pot fi afectate infrastructuri critice, care pot periclita stabilitatea economică, socială, politică etc., a unui stat.

Astfel, la nivel de stat, securitatea cibernetică reprezintă o dimensiune a securității naționale, care are relevanță atât în plan intern cât și extern. Pe componenta internă, aplicarea măsurilor de securitate cibernetică are drept scop tocmai protejarea statului și, implicit, a cetățenilor săi, iar în plan extern, politicile de securitate cibernetică ale statelor influențează relațiile internaționale, întrucât spațiul cibernetic a devenit un nou mediu de conflict și parteneriate între state și, drept urmare, relațiile internaționale au căpătat noi dimensiuni.

Abordarea raportului securitate vs. libertate și a teoriei conform căreia „securitatea poate fi pusă în balanță cu alte valori precum libertatea”[3] nu este una nouă. Acestea apar, întotdeauna, în dezbatere, când se impune luarea de măsuri specifice securității naționale, la nivelul unui stat. Cel mai relevant exemplu îl constituie adoptarea Patriot Act[4], în Statele Unite, în anul 2001. Documentul a constat în „extinderea puterii guvernului în supravegherea, investigarea și reținerea suspecților de terorism”[5]. Deși contestat, de-a lungul timpului, pentru că „unele prevederi erau neconstituționale sau permiteau abuzuri din partea autorităților”[6], a fost adoptat într-un context de criză, în urma atacurilor teroriste de la 11 septembrie 2001, și s-a aplicat, în forma inițială, până în anul 2015, când a intrat în vigoare USA Freedom Act, menit să „limiteze autoritatea guvernului de a colecta date”[7].

În prezent, majoritatea statelor lumii au adoptat o strategie națională de securitate cibernetică, însă există dezbateri cu privire la nevoia semnării unui tratat internațional, odată ce tot mai multe state și organizații internaționale definesc mediul online ca fiind un bun comun, precum spațiul cosmic sau cel maritim, pentru care există astfel de documente internaționale. Totuși, modelele oferite de tratatul privind spațiul cosmic care „interzice intervenția cu rea

[3] Richard Ullman, “Redefining Security”, in *Security Studies. A reader*, ed. Christopher W. Hughes and Lai Yew Meng (London: Routledge, 2011), 12
[4] USA Congress, *Uniting and Strengtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, disponibil la https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf, ultima accesare, iunie 2021
[5] Brian Duignan. "USA PATRIOT Act." Encyclopedia Britannica, November 12, 2020 disponibil la https://www.britannica.com/topic/USA-PATRIOT-Act, ultima accesare, ianuarie 2021
[6] Ibid.
[7] Ibid.

intenție asupra explorării și a utilizării pașnice a spațiului cosmic și lansarea de arme nucleare din spațiu pe Pământ”[8], sau de tratatul asupra teritoriului Antacticii prin care „sunt interzise armele la mai puțin de 60 de grade latitudine sudică”[9], nu sunt suficiente, astfel încât un tratat în privința spațiului cibernetic este departe de a fi semnat.

În privința legislației naționale, dificultățile rezidă, similar domeniului securității naționale, în raportul dintre libertate și securitate, iar utilizatorii se tem că măsurile de securitate adoptate le pot afecta libertatea în spațiul cibernetic. Din această perspectivă, majoritatea statelor membre ale Uniunii Europene au adoptat un astfel de document legislativ, limitându-se la transpunerea în legislația națională a Directivei NIS[10].

Pornind de la aceste date, lucrarea Securitate cibernetică. Libertate vs. securitate în mediul online propune evidențierea aspectelor relevante în domeniu, din următoarele perspective: analiza evoluției amenințărilor, a riscurilor și vulnerabilităților în mediul online, evaluarea cadrului legislativ privind securitatea cibernetică, atât la nivel internațional, cât și național, precum și analiza percepţiei utilizatorilor de internet cu privire la legislația în domeniu și a nivelului culturii de securitate cibernetică a acestora.

Scopul tezei de cercetare îl constituie identificarea de posibile soluții de reducere a manifestării amenințărilor cibernetice, prin propuneri privind modul de abordare a securității cibernetice în legislația națională, în contextul organizațional internațional în care se găsește România, dat de statutul de membru al Uniunii Europene și cel de aliat NATO, precum și ținând cont de percepția utilizatorilor de internet cu privire la legislația în domeniu.

Obiectivul principal al cercetării constă în identificarea rolului pe care îl poate avea cultura de securitate cibernetică în echilibrarea raportului dintre nevoia de libertate a utilizatorilor de internet şi cea de securitate, în fața riscurilor şi amenințărilor cibernetice.

Obiectivele complementare vizează înțelegerea fenomenelor specifice securității cibernetice prin definirea și clarificarea unor termeni, concepte și relații de tip cauză-efect

[8] Peter Warren Singer and Allan Friedman. *Cybersecurity and cyberwar. What everyone needs to know* (New York: Oxford University Press, 2014), 186
[9] Peter Warren Singer and Allan Friedman. *Cybersecurity and cyberwar. What everyone needs to know* (New York: Oxford University Press, 2014), 186
[10] Parlamentul European și Consiliul Uniunii Europene, *Directiva 2016/ 1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, 2016, disponibilă la https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&qid=1596915362573&from=EN, ultima accesare, iunie 2021

specifice mediului online.

În acest context, lucrarea propune demonstrația următoarei ipoteze: dacă nivelul culturii de securitate cibernetică este unul ridicat, atunci numărul atacurilor în mediul online poate scădea.

Este o ipoteză primară, de tip cauzal[11], cu două variabile: o variabilă independentă - nivel ridicat al culturii de securitate cibernetică, ce influențează variabila dependentă – scăderea ratei de succes a amenințărilor cibernetice.

Ipoteza explicativă[12] adaugă încă o variabilă intermediară în relația descrisă mai sus, respectiv echilibrarea raportului dintre nevoia de libertate și cea de securitate, cu rol de efect al variabilei independente și de cauză pentru variabila dependentă.

În dezvoltarea acestei ipoteze, apar noi variabile intermediare care intervin în relația dintre cele trei descrise mai sus, respectiv:

- (1) cunoașterea fenomenelor și a amenințărilor în mediul online și (2) conștientizarea nevoii de securitate, ca efect imediat al variabilei independente – creșterea nivelului culturii de securitate cibernetică;
- (3) cunoașterea și aplicarea măsurilor de securitate, de către fiecare utilizator, ca o consecință directă a celei de-a doua variabile – echilibrarea raportului libertate/ securitate.

Prin urmare, un nivel ridicat al culturii de securitate cibernetică asigură cunoașterea de către utilizatori a amenințărilor în mediul online și conștientizarea nevoii de securitate, ceea ce duce la echilibrarea raportului între nevoia de libertate și cea de securitate, în percepția utilizatorilor care, în acest context, cunosc și pot aplica măsuri de securitate în mediul online, ducând astfel la scăderea ratei de succes a atacurilor cibernetice.

Creșterea nivelului culturii de securitate se poate realiza prin educație de securitate cibernetică și awareness, prin care se asigură acces la informație și asimilarea acesteia de către utilizatori, ceea ce înseamnă că aceste două elemente constituie variabile condiționale[13] pentru variabila independentă. Astfel, variabilele intermediare reprezintă condiții pentru variabilele

[11] Stephen Van Evera, *Guide to methods for students of political science* (Ithaca, New York: Cornell University Press, 1997), 9-13
[12] Ibid.
[13] Stephen Van Evera, *Guide to methods for students of political science* (Ithaca, New York: Cornell University Press, 1997), 9-13

principale (formulate în ipoteza primară). Prin urmare:

- Creşterea nivelului culturii de securitate cibernetică (variabila independentă) se asigură cu condiția existenței unor programe de educație de securitate cibernetică și a unor campanii de awareness (variabile condiționale);
- Echilibrarea raportului libertate/ securitate (variabilă intermediară) se asigură în contextul producerii efectelor variabilei independente – utilizatorii cunosc amenințările şi conştientizează nevoia de securitate, acestea devenind variabile condiționale pentru variabila intermediară;
- Scăderea numărului atacurilor cibernetice (variabila dependentă) se asigură în contextul producerii efectelor variabilei intermediare – utilizatorii aplică măsurile de securitate cibernetică, devenind, de asemenea, condiție pentru variabila dependentă.

În termeni de fenomene, teoria propusă pune în relație de tip explicație specifică[14] creşterea nivelului culturii de securitate cibernetică ce poate echilibra raportul libertate/ securitate, iar raportul libertate/ securitate poate genera scăderea numărului atacurilor cibernetice. Astfel, un nivel ridicat al culturii de securitate cibernetică face ca utilizatorul de internet să fie, în egală măsură, beneficiar și furnizor de securitate, prin aplicarea măsurilor de securitate cibernetică în mediul online.

Teza nu propune o analiză filosofică a raportului libertate vs. securitate, ci, mai degrabă, una din perspectivă pragmatică, care poate constitui un model de abordare a modului de diseminare a informației către utilizatori, fie în demersurile de educație de securitate cibernetică, fie în cele de awareness, în încercarea de a formula o serie de răspunsuri la întrebări precum:

- Ce reprezintă şi cum pot fi abordate amenințările, vulnerabilitățile şi riscurile în mediul online, cu scopul asigurării securității cibernetice?
- Care sunt şi cum pot fi exploatate oportunitățile în mediul online?
- Care sunt punctele comune și unde apar diferențe în legislația privind securitatea cibernetică?

[14] Stephen Van Evera, *Guide to methods for students of political science* (Ithaca, New York: Cornell University Press, 1997), 15-16

- Care este nivelul de cultură de securitate cibernetică a utilizatorilor de internet din România?
- Unde este punctul de echilibru în raportul libertate vs. securitate?
- Libertatea și securitatea sunt concepte care se exclud reciproc?

Lucrarea, structurată în trei părţi, abordează tema securității cibernetice pe trei dimensiuni: analiza evoluţiei ameninţărilor cibernetice, analiza legislației internaționale și naționale în domeniul securității cibernetice și, prin aplicarea unui sondaj de opinie cu privire la comportamentul utilizatorilor de internet, evaluarea nivelului culturii de securitate a utilizatorilor, precum și a percepției lor cu privire la legislația în domeniul securității cibernetice.

Prima parte a lucrării, Criminalitatea cibernetică, tratează ameninţările, vulnerabilitățile și riscurile în mediul online, cu impact asupra societății, la toate nivelurile, de la efectele asupra utilizatorilor simpli, la cele ce reprezintă amenințări la adresa securității naționale. Această secțiune urmărește analiza și definirea relației între cele trei concepte. Pentru o mai bună înțelegere a amenințărilor, capitolul prezintă tipologia criminalității cibernetice, de la atacurile cibernetice comune, la război cibernetic, spionaj cibernetic, terorism cibernetic și hacktivism, precum și instrumentele utilizate cel mai des în mediul online de către autorii atacurilor cibernetice. Vulnerabilitățile, care constituie elementul cheie în securitatea cibernetică, și riscurile de securitate cibernetică sunt prezentate relație cu amenințările. De asemenea, capitolul cuprinde și o evaluare generală a mediului de securitate cibernetică, concentrată pe transformările recente și pe evoluții viitoare.

Principala metodă de cercetare o constituie analiza de documente, provenind din diverse surse de informare, precum lucrări și studii din literatura de specialitate care abordează tema amenințărilor, vulnerabilităților și riscurilor în mediul online atât din perspectivă teoretică, cât și practică, în cazul celor care analizează atacurile cibernetice care au avut loc de-a lungul timpului.

Pentru noțiunile teoretice au fost utilizate, cu precădere, surse primare, precum strategii de securitate cibernetică precum și documente legislative sau ghiduri elaborate la nivelul Uniunii Europene, sau al Organizației Tratatului Atlanticului de Nord, prin structurile desemnate cu atribuții în domeniu, precum ENISA - Agenția Uniunii Europene pentru Securitate Cibernetică sau CCDCOE – Centrul NATO de Excelență pentru Cooperare în Apărare Cibernetică. Acestea

au fost completate cu informații oferite de instituții cu rol în asigurarea securității cibernetice din țară și străinătate.

Amenințările vor continua să existe în spațiul cibernetic, având o tendință de diversificare și creștere numerică, pe măsură ce tehnologia se dezvoltă. Acestea trebuie cunoscute și evaluate și trebuie identificate măsurile optime de oprire a manifestării lor. Securitatea cibernetică trebuie abordată pornind de la caracteristica amenințărilor cibernetice de a exploata vulnerabilitățile dispozitivelor sau ale rețelelor de conectare la internet. Obiectivul principal al securității cibernetice poate fi diminuarea riscului de materializare a amenințărilor cibernetice, ceea ce se poate realiza prin eficientizarea managementului vulnerabilităților. Însă, în această relație există, întotdeauna, și oportunități. Una dintre acestea, oferită de context, constă în faptul că asupra vulnerabilităților pot acționa absolut toate părțile implicate: utilizatorii, autoritățile, dezvoltatorii de softuri și dispozitive de conectare la internet, operatorii de infrastructuri critice și servicii digitale, organizațiile internaționale etc., iar acest lucru va fi posibil când toți cei implicați vor înțelege că securitatea cibernetică este o responsabilitate comună, conștientizând fiecare propria responsabilitate individuală.

Cele mai multe dintre atacurile cibernetice produse de-a lungul timpului ar fi putut fi evitate dacă ar fi fost asigurate măsuri minime de securitate de către utilizatori. De la cele mai importante, precum WannaCry, unde vulnerabilitatea a constat în faptul că computerele afectate rulau o versiune de Windows depășită, care nu mai beneficia de actualizări de securitate[15]. În cazul Stuxnet, virusul a fost introdus în sistem prin conectarea unui USB la unul dintre computere. Cauza succesului celor mai multe atacuri cibernetice, însă, constă în deschiderea atașamentelor sau accesarea link-urilor infectate, primite prin e-mail, mesaje sau pe platformele de social media, iar probabilitatea manifestării acestora crește pe fondul absenței unui program antivirus.

În partea a doua, folosind cu precădere metoda comparativă și analiza de conținut, sunt studiate diferite abordări legislative referitoare la securitatea cibernetică, naţionale şi internaţionale, atât la nivel de strategie, cât și la nivel de reglementare națională, cu evidențierea

[15] Mikko Hypponen, „Mikko Hypponen speaks about WannaCry at SPIECES", 2017, video disponibil la https://www.youtube.com/watch?v=ZqNSoHFtGM0, ultima accesare, iunie 2021

unor principii ale legislației internaționale relevante în domeniu. Astfel, în acest capitol, sunt analizate politicile Uniunii Europene și ale NATO în privința securității cibernetice, strategiile de securitate cibernetică ale statelor membre ale celor două organizații, precum și cele mai relevante legi naționale de securitate cibernetică ale acestora.

Capitolul conține o secțiune dedicată evoluției cadrului legislativ românesc, în domeniul securității cibernetice. Finalul acesteia este reprezentat de studiul de caz, constând în analiza evoluției pachetului de legi Big Brother, în România, în încercarea de a identifica elementele ce au stat la baza insuccesului acestui demers legislativ, ca element de referință în raportul dintre libertate și securitate, în contextul securității naționale.

De asemenea, lucrarea îşi propune analiza şi definirea conceptelor de educaţie şi cultură de securitate cibernetică, precum și alte concepte specifice, reprezentative în cadrul procesului de asigurare a securității cibernetice.

Atacurile cibernetice au la bază neglijența utilizatorilor, a angajaților sau a administratorilor de rețele. De aceea, educația, conştientizarea şi pregătirea personalului, atât în domeniul public, cât și privat, sunt aspecte ce nu pot fi ignorate în prevenirea atacurilor cibernetice. În condițiile în care cele mai multe dintre vulnerabilități sunt generate de utilizatori, prin accesarea internetului fără măsuri minime de securitate, riscurile pot fi gestionate mai eficient în contextul unui nivel ridicat de cultură de securitate cibernetică la nivelul societății, în ansamblu.

Impactul atacurilor cibernetice poate fi devastator, la nivelul sectorului privat, dar mai cu seamă, în sectorul public. De cele mai multe ori, țintele din sectorul public sunt cele guvernamentale sau infrastructurile critice. În ambele situații, costurile de recuperare a sistemelor după un atac major, este unul imens, comparativ cu investiția pe care orice entitate, fie publică, fie privată, o poate face în pregătirea personalului şi în implementarea măsurilor minime de securitate. De altfel, există strategii de securitate cibernetică în care obiectivele, direcțiile de acțiune și măsurile aferente se concentrează, cu precădere, pe pregătirea personalului.

Securitatea cibernetică se realizează pe trei componente: prevenire, intervenție (reacție/ răspuns), în cazul producerii unui atac cibernetic, și reziliență, importante în egală măsură și strâns legate între ele. Astfel, măsurile de prevenire urmăresc, pe de o parte, asigurarea

capacității sistemelor de a rezista în fața amenințărilor cibernetice, iar pe de altă parte, diminuarea impactului atacurilor cibernetice, prin măsuri adecvate de reacție/ răspuns, iar astfel, reziliența sistemelor și a rețelelor se asigură prin eficiența măsurilor de prevenire și a celor de contracarare/ intervenție.

Primordial, măsurile de prevenire au drept scop asigurarea rezilienței sistemelor și a rețelelor informatice, ceea ce presupune ca eficiența lor să asigure eliminarea completă a atacurilor cibernetice. Însă, evoluția rapidă a amenințărilor, capabile să identifice și să exploateze noi vulnerabilități, impune extinderea măsurilor de prevenire, în sensul asigurării rezilienței prin diminuarea impactului eventualelor atacuri cibernetice.

Dacă pe dimensiunile intervenție și reziliență pot acționa, cu precădere, specialiști și responsabili, componenta de prevenire, care constă în măsuri de reducere a riscului de manifestare a atacurilor cibernetice, este, poate, cea mai complexă, dat fiind faptul că toți cei implicați, indiferent de proveniență, nivel de utilizare sau nivel de pregătire ori specializare, pot contribui prin respectarea unui protocol minim de securitate.

Prima categorie de contributori o reprezintă utilizatorii (fie că sunt indivizi, companii, instituții sau organizații, în calitate de consumatori de servicii de internet), care trebuie să ia măsuri de protecție, precum utilizarea unor parole, instalarea unui program antivirus, selectarea rețelelor și a site-urilor, în funcție de gradul în care prezintă elemente de siguranță, sau atenție cu privire la conținutul pe care îl postează, distribuie sau accesează.

O altă categorie este reprezentată de sectorul privat, cu trei componente majore – dezvoltatorii de aplicații și dispozitive, specialiștii în securitate cibernetică – în principiu, dezvoltatorii de softuri de securitate și testerii de securitate, dar și operatorii și furnizorii de servicii digitale. În etapa de prevenire, contribuția acestora constă, în cea mai mare măsură, în furnizarea de produse și servicii specifice sigure, testate anterior lansării pe piață.

În cea de-a treia categorie sunt incluse autoritățile statului – sectorul public, care, la rândul lor se împart în două subcategorii, cu responsabilități diferite. Pe de o parte, autoritățile guvernamentale, în calitate de legiuitori, iar pe de altă parte, instituțiile cu responsabilități în domeniul securității cibernetice, stabilite prin lege.

Există, însă, alte trei categorii distincte, cu rol important în cadrul componentei de prevenire, a securității cibernetice, care nu pot fi asimilate celor de mai sus, respectiv: operatorii

de servicii esențiale naționale, care pot proveni atât din sectorul public, cât și din cel privat, și rețeaua CERT, care are atribuții bine definite, atât în legislația internațională, cât și la nivel național. În plus, la nivelul fiecărui tip de entitate responsabilă în securitatea cibernetică, există evaluatori de risc cibernetic, care formează rețeaua CSIRT și au un rol foarte important în componenta de intervenție în cazul unui incident, la nivelul instituțiilor din sectorul public, cât și la nivelul entităților din mediul privat.

Fiecare dintre actorii enumerați mai sus pot avea obligații, dar pot să fie și beneficiari de securitate în mediul cibernetic, în baza unei legi comprehensive, prin care să se stabilească cu exactitate rolul și atribuțiile fiecărei entități implicate în acest proces.

Fiind parte a securității naționale, securitatea cibernetică s-a dovedit a fi un domeniu dificil de legiferat, însă, în ultimele două decenii, se constată o implicare majoră la nivelul organizațiilor internaționale în reglementarea acestui domeniu, sau a unor componente ale acestuia. NATO a definit și actualizează permanent politica de apărare cibernetică, Uniunea Europeană a emis directive și regulamente, cu obligații sau recomandări pentru statele membre, referitoare la elaborarea legislației naționale, OSCE și Organizația Națiunilor Unite au avut primele inițiative în acest sens. În aceste documente sunt stabilite, adaptate și definite concepte precum suveranitate, jurisdicție sau responsabilitatea statului, însă, un aspect important îl constituie impactul asupra drepturilor omului.

Ceea ce lipsește, în legislația internațională, este un tratat referitor la securitatea spațiului cibernetic, așa cum există pentru spațiul cosmic, cel aerian sau cel maritim, pentru piraterie sau chiar referitor la teritoriul Antarcticii. Aceste tratate conțin prevederi referitoare la acțiuni militare, de aceea modelele oferite de aceste documente nu sunt suficiente. Spațiul cibernetic este caracterizat de accesul la informație și modul în care aceasta poate fi gestionată.

În privința strategiilor de securitate cibernetică, cele mai multe state ale lumii au elaborat un astfel de document. În lucrare, se arată că toate statele membre NATO și ale Uniunii Europene au elaborat și implementat un astfel de document. Problema care se ridică, în privința strategiilor naționale de securitate cibernetică, este că reglementează un domeniu în care evoluțiile sunt rapide, comparativ cu procesele greoaie de elaborare a normelor, iar nevoile statului și ale societății se schimbă odată cu aceste evoluții. Securitatea cibernetică necesită un

efort continuu și constant din partea statelor. Astfel, independent de conținutul strategiilor, care la momentul emiterii poate răspunde în întregime nevoilor unui stat, contextul național trebuie reevaluat/ reanalizat periodic, concomitent cu evaluarea implementării strategiilor, în baza indicatorilor de performanță stabiliți, astfel încât documentele să poată fi reeditate, în funcție de evoluții, în mod proactiv. Astăzi, o parte dintre strategiile de securitate cibernetică ale statelor membre UE și NATO sunt în vigoare de mai mult de șapte ani. Strategia de securitate cibernetică a României este unul dintre aceste documente, fiind emisă în anul 2013.

Dacă la nivel strategic se stabilesc viziuni, principii, obiective, direcții de acțiune și măsuri care să răspundă nevoilor de securitate cibernetică ale unui stat, în funcție de analiza contextului național, la un moment dat, prin legea națională trebuie să se stabilească termenii și modul de implementare a prevederilor strategice, cu stabilirea de responsabilități, atribuții și obligații pentru toate entitățile implicate, dar trebuie să asigure și măsuri și resursele necesare în îndeplinirea acestora.

În prezent, în România, domeniul securității cibernetice reprezintă obiectul Strategiei de Securitate Cibernetică, din anul 2013 și al Legii privind Securitatea Cibernetică, adoptată la finalul anului 2018.

Strategia Națională de Securitate Cibernetică reprezintă un document cuprinzător și coerent, în concordanță cu prevederile reglementărilor Uniunii Europene în domeniu, pentru perioada în care a fost elaborat, însă, raportat la evoluțiile prezente ale mediului pe care îl reglementează, prevederile lui sunt depășite, în mare măsură, raportându-se la evaluarea mediului de securitate la nivelul anului 2013. Adoptarea unui nou document strategic a fost asumată prin Legea 362/2018.

Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, numită generic Legea Securității Cibernetice, conține prevederi referitoare, cu precădere, la rolul și atribuțiile CERT-RO în prevenirea și combaterea atacurilor cibernetice, precum și modul de raportare a celorlalte entități în relația cu acesta. Această lege reprezintă transpunerea în legislația națională a Directivei NIS a Uniunii Europene și răspunde, în mare parte, cerințelor numite în documentul european, însă așa cum reiese din denumire.

Legea vizează strict protecția rețelelor și a sistemelor informatice și prevede stabilirea autorității naționale în domeniul securității cibernetice, în CERT-RO și a rețelei CSIRT, cu atribuții de prevenire și răspuns în caz de incident cibernetic, precum și operatorii de servicii esențiale și furnizorii de servicii digitale, în conformitate cu lista cuprinsă în Anexa documentului.

Cel mai recent document care face referire la domeniul securității cibernetice, în România, este Strategia Națională de Apărare a Țării, care a intrat în vigoare la jumătatea anului 2020. Deși nu este un document dedicat domeniului securității cibernetice, acesta subliniază abordarea conceptului de securitate națională în sens extins, cuprinzând „apărarea națională – înțeleasă în dublă calitate, de apărare națională și apărare colectivă", dar și „alte dimensiuni precum politica externă, ordinea publică, activitatea de informații, contrainformații și de securitate, managementul crizelor, domeniile educație, cultură, sănătate, economic, demografie, financiar, mediu, securitatea energetică sau cea cibernetică, securitatea infrastructurilor critice și a patrimoniului istoric și cultural"[16].

Documentul reprezintă un pas important în evoluția legislației la nivel național, din cel puțin două perspective: are la bază o analiză a contextului de securitate actual, fapt relevat de utilizarea unor termeni care lipseau în documentele precedente, mai cu seamă, la nivelul prevederilor referitoare la amenințări, iar din acest motiv, poate avea un rol important în revizuirea Strategiei Naționale de Securitate Cibernetică, dar și în inițierea demersurilor de actualizare a legislației privind securitatea națională, precum și extinderea legislației privind securitatea cibernetică.

Din analiza cu privire la cadrul normativ al României, în domeniu, rezultă că este nevoie de o lege privind securitatea cibernetică. Aceasta trebuie să cuprindă pe lângă prevederile legate de securitatea rețelelor tuturor instituțiilor, mai cu seamă a celor din categoria infrastructurilor critice/ a serviciilor esențiale, prin stabilirea și definirea unor măsuri pentru: instruirea personalului cu privire la exploatarea sistemelor IT sau obligația utilizării programelor antivirus și a actualizării softurilor și, prin urmare, includerea fondurilor dedicate în bugetul instituțiilor vizate etc. O astfel de lege trebuie să garanteze autorităților competente, așa cum sunt denumite

[16] Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. Împreună, pentru o Românie mai sigură și prosperă într-o lume marcată de noi provocări*, 2020, 7, disponibilă la https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf

în Strategie, instrumentele necesare în asigurarea componentei de prevenire a atacurilor cibernetice. Însă, anterior elaborării legii, este nevoie de un nou document strategic, adaptat mediului de securitate actual, care să conțină atât instrumente de evaluare a îndeplinirii obiectivelor propuse în precedenta ediție, cât și obiective, direcții de acțiune și măsuri care să răspundă noilor provocări de securitate cibernetică, stabilite în baza unei evaluări actualizate a mediului de securitate.

Un alt aspect important în asigurarea securității cibernetice îl constituie cooperarea, atât la nivel internațional, cât și la nivel național. Dacă, la nivel internațional, cooperarea este garantată prin statutul de membru sau aliat în cadrul organizațiilor internaționale, la nivel național constă tocmai în relația dintre sectorul public și cel privat, iar o componentă a acesteia este relația între autorități și deținătorii de rețele de comunicații. Această relație se poate desfășura pe trei dimensiuni. Un prim aspect constă în asigurarea comunicării între entități, prevăzut de Legea 362/2018 care stabilește CERT-RO drept „autoritate competentă la nivel naţional pentru securitatea reţelelor şi a sistemelor informatice", cu atribuții în colectarea notificărilor referitoare la incidentele de securitate cibernetică, precum și instituirea rețelei CSIRT[17]. Celelalte două dimensiuni trebuie asigurate prin prevederi ulterioare: pe de o parte, prin măsuri de implementare a prevederilor referitoare la certificarea produselor, serviciilor și proceselor IT, cu scopul reducerii vulnerabilităților legate de conectarea la internet și, implicit, a protejării utilizatorilor, iar pe de altă parte, prin asigurarea măsurilor și instrumentelor de realizare a securității naționale.

Pregătirea personalului, educația, campaniile de conștientizare și cultura de securitate sunt prevăzute de Strategia din anul 2013, dar nu sunt vizate de actuala lege privind securitatea cibernetică. Dacă pregătirea personalului și educația de securitate cibernetică au nevoie de prevederi legale pentru a se implementa măsuri în consecință, campanii de informare și conștientizare la nivelul utilizatorilor se pot derula și fără o lege dedicată. Acestea sunt cu atât mai importante la nivelul societății românești, cu cât este nevoie ca adoptarea de legi care să răspundă nevoilor de securitate, inclusiv din perspectiva securității naționale.

[17] Parlamentul României, *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice*, 2018, Art.15, disponibilă la https://cert.ro/vezi/document/legea-nr-362-din-28-decembrie-2018, ultima accesare, iunie 2021

Având aceste date și pe fondul unor legi privind securitatea națională, în vigoare de aproape 30 de ani, care sunt adaptate la amenințările din perioada emiterii lor, măsurile de asigurare a securității naționale sunt limitate. De aceea, România are nevoie de o lege a securității cibernetice complexă și coerentă, care să răspundă nevoilor de protecție a tuturor utilizatorilor în mediul cibernetic, cu atât mai mult cu cât astăzi, există foarte puține activități care nu se desfășoară online sau nu sunt conectate, cel puțin parțial, la acesta, dar și nevoilor de definire și actualizare, în contextul erei tehnologice, a capacității de acțiune a autorităților cu atribuții în domeniul securității naționale.

În prezent, legislația stabilește instituțiile cu responsabilități în domeniu, sistemul și modul de lucru în cadrul rețelei CSIRT, care este compusă din astfel de centre în toate domeniile cheie, stabilește lista serviciilor esențiale și pe cea a operatorilor de servicii digitale, precum și modul de coordonare și relaționare a acestora cu CERT-RO, precum și autoritatea națională desemnată și punctul unic de contact în domeniul securității cibernetice, răspunzând, astfel obiectivului strategic de protecție a infrastructurilor critice. Obiectivul vizează monitorizarea amenințărilor cibernetice la adresa infrastructurilor românești și protejarea acestora în consecință. Se poate spune că, astfel a fost creată platforma de comunicare, descrisă în cadrul lucrării drept awareness situațional, care permite, prin coordonare și colaborare directe, scurtarea timpilor de reacție în cazul unei crize de tip cibernetic.

În perioada următoare, conform declarațiilor directorului Centrului Național Cyberint, Anton Rog, în cadrul conferinței Security Talks[18], CERT-RO va deveni Directoratul Național pentru Securitate Cibernetică (DNSC), care va avea „rol de hub între toate instituțiile de aplicare a legii, de intelligence, militar etc. și industria privată, mediul universitar", ceea ce îi va sigura statutul de „instituție (...) de clasă internațională și actor cheie pentru implementarea strategiei naționale de securitate cibernetică. (...) Directoratul să poată să poziționeze ferm România ca un lider recunoscut în securitatea cibernetică"[19].

Prin urmare, DNSC este platforma care poate integra soluții pentru a răspunde obiectivelor de cooperare internă, atât între instituțiile cu responsabilități în domeniul securității

[18] Security Talks Expert, Conferința Security Talks #3, 2020, disponibilă la https://www.youtube.com/watch?v=0nH9TrhenEs, ultima accesare, noiembrie 2020
[19] CERT-RO, „Ce va aduce nou Directoratul Național de Securitate Cibernetică față de CERT-RO", 2020, disponibil la https://cert.ro/citeste/articol-dnsc-cert-ro-transformare, ultima accesare, noiembrie 2020

cibernetice, cât și între mediul public și cel privat, dar și celor de cooperare internațională, prin pozitionarea României ca lider în domeniul securității cibernetice, în sprijinul căreia a fost stabilită și înființarea Centrului European de Competențe în Materie de Securitate Cibernetică la București[20]. Activitatea acestui centru european se va se va concentra pe proiecte de „inovare și cercetare-dezvoltare în domeniul securității cibernetice”[21].

Rămâne, însă, o provocare în elaborarea și implementarea măsurilor de creștere a nivelului culturii de securitate cibernetică a cetățenilor și, mai cu seamă, al culturii de securitate, necesare în echilibrarea raportului dintre securitate și libertate. Așa cum a relevat și sondajul de opinie, detaliat în Capitolul III, se simte nevoia de o mai bună informare cu privire la măsurile de securitate cibernetică pe care le pot adopta utilizatorii.

Multe dintre atacurile cibernetice pot fi evitate dacă există un cadru normativ coerent, cuprinzător și adaptat evoluțiilor mediului pe care îl reglementează. Spre exemplu: atacul cibernetic asupra a patru spitale din România, din iunie 2019. Din declarația autorităților, rezultă că a fost un atac de tip ransomware, activat odată cu accesarea ataşamentului unui e-mail de către personalul spitalelor, pe fondul absenței unui program antivirus[22]. Prin urmare, acest atac ar fi putut fi evitat dacă, în baza unor obligații stabilite prin lege, personalul spitalelor ar fi fost instruit cu privire la măsuri minime de protecție în mediul online, pe de o parte, dar și asigurarea resurselor necesare, pe de altă parte. Incidentul ar fi putut avea efecte mult mai grave, ținând cont de faptul că au fost vizate spitale – elemente constituente ale sistemului de sănătate, inclus în categoria infrastructurilor critice naționale.

În final, în cea de-a treia parte, metoda utilizată este sondajul de opinie, constând în aplicarea, în mediul online, a unui chestionar referitor la comportamentul utilizatorilor de internet, care pune în balanţă, pe de o parte, modul în care aceştia încearcă să se protejeze în spațiul cibernetic, iar pe de altă parte, percepția lor cu privire la reglementarea în domeniu. Acest

[20] Consiliul Uniunii Europene, „Noul centru de competențe european în materie de securitate cibernetică va avea sediul la București, România”, 2020 comunicat disponibil la https://www.consilium.europa.eu/ro/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/, ultima accesare, iunie 2021
[21] Security Talks Expert, Conferința Security Talks #3, 2020
[22] Digi24, „Atac cibernetic la spitalele din România. Avertismentul lansat de ministrul Sănătății”, 2019

instrument poate oferi atât elementele necesare evaluării nivelului culturii de securitate cibernetică la nivelul utilizatorilor, cât și pe cele necesare identificării tocmai a punctului de echilibru între conceptele de libertate și securitate, definit prin limita până la care aceștia pot accepta o reglementare, care poate fi percepută ca fiind limitativă sau chiar intruzivă, în domeniu.

La elaborarea sondajului de opinie, au fost stabilite patru categorii de întrebări, grupate în patru secțiuni:

- Întrebări de introducere sau de cunoaștere a respondenților;
- Întrebări referitoare la comportamentul utilizatorilor în mediul online, precum și la măsurile de securitate pe care le folosesc;
- Întrebări referitoare la opinia respondenților cu privire la posibile amenințări și măsuri de protecție ce pot fi aplicate în mediul online;
- Întrebări referitoare la opinia respondenților față de evenimente din realitate, vizând protecția datelor cu caracter personal, utilizarea tehnologiei de către autorități în anumite situații sau un atac cibernetic produs în România.

Sondajul a fost aplicat pe platforma www.survio.com, iar pentru interpretarea rezultatelor sondajului, a fost utilizat software-ul SPSS.

Metoda cercetării prin utilizarea sondajului prezintă o serie de limitări, care provin, în general, din faptul că va fi aplicat în mediul online. Acesta îi atribuie un caracter voluntar, ceea ce poate influența, în mod direct, atingerea unui număr reprezentativ de subiecți, pe de o parte, iar pe de altă parte, echitabilitatea reprezentativității publicului țintă (utilizatorii de internet), în funcție de criterii precum: vârstă, sex, studii, venituri sau mediul de proveniență.

De asemenea, perioada de timp în care poate fi exploatat un astfel de instrument este influențată direct, întrucât căile de distribuire se epuizează în primele zile de la activare, iar gradul de redistribuire scade proporțional cu timpul scurs de la momentul lansării. De aceea, sondajul poate contura un portret-robot al utilizatorului de internet din România, dar rezultatele se pot extrapola la nivelul societății numai în condițiile atingerii unui eșantion minim de respondenți.

Cercetarea privind evaluarea măsurilor de securitate pe care utilizatorii le iau în activitatea online, a măsurii în care pot identifica posibile cauze ale producerii amenințărilor cibernetice sau posibile soluții, precum și a percepției cu privire la amenințările cibernetice și la responsabilități sau cui aparțin acestea, a relevat un nivel mediu al culturii de securitate cibernetică a utilizatorilor, însă cu potențial de dezvoltare, dată fiind identificarea nevoii utilizatorilor de o mai bună informare, și un nivel scăzut al culturii de securitate, ceea ce reflectă un dezechilibru în raportul libertate – securitate, înclinat în favoarea libertății. Măsurile de securitate asociate intervenției autorităților reprezintă o opțiune pentru utilizatori, numai în mod condiționat. Pe de o parte, se înregistrează un nivel relativ scăzut de acceptare a unor norme legislative în domeniul securității cibernetice și reticența cu privire la măsurile pe care trebuie să le ia autoritățile competente în domeniul securității naționale, iar pe de altă parte, respondenții manifestă deschidere către acțiuni sau atribuții ale acestora, condiționată de cunoașterea fenomenelor, pentru care soluția este tocmai informarea utilizatorilor.

Acest dezechilibru are la bază lipsa de informare și creează un fond periculos, în raport cu legiferarea unor aspecte ce țin de securitatea națională: majoritatea celor care se opun unor reglementări în domeniu, sunt cei care pot opta pentru securitate, în contextul unei crize majore, așa cum s-a întâmplat în cazul adoptării Patriot Act, în Statele Unite.

În contextul dezbaterii libertate vs. securitate, percepția asupra celor două concepte este că măsurile de securitate afectează drepturile și libertățile cetățenilor, mai ales din perspectiva asigurării securității naționale. Însă, într-un stat democratic, securitatea poate fi asigurată, concomitent cu respectarea drepturilor omului, întrucât „cetățeanul participă la asigurarea securității”[23].

Nivelul mediu al culturii de securitate cibernetică, comparativ cu un nivel scăzut al culturii de securitate sunt cauzate de lipsa disponibilității informațiilor în domeniu. Educația de securitate cibernetică, precum și campaniile de awareness și de pregătire a personalului din organizațiile de drept public și privat, în egală măsură, pot constitui măsuri de răspuns la astfel

[23] Monitorul Apărării și Securității, gl. Sergiu Medar, în cadrul Conferinței *Cum răspundem la crizele de securitate națională*?, 2021, video la https://www.facebook.com/monitorulapararii/videos/1136156286802705/?__so__=permalink&__rv__=related_videos, ultima accesare, februarie 2021

de nevoi. Spre deosebire de domeniul securității naționale, unde informația pentru cetățeni este destul de limitată și astfel sunt doar beneficiari de securitate, pe componenta securității cibernetice, aceștia sunt implicați direct, fiind utilizatori ai acestui spațiu, ceea ce îi face, în egală măsură, beneficiari și furnizori de securitate, prin măsurile pe care trebuie să le adopte pentru propria securitate. Dacă aceste informații, puse la dispoziția utilizatorilor, în contextul securității cibernetice, acoperă și responsabilitățile autorităților din domeniul securității naționale, astfel încât măsurile de securitate să poată fi înțelese prin filtrul utilizatorului de mediu online: existența amenințărilor, nevoia de protecție în fața lor, prin înțelegerea efectelor pe care le pot avea și importanța implementării măsurilor de securitate, la nivel de infrastructuri critice, nivelul de cultură de securitate al unei societăți poate fi crescut prin activități de informare dedicate securității cibernetice.

Prin educație și awareness, utilizatorii pot cunoaște amenințările și vulnerabilitățile, precum și efectele pe care le pot avea asupra lor eventuale atacuri cibernetice, pe de o parte, iar pe de altă parte, conștientizând nevoia de securitate, vor utiliza metodele și mijloacele cu care se pot proteja în fața acestora și vor ști cui să se adreseze, în cazul identificării unui incident de securitate cibernetică. Cunoașterea legislației constituie un alt element cheie ce poate face obiectul educației de securitate cibernetică și al campaniilor de conștientizare. În plus, utilizatorii pot cunoaște arhitectura instituțională cu responsabilități în asigurarea securității cibernetice și cum acționează aceste structuri în asigurarea securității cibernetice.

Dacă awareness se poate face prin campanii de informare, orientate către publicul general, cu scopul unic de conștientizare a utilizatorilor cu privire la amenințările cibernetice, precum și a mijloacelor de asigurare a securității în mediul online, componenta educație se referă la programe educaționale adresate elevilor, incluse în curicula scolară, în funcție de vârstă, de la clasele primare, până la liceu. La nivel universitar, se poate dezvolta componenta de specializare. Astfel, beneficiile educației de securitate cibernetică pot căpăta noi forme: pe de o parte, se vor forma utilizatori mai bine pregătiți în a face față provocărilor online, iar pe de altă parte, aprofundarea acestui domeniu în zona academică, poate asigura specialiști în securitate cibernetică, resursă umană ce poate activa atât în sectorul public, cât și în cel privat, atât în zona de elaborare de politici în domeniu, cât și de implementare a acestora. Un alt beneficiu al educației de securitate cibernetică îl poate constitui domeniul cercetare-dezvoltare, prin

implicarea specialiștilor formați într-un astfel de sistem educațional în dezvoltarea de produse și servicii de comunicații și tehnologia informației la standarde superioare de securitate.

O altă metodă de informare constă în pregătirea personalului. Este nevoie de programe de training atât pentru personalul din mediul public, cât și pentru cel din mediul privat, mai cu seamă, în cazul entităților active în asigurarea serviciilor esențiale.

Toate aceste metode de informare și pregătire a utilizatorilor, a specialiștilor și a resursei umane, constau în punerea la dispoziție a informațiilor relevante de securitate cibernetică, inclusiv pe componenta legislativă, prin care se definesc atribuții pentru autoritățile cu responsabilități în domeniu, iar rezultatul acestor demersuri de informare, cumulate, constă în obținerea unui nivel ridicat al culturii de securitate cibernetică, la nivelul societății.

Rezultatul principal al unei astfel de abordări îl constituie echilibrarea raportului între libertate și securitate, prin înțelegerea conceptelor de responsabilitate, atât la nivel individual, cât și colectiv. Aceasta este etapa în care se poate contura un comportament al utilizatorilor online, adaptat la provocările mediului cibernetic, care constă aplicarea permanentă a măsurilor de securitate cibernetică individuală. Acest comportament are la bază conștientizarea, în egală măsură, nevoii de securitate și a celei de libertate, de către utilizatori, astfel încât acestea nu se exclud reciproc, ci mai degrabă, se pot completa.

Consecința imediată a unui astfel de comportament o constituie scăderea ratei de succes a atacurilor cibernetice, ceea ce reprezintă scopul măsurilor de securitate cibernetică.

Raportat la tema Libertate vs securitate în mediul online, pot fi urmate și alte direcții de cercetare. Spre exemplu, lucrarea propune prioritizarea acțiunilor de creștere a nivelului culturii de securitate, ceea ce depinde de derularea unor programe de awareness la nivelul întregii societăți. Pe de altă parte, teza oferă un model de structurare a construirii mesajului unei campanii de awareness pentru utilizatori, care să înțeleagă că trebuie să se protejeze în mediul online, prin informații privind amenințările (de ce să se protejeze) și securitatea cibernetică (cum să se protejeze). Ulterior, prin aplicarea metodei process tracing[24], pot fi evaluate, etapizat, evoluția și impactul pe care le pot avea măsurile de creștere a nivelului culturii de securitate, prin

[24] Stephen Van Evera, *Guide to methods for students of political science* (Ithaca, New York: Cornell University Press, 1997), 64

educație și awareness, la nivelul utilizatorilor, fie într-o analiză dedicată exclusiv acestei evoluții, fie în relație cu nivelul de acceptare a implementării unor prevederi legislative privind securitatea națională, raportul libertate-securitate fiind specific acestui domeniu. Sondajul de opinie prezentat în lucrare poate constitui, de asemenea, un instrument de evaluare, ce poate fi utilizat atât de cercetători independenți, cât și la nivelul autorităților, cu prilejul revizuirii documentelor strategice privind securitatea cibernetică. Actualizarea acestora se impune din perspectiva evoluției permanente a amenințărilor, influențată, la rândul ei de dezvoltarea tehnologică.