UNIVERSITATEA BABEȘ-BOLYAI
Facultatea de Istorie și Filosofie

Școala doctorală „Relații internaționale și studii de securitate”

Teză de doctorat

***

SECURITATEA ȘI GUVERNANȚA SPAȚIULUI CIBERNETIC CONTEMPORAN

Conducător de doctorat,

Prof. univ. dr. Michael SHAFIR

Autor,

Iulian Florentin POPA

Cluj-Napoca

2015

C U P R I N S

REZUMAT

Deşi în ultimii ani asistăm la o dezvoltare relativ pașnică a spațiului cibernetic, avem suficiente motive să credem că guvernanța și securitatea spațiului cibernetic contemporan se află printre cele mai serioase provocări cu care se confruntă comunitatea internațională la momentul actual. Am ales ca obiect de cercetare concomitentă securitatea și guvernanța spațiului cibernetic contemporan, deoarece cred cu tărie că dezvoltarea durabilă a spațiului cibernetic – fundamentată pe ideea în sine de bună guvernanță – transcende securității și apărării naționale și are rădăcini puternice în zona economică, socială, societală și culturală. Pe lângă rolul de facilitator al creșterii economice, observ la rândul meu că mediul virtual tinde să devină un spațiu de insecuritate la nivel global.

La umbra argumentului potrivit căruia interdependențele complexe domină dinamica relațiilor internaționale contemporane[1], teza de față subliniază faptul că înțelegerea și cunoașterea în profunzime a relației dintre securitatea și guvernanța spațiului cibernetic este primordială pentru proiectarea unor politici și strategii eficiente cu privire la spațiul cibernetic. Dacă ar fi să încadrez cercetarea mea în tabloul vast al curentelor de gândire consacrate în domeniul relațiilor internaționale, înclin să cred că aceasta se situează la granița dintre instituționalismul neoliberal promovat de către Robert Keohane[2] și noul liberalism de sorginte hobsoniană[3]. De fapt, eu argumentez că buna guvernanța a spațiului cibernetic constituie, mai degrabă, un set de mecanisme și acțiuni ce vizează optimizarea balanței de putere cibernetică în scopul dezvoltării durabile și pașnice a spațiului cibernetic și, implicit, prevenirii și combaterii dilemei de securitate cibernetică, prin stimularea proactivă și controlul pașnic al interacțiunii dintre actorii internaționali în acord cu principiile pe care le-am identificat și cercetat în cele ce urmează.

În esență, cercetarea mea a verificat dacă menținerea în parametri optimi a securității spațiului cibernetic se fundamentează pe promovarea și adoptarea unor principii de (bună) guvernanță care pot să sprijine și garanteze protejarea concomitentă a intereselor utilizatorilor, mediului de afaceri și organizațiilor guvernamentale. Cu toate că cercetarea științifică privitoare la spațiul cibernetic a înregistrat progrese substanțiale în ultimii ani,

[1] Robert Keohane, Joseph Nye, *Power and Interdependence: World Politics in Transition*, Boston, Little, Brown and Company, 1989, p. 23.
[2] Robert Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton, Princeton University Press, 2005., *passim.*
[3] John Atkinson Hobson, *The State and International Relations*, Cambridge, Cambridge University Press, 2000, p. 65.

anterior alegerii temei de cercetare am constatat cu surprindere că multe dintre încercările academice care au vizat elaborarea unor teorii generalizate ale securității spațiului cibernetic au omis aproape sistematic studiul amănunțit al interdependețelor existente între calitatea guvernanței spațiului cibernetic și nivelul general de securitate pe care îl resimt utilizatorii spațiului cibernetic.

Obiectivul general al tezei a constat în studiul aprofundat al relației dintre securitatea și guvernanța spațiului cibernetic, în vederea confirmării sau infirmării interdependenței existente între nivelul de securitate și calitatea guvernanței spațiului cibernetic. În subsidiar, am evidențiat și am propus o serie de clarificări conceptuale la nivelul lexiconului de specialitate – acolo unde am considerat necesar – și am studiat dacă dilema de securitate cibernetică este rezolvabilă într-o manieră pașnică, prin intermediul sau cu ajutorul bunei guvernanțe.

Practic, am pornit de la ipoteza generală conform căreia buna guvernanță poate să contribuie la prevenirea și detensionarea pașnică a dilemei de securitate în spațiul cibernetic. În funcție de consistența acestei ipoteze am evaluat dacă există într-adevăr o relație de interdependență între nivelul de securitate și calitatea guvernanței spațiului cibernetic. În acest context, obiectivele și ipotezele secundare propuse au avut rolul de a substanția scopul realizării acestei lucrări, și anume acela de a a arăta că există suficiente motive demne de luat în considerare potrivit cărora spațiul cibernetic poate fi considerat deja un domeniu strategic, alături de mediile terestru, aero, naval și spațial.

Dată fiind strategia de cercetare adoptată, am optat pentru enunțarea distinctă a ipotezelor secundare de cercetare în cadrul fiecărui capitol în parte. Fac precizarea că ipotezele secundare de cercetare au avut un rol determinant în formularea unor posibile răspunsuri în direcția următoarelor întrebări de cercetare:

Î1. În ce măsură este rezolvabilă pașnic dilema de securitate cibernetică?

Î2. Cât de eficientă se poate dovedi buna guvernanță în rezolvarea și detensionarea pașnică a dilemei de securitate cibernetică?

Cu privire la gradul de actualitate al temei de cercetare propuse, apreciez că securitatea și guvernanța spațiului cibernetic constituie aspecte de interes și actualitate pentru comunicatea științifică din sfera studiile strategice contemporane. De fapt, am încercat să sugerez că dinamica unor evenimente internaționale recente precum „Primăvara Arabă” sau „Revoluția Twitter” demonstrează că înțelegerea adecvată a fenomenelor ce au

loc în cadrul „arenei cibernetice” prezintă o importanță deosebită pentru studiul relațiilor internaționale și studiilor de securitate.

Cât privește alegerea temei, am avut în vedere faptul că o bună parte a utilizatorilor și chiar a decidenților are o viziune distorsionată, să-i spunem, asupra importanței problematicilor contemporane de securitate și guvernanță a spațiului cibernetic. În esență, nu am putut neglija faptul că subiectul ales constituie o bună ocazie pentru a atrage atenția tuturor celor interesați asupra faptului că securitatea și guvernanța spațiului cibernetic constituie factori esențiali pentru funcționarea sustenabilă și dezvoltarea durabilă a oricărei organizații și societăți. De fapt, în viziunea mea, securitatea și guvernanța spațiului cibernetic ar trebui să constituie o preocupare fundamentală a oricăror actori internaționali ce se doresc a fi cât mai competitivi pe plan național și internațional deopotrivă.

Din punct de vedere academic, teza reprezintă o aprofundare și o continuare firească a cercetărilor introductive și aparent eclectice pe care le-am întreprins pe durata studiilor de master urmate în domeniul studiilor de securitate în cadrul Universității Babeș-Bolyai, studii ce au fost finalizate cu o lucrare de disertație ce a vizat violența și agresiunea la nivelul spațiului cibernetic[4]. După cum se poate constata, nu întâmplător am optat pentru cercetarea securității și guvernanței spațiului cibernetic contemporan. Mai mult, am ales această temă de cercetare din dorința de a valorifica în plan științific experiența mea profesională acumulată pe parcursul ultimilor ani în domeniul consultanței IT, analizei informațiilor și evaluării tendințelor. De asemenea, nu am trecut să trec cu vederea faptul că numărul actual al cercetătorilor dedicați problematicilor specifice relațiilor internaționale și studiilor de securitate privitoare la spațiului cibernetic este cu mult sub nevoile strategice ale României – un stat cu ambiții euroatlantice considerabile, cel puțin în domeniul securității cibernetice.

Cât privește metodologia de cercetare specifică acestei teze, aprecizez că acesta nu se subscrie în totalitate unui tipar anume, specific doar studiului relațiilor internaționale. De fapt, în alegerea strategiei de cercetare am pornit de la premisa că unele metode transdisciplinare de cercetare și analiză a informațiilor – ce nu se-nscriu neapărat prescripțiilor metodologice „standard” – pot să contribuie semnificativ la elaborarea unor

[4] Iulian Popa, Dacian Duna (coord. ştiinţific), *Violența cibernetică: Între război convențional și terorism (lucrare de disertație),* Cluj-Napoca, Universitatea Babeș-Bolyai, 2012.

produse analitice sensibil mai cuprinzătoare și chiar mai promițătoare[5]. Deși m-am conformat îndeaproape recomandărilor de bune practici și rigorilor metodologice impuse de specificul lucrării de față, am ținut cont de faptul că există totuși un risc considerabil ca anumite „automatisme" metodologice în activitatea de cercetare sau analiză a informațiilor să nu fie întocmai benefice[6]. Nu de puține ori, „stereotipurile metodologice" pot împiedica cercetătorul sau analistul să evalueze și să valorifice eficient anumite „semnale" slabe, dar cu potențial semnificativ de îmbunătățire a cunoașterii științifice. Prin urmare, având în vedere gradul însemnat de abstractizare al temei de față, am optat pentru utilizarea unei metodologii de studiu și analiză ce mi-a permis cât mai mult cu putință jalonarea sistematică între perspectivele empirice și cele științifice de generare a cunoașterii. Deloc întâmplător, am considerat oportun ca o bună parte a acestei lucrări să aibă un fundament empiric subsecvent, în paralel cu cel științific, care să pună mai bine în valoare contribuția personală adusă domeniului de studiu propus.

Prin prisma strategiei de cercetare adoptate, lucrarea de față nu s-a axat doar pe inventarierea și analizarea dovezilor și surselor care pot să confirme ipotezele dominante, ci mai ales pe cartografierea și evaluarea calitativă a ipotezelor și surselor contrare acestora. Atât ipotezele de cercetare, cât și argumentele calitative și cantitative în favoarea sau defavoarea acestora au fost culese experimental din practica curentă și din literatura de specialitate, prin tehnici și procedee de observare directă și indirectă, respectiv prin studiul bibliografiei propuse. Anterior culegerii ipotezelor, reperele epistemologice au fost selectate și completate ulterior în acord cu specificul temei, optându-se pentru utilizarea proporțională a mijloacelor de cercetare calitativă și cantitativă. În esență, relevanța și credibilitatea surselor folosite au fost evaluate și prin consultarea unor experți și practicieni cu vastă experiență în domeniul securității și guvernanței spațiului cibernetic.

Metoda principală de analiză a informațiilor și evaluare a variabilelor de cercetare a fost analiza (sau metoda) ipotezelor concurente (AIC), metodă ce a fost utilizată într-o varianta simplificată și particularizată în ceea ce privește evaluarea inconsistenței ipotezelor propuse. Pentru a preveni sau înlătura eventualele erori de analiză, în formularea concluziilor am folosit experimental programul specializat de analiză a ipotezelor concurente ACH 2.05 dezvoltat de către Palo Alto Research Center. În particular, am

[5] Ionel Nițu, „Metode și proceduri utilizabile în analiza de intelligence", în *Ars Analytica – Provocări și tendințe în analiza de intelligence*, George Cristian Maior și Ionel Nițu (coord.), București, Editura RAO, 2013, pp. 205-218.
[6] *Ibidem.*

utilizat metoda studiului de caz (sub forma unui cumul de analize SWOT) pentru a testa şi verifica experimental valoarea teoretic-aplicativă a rezultatelor de cercetare obținute de pe urma cercetării temei propuse.

Din rațiuni de echidistanță academică şi echilibru am avut în vedere respectarea următoarelor principii fundamentale de cercetare:

- ✓ principiul cauzalităţii și complementarității;
- ✓ principiul corespondenţei;
- ✓ principiul observabilităţii;

Practic, principiile enunțate mai sus au fost respectate îndeaproape datorită consultărilor permanente pe care le-am avut cu practicieni din domeniu ori din domenii conexe şi studiului extensiv al documentelor primare, secundare și terțiare precum: raporte ale agențiilor guvernamentale şi ale centrelor de analiză și studii strategice; teze de disertaţie și doctorat (din țară și din străinătate); lucrări ştiinţifice, reviste și articole tematice indexate în BDI; publicații online diverse; manuale şi standarde; documente guvernamentale declasificate; alte documentele declasificate ca urmare a unor scurgeri de informații; literatură „gri".

Capitolul I

Primul capitol este unul strict teoretic, în sensul că am urmărit pe parcursul acestuia să inventariez selectiv şi să analizez cele mai semnificative repere teoretice disponibile în literatura de specialitate care vizează securitatea și guvernanța spațiului cibernetic contemporan.

Fără a avea pretenția unei cronologii anume, am optat pentru prezentarea dialectică a cunoaşterii academice specifice, deoarece, foarte probabil, *liniile clasice de delimitare conceptuală* dintre curentele actuale de gândire specifice studiilor strategice *par a fi devenit tot mai flexibile și mai modelabile la nivel paradigmatic*[7]. În subsidiar, pe lângă contribuțiile propuse pentru îmbunătățirea lexiconului de specialitate, am urmărit la rândul meu să subliniez faptul că există premise destul de solide pentru integrarea studiului relațiilor internaționale în spațiul cibernetic în rândul axelor prioritare de cercetare, dezvoltare și inovare în studiile strategice contemporane. De asemenea, am identificat şi analizat cele mai semnificative argumente potrivit cărora securitatea cibernetică este vitală

[7] George Cristian Maior (coord.), *Un război al minții: Intelligence, servicii de informații și cunoaștere strategică în secolul XXI,* Bucureşti, Editura RAO, 2010, pp. 58-59.

funcționării și dezvoltării sustenabile a oricărei societăți și am arătat de ce spațiul cibernetic poate să constituie, în viziunea mea, un activ de importanță strategică. Nu în ultimul rând, pornind de la observația potrivit căreia spectrul amenințărilor la adresa securității globale și dezvoltării durabile se diversifică aproape exponențial odată cu creşterea gradului de cibernetizare, am arătat în ce condiții atacurile cibernetice pot fi asimilate utilizării forței (armate) și când pot produce daune materiale însemnate și/sau indirect pagube ori victime umane prin disruperea unor infrastructuri, sisteme ori terminale cibernetice critice.

Capitolul al II-lea

Pornind de la observația potrivit căreia spațiul ciberrnetic este un focar de insecuritate, dar și un important generator de oportunități, am încercat să verific în cadrul capitolului al doilea dacă dilema de securitate în spațiul cibernetic există și dacă aceasta este, într-adevăr, o formă particularizată a dilemei de securitate.

Ca atare, capitolul al doilea se concentrează pe studiul și fundamentarea teoretică a ceea ce am denumit generic „dilema strategică de securitate cibernetică” sau „dilema apărării cibernetice”, respectiv „dilema tactică de securitate cibernetică” sau „tentația suprasecurizării cibernetice pe timp de pace”. În ansamblu, am reușit să identific motivele pentru care consider dilema de securitate cibernetică drept o subspecie a dilemei de securitate și să arăt de ce aceasta apare în contextul luării deciziilor și optimizării posturii proprii de securitate și apărare în plan cibernetic. În particular, am identificat indicii consistente potrivit cărora nu neapărat inițierea și escaladarea dilemei de securitate cibernetică generează mai puțină predictibilitate, prosperitate și securitate în spațiul cibernetic, ci mai degrabă viceversa, adică un nivel inadecvat de securitate cibernetică – fie slabă securizare, fie suprasecurizare – cauzează cel mai probabil inițierea și escaladarea dilemei de securitate cibernetică. De fapt, potrivit uneia dintre concluziile preliminare ale capitolului al doilea, dilema de securitate cibernetică este mai degrabă un efect și mai puțin o cauză a slabei guvernanțe a spațiului cibernetic.

În contextul discuției privind ostilitatea cibernetică, nu am putut stabili cu exactitate dacă ierarhiile din spațiul cibernetic respectă îndeaproape configurația celor specifice altor medii strategice. În schimb, am validat teoriile potrivit cărora majoritatea actorilor internaționali își poate disputa liber ierarhiile de putere și securitate din spațiul cibernetic, fără ca cele specifice altor medii strategice să fie neapărat determinante în acest sens. Din

această perspectivă, am constatat că există suficiente motive potrivit cărora studiul geopoliticii spațiului cibernetic va căpăta o atenție mult mai semnificativă în ochii membrilor comunității științifice internaționale în perioada imediat următoare.

Cu privire la aplicarea reglementărilor dreptului internațional în spațiul cibernetic, am analizat care sunt cele mai semnificative impedimente în calea prevenirii și combaterii factorilor care pot contribui la inițierea și escaladarea unei spirale de insecuritate. Totuși, față de realitatea exprimată adesea de către majoritatea autorilor – nu neapărat inexactă, dar puțin probabilă – am subliniat principalele motive pentru care nu cred că asistăm acum unui vid legislativ în materie de reglementare a spațiul cibernetic, ci mai degrabă unui deficit de jurisprudență relevantă în domeniu. Nu în ultimul rând, am identificat motivele principale pentru care cred cu tărie că respectarea drepturilor și libertăților fundamentale ale utilizatorilor și non-combatanților ar trebui să primeze în fața celorlalte principii de drept internațional, mai ales atunci când se are în vedere angajarea legitimă a răspunderii și utilizarea justă a forței cibernetice sub auspiciile generării de daune colaterale, efecte tactice și operaționale predictibile, graduale și controlabile asupra terților și mediului strategic.

În sinteză, în capitolul al doilea am descris dilema de securitate cibernetică drept un joc tactic sau strategic de minimizare pe cât posibil a incertitudiniilor, în vederea menținerii avantajelor operaționale, tactice și strategice dobândite sau a maximizării acestora prin mijloace și operații cibernetice. Deși am constatat că instrumentele cibernetice pot avea un rol determinant în cadrul operațiilor specifice câmpului de luptă contemporan, din perspectiva unei dileme de securitate am argumentat că puterea acestora de a înlocui efectul distructiv al armamentelor convenționale prin intermediului celui distruptiv este încă limitată. Prin urmare, dacă tensiunile de inițializare determină escaladarea dilemei și în afara spațiul cibernetic, am concluzionat că este puțin probabil să mai putem vorbi de existența unei dileme de securitate cibernetică în adevăratul sens al cuvântului.

Capitolul al III-lea

Luând drept reper observațiile lui Robert Cooper, potrivit cărora secolul XXI *riscă să fie deturnat […] de anarhie și tehnologie*[8], în cadrul capitolului al treilea am verificat

[8] Robert Cooper, *Destrămarea națiunilor: Ordine și haos în secolul XXI*, București, Univers Enciclopedic, 2007, prefață, p. fn.

dacă buna guvernanță a spațiului cibernetic are într-adevăr o contribuție semnificativă la detensionarea și rezolvarea pașnică a dilemei de securitate cibernetică.

Pentru început, contrar așteptărilor inițiale, am constatat că rațiunile pentru care actorii spațiului cibernetic optează în direcția bunei guvernanțe nu sunt dintre cele mai diverse. În acest context, am observat că buna guvernanță în spațiului cibernetic nu se desprinde drept o preocupare primordială a actorilor competitivi ai spațiului cibernetic. De multe ori, atât în cazul actorilor statali, cât și a celor non-statali competitivi vorbim, de fapt, de o pseudo-bună guvernanță și conduită, în sensul că nu de puține ori mecanismele și angajamentele luate în direcția bunei guvernanțe sunt neglijate „atunci când este nevoie", deoarece ele se pot dovedi o frână în protejarea unor interese operaționale și tactice, mai mult sau mai puțin legitime și legale în materie de securitate cibernetică[9]. În schimb, în cazul eșaloanelor secunde de actori cibernetici am observat că dorința de aliniere (eng. *bandwagoning*) și nevoia de partajare a oportunităților, dar și a riscurilor și amenințărilor de securitate cibernetică fac ca nevoia de bună guvernanță să fie ceva mai pregnantă, din simplul motiv că aceasta poate să contribuie semnificativ la prevenirea și combaterea comportamentului hegemonic al primului eșalon de actori competitivi și poate oferi premise destul de solide și constructive de securizare rațională și reducere a presiunii asupra fiecărui subsistem de securitate și apărare cibernetică în parte.

Fără a avea pretenția de a fi găsit o soluție universal valabilă pentru dilema de securitate cibernetică, în capitolul al treilea am argumentat necesitatea implementării unui set de (cinci) principii fundamentale de bună guvernanță a spațiului cibernetic care pot să contribuie semnificativ la rezolvarea pașnică a dilemei de securitate cibernetică. În identificarea acestora am pornit de la observația personală potrivit căreia spațiul cibernetic nu duce neapărat lipsă de o reglementare mai strictă a conduitei actorilor internaționali, ci mai degrabă are nevoie de mai multă bună guvernanță pentru atingerea unui nivel optim de securitate, libertate și prosperitate, atât în rândul generatorilor, cât și în rândul consumatorilor de securitate cibernetică.

Prin urmare, pentru rezolvarea pașnică a dilemei de securitate cibernetică și evitarea coliziunii dintre nevoia de mai multă securitate, respectiv mai multe drepturi și libertăți în spațiul cibernetic am propus ca securitatea, libertatea și prosperitatea economică în mediul virtual să fie universal recunoscute drept drepturi fundamentale ale

[9] Cu precădere, mă refer la practicile de supraveghere la scară largă realizate prin instrumente de tip CYBERINT și SIGINT.

utilizatorilor în egală măsură. Pentru atingerea acestui deziderat, am argumentat (indirect) necesitatea adoptării la nivel internațional a „Cartei bunei guvernanțe în spațiul cibernetic", atât pentru ocrotirea perspectivelor de dezvoltare durabilă a spațiului cibernetic la nivel global, cât și pentru prevenirea inițializării și/sau a escaladării dilemei de securitate și protejarea drepturilor fundamentale ale utilizatorilor de bună credință.

Una dintre concluziile principale ale capitolului al treilea este că bună guvernanță contribuie la rezolvarea pașnică a dilemei de securitate cibernetică și optimul de guvernanță în spațiul cibernetic este atins când există o analogie ușor identificabilă între securitatea, libertatea, prosperitatea și perspectivele de dezvoltare durabilă ale spațiul cibernetic. Într-o primă fază, am sugerat că o posibilă soluție pentru atingerea acestui deziderat ar fi ca avertizarea timpurie sau colectarea de date tehnice și metadate în domeniul securității naționale să fie realizate preponderent de către entități public private anume desemnate – pe baza unor criterii de eligibilitate fundamentate pe nevoia pe integritate și transparență lărgită, caz în care cooperarea sinergică dintre public și privat este esențială, dar nu și suficientă în absența transparenței decizionale extinse. În acest sens, am argumentat că transparența extinsă în realizarea securității naționale în spațiul cibernetic poate oferi garanții valoroase privind utilizarea avertizării timpurii exclusiv în slujba protejării statului de drept, prosperității și dezvoltării durabile a spațiului cibernetic. Prin urmare, în plan secund, am ajuns la concluzia potrivit căreia cooperarea sinergică dintre actorii internaționali nu ar putea produce efecte benefice pentru securitatea și guvernanța spațiului cibernetic în condiții austere de trasparență decizională. Cât privește nevoia unui nivel optim de transparență în privința principiilor care guvernează activitatea de informații, am observat că asigurarea securității în spațiul cibernetic nu impune neapărat exigențe speciale de natură legală și procedurală, prin comparație cu alte medii strategice. În acest sens, am conncluzionat că exigențele de securitate națională și de clasificare a datelor și informațiilor nu sunt neapărat o frână în calea adoptăriile și implementării principiilor de bună guvernanță pe care le-am identificat. Prin urmare, am subliniat că libera circulație a datelor și informațiilor prin mijloace cibernetice, condiționată de reguli de bună conduită, n-ar trebuit privită, într-o primă fază, drept un impediment pentru securitatea națională și, totodată, pentru protejarea drepturilor utilizatorilor la viață privată, intimă și famială.

Nu în ultimul rând, am sugerat că implicarea activă și responsabilă a unui spectru cât mai larg de actori relevanți și capabili de a contribui cu succes la sporirea calității

guvernanței spațiului cibernetic poate determina, în multe dintre cazuri, creșterea nivelului general de securitate din mediul virtual și rezolvarea, cel puțin parțială, a dilemei. În ciuda eventualelor critici, mi-am permis să deschid dezbaterea academică în direcția studierii pe viitor a manierei în care actorii disidenți (sau cei cu potențial de disidență) față de securizarea rațională a spațiului cibernetic pot fi cooptați în cadrul cadrul mecanismelor și instrumentelor de asigurare a bunei guvernanțe a spațiului cibernetic. Pentru moment, am identificat unele tendințe potrivit cărora există motive să credem că avantajele nu sunt de neglijat, mai ales din perspectiva facilitării dialogului și creșterii nivelului de transparență decizională în realizarea securității spațiului cibernetic.

Pe scurt, în linia concluziilor capitolului al treilea, nu putem vorbi de bună guvernanță când între nivelurile de securitate, libertate și prosperitate din spațiul cibernetic există discrepanțe obiective. Totodată, buna guvernanță poate determina ca atitudinea ostilă la nivel cibernetic să fie cât se poate de predictibilă, spre a fi prevenită și, în ultimă instanță, combătută ca atare și poate avea are un rol esențial în prevenirea escaladării și rezolvarea pașnică a dilemei de securitate cibernetică.

Capitolul al IV-lea

Dat fiind faptul că am identificat suficiente argumente teoretice care să confirme consistența ridicată a ipotezei generale a tezei, în cadrul capitolului al patrulea am realizat un studiu de caz care să exemplifice practic și să individualizeze relația de interdependență dintre nivelul de securitate cibernetică al României și calitatea guvernanței spațiului cibernetic autohton. Am ales să analizez cazul României, deoarece îl consider un exemplu reprezentativ pentru verificarea teoretic-aplicativă a rezultatelor obținute în urma cercetării temei propuse. De asemenea, am dorit să atrag atenția asupra faptului că cercetarea interdependențelor dintre nivelul de securitate cibernetică al României și calitatea guvernanței spațiului cibernetic românesc este cvasi-absentă în spațiul academic autohton al relațiilor internaționale și studiilor de securitate.

Pe scurt, am obținut indicii semnificative potrivit cărora „tiparele tradiționale” de guvernanță a securității specifice altor medii strategice și altor categorii de provocări pot fi dăunătoare dezvoltării durabile a spațiului cibernetic. Pentru început, cel puțin în materie de transparență, cooperare și securizare, am observat că „tiparele tradiționale” de guvernanță a securității au dovedit o eficiență discutabilă în timp și au sporit semnificativ reticența și scepticismul utilizatorilor români cu privire la nevoia concomitentă de

securitate națională, libertate individuală și dezvoltare durabilă a spațiului cibernetic, uneori chiar până la atingerea unor limite de auto-radicalizare.

Contrar așteptărilor inițiale, discrepanțele identificate în privința securității și guvernanței spațiului cibernetic autohton nu sunt foarte alarmante. Cu toate acestea, am constatat că progresele făcute de România în ultimii ani de la accederea în cadrul organizațiilor transatlantice sunt într-adevăr semnificative și salutare, dar sunt încă insuficiente pentru atingerea optimului de securitate, libertate și prosperitate în spațiul cibernetic autohton.

Cât privește securitatea spațiului cibernetic național, am observat că România nu face notă discordantă față de alte state democratice din spațiul european. În acest sens, am apreciat în mod pozitiv faptul că România nu s-a angrenat recent în derularea unor programe clandestine de supraveghere în masă a cetățenilor și nici în jocul periculos al unor spirale de securitate cibernetică, ba chiar a contribuit la detensionarea unora dintre acestea pe plan internațional.

Sumarul concluziilor

În ansamblu, teza de față oferă indicii solide potrivit cărora între nivelul de securitate și calitatea guvernanței spațiului cibernetic contemporan există o strânsă relație de interdependență. Contrar scepticismului inițial, se confirmă ipoteza generală a tezei și faptul că dilema de securitate este prezentă într-o formă particularizată în spațiul cibernetic. De asemenea, în urma cercetării întreprinse nu se atestă ipoteza potrivit căreia buna guvernanță produce efecte limitate și greu măsurabile în direcția rezolvării pașnice a dilemei și dezvoltării durabile a spațiului cibernetic.

Cuvinte cheie: securitate cibernetică, bună guvernanță, dilema securității cibernetice, spațiu cibernetic, amenințare cibernetică