UNIVERSITATEA BABEȘ-BOLYAI
FACULTATEA DE ISTORIE ȘI FILOSOFIE
ȘCOALA DOCTORALĂ „*RELAȚII INTERNAȚIONALE ȘI STUDII DE SECURITATE*”

GUVERNANȚA SECURITĂȚII NAȚIONALE: MANAGEMENTUL SECURITĂȚII SPAȚIULUI VIRTUAL ÎNTRE REALISM ȘI SUPRANAȚIONALISM

****

REZUMAT TEZĂ DE DOCTORAT

Conducător de doctorat:
Prof. univ. dr. ADRIAN-LIVIU IVAN

Student-doctorand
George-Marius ȘINCA

Cluj-Napoca
2021

CUPRINS

ARGUMENT 1
OBIECTIVE, IPOTEZE ȘI SCOP 9
METODOLOGIA ȘI STRATEGIA DE CERCETARE 13
MOTIVAȚIA ALEGERII TEMEI DE CERCETARE 18
CUVINTE CHEIE 20
GLOSAR DE ABREVIERI ȘI ACRONIME 23
CAPITOLUL I. INTRODUCERE 29
CAPITOLUL II. MANAGEMENTUL INFORMAȚIILOR ELECTRONICE VEHICULATE ÎN MEDIUL VIRTUAL 42
II.1. Organizația sursă generatoare de securitate a informației 45
II.1.1. Analiza organizației 46
II.2. Informația în organizație 51
II.2.1. Forma și conținutul informației utile 53
II.2.2. Valoarea informației 55
II.2.3. Moduri și canalele de comunicare a informației 57
II.2.4. Protejarea informației vehiculate în mediul virtual 59
II.2.5. Managementul informației electronice în organizație 62
II.3. Condiția informației vitale 64
II.3.1. Clasificarea informației 66
II.3.2. Cadru normativ și legislativ românesc privind prelucrarea datelor și informațiilor 69
II.3.3. Criterii generale ale clasificării informațiilor în organizație 71
II.3.4. Sistemul decizional bazat pe sisteme informaționale. 72
II.3.5. Surse generatoare de insecuritate informațională 75
II.4. Managementul riscului în organizație 77
II.4.1. Elita, actorul de securitate și decidentul 78
II.4.2. Riscul cibernetic - Cadru de analiză 82
II.4.3. Modelul cibernetic al managementului riscului 87
II.4.4. Minimizarea Riscului 88
II.4.5. Predicție Și Previziune - Riscurile Securității Cibernetice în 2019 90
II.4.6. Capacități necesare unui management al riscului competitiv în organizațiile digitalizate 97
II.4.7. Aplicarea și implementarea politicilor de securitate asupra sistemelor informaționale în mediile virtuale 100
II.5. Teoria schimbărilor 105
Concluzii preliminare 109

CAPITOLUL III. GUVERNANȚA SPAȚIULUI VIRTUAL ÎN CONCEPȚIA REALISMULUI ȘI SUPRANAȚIONALISMULUI 112
III.1. Implicațiile arealului cibernetic asupra relațiilor internaționale în viziunea teoriilor realismului. 112
III.1.1. Raportul forțelor din mediul internațional în contextul realismului 112
III.1.2. Școala de gândire realistă 114
III.1.3. Echilibrul puterilor 116
III.1.4. Puterea cibernetică în contextul realismului contemporan 117
III.1.5. Neorealismul și distribuția puterii 122
III.1.6. Punctele tari și puncte slabe ale realismului 124
III.1.7. Realismul aplicat: securitatea cibernetică 125
III.1.8. Conceptul de anarhie în contextul securității cibernetice 130
III.1.9. Cursa înarmărilor cibernetice 132
III.1.10. Analiza „spiralei" de (in)securitate cibernetică în context contemporan 135
III.1.11. Teoretizarea balanței ofensiv-defensiv în sectorul cibernetic 142
III.2. Supranaționalism 144
III.2.1. Supranaționalism și securitate cibernetică 149
III.2.2. Istoricul atacurilor cibernetice 151
III.2.3. Guvernare supranațională elitistă asupra sectorului de securitate cibernetic 158
III.2.4. Teoria elitelor și decidentul în actul de guvernare a spațiului cibernetic 159
III.2.5. Actorul de securitate 160
III.2.6. Organigrama sectoarelor securității cibernetice din spațiului cibernetic 161
Concluzii preliminare 165

CAPITOLUL IV. DIPLOMAȚIA ÎN SPAȚIULUI CIBERNETIC 168
IV.1. „România Digitală" o nouă perspectivă 168
IV.2. Diplomația digitală și Diplomația cibernetică 171
IV.2.1. Tehnologia „Big Data" și Diplomația digitală 175
IV.2.2. Tehnologii de comunicare și monitorizare 176
IV.2.3. Instrumentarul diplomatic digital 177
IV.2.4. Rețelele diplomatice - interdependența real/virtual 180
IV.2.5. Culegerea de informații și managementul cunoașterii 182
IV.3. Securitate diplomatică și guvernare prin reziliență cibernetică 191
IV.3.1. Evoluția rezilienței cibernetice ca și efecte ale politicilor de securitate diplomatică 192
IV.3.2. Provocările Agendei UE în contextul securității cibernetice 194
IV.3.3. Programul Europa digitală un nou orizont o nouă abordare 197
IV.3.4. Paradigma diplomației securității cibernetice 199
Concluzii preliminare 201

CAPITOLUL V. INFLUENȚE ALE UNEI POLITICI UNITARE EUROPENE PRIVIND SECURITATEA INFORMAȚIEI ELECTRONICE ÎN ACTUALA STARE GEOPOLITICĂ GLOBALĂ 206
V.1. Abordarea de politică externă a României 206
V.1.1. Contextul securității prin reziliență cibernetică 210
V.2. Problematica securității cibernetice din perspectiva organismelor internaționale şi implicarea României ca membru al acestora 216
V.2.1. Uniunea Europeană - UE 216
V.2.2. Organizația Tratatului Atlanticului de Nord - NATO 217
V.2.3. CONSILIUL EUROPEI - CoE 222
V.2.4. Organizația pentru Securitate și Cooperare în Europa - OSCE 224
V.3.Modele internaționale și organisme europene cu atribuții în domeniul securității cibernetice 226
V.4. Modele și organisme naționale cu atribuții în domeniul securității cibernetice 235
V.5. Strategii de securitate cibernetică în zona UE în raport cu restul lumii 238
V.5.1. Cooperarea comunitară și internațională. 238
Concluzii preliminare 245

CAPITOLUL VI. STUDIU DE CAZ - CULTURA DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA 247
VI.1. Analiza statistică.
VI.2. Identificarea necesității de conștientizare și protecție a societății contemporane în raport cu provocările cibernetice actuale și viitoare 249 249
VI.3. Chestionarul de evaluare a nivelului culturii de securitate cibernetică în România 250
VI.4. Plan analitic 252
VI.4.1. Indici Descriptivi ai Eșantionului 256
VI.4.2. Analiza Competențelor Digitale ale Utilizatorilor Români 257
VI.5. Analiza culturii de securitate informațională a utilizatorilor din România 267
Concluzii preliminare 278

CONSIDERAȚII FINALE 280
Limitări și direcții viitoare de cercetare 280
Precizări referitoare la contribuțiile personale 281

CONCLUZII 284

BIBLIOGRAFIE 289
CĂRȚI (inclusiv ediții electronice) 289
ARTICOLE ȘTIINȚIFICE ȘI CAPITOLE ÎN CĂRȚI (inclusiv ediții electronice) 293
STUDII ȘI PUBLICAȚII ALE INSTITUȚIILOR NAȚIONALE / INTERNAȚIONALE 299
LEGISLAȚIE 304

ALTE STUDII ȘI PUBLICAȚII 306
SURSE ELECTRONICE 314

LISTA FIGURILOR 318

ANEXE 320
ANEXA NR.1. CHESTIONAR „CULTURA DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA” 320
ANEXA NR.2. MACHETA CENTRALIZATOARE PENTRU CHESTIONARUL „CULTURA DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA” 322
ANEXA NR.3 ORGANIGRAMA DOMENIILOR GUVERNANȚEI SECURITĂȚII CIBERNETICE 324

CUVINTE CHEIE:

CULTURA DE SECURITATE CIBERNETICĂ, REALISM ŞI SUPRANAȚIONALISM, GUVERNANȚA SECURITĂȚII CIBERNETICE, DIPLOMAȚIA SPAȚIULUI CIBERNETIC, REZILIENȚA CIBERNETICĂ, BUNA GUVERNANȚĂ CIBERNETICĂ

În actualul contextul de securitate global, efectele globalizării, noile contexte geostrategice, geopolitice precum și cele ale transformării sau hibridizării mecanismelor financiare și economice - *care reprezintă rezultate ale exploziei informaționale și hiperdezvoltării tehnologice din domeniul tehnologiei informației și comunicațiilor*-, apar noi paradigme care adesea răstoarnă teorii sau schimbă traiectoria evolutivă a domeniilor de referință precum cel economic, știința politică (*națională și internațională*) și a relațiilor internaționale. Așadar se dezvoltă noi subdomenii în sectorul diplomatic (*diplomația digitală și diplomația cibernetică*) care schimbă paradigma securității naționale și internaționale – odată cu aceste schimbări apar elemente care duc la o reconceptualizare a sectorului de intelligence. Asistăm așadar la o transformare naturală a tuturor domeniilor conectate existente și conectate la domeniul cibernetic, în toate sectoarele societății contemporane.

Această paradigmă globală generează o dinamică internațională complexă care impune o analiză permanentă a efectelor înregistrate la nivel internațional, supranațional și național. Pornind de la acest fenomen și completând exemple de caz concludente precum sunt elementele constitutive ale incidentelor de securitate cibernetică națională - *Estonia*[1] *(2007)* – și desigur ale semnalmentelor atacurilor cibernetice tot mai dese direcționate către sectorului privat sau guvernamental din Europa și alte state cu o poziție ofensivă sau defensivă, am căutat să identific măsurile și contramăsurile luate de state, federații sau uniuni de state pentru a limita aceste atacuri și pentru a obține o viziune cât mai clară asupra nevoii de asigurare a unui grad de reziliență potrivit cu gradul de risc asociat fiecărui caz în parte.

Lucrarea de față se prezintă ca o perspectivă explorativă și nu neapărat exhaustivă privind protejarea resurselor și valorilor naționale în spiritul conceptului supranațional. Un al doilea element care mi-a atras atenția în perioada alocată analizei atacurilor cibernetice a fost factorul de vulnerabilitate dat de lipsa unei culturi de securitate a întregii populații și un vid de cunoaștere a securității în mediul cibernetic, atât în rândul decidenților cât și a sectorului diplomatic general.

Obiectivul general al tezei constă în cercetarea raportului dintre elemente precum guvernanța securității naționale, reziliența, diplomația, jurisdicția și buna guvernare a spațiului cibernetic în vederea confirmării sau infirmării tipologiilor și noilor sisteme informaționale din spațiul virtual precum și aportul adus de acestea în balanța guvernanței spațiului virtual între realism și supranaționalism.

Concret s-au formulat trei obiective secundare de cercetare pentru *identificarea interdependenței dintre guvernanța sectorului cibernetic și securitatea națională*, *identificarea*

[1] Rain Ottis, CCDCOE, „*Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*”, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2018, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, accesat astăzi 20.12.2019.

determinantelor guvernanței securității naționale rezultate în urma adaptării sistemului de management al securității informației în spațiul virtual și *studiul paradigmei guvernanței securității informației în spațiul virtual în asentimentul realismului și a supranaționalismului*.

Scopul activităților științifice desfășurate în perioada de documentare și în etapa de conceptualizare și scriere a lucrării, a fost cel de a identifica și trata o nouă abordare de asigurare a securității naționale prin crearea de conexiuni și relații logice și interdependente între concepte precum: *organizația, managementul informației, arealul cibernetic, supranaționalism / realism, diplomația, cultura de securitate cibernetică și securitatea națională*.

Ipoteza generală de cercetare, vine în vederea atingerii obiectivelor propuse, unde s-a considerat că buna guvernanță în spațiul cibernetic poate să contribuie la soluționarea paradigmei și dilemei de securitate în acest nou areal. Teoretizând prin resursele metodelor de cercetare științifice abordate și aplicate voi putea evidenția dacă există o relație de interdependență între practicile de guvernare a sistemelor naționale de securitate a informației și cele supranaționale cât și a raporturilor dintre acestea. Ipoteza de lucru a fost testată prin intermediul unui studiu de caz, în ultimul capitol al Tezei.

Metodologia de cercetare care stă la baza conceptului prezentei lucrări este una bazată pe studiul inductiv al pachetului legislativ național, european și internațional cu privire la securitatea cibernetică, studiul literaturii de specialitate confirmat de rezultatele exhaustive a studiului de caz privind cultura de securitate cibernetică a populației rezidente din România. Fundamentată în existența „binomului de cercetare" general-specific aplicată pe parcursul lucrării, și-a propus generarea de concluzii generale privind guvernanța securității naționale prin demistificarea managementul securității spațiului virtual în perspectiva realismului și supranaționalismului. Metodologic, concluziile preliminare ale primelor cinci capitole coroborate cu întregul capitol șase, sunt rezultatul unei analize granulare, cantitative și calitative. Printre metodele principale de analiză a datelor și evaluare a variabilelor de cercetare a fost folosită *metoda ipotezelor concurente* (*utilizată în varianta simplificată de evaluare a inconsistenței ipotezelor*). *Metoda studiului de caz* în prezenta lucrare este edificată prin utilizarea metodelor de verificare încrucișată, pentru a testa și verifica experimental valoarea teoretic-aplicativă a rezultatelor de cercetare obținute de pe urma cercetării temei propuse. În cadrul lucrării de față, studiul de caz este raportat la un eșantion final de 5.446 persoane din totalul de ~7.600 chestionare aplicate, care reprezintă ~0.03% din 19.644.350[2] persoane care este numărul estimat al populației rezidente în România anului 2017.

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

[2] Breviar Statistic, România în cifre, Institutul Național de Statistică, INS 2018, p.9, http://www.insse.ro/cms/sites/default/files/field/publicatii/romania_in_cifre_breviar_statistic_1.pdf, accesat astăzi 01.04.2019.

- *principiul explorării și al descrierii fenomenelor* – lucrarea s-a axat pe un studiu explorativ anume pe descrierea și explorarea relațiilor dintre fenomene;
- *principiul corespondenței* – rezultatele au fost bazate pe o permanentă racordare la cunoașterea academică și științifică contemporană;
- *principiul observabilității* – pe parcursul lucrării s-au expus rațional argumente ce pot fi verificabile cel puțin la nivel cognitiv.
  - *aplicarea de interviuri* bazate pe rezultatele chestionarelor obținute în cursul cercetării;
  - *consultarea* unor practicieni din domeniu sau din domenii conexe –în cadru formal și informal;
  - *studierea documentelor primare, secundare și terțiare;*

Cele mai importante instrumente de lucru în procesul de cercetare științifică au fost următoarele:

- The Brain, R, IBM SPSS Statistics for Windows, ACH 2.05, IBM i2 Analyst's Notebook, MsOffice 365;
- Mendeley, O'Reilly, Safari, Archive.org, Statista, Klarmedia, IEEE Xplore Digital Library.

Teza este *structurată* în două mari părți, respectiv în șase capitole. Prima parte este compusă din argumentul lucrării care reprezintă desigur, o perspectivă empirică asupra conținutului și care expune sumar informația din perspectiva organizațională ce va fi ulterior în primul capitol analizată într-un mod inductiv și într-o manieră introspectă. În primele cinci capitole toate referirile la informație sunt finalmente orientate spre tratarea acesteia și asupra efectele acesteia, în forma sa digitală în context de securitate contemporan. Partea a doua, este reprezentată de al cincilea capitol care este și cel ultim unde se demonstrează relația dintre cultura de securitate a individului care este în același timp și utilizator de terminal conectat în arealul cibernetic, cu securitatea în toate formele sale dintre care enumerăm specific, securitatea umană și securitatea cibernetică în calitate de subdomeniu al securității naționale. De menționat este faptul că sursele generatoare de insecuritate, precum sunt comunitățile sau societățile digitale care nu au un bagaj de cunoștințe sau o cultură generală de securitate sunt fără de tăgadă un factor de insecuritate adus la conceptul de securitate națională. Desigur, ultimul capitol devine prin extrapolare un nou domeniu de studiu pentru autor și de cercetare academică pentru comunitatea științifică, dar cu toate acestea nu este tratat ca un studiu separat ce mai degrabă orientat pe obținerea de date cantitative și calitative care să fundamenteze și să valideze sau să invalideze ipotezele de cercetare din prima parte a lucrării. Fiind vorba despre o cercetare explorativă, pe parcursul științific și bazat pe un spirit critic pozitiv, s-au făcut remarci privind caracterul dinamic al lucrării, considerându-se că cercetarea merge de la general la specific și contextual de la specific la general dar care în final duce la o poziționare obiectivă a unor concluzii privind tema aleasă. Fiecare capitol are secțiuni și subsecțiuni și prezintă elemente care contribuie la testarea ipotezei noastre de cercetare.

CAPITOLUL I

INTRODUCERE

Într-un mod natural, bazată pe experiența autorului în domeniu, a fost identificată o nevoie absolută de a cerceta noile sectoare ale securității și guvernanței spațiului cibernetic. Aceste domenii reprezintă o arie prioritară de cercetare și inovare pentru România și pentru UE. Din perspectiva dezvoltării durabile a spațiului cibernetic se identifică o lipsă a cercetării securității cibernetice, în contextul relațiilor internaționale. Numărul cercetătorilor români dedicați studiului și identificării de soluții specifice în domeniul relațiilor internaționale și studiilor de securitate și de nișă în domeniul cibernetic, fapt care duce la o scădere a capacității sistemului de apărare și securitate contemporan românesc precum și la o privare față de resursele de securitate strategice, atât de necesare azi unui stat cu ambiții euroatlantice considerabile cel puțin în domeniul securității cibernetice și aflat pentru o scurtă perioadă la conducerea Uniunii Europene.

O listă obiectivă a factorilor ce au dus la alegerea acestui studiu este dată nu în ultimul rând de ipoteza securității și guvernanței spațiului cibernetic european identificat ca și subiect prioritar pe agenda Comunității Europene și internaționale, unde realizările științifice ale autorilor români sunt în general relativ scăzute motiv pentru care autorul a fost nevoit să studieze și să analizeze lucrările autorilor consacrați în acest domeniu din mediul internațional. Un factor limitativ, autoimpus, în ceea ce privește studierea și citarea surselor a fost dat de dorința de separare a argumentelor aparținătoare științelor relațiilor internaționale și studiilor de securitate față de argumentele de drept și jurisprudență aduse de științele juridice de drept național și internațional. Motivația acestei alegeri a fost dată de necesitatea de raportare și concentrare a procesului de cercetare pe domeniul de studiu al autorului, anume cel al relațiilor internaționale și studiilor europene.

Conceptul de „securitate națională”. Pe parcursul anilor, în contextul diferitelor arii de cercetare, s-au aliniat în cadrul nenumăratelor cercuri științifice, dezbateri teoretice mai mult sau mai puțin fundamentate în concret. Conceptul de securitate își păstrează în continuare caracterul ambiguu dar care, în procesul de cercetare a relațiilor internaționale este uzitat adesea ca pretext, scuză ori justificare pentru diverselor obiective sau rezultate politice sau strategice. Cât despre definirea termenului de „securitate națională”, acesta suferă adesea reinterpretări date de interpretarea în spiritul legii a unui set de documente oficiale care sunt actualizate anual sau la o frecvență de cinci ani - aici făcându-se referire directă la strategiile naționale ori sectoriale în domeniul apărării, securității naționale, a planurilor de priorități emise de C.S.A.T. sau C.N.I.

Pe parcursul documentării și chiar înaintea procesului de cercetare propriu zis, s-a ridicat întrebarea dacă evaluarea nivelului de securitate cibernetică a populației reflectă într-o măsură suficient de mare vreun aspect al securității naționale. Considerând că, prezumția de nevinovăție și factorul uman - de încredere - a stat la bazele proiectării și consolidării spațiul cibernetic, se consideră această evaluare absolut necesară. Unul dintre foștii consilieri prezidențiali pe probleme de securitate națională a expus următoarele, „*în politica de securitate naţională trebuie să gestionezi acele evoluții, acele probleme care pot genera rapid crize de securitate națională, care în decurs de zile sau chiar ore, îți pun în pericol integritatea teritorială, suveranitatea, siguranța unui mare număr de oameni.*” – din această afirmație puternic fundamentată în fapte,

acțiuni politice și istorie europeană înțelegem că arealul cibernetic este extrem de important în asigurarea unui grad ridicat de securitate națională.

CAPITOLUL II

MANAGEMENTUL INFORMAȚIILOR VEHICULATE ÎN MEDIUL ELECTRONIC

În contextul tezei, ***managementul informației*** este rezultatul gestionării raportului între *identificarea informației vitale – centralizarea - analiza și sinteza în vederea clasificării și valorificării acesteia* pentru o livrare către factorul de decizie și utilizarea acesteia într-un mod eficient. Ținând cont de faptul că gradul de performanță al guvernanței unui mediu, chiar și a celui virtual, se rapor0tează la calitatea, veridicitatea și momentul livrării informației – așadar putem spune în centrul guvernanței sistemelor informaționale și a întregului areal cibernetic stă informația. Fie că vorbim de sectorul militar, cel de guvernământ sau cel civil, indiferent în ce scop este utilizată, informația preia un atribut atât tactic cât și operațional[3] considerabil.

Informația, în orice formă s-ar afla este necesar a fi identificată, observată, extrasă, analizată și prelucrată pentru a-i putea atribui o valoare în vederea folosirii acesteia, de aceea relevanța managementului informațiilor din mediile electronice în contextul domeniului de analiză al studiilor de securitate este unul vital atât pentru beneficiar cât și pentru decidenții corporativi, industriali, guvernamentali, politici, diplomați, înalți guvernanți sau pentru orice actor statal sau non statal ale căror decizii se învârt în jurul acestor informații[4].

Nevoia unui ***sistem informațional*** bine structurat se face simțită în cadrul organizațiilor unde informația este nu doar sensibilă, atributul său dinamic face ca o informație care nu se află în format electronic să fie mult mai greu de multiplicat, gestionat sau arhivat; pe de altă parte alterarea acestora este oricum inevitabilă pe când un document în format electronic (*text, audio, video*) gestionat conform normelor minime de securitate nu este la fel de vulnerabil la aceste riscuri. Cu toate acestea trebuie menționat că volumul informației crește exponențial și cu progresul tehnologic, creșterea populației și a surselor generatoare de informații, drept urmare informația are un alt ritm de generare, propagare și diseminare, motiv pentru care trebuie să acordăm o atenție sporită verificării acesteia fără a-i atinge unicitatea și factorul generator.

Întrebările din a căror răspunsuri vor rezulta eventuale soluții la situațiile stringente ale sistemului organizațional contemporan în ceea ce privește managementul informației sunt următoarele:

- *Ce reprezintă din punct de vedere informațional organizația?*
- *Care sunt din perspectiva managementului riscului, vulnerabilitățile, variabilele de risc și implicațiile la care sunt supuse sisteme informaționale asupra și în cadrul organizației?*
- *Putem vorbi despre nevoia unei reorganizări de securitate și management al informației într-o organizație?*

Organizația reprezintă o entitate dominantă în toate sectoarele societății, ca formă prin care acțiunea colectivă este combinată cu abilitățile individuale agregate, pentru realizarea majorității

---

[3] Aurelia Peru-Balan, Vitalina Bahneanu, MOLDOSCOPIE, Nr.1, Vol. LXXX, *Războiul informațional, Propaganda, Fake-News: Controlul asupra percepției publice*, Chișinău, 2018, pp.129-131.

[4] Teodor Frunzeti, Cristian Bărbulescu, Academia Oamenilor de Știință din România, Cultura de securitate și reziliența națională la amenințările hibride , *Reziliența național la amenințările hibride și cultura de securitate. Un cadru de analiză*., p.4, http://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf, accesat astăzi 23.07.2019.

categoriilor de bunuri economice[5]. Astfel pusă problema definiției, se poate afirma că „*o organizație este un grup de oameni care acționează într-un mod corelat pentru atingerea unui scop comun*". În contextul sustenabilității și guvernanței sistemului de management, ne regăsim într-un sector dinamic, sensibil la modificări, contextual unele organizaţii apar, altele dispar, unele fuzionează, altele îşi diminuează ponderea pe când altele cresc rapid, iar altele luptă să supravieţuiască. Au apărut organizaţiile virtuale care sunt constituite sub forma reţelelor de comunicare rapidă intermediată de noile tehnologii informatice. Dar chiar și așa datorită surselor generatoare de diversitate, timpul de supravieţuire a unei organizații într-o formă, mărime și profil s-a redus considerabil, după unele estimări la 5-10 ani[6].

Caracterul informației trebuie tratat în conformitate cu dependența acesteia de ***factorul temporar*** precum: *planificare, actualitate, frecvența și moment de timp* în materie de ***formă a informației*** ca și *claritatea, granularitatea, secvențialitatea, modalitatea de expunere și suportul pe care informația poate fi livrată*. În materie de ***conținut***, informația trebuie să se remarce prin *acurateţe, relevanță, completitudine*: *conciziune, obiectivism* și *performanță*[7].

Valoarea informației, a datelor, precum şi costurile şi beneficiile rezultate în urma prelucrării acesteia devin din ce în ce mai mult transnaționale. Informația reprezintă în orice domeniu de activitate – *academic, cercetare , inovare, industrie, administrație locală sau centrală, guvernământ, legislativ, securitate națională , ș.a.m.d*. - o resursă incontestabilă de o putere cu un înalt impact decizional, cu o valoare adesea incontestabilă și inestimabilă, completată adesea de sisteme de stocare şi procesare care poate furniza un cert avantaj în gestionarea evenimentelor sensibile sau conflictelor închise sau deschise.

Din analiza ***managementului riscului în organizațiile*** contemporane în raport cu populația rezidentă din România și activă în câmpul muncii, se poate observa o cultură de securitate cibernetică lacunară, motiv pentru care incidentele de securitate și infracțiunile informatice sunt atât de des întâlnite și au un impact atât de mare atât asupra indivizilor cât și asupra organizațiilor. Pregătirea continuă pe specificul protecției informației și apărării împotriva factorilor de risc este de necontestat printre primele nevoi ale organizației. Calitatea și existența unui cult a elitelor de securitate a informației în orice organizație este imperios necesară pentru a acoperi cel al doilea nivel de nevoie fundamentală a omului anume siguranța și securitatea, aceasta fiind în zilele de azi, în mare parte reprezentată de arealul cibernetic. Crearea de relații interumane prin comunicare, consult și colaborare între zona de management și cea de execuție în organizație crește nivelul de încredere al sistemului de securitate. Neacoperirea nevoilor logistice primare ale sistemului de securitate (*echipamente, audit, management, cercetare, experți în studii de securitate și ingineri de securitate*) duce negreșit la un colaps informațional. Datorită permanentelor evoluții ale lumii cibernetice pentru o mai bună guvernare este nevoie de o permanentă actualizare a cadrului legal atât național cât și internațional.

---

[5] Vlăsceanu Mihaela, *Organizatii și comportament organizational,* Ed. Polirom, Iași, 2003;

[6] Mihaela Vlăsceanu, *„Organizația: proiectare și schimbare – Introducere în comportamentul organizațional"*, Ed. Comunicare.ro, București, 2005, pp.60-61.

[7] Ofelia Hobincu, „*Caracteristicile informației, martie 2008",* http://www.perfect-service.ro/intelinet/2008/martie/intel%28i%29net.php?legatura=2, accesat astăzi 19.06.2016.

Bazată pe nevoia unei bune guvernanțe a sistemului informațional și în mod deosebit a informației, pentru obținerea celei mai eficiente și bune decizii - cu atât mai mult în contextul securității naționale – observăm că nu este loc de erori sau de asumare a unor greșeli, fie ele și din partea sectorului guvernamental. Și totuși fie că vorbim de atâtea națiuni, federații, uniuni sau alte forme supranaționale, trebuie să ținem cont că orice stat are nevoie să fie suveran sau suveran în cadrul alianței. Resursa primară cu care se lucrează, deocamdată, este cea umană, motiv pentru care informația poate fi ușor alterată (direct sau indirect). Datorată limitărilor resursei umane, din lipsa capacității de procesare umană a acesteia, s-au dezvoltat noi sisteme inteligente de prelucrare a acestora - regăsim în această sferă de interes și cercetare:

- automatisme și mecanisme bazate pe inteligența artificială cu capacități de procesare extraordinare, cărora le lipsește doar rațiunea și emoția umană;
- sisteme de învățare automată bazată pe procese anterioare (succes/eșec) numite inteligență artificială și sub-dimensiuni ale acesteia precum este conceptul de „*machine learning*[89]” sau „*deep learning*[10]”;
- sisteme consacrate cu ajutorul căror funcții de procesare și predicție se pot obține cele mai bune rezultate pentru managementul și progresul organizațional, care de fiecare date se cuantifică în resurse financiare.

Politicile de securitate capătă forme diferite, în funcție de „*bunul*” care are nevoie de a fi securizat, valoarea efectivă a acestuia, „*puterea de cumpărare*”, proprietarul și beneficiarul informației, interesele și efectele diseminării acesteia în anumite medii de interes, menționând că de obicei efectele se măsoară în dimensiuni economice, financiare sau dimensiuni ale puterii.

Elementele de noutate apărute în acest capitol sunt date de expunerea nevoii de conceptualizare a unui nou cadru de analiză și guvernare a resurselor materiale și cibernetice pentru o bună guvernanță a spațiului cibernetic cu ajutorul elitelor formate pe sectoarele de nișă noi apărute. Pentru a întări această viziune, consider aplicabilă teoria schimbării în primul rând în zona de cercetare a relațiilor internaționale raportată la acest nou areal virtual apărut și a cărui efecte în zona de guvernanță a sectorului informațional nu pot fi ignorate.

Teoria schimbării este un element cheie în progresul tuturor științelor, motiv pentru care aceasta trebuie adaptată și noului context informațional digital contemporan. Teoria schimbării și arealul cibernetic sunt două dintre cele mai importante elemente constitutive ale noii ere – fie că este vorba de cuantică sau ceva mai mult de atât.

Relațiile Internaționale este unul dintre domeniile în care Teoria schimbării este aplicată în două forme, anume într-o formă controlată bazată pe interdependențe sau într-o formă impusă, fie supranațional fie bazată pe contextul internațional ori global.

---

[8] Machine learning: *termen în limba engleză tradus în limba română ca și sistem informatic de inteligență artificială pentru învățare automată*.

[9] Léon Bottou, Frank E. Curtis, Jorge Nocedal, Vol. 60, Nr. 2, „*Optimization Methods for Large-Scale Machine Learning”*, https://doi.org/10.1137/16M1080173, SIAM Review, 2018, pp. 223-311.

[10] Deep Learning: *concept AI bazat pe „machine learning” definit prin introducerea unei mari cantități de date într-un sistem computerizat, prin intermediul unor rețele neuronale care are capacitatea de a analiza informațiile mult mai în detaliu.*

În această ordine de idei, se confirmă faptul că buna guvernanță are la bază aplicabilitatea teoriei schimbării într-un context supranațional cu păstrarea suveranității statelor și alinierea la viziunea de grup. Această teorie definește chiar și balanța *realism – supranaționalism*.

CAPITOLUL III
GUVERNANȚA SPAȚIULUI VIRTUAL ÎN CONCEPTUL REALISMULUI ȘI SUPRANAȚIONALISMULUI

În actualul context geopolitic și de securitate internațional, influențat de arealul cibernetic care este lipsit de granițe tangibile, realismul politic capătă cu totul altă definiție - paradigma realismului este parțial schimbată. Totuși, pentru a fi precaut cu privire la afirmații de o asemenea magnitudine, consider că este nevoie de o interpretare a realismului, ținându-se cont de influențele progresului și inovației tehnologiei contemporane respectiv de paradigma securității cibernetice în contextul guvernării la nivel național și federal ori chiar global.

Pentru a putea analiza realismul în contextul guvernanței relațiilor internaționale, se identifică necesitatea de a înțelege conceptul realismului ca termen definitoriu teoriei ce îl susține. Așadar cunoscând faptul că relațiile internaționale reprezintă și studiul inductiv al interacțiunilor și raportărilor actorilor statali la cei non-statali, considerăm realismul politic ca fiind una dintre principalele teorii care încearcă să explice relațiile dintre acestea, adică dintre state. În încercarea de a explica relațiile internaționale dintre state în termeni de putere, realismul politic aduce argumente concretizate și adaptate pe capacitatea statelor de autoguvernare.

Termeni de putere în contextul realismului

În contextul relațiilor internaționale termenul de puterea este, în principiu reprezentat de capacitatea unui stat de a convinge un alt stat în luarea de decizii pe care în mod obișnuit și natural acesta nu l-ar lua sau puterea unui stat de a opri acțiunile interne sau externe ale unui alt stat, acțiuni pe care în mod natural acesta dorește să le facă. Un aspect definitoriu în acest caz este puterea „impusă” a unor state asupra deciziilor altor state indiferent de influența și presiunea internă a statului asupra căruia se manifesta puterea politică internațională.

Ipotezele realismului

Se dorește o înțelegere a mecanismului de guvernare a spațiului cibernetic din perspectiva securității naționale prin conceptul realismului și al supranaționalismului. Urmărind ipotezele enumerate mai sus. Se pot identifica anumite corelări între tipul de guvernare al UE în raport cu statele membre și cu statele non membre dar partenere. Totodată se poate observa foarte simplu cum statele duc o luptă de a păstra un echilibru între a-și păstra suveranitatea într-o construcție federală și în același timp de a încerca o aliniere la obiectivele și viziunea comună.

Spre exemplu, în contextul realismului şi liberalismului suveranitatea poate fi definită de calitatea atributului principal al statului unde, aceasta presupune ideea de *teritoriu*, *populație* şi un *guvern* eficient și desigur pe de altă parte, dacă considerăm cele trei elemente constitutive ale statului, se poate observa că această definiție este unanim aplicată de toate cele 193 de state membre în cadrul ONU[11]. În prezent sunt disputate două interpretări ale suveranității, anume *suveranitatea statală* și *suveranitatea naţională*.

Echilibrul puterilor

Luând exemplu performerilor sportivi care posedă calități fizice pe care majoritatea persoanelor nu le au sau observând resursele intelectuale pe care geniile le au, putem înțelege de

[11] Lista cu satatele membre ONU, „*Member states*”, https://www.un.org/en/member-states/, accesat astăzi 10.08.2019.

ce nu toate țările au capacitatea naturală de a deveni suficient de puternice pentru a rezista de unele singure sau de a domina în sectorul relațiilor internaționale.

Și în sectorul relațiilor internaționale există state sau actori non-statali care aduc în arena internațională potențiale riscuri la adresa securității naționale sau la adresa integrității aliaților, aceștia mizează aproape de fiecare dată pe evidențierea raportului de forțe și de implicații aduse de valoarea lor pe „*piața*" relațiilor internaționale.

În aceste condiții, un stat care nu are resursele necesare pentru a se opune, poate să facă apel, conform susținătorilor curentului realismului, la principiul echilibrului puterilor. Aceasta aduce în prim plan posibilitatea de a capacita resursele unei puterii sau a mai multor state care să echilibreze puterea unui stat sau a mai multor state cu scopul de a se armoniza o stare de echilibru[12].

Puterea cibernetică în contextul realismului contemporan

Puterea reprezintă un element definitoriu, esențial chiar pentru realism, deoarece poate asigura independența și supraviețuirea statului într-un mediu autoguvernat și autosuficient.[13] După cum afirmă Morgenthau *„oricare ar fi ultimul scop al politicii internaționale, puterea este întotdeauna obiectivul imediat"*[14]. Adesea susținătorii realismului echivalează puterea cu o resursă esențială a statului precum sunt resursele naturale, capacitatea industrială, forța militară și populația unui stat[15]. Puterea cibernetică este definită de Nye[16] ca fiind *„abilitatea de a obține rezultate scontate prin utilizarea resurselor sistemelor informaționale interconectate din sectorul cibernetic",* iar potențialul acestui tip de putere de a transforma sau redefini conceptual dar și practic relațiile internaționale, a devenit o dezbatere proeminentă la nivel global. Deși cum putem observa, inexistența unei teorii privind puterea cibernetică în literatura realistă nu oprește realismul în a dezvolta un cadru de studiu larg în care să se genereze diverse ipoteze de distribuire a puterii între actori statali și non statali în sectorul virtual precum și la modul în care este tratat conflictul cibernetic din perspectiva realismului.

Neorealismul și distribuția puterii

Ca și multe alte teorii, realismul a evoluat de-a lungul timpului. Neorealismul, denumit și realism structural, se concentrează mai degrabă pe structura și distribuția puterii în sistemul internațional decât pe caracteristicile de putere ale statelor percepute individual. Un concept cheie în neorealism este cel al polarității, care descrie structura de putere din sistemul internațional. Vă puteți gândi la un pol ca un stat care este un centru de putere care îi atrage pe alții în sfera sa de influență, la fel ca polul unui magnet atrage pilitura metalică sau gravitatea soarelui atrage planetele pe o orbită în jurul ei.

---

[12] Cristopher Daase, *op.cit.*, p.151.
[13] Mearsheimer John J., „Structural Realism, *International Relations Theories: Discipline and Diversity"*, Rev. de Tim Dunne, Milja Kurki, Steve Smith, Oxford, 2006, Ed. Oxford University Press, pp. 71–88.
[14] Morgenthau Hans J., "*Politics among Nations: The Struggle for Power and Peace*", 1949, New York, Ed. Alfred A. Knopf, p.13, https://archive.org/details/in.ernet.dli.2015.74487/page/n35, accesat astăzi 29.11.2018.
[15] *Ibidem*, pp.80-108.
[16] Nye Joseph S., „*The Future of Power",* 2011, New York, Ed. Public Affairs, p.123.

Una dintre dezbaterile pe termen lung a fost cea privitoare la o posibilă configurație de putere multipolară, bipolară sau unipolară pentru a găsi echilibrul și gestionarea acesteia în crearea unei lumi mai pașnice.[17]

Distribuția unor astfel de capacități între state este considerată ca având implicații semnificative pentru stabilitatea sistemului internațional, mai ales din perspectiva securității naționale.

Realismul aplicat: securitatea cibernetică

Realismul a fost mult timp și încă este o paradigmă dominantă în sistemul relațiilor internaționale, bine definit dar într-o oarecare dilemă în ceea ce privește sectorul securității cibernetice care este în curs de dezvoltare. Acest nou areal prezintă o revigorare a perspectivelor influențate de realism, cu accent vizibil orientat pe securitate și concurență, pe redistribuirea puterii, pe avantajul ofensivei asupra defensivei și beneficiile strategiilor de descurajare, oferind astfel o oportunitate de a evalua rolul realismului în aceste dezbateri nerostite„[18].

Teoria realismului, având în general ca preocupare, problematica securității și factorul de putere națională, pare a fi una dintre perspectivele și instrumentele preferate în procesul de analiză asupra înțelegerii conflictelor din sectorul cibernetic în contextul relațiilor internaționale. Realismul rămâne un cadru relevant pentru identificarea problemelor importante legate de securitate în domeniul cibernetic și poate oferi uneori informații utile în ceea ce privește unele caracteristici ale relațiilor internaționale. Cu toate acestea, teoriile realiste despre conflicte, adesea nu sunt suficient de relevante în ceea ce privește explicarea dinamicii unice a conflictului cibernetic sau în crearea unei prognoze obiective asupra conflictelor.

Cursa înarmărilor cibernetice rezultat al realismului contemporan

Cât despre rapoartele apărute în media cu privire la o posibilă cursă a înarmărilor cibernetice, acestea sunt din ce în ce mai frecvente[192021], iar această tendință a militarizării statelor în spațiului cibernetic este evidentă. Semnale clare ale înarmării sunt și apariția unor noi organizații militare sau forme de organizare militară la nivelul armatelor statelor, elaborarea unor doctrine și strategii cibernetice în sectorul militar, creșterea bugetelor pe sectorul dezvoltării și inovării securității cibernetice, precum și angajarea „războinicilor" cibernetici. Putem să ne creăm o viziune de ansamblu privind zona de dezvoltare în sectorul cibernetic doar privind asupra programelor

[17] Mearsheimer John Joseph, International Relations Theories: *Discipline and Diversity, "Structural Realism"*. revizuit de Tim Dunne, Milja Kurki, Steve Smith, Oxford, Anglia, 2006, Ed. Oxford University Press, pp.71–88.

[18] Anthony J.S. Craig, Brandon Valeriano, „*Realism and Cyber Conflict: Security in the Digital Age*",Ed. E-International Relations Publishing, Bristol, Anglia, 2018, p.86.

[19] Steve Ranger, TechRepublic.com, „*Inside the secret digital arms race: Facing the threat of a global cyberwar"*, 12.09.2018,https://www.techrepublic.com/article/inside-the-secret-digital-arms-race/, accesată astăzi 04.12.2018.

[20] Vesa Kanniainen, HECER Discussion Paper No. 424, *„Cyber Technology and the Arms Race",* februarie 2018, pp.1-2, https://helda.helsinki.fi/bitstream/handle/10138/232974/HECER-DP424.pdf?sequence=1, accesată astăzi 04.12.2018.

[21] Gordon Corera, BBC News, *„Rapid escalation of the cyber-arms race",* 29.04.2015, https://www.bbc.com/news/uk-32493516, accesată astăzi 04.12.2018.

malițioase precum „*Stuxnet*”, care a fost dezvoltat în cel mai mare secret și utilizat exact în ideea atingerii scopurilor realiste ale unei țări privitoare la un alt stat care era generator de insecuritate la nivel global. Putem afirma că în arsenalul militar al unei țări poate intra fără nici o restricție acest nou tip de „produs”, deși intangibil, extrem de periculos, arma cibernetică. În plus, un număr semnificativ de specialiști, jurnaliști, observatori sau rapoarte de securitate ale statelor oferă dovezi empirice care demonstrează o relație de interdependență între dezvoltarea sectorului cibernetic și percepțiile celorlalte state privind posibila amenințare cibernetică precum și generarea unui spirit concurențial între state[22].

Analiza „spiralei” de (in)securitate cibernetică în context contemporan

În aceste momente se poartă discuții mai mult sau mai puțin diplomatice care au ca scop principal dezarmarea nucleară, provenită tocmai din motive obiective susținute de ideologia realistă a statelor, cu rezultate mai puțin favorabile în interes global și favorabile celor puțini. Întrebarea care natural apare este cu privire la existența sau modalitatea de dezarmare digitală a unei țări.

În acest context ipotetic, al nevoii de dezarmare digitală a unui stat națiune, care sunt implicațiile și care este dimensiunea daunelor colaterale aduse nu doar sectorului guvernamental ce și celui civil. Dacă dimensiunea adusă de dezarmarea nucleară a unei țări este de ordin militar și destul de puțin probabil să se răsfrângă direct asupra sectorului civil sau asupra sectorului public-privat, în contextul unei incapacități sau dezarmări digitale, simptomele vor fi resimțite în raport invers în rândul populației.

Teoretizarea balanței ofensiv-defensiv în sectorul cibernetic

Când avantajul se află în de partea atacatorilor, marile puteri sunt puternic provocate în a-și spori capacitățile lor ofensive și pentru a căuta modalități de expansiune teritorială sau a puterii prin noi alianțe strategice cu scopul de a-și consolida poziția, altfel riscă de a se identifica într-o poziție defensivă ceea ce nu este de dorit deoarece presiunea și riscul de a fi atacate este iminent. Se consideră că factorii dați de evoluția tehnologică definesc balanța de apărare-eficiență și oferă noi perspective. De exemplu, se spune că tehnologiile de îmbunătățire a mobilității în cele cinci mari arealuri (*terestru, maritim, aerian, cibernetic și cosmic*) favorizează atacatorii, în timp ce tehnologiile care sporesc și optimizează puterea de foc întăresc sectorul de apărare, făcându-l mai eficient. Teoria a fost pusă în aplicare pentru a defini posibilele debuturi de conflicte sau absența războaielor în cursul istoriei.

Teoria balanței ofensiv-defensive s-a reconceptualizat în mod absolut natural datorită apariției acestui nou areal unde aplicabilitatea acestei teorii a fost posibilă. Reconceptualizarea s-a datorat, în mod deosebit, naturii non-teritoriale a tehnologiilor cibernetice versatile și bazate pe liniile de cod binar în detrimentul muniției de foc, lucru care înlocuiește cu brio nevoia de mobilitate și capacitatea armelor de foc din celelalte patru spații reale.

Supranaționalism

Înțelegerea termenului supranațional ca și o ideologie opusă realismului este din punctul meu de vedere una total eronată și lipsită de fundament rațional. Organismelor supranaționale le sunt

[22] Anthony Craig, Brandon Valeriano, „*Conceptualising cyber arms races*”, *8th International Conference on Cyber Conflict (CyCon),* Ed. NATO CCD COE Publication, Tallin, 2016, https://www.researchgate.net/publication/305871947_Conceptualising_cyber_arms_races, accesat astăzi 06.12.2018.

date puteri sporite și autoritate asupra unor certe aspecte ale uniunii și statelor membre acestor uniuni dar nu trebuie să omitem scopul și obiectivele pentru care aceste state au aderat la aceste uniuni. „*Prin forțele proprii, statele, cu siguranță nu ar putea trata anumite problematici sau cu atât mai mult nu le-ar putea gestiona eficient sau administra în condițiile progresiste ale uniunilor precum este cazul Uniunii Europene sau cazul precum este modelul de dorit al Statelor Unite ale Americii. În cazul României care are calitate de țară membră a Uniunii Europene, putem afirma faptul că strategia și procesul de construcție europeană se bazează sau chiar începe cu întărirea suveranității naționale. Oricare ar fi acela, proiectul național în nici un caz nu se poate opune proiectului european"*[23].

Dacă facem o scurtă analiză a UE, plecând de la premisele anterioare, putem spune că aceasta este o organizație supranațională care are elemente con-federaliste (tratate, un Consiliu de Miniștri, care deține puteri legislative și decizionale, Consiliul, principala autoritate politică, regula unanimității în procesul de luare a deciziilor) cele federale (cetățenia comună, moneda unică, primatul dreptului Uniunii față de legea statelor membre, instituțiile supranaționale etc.).

Pentru a deveni un stat federal, Uniunea Europeană are nevoie de o Constituție.,,[24]

Formându-se această federație de state, apare Uniunea Europeană care subit este înzestrată cu întreg arsenalul organism supranațional.

Supranaționalism și securitate cibernetică

Experții și strategii în domeniul securității informatice sunt de acord că infrastructurile critice și sistemele de comandă și control din sectorul industrial / SCADA, reprezintă din perspectivă economică, coloana vertebrală a oricărei țări moderne sau contemporane. Grupări de hacktiviști profesioniști și chiar unele state prin structurile lor specializate, s-au concentrat pe atacuri infrastructurilor critice pentru a le sabota, dezafecta sau în unele cazuri de a le neutraliza. Un astfel de caz a fost identificat în cursul anului 2018, în care serviciile de informații israeliene cu ajutorul unui program malițios similar Stuxnet dar mult mai complex au extras date privind infrastructura critică și nucleară a Iranului, tocmai cu ajutorul telefonului mobil al președintelui Hassan Rouhani[25], ocazie cu care au fost expuse locația arhivelor nucleare cât și a depozitelor de materiale nucleare[26] în fața Adunării Generale a Națiunilor Unite din 27 septembrie 2018[27].

Istoricul atacurilor cibernetice

Pentru a putea afirma nevoia de a guverna un anumit spațiu sau domeniu, consider necesară cunoașterea acestuia, și cum poate fi cunoscut mai bine dacă nu prin întocmirea unui itinerar,

---

[23] Prof. univ.dr Adrian Liviu-Ivan, Conferința „*O Europă mai sigură*", Universitatea din Oradea, Oradea, 15.01.2019.

[24] Ivan Adrian-Liviu, Transylvanian Review of Administrative Sciences, Vol.4, Nr.22, „*Governance and "European Constitution*", 2008, p.79, http://rtsa.ro/tras/index.php/tras/article/view/382/372, accesat astăzi 30.04.2019.

[25]Toi Staff, The Times of Israel, „*TV report: Israel silent as Iran hit by computer virus more violent than Stuxnet",* 31.10.2018, https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virus-more-violent-than-stuxnet/, accesat astăzi 14.02.2019;

[26]Michael Bachner, Toi Staff, The Times of Israel, At UN, „*Netanyahu reveals Iranian nuclear warehouse, urges IAEA to go inspect it",* https://www.timesofisrael.com/netanyahu-reveals-secret-iranian-nuclear-warehouse-in-un-speech/, accesat astăzi 14.02.2019;

[27] Consiliul European, Consiliul Europei, *Adunarea Generală a ONU, New York, 27/09/2018*, https://www.consilium.europa.eu/ro/meetings/international-summit/2018/09/27/, accest astăzi 14.02.2019;

istoric chiar sau un traseu al evenimentelor care a adus această nevoie de a guverna spațiul sau domeniul în care acestea s-au desfășurat și încă se propagă.

Drept urmare, primul atac, mediatizat, suspectat a fi un atac cibernetic, asupra infrastructurii critice industriale a fost în 1982 când conducta de gaz Trans-Siberiană a explodat unde se presupune că explozia a fost provocată de un troian care a activat prin instalarea acestuia la sistemul de control.

Stuxnet, un alt vierme informatic cu capacități extraordinare, descoperit în 2010, a reușit să infecteze cele mai securizate instalații nucleare iraniene cu ajutorul unui dispozitiv fizic - unitate de memorie externă de tipul flash-drive USB. Prin intermediul acestui vierme informatic instalat, s-a reușit modificarea parametrilor de viteză ale rotoarelor reactoarelor nucleare. În urma unei analize de detaliu reiese faptul că odată cu o cunoaștere a echipamentelor și tehnologiilor utilizate, chiar și în zilele de azi, se pot crea soluții potrivite și croite pe nevoile exacte ale atacatorului .

Atacurile cibernetice orientate împotriva infrastructurilor critice primesc credit și valoare acestora sau a resurselor respectiv a serviciilor acestora este destabilizată. Așa numitul „război cibernetic" a devenit în prezent o parte oarecum intrinsecă a conflictelor internaționale. Cu atât mai mult cu cât datorită naturii sale nedetectabile și a potențialului de a provoca daune fizice fără a detașa forțe militare umane sau mecanizate, devine de departe o metodă preferată de atac, tot mai des întâlnită.

Fără a face o analiză asupra „cifrei negre" a atacurilor asupra infrastructurilor critice ale oricărui stat pot afirma că există o nevoie crescândă de specialiști de securitate cibernetică pentru identificarea și gestionarea nu doar a breșelor de securitate ce și a atacurilor de tip persistent sau ascuns.

Chiar și azi, deși a fost mediatizată problema, angajații sectorului militar utilizează echipamente și aplicații, care au capacitatea nu doar de geo-localizare cât și de a fi utilizate de la distanță ori interceptate pentru a l-i se urmări activitatea deținătorilor și a celor cu care interacționează. Nu este un caz singular și nu este vorba doar despre personalul militar român, american, ș.a.m.d. Unul dintre cazurile cele mai sensibile este dat de deconspirarea unor baze militare secrete, a traseelor urmate de personalul acestora și de identitate lor[28], iar un alt caz este asemănător dar cu date nu atât de sensibile ar fi cel al bazei militare de la Deveselu unde este instalat scutul antirachetă al SUA[29]

Cât despre scurgerea de informații din telefoanele mobile inteligente, această breșă fiind dată în mod deosebit de utilizarea unor aplicații care oferă această oportunitate, drept urmare, datele culese de pe echipamentele de comunicații inteligente sunt într-o proporție de 63% numere de telefoane mobile și un număr de 37% locații ale dispozitivelor. Odată cu aceste meta-date[30] sunt

---

[28] Liz Sly, The Washington Post, 29.01.2018, „*U.S. soldiers are revealing sensitive and dangerous information by jogging*", https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?noredirect=on&utm_term=.c3748d111f92, accesat astăzi 03.05.2019.

[29] Harta Interactivă STRAVA, Baza Militară de la Deveselu, Jud. Olt, 03.05.2019, https://www.strava.com/heatmap#14.04/24.38239/44.07120/hot/all, accesat astăzi 03.05.2019.

[30] Aleksandar Kovačević, Dragan Ivanović, Branko Milosavljević, Zora Konjović, Dušan Surla, Program electronic library and information systems, Vol. 45, Nr.4, „*Automatic extraction of metadata from scientific publications for*

culese adrese de email, date bancare, utilizatori și parole. Se prognozează ca până în 2020 numărul total de parole utilizate de sistemele automate și utilizatori să ajungă la ~300 miliarde. Prognozele arată că atacurile cibernetice asupra industriei medicale se vor multiplica cu 400% iar organizațiile în general vor cădea victimă atacurilor cibernetice de tip „*ransomware*" cu ritm de o organizație la fiecare 14 secunde iar costurile acestor tipuri de atacuri, estimate în anul 2019, sunt de ~11.5 miliarde $.

În contextul de securitate al Uniunii Europene, apare în 2013 un nou element de noutate. ***Politica cibernetică a UE***, pentru a asigura un grad de reziliență echidistant, real și egal la nivelul statelor membre, aduce în prim plan necesitatea de armonizare a legislației orientate pe securitate și reziliență cibernetică. Urmare a acestor tumultoase interese comune, Comisia Europeană emite *Comunicare Comună* către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, „*Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat"*.[31]

Uniunea Europeană drept urmare se obligă să asigure și să întărească eforturile țărilor membre în această materie și în demersul de a oferi cetățenilor proprii acces la resursele internetului la scară largă, condiționat de asigurarea integrității și securității spațiului virtual și de perspectiva respectiv atitudinea mai ofensivă și reziliență la actele malițioase sau criminale în sectorul cibernetic.

Guvernare supranațională elitistă asupra sectorului de securitate cibernetic

Elita cibernetică este reprezentată mai departe atât de capacitățile de necontestat și de dorit ale persoanelor active în mediile profesionale în diversitatea lor cât și funcția potrivită acesteia cu rol consultativ ori de decizie într-o problematică de securitate a informației. Necesitatea acestui concept, elitismul, în arealul de guvernare al sectorului informațional, este nu doar o nevoie reală cât este o obligativitate a statelor de a-și împlini nevoile și îndeplini obiectivul primordial, de protejare a suveranității teritoriale, din punct de vedere jurisdicțional, geografic și virtual. Decidenții, în toate nuanțele lor, precum cei politici, financiari și de ce nu, decidenții autodeclarați, recunoscuți sau anonimi dar care au un cert impact în zona de formare a opiniei publice, pot lua cea mai înaltă formă decizională în ceea ce privește elitismul societal în raport cu impactul pe care îl au asupra societății și factorilor de decizie naționali (*n.r. liderii organizațiilor non guvernamentale, asociațiilor civile, asociațiilor profesionale sau comunităților religioase*).

Organigrama sectoarelor securității cibernetice din spațiului cibernetic

Reglementarea spațiului cibernetic în spațiul internațional și implicit în spațiul național, și aplicarea legii nu pot fi nicidecum neglijate devreme ce spațiul cibernetic este un areal activ (virtual) comun de securitate, libertate și prosperitate economică. Posibilitatea unei soluții de

---

CRIS systems", p. 377, https://www.researchgate.net/profile/Dragan_Ivanovic/publication/216592386_Automatic_extraction_of_metadata_from_scientific_publications_for_CRIS_systems/links/0fcfd50cb052fcdf77000000/Automatic-extraction-of-metadata-from-scientific-publications-for-CRIS-systems, accesat astăzi 03.05.2019.

[31] Comisia Europeană, „*Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat",* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:RO:PDF, accesat astăzi 22.04.2019.

implementat pentru soluționarea pașnică a dilemei de securitate cibernetică și evitarea coliziunii dintre nevoia de supra-securizare, „*și pentru a obține mai multe drepturi și libertăți în spațiul cibernetic ar fi ca securitatea, libertatea și prosperitatea economică în mediul virtual să fie universal recunoscute drept drepturi fundamentale ale utilizatorilor în egală măsură. De principiu, optimul de guvernanță în spațiul cibernetic va fi atins atunci când va exista o analogie ușor identificabilă între nivelul de securitate, libertate și prosperitate din spațiul cibernetic*”[32].

Domeniul guvernanței securității spațiului cibernetic este susținută de nouă piloni principali, anume: Arhitectura de Securitate, Operațiuni de Securitate, Guvernanța Cibernetică. Managementul Riscului, Educația de Securitate, Pregătire profesională continuă, Intelligence de Securitate, Norme și Standarde, Securitate Fizică.

În actual context geopolitic și de securitate în care România deține calitatea de stat membru al UE, pot afirma cu tărie și convingere că progresul UE în lumina supranaționalismului dă roade vizibile, iar țările membre se aliniază într-un mod natural. Se pare că Organismele supranaționale ale UE se bucură de o atenție sporită din partea statelor membre, iar în ultimul an se discută tot mai des de apariția unei armate a UE, care să fie compusă din resursele militare ale statelor din întreaga uniune. În acest context, văd oportun o readaptare a teoriei elitelor și a decidentul de securitate în actul de guvernare a spațiului cibernetic, orientată spre progres tehnologic, cercetare și inovare și dezvoltare a sistemelor de securitate.

[32] Iulian Popa, Teză de doctorat, „*Securitatea și guvernanța spațiului cibernetic contemporan*”, Universitatea Babeș-Bolyai, Școala doctorală „*Relații internaționale și studii de securitate*”, Cluj-Napoca, 2015, pp.133-134.

CAPITOLUL IV
DIPLOMAȚIA ÎN SPAȚIULUI CIBERNETIC

În mod evident, un simplă afiliere cu un anumit actor politic pe platforme sociale precum Facebook sau un „*tweet*” cu frânturi de informație pot duce nu doar la instabilitatea unui preț pe bursă ce la instabilitatea economică sau de securitate a unei țări.

În România până în acest moment nu am identificat o analiză a acestui subiect, motiv pentru care elementele de noutate sunt date de studierea atât a diplomației digitale cât și a diplomației cibernetice în raport cu noul context de securitate național, european și de ce nu global. Dezvoltarea subiectului a dus la înțelegerea noului instrumentar diplomatic cu elemente ce țin de arealul cibernetic și utilizarea acestuia în raport cu respectarea și aplicarea, în continuare, a protocolului diplomatic tradițional.

Apariția diplomației publice și digitale a fost determinată de intrarea unor noi actori, atât guvernamentali cât și non guvernamentali în mediul internațional, de dezvoltarea unei noi agende internaționale de securitate și facilitată de noile tehnologii informatice și de comunicații. Toate acestea sunt instrumente importante care își fac simțit aportul în sprijinul unor strategii diplomatice mai largi.

Diplomația digitală trebuie să scape de eticheta „*obscură*” avută în acest moment în zona cibernetică și să își cultive o cultură proprie cu un rol bine stabilit și echilibrat în știința sau arta diplomației. Diplomația digitală trebuie să se concentreze asupra domeniilor în care poate sprijini strategiile diplomatice mai largi - diplomația publică, crearea de rețele, colectarea informațiilor și gestionarea cunoștințelor, rezolvarea conflictelor și medierea - și evoluția tehnologiilor și a platformelor și instrumentelor online care pot oferi cele mai eficiente rezultate. Mijloacele sociale existente vor continua să joace un rol, atunci când vor fi folosite inovator și creativ, însă actorii diplomatici nu ar trebui să depindă de ele. Aceasta ar trebui să includă platforme online care să promoveze utilizarea mai intensă a tehnicilor de construire a scenariilor, de simulare și de adaptare a activităților din mediul online (*jocuri, manuale interactive, ș.a.m.d.*). Aceste instrumente noi din arsenalul diplomației digitale vor cântări mult în favoarea organizațiilor non guvernamentale și altor grupuri și comunități ale societății civile.

În plan european, România este evidențiată de o participare diplomatică pro-activă la reglementarea, spațiului cibernetic precum cazul Comisiei pentru Ocuparea Forței de Muncă și Afaceri Sociale și cadrul Comisiei pentru Libertăți Civile, Justiție și Afaceri Interne din Parlamentul European unde reprezentanți diplomatici români și membri ai Parlamentului European au fost desemnați ca și raportori ai diferitelor grupuri politice, pentru dosarul privind Piața Unică Digitală. Actul „*Piața Unică Digitală*” este un document foarte tehnic, iar dată fiind competența Comisiei, în cadrul acesteia au fost cooptați membrii care și-au adus contribuția concentrată pe subiectul combaterii conținutului ilegal, în orice formă pe internet dar și asupra protecției datelor cu caracter personal. Ocazie cu care s-a cerut opinia prin forme de consultanță „pro-bono” din partea unor specialiști în domeniu. În acest grup de lucru am luat și eu parte unde am contribuit cu informații relevante și deosebit de utile cu privire la raportul Piața Unică Digitală Europeană.

Adânc fundamentată în amenințările aduse la securitatea uniunii și alianței (*care este din ce în ce mai fragilă*), tot mai frecvente, complexe, distructive și coercitive, tratate printr-o politică

diplomatică persuasivă bazată pe putere militară și adesea economică statele aliate sunt în poziția în care sunt nevoite să își asume un set nou de reguli, politici și proceduri. Această nouă formă de diplomație de departe diferită de diplomația tradițională bazată pe relații interumane, este una bazată pe gestionarea puterii și securității informației în sectorul cibernetic în egală măsură cu capacitatea întregii uniuni, alianțe și națiuni de a-și păstra și proteja valorile fundamentale.

CAPITOLUL V

INFLUENȚE ALE UNEI POLITICI UNITARE EUROPENE PRIVIND SECURITATEA INFORMAȚIEI ELECTRONICE ÎN ACTUALA STARE GEOPOLITICĂ GLOBALĂ

Studierea implicațiilor aduse de diplomația digitală și diplomația cibernetică, în mod natural ne duce la nevoia de aprofundare a influențelor politicii europene privind securitatea informației electronice în actuala stare geopolitică globală. Primul aspect care iese în evidență este aportul adus de președinția României și personalul guvernamental (*MAI, MAE, MECT, ș.a.m.d.*) în cadrul UE dar și a statelor partenere cu care țara noastră colaborează.

România aduce în prim plan, prin expunerea oficială a Ministerului Afacerilor Externe, un comunicat prin care afirmă că oficial s-a luat atitudine privind noile trenduri prin adoptarea Strategiei de securitate cibernetică a României și acțiunile MAE în privința securității cibernetice la nivel național, iar internațional prin existența Directivelor Uniunii Europene precum Directiva 2016/1148 privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (*intrată în vigoare în august 2016*).

Reziliența cibernetică, poate fi descrisă ca abilitatea de a furniza continuu rezultatul dorit, în ciuda evenimentelor cibernetice adverse. Această abilitate poate fi luată în considerare la diferite nivele, unde fiecare nivel aduce provocări, metode și tipuri de controale conceptuale unice în raport cu reziliența cibernetică. Prin urmare, capacitatea de a furniza în mod continuu rezultatul dorit se referă nu numai la o națiune, ci și la o organizație sau chiar la un sistem IT specific. Cu toate acestea, pentru ca reziliența cibernetică să fie eficientă, aceasta trebuie abordată în mod holistic, pe mai multe nivele și în paralel.

Siguranța cibernetică transcende înțelegerea convențională a literaturii de specialitate în domeniul securității naționale în raport cu relațiile internaționale. Dilema de securitate în acest caz este provocată în mod direct de caracterul transfrontalier al infracțiunilor informatice și de nevoia cooperării statelor prin organismele sale specializate din spectrul internațional. În ajutorul acestor organisme de regulă este cerută expertiza de specialitate din sectorul securității cibernetice și din partea actorilor non statali, din sectorul privat. Orientându-ne atenția spre tipologia atacurilor cibernetice, putem observa că primul răspuns la astfel de atacuri vine din partea țintei sau victime. Prin urmare, sectorul general de securitate s-a privatizat în toată lumea, rămânând privată de ochii actorilor non statali doar securitatea națională.

Pentru a exprima cât mai coerent această relație și capacitatea de interdependență, este nevoie să observăm pe fiecare nivel al guvernanței spațiului cibernetic provocările, metodele și tipurile de controale conceptuale unice în raport cu reziliența cibernetică, înțelegând capacitatea de furnizare permanentă a rezultatul de securitate dorit care se referă la o alianță, o națiune, o organizație sau chiar la un sistem informațional specific. După cum s-a constatat, pentru ca reziliența cibernetică să fie eficientă, aceasta trebuie abordată în mod holistic pe toate nivelurile existente și în paralel.

Elementele de noutate sunt aduse de analiza problematicii securității cibernetice din perspectiva organismelor supranaționale prin entitățile internaționale de profil şi implicarea României în calitate de membru pro-activ în domeniu, context în care am realizat un studiu comparativ a rezilienței cibernetice și a securității cibernetice pentru a înțelege poziția României

în raport cu Uniunea Europeană – UE, Organizația Tratatului Atlanticului de Nord – NATO, CONSILIUL EUROPEI - CoE Organizația pentru Securitate și Cooperare în Europa – OSCE.

CAPITOLUL V

STUDIU DE CAZ - CULTURA DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA

Într-o proporție covârșitoare, aproape tot ceea ce facem, zi de zi, este conectat de domeniul cibernetic prin echipamentele de comunicații moderne. Acest fenomen este rodul progresului tehnologic din sectorul industriei comunicației și tehnologiei informației.

Unul dintre pilonii acestei revoluții tehnologice este digitalizarea datelor și a informațiilor.

Acest rezultat extraordinar al modernizării, al progresului tehnologic, „*digitalizarea*", este un element central și necesar procesul de înțelegere a acestei noi ere, a globalizării.[33] În aceeași ordine de idei, putem spune că democratizarea tehnologiei este promotorul globalizării producției.[34] Spun asta deoarece unul din lucrurile urmărite în acest studiu de caz este nivelul și implicațiile aduse de utilizarea tehnologiilor (*hardware și software*) moderne asupra vieții personale, sociale și profesionale a populației din România anilor 2016-2018.

În mediul academic pentru a putea face o afirmație, în contextul unei cercetări științifice și într-o mai mare măsură în contextul securității naționale, este nevoie de un fond de cunoștințe de la care să pornești o discuție și pe baza cărora să-ți argumentezi expunerea, drept urmare, acest ultim capitol al tezei este dedicat în exclusivitate studiului factorului numit „*cultura de securitate cibernetică*" în raport cu topicul celorlalte patru capitole tematice (cap. II - cap. IV), pentru a valida și invalida ipotezele și pentru a răspunde la întrebările de cercetare propuse în introducere.

Analiza statistică asupra culturii de securitate cibernetică a populației rezidente în România, s-a obținut și din surse deschise de informații. Desigur, astfel de analize pot fi întocmite prin colectarea, evaluarea, verificarea și centralizarea datelor din comunicările și rapoartele emise de producătorii și furnizorii de soluții de securitate cibernetică, de CERT-RO, de Institutul Național de Statistică și de alte organisme naționale sau internaționale dar nu în ultimul rând de cercetările de nișă orientate pe furnizarea de evaluări statistice și expunerea sau soluționarea problematicilor de securitate în general. Drept urmare, raportându-ne la ultimul Breviar Statistic al INS din 2018 putem realiza faptul că în cadrul lucrării de față ne raportăm la un eșantion final de 5.446 persoane din totalul de ~7.600 chestionare, care reprezintă ~0.03% din 19.644.350[35] persoane care este numărul estimat al populației rezidente în România anului 2017.

Chestionarul

Pornim de la considerentul că o evaluare reală, fidelă și granulară a nivelului culturii de securitate cibernetică în România, nu poate să fie generată doar de aplicarea unor interviuri în rândul elitelor (*experți, specialiști, analiști, profesori, consultanți, ș.a.m.d.*) care activează în sectorul securității cibernetice sau a decidenților ori a instituțiilor de profil din sectorul public/privat. O astfel de abordare probabil ar genera o evaluare a nivelului de profesionalism raportat la persoanele evaluate în raport cu poziționarea pe „*piață*" a organizațiilor din care acestea fac parte, dar sub nici o formă nu ar oglindi nivelul de cultură de securitate.

---

[33] Thomas L. Friedman, „*The Lexus and the Olive Tree – Understanding Globalization*", Ediția revizuită, Ed. Farrar, Straus and Giroux, New Yok, SUA, 2000, pp.46-47.

[34] Ibidem, p.49.

[35] Breviar Statistic, România în cifre, Institutul Național de Statistică, INS 2018, p.9, http://www.insse.ro/cms/sites/default/files/field/publicatii/romania_in_cifre_breviar_statistic_1.pdf, accesat astăzi 01.04.2019.

Motivat fiind de considerentele expuse mai sus și de necesitatea de a răspunde întrebărilor de cercetare propuse am considerat potrivită aplicarea metodei chestionarului. Chestionarul este rezultatul a trei etape de validare. Toate cele trei forme au fost supuse analizei într-o comisie de specialitate. Persoanele identificate în această comisie au fost alese pe principiul expertize în domeniul specialităților practicate de aceștia, anume un sociolog, un psiholog, un expert în securitate națională și a un expert în studiile statistice.

Pentru a-l putea valida și pentru a-i putea da o formă, chestionarul a fost aplicat unui număr de zece specialiști din sectorul tehnologiei informației și a comunicațiilor. Aceștia, unanim au sugerat ca fiind existentă nevoia introducerii de întrebări concrete și suficient de tehnice cu privire la nivelul de cunoștințe în domeniul IT&C pentru a se putea evalua nivelul de cunoaștere a tehnologiei de comunicare și gestionare a informației în mediul virtual.

O a doua formă a fost dată după ce au fost aplicate un alt set de 10 chestionare experților din sectorul legislativ care au comentat și evidențiat o nevoie de accentuare a aspectelor privind criminalitatea cibernetică, identificate tot mai des în sectorul economic virtual și nu numai.

Cea de-a treia etapă de actualizare și validare a întrebărilor chestionarului a fost marcată de evaluarea din punct de vedere statistic, etapă care a fost desfășurată sub atenta supraveghere a Departamentului Psihometrie și Statistică din cadrul Facultății de Științe Comportamentale și Sociale a Universității Groningen, cu ajutorul resurselor cărora am și finalizat studiul statistic al chestionarelor aplicate și care m-au orientat pas cu pas până la finalizarea studiului statistic.

Analiza statistică

Centralizarea datelor din chestionarele aplicate s-a întins pe o perioadă de aproximativ patru luni. În primele trei luni, au fost introduse datele din chestionarele aplicate, care au fost în format scris pe hârtie. Din motive de autenticitate și veridicitate a datelor utilizate în acest studiu, chestionare originale sunt păstrate pentru o perioadă nedeterminată de timp. Predominant, analiza cantitativă a stat la bazele analizei calitative, utilizând în acest timp literatura de specialitate și aplicațiile informatice specializate în acest sens. În ceea ce privește interpretarea datelor pentru obținerea unui rezultat concludent în analiza calitativă, studiul și experiența acumulată pe parcursul celor trei ani au oferit rezultatul scontat, prin înțelegerea gradului de cultură de securitate pe care populația rezidentă în România îl are. De menționat, în ceea ce privește întrebările cercetare ale tezei, în acest context este faptul că, această analiză reprezintă o nouă posibilitate de cercetare, a unei arii de interes major și obținerea unui indicator vital pe „barometrul" culturii de securitate cibernetică raportată desigur la securitatea națională.

Acest proces a presupus identificarea și excluderea cazurilor duplicate din baza de date, identificarea și excluderea cazurilor ce conțin răspunsuri logic imposibile sau improbabile (*de exemplu utilizatori care au declarat că au vârsta de 0 ani sau că petrec mai mult de 24 ore pe zi utilizând tehnologia digitală*), identificarea și excluderea răspunsurilor participanților cu vârsta prea mică (mai mică de 14 ani) sau prea mare (*mai mare de 70 ani*) pentru scopul acestui studiu, și identificarea, respectiv excluderea cazurilor cu rate ridicate de răspunsuri lipsă (*de exemplu cazurile cu răspuns lipsă pentru mai mult de 80% din întrebări*).

Pentru a putea analiza datele în mod consecvent, utilizând același test statistic pentru analiza răspunsurilor la toate întrebările, variabila numerică „*vârsta*" a fost transformată în variabilă categorială. În acest sens, utilizatorii cu vârsta sub 20 de ani au fost catalogați drept

„*tineri*", cei cu vârsta între 20 și 60 de ani au fost catalogați drept „*adulți*", iar cei cu vârsta peste 60 de ani au fost catalogați drept „*vârstnici*".

Deoarece aproape toate întrebările din chestionarul utilizat au generat date categoriale de tip nominal prin răspunsuri de tipul DA/NU sau de tip ordinal și scalabil (*de exemplu evaluarea importanței securității informatice pe o scala de la 1 la 5*), principala strategie analitică pe care am utilizat-o a fost analiza frecvențelor. Scopul a fost acela de a determina dacă există diferențe semnificative între participanți în ceea ce privește variabilele de interes din acest studiu, un exemplu ar fi cel în care cuantificăm măsura în care utilizatorii români consideră tehnologia digitală ca fiind importantă. De asemenea, ne-am propus să determinăm dacă există asocieri între anumite aspecte evaluate în cadrul acestui studiu precum măsura în care utilizatorii au fost victime ale unor infracțiuni informatice în raport cu anumite aspecte ce țin de securitatea informatică.

Testul statistic potrivit pentru analiza frecvențelor este așa-numitul test hi-pătrat, Pearson $\chi 2$. Acest test statistic poate fi utilizat pentru a determina dacă există diferențe semnificative statistic între frecvențele observate și cele teoretice (așteptate) în cadrul uneia sau a mai multor categorii de răspuns.

Toate analizele statistice au fost realizate în programele pentru analiză statistică R (*R programming language for statistical computing; R*[36] *Core Team, 2019 și SPSS*[37] *v.25.*

Un număr de 5,446 persoane au participat la acest studiu în mod voluntar, la întâlniri programate, față în față, completând chestionarul. Răspunsurile a 52 participanți au fost eliminate din analiza finală a datelor deoarece aceștia au declarat că au vârsta mai mică de 14 ani sau mai mare de 70 de ani. Așadar, pentru analiza finală a datelor au fost utilizate răspunsurile a unui număr de 5,141 participanți reprezentând aproximativ 94% din eșantionul original. Dintre aceștia, 3,254 (63.3%) participanți au oferit răspunsuri complete la întrebările cu răspuns închis.

Analiza răspunsurilor incomplete arată că cele mai numeroase date lipsă (12.5% din totalul participanților) corespund întrebării "*Ați urmat vreodată cursuri în domeniul informatic?*", urmată de întrebarea "*Ați fost vreodată victimă a unei infracțiuni informatice?*" cu 7.4% răspunsuri lipsă și de întrebarea "*Considerați că România este pregătită pentru un eventual val de atacuri cibernetice?*" cu 6.7% răspunsuri lipsă.

Distribuția participanților în funcție de gen a fost date de 53.8% participanți de gen feminin, 46.2% de gen masculin iar un număr de 1.5% nu au declarat apartenența de gen.

Vârsta participanților are o distribuție asimetrică spre dreapta, fiind reprezentată de o mediană egală cu 23 ani, iar 75% dintre participanți au sub 35 ani. Un procent de 2.2% dintre participanți nu și-au declarat vârsta.

[36] R Core Team (2019*), „R: A language and environment for statistical computing"*, R Foundation for Statistical Computing, Vienna, Austria, URL: https://www.R-project.org/, accesat astăzi 19.03.2019.
[37] IBM Corp. (2017), „*IBM SPSS Statistics for Windows - Statistical Package for Social Sciences"*, Version 25.0, Armonk, NY: IBM Corp, URL: https://www-01.ibm.com/support/docview.wss?uid=swg24043678, accesat astăzi 19.03.2019.

În ceea ce privește mediul de proveniență al participanților, 29.3% dintre aceștia provin din mediul rural, iar 70.7% din mediul urban. Un procent de 6.6% dintre participanți nu și-au declarat mediul de proveniență.

Totodată, în funcție de statutul social, participanții se distribuie astfel: elevi și studenți în procente similare (45.0%, respectiv 41.9%), angajați și liber profesioniști în procente similare (5.3%. respectiv 5.2%), 2.6% șomeri și niciun pensionar. Un procent de 1.8% dintre participanți nu și-au declarat statutul social.

Analiza Competențelor Digitale ale Utilizatorilor Români

Competențele digitale ale utilizatorilor români au fost evaluate printr-un set de 7 întrebări ce vizează aspecte precum nivelul competențelor digitale, tipul și scopul echipamentelor digitale utilizate, timpul petrecut utilizând tehnologia digitală, precum și importanța percepută a tehnologiei digitale. Timpul petrecut utilizând tehnologia digitală, este considerat un indicator deoarece, acesta este raportat la gradul de vulnerabilitate și riscurile asociate pe platformele online sau în utilizarea resurselor informatice. Desigur, acest timp de utilizare a tehnologiei oferă o perspectivă, asupra gradul de expertiză și adaptabilitate la mediile virtuale, raportarea și chiar dependența de acesta.

S-a evaluat, de asemenea, măsura în care competențele digitale sunt asociate cu variabile socio-demografice precum genul, vârsta (*tineri sub 20 ani, adulți între 20 și 60 ani, vârstnici peste 60 ani*), mediul de proveniență (*urban sau rural*) și ocupația participanților (*elev, student angajat, antreprenor/liber profesionist, sau șomer/fără ocupație*). Rezultatele acestor analize sunt prezentate în următoarele paragrafe.

Deoarece majoritate breșelor de securitate sunt datorate, fie lipsei de competențe digitale fie de lipsa unei culturi de securitate, se consideră oportun cunoașterea autopercepției utilizatorului în ceea ce privește nivelul său de competențe digitale. În cadrul întâlnirilor, după completarea chestionarului, adesea am pus întrebări de lămurire. Printre acestea se număra și „*Considerați că sunteți suficient de pregătit în ceea ce privește tehnologia utilizată?*”, iar răspunsurile, erau de cele mai multe ori afirmative. Aceste întrebări de clarificare erau puse și cu scopul de a verifica încrucișat alte întrebări din conținutul chestionarului aplicat, precum „*Ați fost vreodată victimă a unei infracțiuni informatice?*” sau „*Aveți conturi online pe care le utilizați împreună cu altcineva?*”. De aici rezulta, adesea, faptul că nivelul de autopercepție asupra gradului de deținere a competențelor digitale sau nivelului culturii de securitate este eronat.

În ceea ce privește nivelul declarat al competențelor digitale ale participanților, mai mult de jumătate dintre aceștia dețin un nivel mediu de competențe, iar aproximativ o treime dețin un nivel ridicat.

În ceea ce privește pregătirea formală în domeniul informatic, 42.5% dintre participanți au urmat cursuri de specializare, iar 57.5% dintre aceștia nu au urmat.

Astfel, dintre cei care au urmat cursuri de formare în domeniu informatic, un procent ridicat sunt elevi (48.7%). De asemenea, semnificativ mai puțini sunt liber-profesioniștii (24.2%), șomerii sau persoane fără ocupație (17.1%) care au urmat astfel de cursuri. Așadar, urmarea unor cursuri în domeniu informatic este asociată cu un nivel avansat al competențelor digitale: 49.0% dintre cei care au urmat astfel de cursuri dețin un nivel avansat al competențelor digitale. În ceea ce privește numărul de ore petrecute utilizând tehnologia digitală, în medie utilizatorii din cadrul

acestui eșantion fac acest lucru timp de 5 ore pe zi. Un sfert dintre participanți petrec mai puțin de 3 ore pe zi utilizând tehnologia digitală, în timp ce un sfert sunt online mai mult de 10 ore pe zi. Referitor la măsura în care acest timp este petrecut în mediul online, datele arată că jumătate dintre respondenți petrec în mediul online între 50% și 100% din timpul dedicat utilizării tehnologiei digitale. Un sfert dintre respondenți petrec mai puțin de 50% din timp în mediul online, în timp ce un sfert dintre ei petrec timpul dedicat tehnologiei digitale în mediul online în proporție de 100%.

Utilizarea aplicațiilor informatice este practicată în proporție de 90% de către utilizatorii români, diferența fiind semnificativă statistic și importantă din punct de vedere practic.

Printre aplicațiile informatice menționate se numără *Facebook, Microsoft Office, WhatsApp, Instagram*, motoare de căutare online, sau diverse servicii de e-mail. Utilizarea acestor aplicații este statistic asociată cu vârsta utilizatorilor și cu statutul socio-economic al acestora însă aceste asocieri sunt neglijabile. Acest lucru sugerează că românii utilizează aplicațiile informatice în aceeași măsură indiferent de vârstă, mediu de proveniență sau statut socio-economic.

Referitor la importanța tehnologiei digitale pentru utilizatorii români, 31.3% dintre aceștia au declarat că tehnologia digitală este importantă pentru ei, 30.3% au declarat că aceasta este destul de importantă, iar 26.5% au declarat că aceasta este foarte importantă. Procentul de 11.8% rămas au declarat că pentru ei tehnologia digitală este puțin sau deloc importantă. Importanța percepută a tehnologiei digitale la români este asociată semnificativ statistic cu mediul de proveniență și statutul socio-economic al utilizatorilor. Utilizatorii care consideră tehnologia digitală ca fiind foarte importantă provin din mediul urban într-un procent mai ridicat (20.5%) decât ne-am fi așteptat în lipsa asocierii dintre variabile.

Analiza corelației dintre importanța percepută a tehnologiei digitale și statutul socio-economic al utilizatorilor români arată că, dintre cei care consideră tehnologia digitală ca fiind deloc importantă, un procent mai ridicat decât ne-am fi așteptat în lipsa asocierii sunt șomeri sau liber profesioniști (23.2%). În ceea ce îi privește pe ce care consideră tehnologia digitală ca fiind puțin importantă, cei mai mulți utilizatori, mai mulți decât era de așteptat sunt șomeri sau liber profesioniști (26.7%). Pentru un număr mai mare de elevi decât ne-am fi așteptat (66.7%) tehnologia digitală este foarte importantă, iar 33.9% dintre studenți consideră tehnologia digitală ca fiind destul de importantă, un procent mai mare decât ne-am fi așteptat în lipsa asocierii dintre variabile. Cu alte cuvinte, observăm că importanța percepută a tehnologiei digitale diferă în funcție de statutul socio-economic al utilizatorilor. Astfel, elevii sunt cei mai mulți care conferă o importanță ridicată sau foarte ridicată tehnologiei digitale, în timp ce mai mulți liber profesioniști și șomeri decât ne-am fi așteptat o consideră ca fiind puțin sau deloc importantă. Surprinzător este faptul că studenții consideră tehnologia digitală ca fiind foarte importantă într-un procent semnificativ mai mic (37.0%) și o consideră ca fiind puțin sau destul de importantă într-un procent mai ridicat (33.3%) decât era de așteptat. Interesant este și că în rândul angajaților nu există o tendință referitor la importanța percepută a tehnologiei digitale, întrucât răspunsurile acestora sunt omogene.

Referitor la tipul echipamentelor digitale utilizate, cel mai utilizat echipament este „*smartphone*”-ul, corespunzându-i un procent de 31.5% din totalul răspunsurilor și fiind folosit

de 83.3% dintre participanți. Acesta este urmat de laptop și calculator (PC), cu 28.6% și 22.2% din totalul răspunsurilor. Astfel, 75.7% respectiv 58.7% dintre participanți utilizează laptopul și PC-ul. Tableta este utilizată cel mai puțin (15.7% din totalul răspunsurilor), un procent de 41.7% dintre utilizatori folosind acest echipament. Un procent de 5.5% dintre utilizatori folosesc și alte echipamente, precum ceasurile inteligente, „*smart TV*”-urile, dronele, sau aparatele foto/video digitale. Datele arată că, în general, echipamentele digitale precum „*smartphone*”-ul, laptopul, PC-ul sau tableta sunt utilizate de către persoane de gen feminin și persoane de gen masculin în proporții asemănătoare, însă preponderent de către adulți sau tineri, elevi sau studenți, și persoane ce provin din mediul urban.

În ceea ce privește scopul utilizării tehnologiilor digitale, corespondenții au subliniat faptul că scopul utilizării acestor tehnologii moderne este dat de dorința și nevoia de utilizare a mediilor de comunicare și canalelor de socializare contemporane, cu 21.5% din totalul răspunsurilor și fiind ales de 80% dintre participanți. Monitorizând activitățile infracționale în mediul online din ultimii ani, am observat că vulnerabilizarea utilizatorilor de tehnologie modernă se face tocmai prin spargerea conturilor de utilizator pentru obținerea de informații și date confidențiale[38], personale și din păcate uneori chiar cu caracter clasificat.

Un procent de 70.5% dintre utilizatori folosesc echipamentele digitale în scop de relaxare/distracție, 67.6% le folosesc în scop informațional, 51.7% pentru corespondență, 50.8% le folosesc pentru achiziții sau servicii online, 48.1% le folosesc în scop profesional, iar 3.8% dintre participanți folosesc echipamentele digitale în alte scopuri. Tabelul nr.2 prezintă procentul în care echipamente digitale sunt utilizate în diverse scopuri, în funcție de variabilele socio-demografice. Astfel, majoritatea categoriilor socio-economice și demografice utilizează echipamentele digitale preponderent în scop de socializare, relaxare/distracție, sau în scop informațional.

Vârstnicii mai utilizează tehnologia digitală în scop de corespondență, iar studenții și angajații fac acest lucru și în scop profesional și de corespondență.

un procent de 46.1% dintre utilizatori au declarat că au oferit, prin constrângere, documente (67.7%), parole/conturi de acces (27.7%) și/sau informații cu caracter confidențial (29.4%).

Un procent de 57.8% din utilizatori au fost înștiințați, prin telefon sau e-mail că au câștigat un premiu/sumă de bani fără să fi participat la vreun concurs sau tombolă. Dintre aceștia, 83.5% au deschis mesajul, 14.6% au răspuns mesajului, 8.1% au urmat instrucțiunile din mesaj, iar 13.8% au șters mesajul.

O parte din acțiunile și caracteristicile descrise anterior sunt asociate cu variabile socio-demografice și/sau cu importanța percepută a securității informatice a utilizatorilor.

Surprinzător, dintre cei care consideră securitatea informatică ca fiind foarte importantă, un număr mai mare decât ne-am fi așteptat (44.6%) subscriu diferitelor cauze utilizând adresa de e-mail sau declară că au primit mesaje nesolicitate prin telefon sau e-mail prin care au fost

[38] Teodora Marinescu, MEDIAFAX 04.01.2019, „*Un grup de hackeri a spart conturile mai multor politicieni din Germania şi a publicat datele personale”*, https://www.mediafax.ro/externe/un-grup-de-hackeri-a-spart-conturile-mai-multor-politicieni-din-germania-si-a-publicat-datele-personale-17810355/foto, accesat astăzi 12.03.2019.

înștiințați că au câștigat un premiu sau o sumă de bani, fără să fi participat la vreo formă de concurs sau tombolă.

Mai mult, dintre cei care primesc astfel de mesaje sau e-mailuri, un număr mai mare decât ne-am fi așteptat deschid aceste mesaje deși declară că pentru ei securitatea informatică este foarte importantă (49.4% dintre utilizatorii care conferă o importanță ridicată securității deschid mesajele primite ceea ce ne spune că pe deoparte ori nu înțeleg noțiunea de securitate informatică pe deplin ori duc la împlinire acțiuni fără a raționa efectele și riscurile la care aceștia se supun. Totodată, majoritatea celor care deschid acest tip de mesajele, sunt elevi.

Dintre cei care susțin campanii umanitare sau sociale cu sume mici de bani, un procent destul de mare este dat de studenți (45.9%) sau angajați și care conferă o importanță ridicată sau foarte ridicată securității informatice.

În ceea ce privește divulgarea prin constrângere a parolelor / conturilor de acces, elevii prezintă un risc mai ridicat la acest capitol, un procent de 59.4% dintre cei care au declarat că au fost constrânși să divulge parole sau conturi de acces fiind elevi

Mai mulți elevi (47.3% dintre elevi) și tineri până în 20 de ani (48.6% dintre tineri) decât ne-am fi așteptat au în lista lor de contacte persoane pe care nu le cunosc.

Un procent de 36.6% dintre utilizatori au în cercul lor de prieteni persoane victime ale unor infracțiuni informatice, iar 17.8% dintre utilizatori au fost ei înșiși victime ale unor astfel de infracțiuni. Dintre aceștia din urmă, 66.6% au fost victimele infectării sistemului informatic cu aplicații și programe malițios intenționate, 35.2% au fost victimele furtului de date personale, iar 32.5% au fost victimele furtului de identitate.

În general, un risc mai ridicat de a deveni victime ale infracțiunilor informatice prezintă utilizatorii care: au în cercul lor de prieteni persoane care au fost victime ale unor infracțiuni informatice, împărtășesc aspecte din viața lor personală cu persoane necunoscute, încredințează date personale unor persoane străine, oferă copii după documente personale, oferă sau solicită ajutorul pentru utilizarea unui card bancar, dețin conturi online pe care le utilizează cu altcineva, primesc mesaje prin telefon sau e-mail că au câștigat un premiu sau sumă de bani fără să fi participat la vreun concurs sau tombolă.

Întrebați dacă cred că România este pregătită pentru un eventual val de atacuri cibernetice, semnificativ mai mulți utilizatori au răspuns în mod negativ (63.9%).

Printre motivele enumerate de aceștia se numără lipsa specialiștilor și a pregătirii profesionale în acest domeniu, lipsa fondurilor și a infrastructurii necesare, instabilitatea sistemului informatic sau o informare slabă despre securitatea informatică. Dintre utilizatori, semnificativ mai mulți cred că este importantă sau foarte importantă introducerea studiului securității informatice în mediul preuniversitar (65.7% dintre utilizatori) și în mediul universitar (72.9% dintre utilizatori). Aceste răspunsuri sunt asociate semnificativ statistic cu o importanță percepută foarte ridicată a securității informatice, atât în ceea ce privește introducerea acestor studii în mediul preuniversitar, cât și în mediul universitar.

Printre motivele pentru care utilizatorii cred că este importantă sau foarte importantă introducerea studiului securității informatice se numără protejarea identității și a datelor personale, cunoașterea riscurilor la care sunt expuși utilizatorii tehnologiilor informatice sau evitarea fraudelor și a escrocheriilor.

Urmând modelul cercetării calitative[39], este important de menționat faptul că în cadrul fiecărui interviu au fost evaluați un număr de 27 întrebări principale în complexitatea cărora au fost atinse un număr de 57 aspecte punctuale la care s-au răspuns prin aplicat chestionarul

CONSIDERAȚII FINALE

Limitări și direcții viitoare de cercetare

Guvernarea domeniului cibernetic în contextul de securitate european, este marcată de o evoluție strategică a reconstrucției europene. Concluzionez că domeniul cibernetic poate fi guvernat de state membre suverane într-o Uniune Europeană echilibrată între cele trei modele de guvernanță: „*guvernanță distribuită, guvernanță multilaterală și guvernanță de tipul multi-stakeholderismul”*.[40] Acest lucru nu exclude parteneriatele strategice ale țărilor membre sau ale Uniunii.

Datorată abordării metodelor de cercetare explorativă a securității domeniul cibernetic, sunt îndemnat să remarc faptul că buna guvernanță, percepută în contextul prezentei lucrări, este perfectibilă și încă departe de a fi un panaceu universal pentru dilema de securitate din spațiul cibernetic. În urma unei analize inductive a rezultatelor prezentei lucrări, identific realitatea necesității construcției unui forum pentru dezvoltarea unui nou model de bună guvernanță a arealului cibernetic prin asocierea cu această formă de guvernare a instituțiile și organismele guvernamentale, a sectorului privat și a actorilor societății civile. Sunt pe deplin încrezător că teza de față a deschis noi orizonturi de cercetare științifică a bunei guvernanțe în spațiul cibernetic. Odată cu motivația dată de identificarea acestor orizonturi, tangibile de altfel, precum și de atingerea în parte a obiectivelor propuse, intenționez ca rezultatele obținute în prezenta teză să reprezinte bazele unor extinderi a cercetării de față și să aduc în atenția comunității academice, noi perspective și rezultate ce privesc buna guvernanță a securității spațiului cibernetic.

Prin raportarea la celelalte patru arealuri strategice identificate, studiul bunei guvernanțe în spațiul cibernetic, reprezintă în momentul de față domeniul cel mai lacunar unde am identificat, în ceea ce privește securitatea națională, o deosebită nevoie de control democratic din partea societății civile, obținut în asentimentul instituțiilor supranaționale sau naționale. Problematica escaladării spiralei de securitate reprezintă mai departe pentru mine un punct de interes major, intenționând ca pe viitor să cercetez posibilități și ipoteze reale cu ajutorul cărora o nouă formă de bună guvernare a spațiului cibernetic să poată soluționa aspecte ale dilemei de securitate.

Finalmente, în ceea ce privește motivarea alegerii viitoarelor direcții de cercetare, un ultim argument este dat de abordarea strategică din ultimii zece ani pe care o nutresc asupra cercetării domeniului securității naționale în context cibernetic, prin capacitatea dinamică a celor trei elemente de a schimba direcția sau regulile în timpul „*jocului*”, anume: *progresul tehnologic, relațiile internaționale și securitatea*.

---

[39] Jonathan Grix, *Op. Cit.* , pp.27-30.

[40] Andrew N. Liaropoulos, Democracy and an Open-Economy World Order, „*Cyberspace Governance and State Sovereignty*”, Ed. Springer International Publishing AG, p.29, https://www.researchgate.net/publication/316040640_Cyberspace_Governance_and_State_Sovereignty, accesat astăzi, 07.05.2019.

Precizări referitoare la contribuțiile personale

Pornind de la înțelegerea unei necesități de imparțialitate din partea cercetătorului privind subiectul cercetării, m-am detașat de orice influențe ce ar putea afecta cursul natural și obiectiv al lucrării. Fără a contesta faptul că oricând, subiectivitatea, chiar și într-o măsură neglijabilă, poate să apară datorată naturii noastre umane și apartenenței la un anumit grup sau clasă socială, menționând că încă de la început, analiza și abordarea problematicii s-a desfășurat la un grad ridicat de dificultate, finalmente concretizându-se conform viziunii autorului, prin utilizarea unui mecanism propriu de analiză, sinteză și generare sistematică a rezultatelor confirmându-le prin verificarea acestora în lumina studiului comparativ. Pentru o mai bună conceptualizare și înțelegere a cercetării, elementele de noutate sunt expuse la finele fiecărui capitol, reiterând în cele ce urmează printr-o concluzie comună, privind întregul studiu.

Principalul element de noutate și originalitate adus domeniul de cercetare în care se înscrie teza de față este dat de obținerea unei relații de interdependență dintre cultura de securitate, nivelul de securitate națională existent și modalitatea de guvernanță a spațiului cibernetic.

Un element de noutate secundar este dat de construirea unui caz structurat pe demonstrarea argumentelor solid susținut de nivelul culturii de securitate din România raportat la managementul informațiilor vehiculate în mediul electronic pentru o bună guvernanță a spațiului cibernetic în context național și predominant european. Lipsa surselor bibliografice de specialitate orientate în direcția problematicii spiralelor de securitate cibernetică, oferă o validare a demersul meu, realizat sub atenta monitorizare a profesorilor coordonatori. Validarea și confirmarea acestui demers de cercetare explorativă, este dată și de obținerea de rezultate concrete, în favoarea ipotezei potrivit căreia dilema de securitate cibernetică este o sub dimensiune sau o terminologie hibridă, diferențiată de înțelesul uzual al dilemei de securitate prin transpunerea acesteia, conceptual, în contextul securității cibernetice.

În esență, prin asumarea rezultatelor cercetării dilemei de securitate cibernetică în perspectiva guvernanței spațiului virtual în conceptul realismului și supranaționalismului, înțeleg că, în următoarea decadă, până la apariția următoarei revoluții a tehnologiei în spațiul cibernetic, rolul organismelor publice și private, naționale și supranaționale, aste acela de a norma acest areal pentru diminuarea impactului adus de riscurile de securitate în toate mediile asupra cărora dilema de securitate își face simțită prezența. Deși este puțin probabilă o ofensivă militară de anvergură prin mediul cibernetic, apar din ce în ce mai des cazuri izolate cu un enorm impact financiar și de intimidare atât a personalităților juridice cât și a persoanelor care folosesc acest mediu. Analizând din perspectiva studiilor relațiilor internaționale, diplomația a ajuns la un nou prag, acela de transformare și capătă în portofoliu un noi domenii de interes, diplomația cibernetică și diplomația digitală care reprezintă în contextul globalizării, interfața statelor, care este și unul dintre sursele generatoare de securitate principale.

Un considerent final este cel cu privire la viitoarea obligativitate de neproliferare a capabilităților cibernetice cu potențial ostil. Prin exemplele date și studiul efectelor acestora asupra statelor și alianțelor, se confirmă parțial, posibilitatea identificată la nivel teoretic de utilizare a atacurilor cibernetice la nivel global în vederea producerii de efecte masiv dăunătoare din partea statelor. Cu toate acestea, sunt pe deplin încredințat că printr-o bună guvernanță și

creștere a capacității de reziliență cibernetică a sistemelor informaționale, la nivel global, și totodată printr-o participare activă a statelor, uniunilor, formelor federative și alianțelor în vederea armonizării și reglementării consensuale a acestui domeniu, se poate păstra indiferent de ideologia de guvernământ a statelor, un mediu cibernetic sigur și curat.

Firul central al viziunii autorului este dat de identificarea unei noi perspective asupra managementului securității spațiului cibernetic. Elementele de bază ale acestei noi perspective sunt evidențiate atât prin cuvintele cheie de la începutul lucrării cât și definitoriu, în conținutul capitolelor prezentei teze. Desigur, în viziunea autorului, această perspectivă, reprezintă un cadru de analiză nou și un element de noutate care poate aduce o lumină asupra viitoarelor direcții de cercetare în domeniul științelor relațiilor internaționale și studiilor de securitate.

De asemenea, în contextul prezentei lucrări, datorită caracterului multidisciplinar al acesteia, această nouă perspectivă de analiză mai sus menționată, consider că își poate aduce aportul în identificarea unor noi provocări în domeniul cercetării și studiilor de diplomatice și a celor din aria științelor comunicațiilor și tehnologiei informației.

Tratarea temei alese a fost inițial studiată și cercetată cu scopul de a aduce în completare din punct de vedere științific a cunoștințelor comunității academice și de a încerca să transpună problematică prin prisma conceptelor realismului și a supranaționalismului. Validarea studiului este desigur lăsată la latitudinea criticilor și în speranța unor reacții constructive dorința autorului este de a dezvolta în parte sau în întregime subiectul de cercetare ales.

BIBLIOGRAFIE

Dat fiind volumul considerabil crescut de materiale bibliografice utilizat pe parcursul studiului, în cele ce urmează vor fi enumerate cele mai importante resurse bibliografice relevante temei de cercetare.

CĂRȚI (*inclusiv ediții electronice*)

- Adrian V. Cămărășan, Informații clasificate – Note de curs, Ed. CA Publishing, Cluj-Napoca, 2014.
- Adrian-Liviu Ivan, Colecţia Studii Europene, „Statele Unite ale Europei: Uniunea Europeană între interguvernamentalism şi supranaţionalism”, Editura Institutul European Iaşi, Iași, 2007.
- Alexandra Sarcinschi, „Elemente noi în studiul securităţii naţionale şi internaţionale”, Editura Universităţii Naţionale de Apărare, Bucureşti, 2005.
- Andreas Schmidt, The fierce domain –conflicts in cyberspace 1986-2012, „The Estonian Cyberattacks”, Ed. Atlantic Council, Washington, D.C, 2013.
- Annette Freyberg-Inan, What Moves Man: The Realist Theory of International Relations and Its Judgement of Human Nature, Ed. State University of New York Press, Albany, SUA, 2004.
- Anișoara Duică, Management, Ediția a II-a (revizuită și adăugită), Ed. Bibliotheca, Târgoviște, 2008.
- Anthony J.S. Craig, Brandon Valeriano, „Realism and Cyber Conflict: Security in the Digital Age”, Ed. E-INTERNATIONAL RELATIONS PUBLISHING, Bristol, Anglia, 2018.
- Arnold Wolfers, Political Science Quarterly, Vol.67, Nr. 4, „National Security as an Ambiguous Symbol”, Ed. Academy of Political Science, New York, SUA, 1952.
- Barry Buzan, „Popoarele, statele şi teama. O agendă pentru studii de securitate internaţională în epoca de după Războiul Rece”, Ed. Cartier, Chișinău, 2000.
- Barry Buzan, Ole Wæver, Jaap de Wilde, „Securitatea. Un nou cadru de analiză”, Ed. CA Publishing, Cluj-Napoca, 2011.
- Bogdan Băcanu, „Organizați publică – Teorie și management”, Ed. Polirom, Iași, 2008.
- Cavelty Myriam Dunn, „Cyber-Security and Threat Politics: US efforts to secure the information age”, CSS Studies in Security and International Relations, Prima Ediție, Ed. Routledge, London, UK, 2008.
- Ciprian Nițu, „Cosmopolitismul-Către o nouă paradigmă în teoria politică”, Ed. Adenium, Iași, 2014.
- Clarke A.Richard, Robert K. Knake, „Cyber War: The Next Threat to National Security and What to Do About It”, New York: Ecco, SUA, 2010.
- Clifford Paul Stoll, „The Cukoo's Egg: Tracking a Spy Through the Maze of Computer Espionage”, New York, Doubleday, 1989.
- Colin Robson, „Real World Research: A resource for Social Scientists and Practitioner-Researchers”, Cap. II.6. Flexible Design, Ediția a-II-a, Anglia, Ed. Blackwell Publisher, Oxford, 2002.
- David Wright-Neville, „Dicționar de Terorism”, Traducere Sorina Pricop, Ed. CA Publishing, Cluj-Napoca, 2010.
- Dumitru Oprea, „Protecția și securitatea informațiilor”, Ediția a II-a, Ed. Polirom, Iași, 2007.
- George Christou, New Security Challenges, „Cybersecurity in the European Union - Resilience and Adaptability in Governance Policy”, Ed. Palgrave Macmillan, 2016.

- Georgeta Chirlesan , „Strategia de securitate naţională a României: evoluţii şi tendinţe între securitatea regională şi cea euro-atlantică”, Editura Academiei Forțelor Terestre „Nicolae Balcescu”, Sibiu, 2013.
- Gheorghe Ilie, „De la management la guvernare prin risc”, Ed. Detectiv/Ed. UTI Press, București, 2009.
- Gheorghe Ilie, Ion Ciobanu, Aurel Nour, „Confruntarea informațională și protecția informațiilor”, Ed.Detectiv, București, 2006.
- Gheorghe Ilie, „Riscul-Măsura Incertitudinii – Elemente conceptuale, corelații și determinări” -, Ed. UTI Press, București, 2011.
- Ioana Vasiu, Lucian Vasiu, Criminalitatea în cyberspațiu, Ed. Univers Juridic, București, 2011.
- Ioana Vasiu, Lucian Vasiu, Informatică Juridică și Drept Informatic, Editura Albastră, Cluj-Napoca, 2009.
- Ionel Nițu, „Analiza de Intelligence, O abordare din perspectiva teoriilor schimbării”, Ed. Rao, București, 2012.
- Jervis Robert, World Politics, Vol.30, Nr.2, „Cooperation Under the Security Dilemma”, Ed. The Johns Hopkins University Press, 1978.
- Jonathan Grix, „Demistificarea cercetării postuniversitare: De la masterat la doctorat”, Traducere de Nicolae Melinescu, Ed. CA Publishing, Cluj-Napoca, 2014.
- Lillian Ablon, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, Julia A. Thompson, PE-329-NATO, „Operationalizing Cyberspace as a Military Domain: Lessons for NATO”, Ed. RAND Corporation, Santa Monica, USA, 2019.
- Mary Kaldor, „Securitatea Umană”, Ed. CA Publishing, Cluj-Napoca, 2010.
- Mihaela Vlăsceanu, Organizația: proiectare și schimbare – Introducere în comportamentul organizațional, Ed. Comunicare.ro, București, 2005.
- Morgenthau Hans J., ”Politics among Nations: The Struggle for Power and Peace”, New York, Ed. Alfred A. Knopf, 1949.
- Nasty Vlădoiu, „Protecţia Informaţiilor, De la concept la implementare”, Ed. Tritonic, București, 2005.
- Martin Griffiths, „Relaţii internaţionale. Şcoli, curente, gânditori”, Traducere: Cristea Darie, Popistaşu Olga, Barna Cristian, Editura Ziua, Bucureşti, 2003.
- Mireille Rădoi, Serviciile de informații și decizia politică, Ed. Tritonic, București, 2003.
- Norman Blaikie, Colecția Sociologie, „Modele ale cercetării sociale: Producerea cunoașterii”, Ediția a II-a, (Trad. Coca Vieru, Ana Gruia), Ed. CA Publishing, Cluj-Napfoca, 2010.
- Nye Joseph S., „The Future of Power”, New York, Ed. Public Affairs, 2011.
- Nye Joseph S., Foreign Policy, Nr.80, “Soft Power”, Washington, Ed. Washingtonpost, Newsweek Interactive, LLC, 1990.
- Ole Wæver, „Securitization and Desecuritization’, Rev. Ronnie D. Lipschutz „On Security”, Ed. Columbia University Press, New York, 1995.
- Paul Robinson, „Dicționar de securitate internațională”, Traducere Monica Neamț, Ed. CA Publishing, Cluj-Napoca, 2010.
- Penelope Hartland-Thunberg, National Economic Security: Perceptions, Threats, and Policies: “National Economic Security: Interdependence and Vulnerability”, Ed. John F. Kennedy Institute, Olanda, 1982.
- Robert K. Yin, „Case Study Research: Design and Method, Ediția a-V-a”, SUA, California, Thousand Oaks, Ed. SAGE Publications, 2014.

- Rid Thomas, „Cyber War Will Not Take Place" Londra, UK, Ed. C Hurst & Co Publishers Ltd., 2013.
- Russett Bruce, John Oneal, Triangulating Peace, Democracy, Interdependence, and International Organizations, New York-Londra, Ed. W.W. Norton & Company, 2001.
- Senese Paul D., John A. Vasquez, „The Steps to War: An Empirical Study", Ed. Princeton University Press, Princeton, SUA, 2008.
- Shaun Riordan, „The Strategic Use of Digital and Public Diplomacy in Pursuit of National Objectives", Ed. Top Open Printing Sytems S.L., Barcelona, 2016.
- Thomas L. Friedman, „The Lexus and the Olive Tree – Understanding Globalization", Ediția revizuită, Ed. Farrar, Straus and Giroux, New Yok, SUA, 2000.
- Țicu Dorina, „Politicile publice. Raționalitate și decizie în spațiul administrativ", Ed. Adenium, Iași, 2014.
- Vasquez A. John, „The War Puzzle", revizuită de Thomas B. Mackie, Cambridge, Cambridge, Ed. Cambridge University Press, 1993.
- Waltz Kenneth N., „Theory of International Politics", Londra, Ed. Addison-Wesley Publishing Company, 1979.

ARTICOLE ȘTIINȚIFICE ȘI CAPITOLE ÎN CĂRȚI (*inclusiv ediții electronice*)

- Adrian Liviu-Ivan, Hello World!: Contemporaneitate și provocările globalizării, CRIISS/1, „Constructivismul și Integrarea Europeană: Contribuții și Limite", Ed. CA Publishing, Cluj-Napoca, 2014, p.146.
- Alexander Klimburg, Hugo Zylberberg, NUPI Report nr.6, "Cyber Security Capacity Building: Developing Access", Ed. Norwegian Institute of International Affairs, Oslo, Norvegia, 2015, p.23.
- Alexandru Nicolae CLAIN, Revista „Continuitate și schimbare în guvernanța europeană", Vol. 4, Nr. 1, „Consiliul Europei – instituţie supranaţională sau conferinţă interguvernamentală?", p.14, http://europolity.eu/wp-content/uploads/2014/05/Vol.4.1.-2010.pdf, accesată astăzi 04.05.2019.
- Andreea-Maria Tirziu, MPRA Munich Personal RePEc Archive, „Protection and security of information at the level of national public authorities from Romania", p.127, https://mpra.ub.uni-muenchen.de/77711/1/MPRA_paper_77711.pdf, accesat astăzi 14.03.2019;
- Andrew N. Liaropoulos, Democracy and an Open-Economy World Order, „Cyberspace Governance and State Sovereignty", Ed. Springer International Publishing AG, p.29, https://www.researchgate.net/publication/316040640_Cyberspace_Governance_and_State_Sovereignty, accesat astăzi, 07.05.2019.
- Anthony Craig, Brandon Valeriano, „Conceptualising cyber arms races", 8th International Conference on Cyber Conflict (CyCon), Ed. NATO CCD COE Publication, Tallin, 2016.
- Anton Rog, Cristian Condruț, Intelligence în serviciul tău, Nr.38, „Evoluția amenințării cibernetice", Ed. SRI, București, 2019, pp.10-11.
- Aurelia PERU-BALAN, Vitalina BAHNEANU, MOLDOSCOPIE, Nr.1, Vol. LXXX, Războiul informațional, Propaganda, Fake-News: Controlul asupra percepției publice, Chișinău, 2018, pp.129-131.
- Arquilla John, Ronfeldt David, „Comparative Strategy", Vol.12, Nr.2, "Cyberwar is Coming!", 1993, pp.141–165.
- Aseema Sinha, International Studies Review, Vol. 20, Nr. 2, „Building a Theory of Change in International Relations: Pathways of Disruptive and Incremental Change in World Politics", Ed. Oxford University Press, Oxford, Regatul Unit, 2018, pp.195–203.

- Avidit Acharya, Kristopher W. Ramsay, Quarterly Journal of Political Science, "The Calculus of the Security Dilemma", Vol. 8, nr. 2, Princeton, USA, 2013, pp. 184-185.
- Babak Bashari Rad, Nafisseh Akbarzadeh, Pouya Ataei, Yasaman Khakbiz, International Journal of Control Theory and Applications, Vol. 9, nr.43, „Security and Privacy Challenges in Big Data Era", 2016, pp.438-441, https://www.researchgate.net/publication/327111196, accesat astăzi 11.08.2019.
- Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) „Cyber Resilience – Fundamentals for a Definition". In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353, Ed. Springer, Cham, pp.311-312;
- Brandon Valeriano, International Interactions Vol. 35, Nr.2, „The Tragedy of Offensive Realism: Testing Aggressive Power Politics Models", Londra, Anglia, 2009, Ed. Routledge Taylor&Francis Group, p.180.
- Cătălina Todor, Strategic Impact, Vol.63, Nr.2, „The topicality of security dilemma's spiral model in analysing the international environment", București, 2017, Ed. "Carol I" National Defence University Publishing House, p.25.
- Charles L. Glasser, The Perils of Anarchy: Contemporary Realism and International Security, „Realists as Optimists: Cooperation as Self-Help", Ed. The MIT Press, Massachusetts, 1995, pp.336-340.
- Charles L. Glaser, Chaim Kaufmann, International Security, Vol. 22, nr. 4, „What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics)", 1998, Massachusetts, Ed. Massachusetts Institute of Technology, p.44.
- Corneliu Bjola, Global Affairs, Vol.2, Nr.3, Digital diplomacy – the state of the art, Ed. Routledge Taylor & Francis Group, 2016, https://doi.org/10.1080/23340460.2016.1239372, pp.297-298.
- Cristian Niță, Securitatea Naţională – O Perspectivă Academică, p.3, http://www.nos.iem.ro/bitstream/handle/123456789/33/4.1.Sec%20Academic%20nita.pdf?sequence=1&isAllowed=y, accesat astăzi 30.07.2019.
- Cristopher Daase, Theories of International Relations, „The English School", Ed. Routledge Taylor & Francis Group, Londra, 2014, pp.150-151.
- Damien van Puyvelde, Stephen Coulthart, Shahriar M. Hossain, International Affairs Vol. 93, Nr.6 „Beyond the buzzword: big data and national security decision-making", https://doi.org/10.1093/ia/iix184, 2017, p.1400.
- Deborah J. Bodeau, Richard Graubart, MITRE Tehnical Report (2011), "Cyber Resiliency Engineering Framework", Bedford, Massachusetts, SUA, 2011, p.37.
- Dumitru Iancu, Anuarul Academiei Fortelor Terestre "Nicolae Balcescu", Informaţia– Sursã de avantaj concurenţial, 2007, http://www.armyacademy.ro/biblioteca/anuare/2007/a21.pdf, accesat astăzi 23.07.2019.
- Emily Goldman, John O.Arquilla, Defense Analysis, „Cyber Analogies", Ed. Naval Postgraduate School, Monterey, California, 2014, http://hdl.handle.net/10945/40037, accesat astăzi 05.05.2019.
- Erica Moret, Patryk Pawlak, Brief SSUE, 24/2017, „The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf, accesat astăzi 04.03.2019;
- Eriksson Johan, Giampiero Giacomello, International Political Science Review Vol. 27, nr. 3,"The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", 2006, pp. 228–229.

- Fredrik Björck, Martin Henkel, Janis Stirna, Jelena Zdravkovic, New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing, Vol.353, „Cyber Resilience – Fundamentals for a Definition", Ed. Springer, Cham, 2015, p.313.
- George-Marius Șinca, AGORA International Journal of Juridical Sciences, Nr.1, „Cibercriminologia - O analiză succintă a fenomenului de tranziție de la criminalitatea tradițională la cibercriminalitate", Oradea, 2015, p.66.
- George-Marius Șinca, De la Elitele Securității la Securitatea Elitelor, „Managementul Elitelor în Managementul Riscurilor Cibernetice", Ed. Presa Universitară Clujeană, Cluj-Napoca, 2017, pp.65-82.
- Georgeta Ghenghea, Zinaida Stratan, Natalia Zavtur, Impactul culturii informaţiei asupra utilizatorilor doctoranzi (studiu de caz), pp.42-45, 2019, http://repository.utm.md/handle/5014/1667, accesat astăzi 23.07.2019.
- Gortzak Yoav, Haftel Z. Yoram, Kevin Sweeney, Journal of Conflict Resolution Vol. 49, Nr.1, "Offense-Defense Theory: An Empirical Assessment", Ed. Sage Publications, Inc., Ohio, SUA, 2005, pp.67–89.
- Harald Cramér, Capitolul 2. Linear Point Sets, „Mathematical Methods of Statistics", Ed. Princeton University Press, 1946, SUA, Princeton, pp.10-14;
- Ilan Manor, Elad Segev, Ronit Kampf, The Hague Journal of Diplomacy Vol.10, nr.4, „Digital Diplomacy 2.0? A Cross-national Comparison of Public Engagement in Facebook and Twitter", DOI: 10.1163/1871191X-12341318, Haga, 2015, p.331.
- Iulian Popa, Teză de doctorat: „Securitatea și guvernanța spațiului cibernetic contemporan", Universitatea Babeș-Bolyai, Școala doctorală „Relații internaționale și studii de securitate", Cluj-Napoca, 2015, pp.133-134.
- Iulian F. Popa, Globalizare. Identitate. Securitate, Metoda scenariilor în analiza informațiilor de securitate națională. Studiu teoretic-aplicativ, Cluj-Napoca, CA Publishing, 2015, pp. 157-178.
- Ivan Adrian-Liviu, Transylvanian Review of Administrative Sciences, Vol.4, Nr.22, „Governance and "European Constitution", 2008, p.79, http://rtsa.ro/tras/index.php/tras/article/view/382/372, accesat astăzi 30.04.2019.
- Jeffrey W. Taliaferro, International Security, Vol.25, Nr.3, Security Seeking under Anarchy: Defensive Realism Revisited, Ed. The MIT Press Journals, Massachusetts, 2000, p.128-161, https://www.mitpressjournals.org/doi/10.1162/016228800560543, accesat astăzi 05.05.2019.
- Joyce, A. L., Petit, F. D., Phillips, J. A., Nowak, L. B., Evans, N. J., Raport Tehnic OSTI.gov, „Cyber Protection and Resilience Index: An Indicator of an Organization's Cyber Protection and Resilience Program", Global Security Sciences Division, Argonne National Laboratory, SUA, 2017, https://publications.anl.gov/anlpubs/2018/03/140164.pdf, accesat astăzi 05.05.2019.
- Kristin M. Lord, Travis Sharp, Vol.1, America's Cyber Future, Security and Prosperity in the Information Age, Ed. Center for a New American Security, Washington, DC, SUA, 2011, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf, accesat astăzi 05.05.2019.
- Léon Bottou, Frank E. Curtis, Jorge Nocedal, Vol. 60, Nr. 2, „Optimization Methods for Large-Scale Machine Learning", https://doi.org/10.1137/16M1080173, SIAM Review, 2018, pp. 223-311;

- Lieber Keir, Cyber Analogies, "The Offense-Defense Balance and Cyber Warfare", Monterey, California, SUA, 2014, Ed. Calhoun: Institutional Archive of the Naval Postgraduate School, p.96.
- Lori Murray, John Budenske, Shubhagat Gangopadhyay, Robert K.Finstad, Proceedings of the SPIE Defense + Security, Vol.10651, „Cyber resilience and integrity self-awareness of mobile autonomous systems", Orlando, Florida, SUA, 2018, p.8, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10651/2307854/Cyber-resilience-and-integrity-self-awareness-of-mobile-autonomous-systems/10.1117/12.2307854.short?SSO=1, accesat astăzi, 01.05.2019.
- Mearsheimer John Joseph, International Relations Theories: Discipline and Diversity, "Structural Realism". revizuit de Tim Dunne, Milja Kurki, Steve Smith, Oxford, Anglia, Ed. Oxford University Press, 2006, pp.71–88.
- Radu-Sebastian Ungureanu, Radu-Alexandru Cucută, New Challenges to the Balkan Security - Thematic Collective Book, Vol.3, „EUROPENIZATION AS A HEGEMONIC PROJECT: EU INFLUENCE IN APPROACHING THE SECURITY ISSUES IN THE BALKANS", Ed. Ivis, Veliko Târnovo, Bulgaria, 2016, p.169.
- Teodor Frunzeti, Cristian Bărbulescu, Academia Oamenilor de Știință din România, Cultura de securitate și reziliența națională la amenințările hibride , Reziliența național la amenințările hibride și cultura de securitate. Un cadru de analiză., p.4, http://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf, accesat astăzi 23.07.2019.
- Theodor Mitu, Daniela Mitu, Revista Română de Studii de Intelligence, nr. 4, „OSINT – la grania dintre secret și public", București, Ed. Serviciul Român de Informații, 2010, pp.42-43.
- Valeriano Brandon, Ryan C. Maness., „Cyber War versus Cyber Realities: Cyber Conflict in the International System", New York, SUA, Ed. Oxford University Press, 2015, pp.164-187.
- Vasquez John, „The American Political Science Review", Vol.91, Nr.4, "The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition", 1997, pp.899–912.
- Vesa Kanniainen, HECER Discussion Paper No. 424, „Cyber Technology and the Arms Race", Helsinki, 2018, pp.1-2.
- William Arthur Conklin, Dan Shoemaker, The EDP Audit, Control, and Security Newsletter, Vol.55, Nr.2 "Cyber-Resilience: Seven Steps for Institutional Survival", Ed. Taylor & Francis Group, 2017, pp. 14-22.
- Wojciech Samek, Klaus-Robert Műller, Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, LNAI11700, DOI.ORG/10.1007/978-3-030-28954-6, „Towards Explainable Artificial Intelligence", Ed. Springer, Elveția, Cham, 2019, pp.8-9.
- Cristian Barna, Intelligence, Nr.35, „Pregătire și formare în societatea cunoașterii.", București, 2017, Serviciul Român de Informații, pp.26-27.
- EEAS, Strategie globală pentru politica externă și de securitate a Uniunii Europene, http://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf, accesat astăzi 04.07.2018