UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

Facultatea de Istorie și Filosofie
Str. M. Kogălniceanu nr. 1
Cluj-Napoca, 400084
Tel.: 0264 405 300 int.5275
Fax: 0264 405 326
hiphi@ubbcluj.ro
hiphi.ubbcluj.ro

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

Securitatea cibernetică a infrastructurii critice în relațiile internaționale. Studiu de caz: sectorul sănătății din România

REZUMATUL TEZEI DE DOCTORAT

Conducător de doctorat
Prof. univ. dr. Adrian-Liviu Ivan

Student-doctorand
Darius-Antoniu Ferenț

Cluj-Napoca
2026

CUPRINS

Cuvinte-cheie: securitate cibernetică, infrastructură critică, infrastructură IT&C, ransomware, sistem informatic, război cibernetic, apărare cibernetică, securitate națională, securitate internațională, puterea cibernetică, cultură de securitate, criminalitate cibernetică, Man-in-the-Middle.

Securitatea cibernetică este, în prezent, o preocupare pentru indivizi, organizații, companii și state, iar atacurile informatice asupra infrastructurilor critice reprezintă o constantă și o problemă gravă pentru securitatea națională. Tema de cercetare se încadrează în domeniul vast al studiilor de securitate, fiind situată la granița dintre această arie și științele din sfera IT&C (Tehnologiei informației și comunicațiilor).

În literatura de specialitate națională și internațională, securitatea cibernetică are o multitudine de definiții. Cu toate acestea, am ales să utilizez în cadrul cercetării următoarea definiție: Securitatea cibernetică reprezintă „o colecție de instrumente, politici, concepte de securitate, măsuri de securitate, linii directoare, managementul riscurilor, acțiuni, instruire, bune practici și tehnologii care pot fi utilizate pentru a proteja spațiul cibernetic și organizația împreună cu toate bunurile utilizatorilor."[1]

În cadrul cercetării științifice am utilizat atât metode cantitative, cât și calitative. Un avantaj al cercetării cantitative este că întregul demers științific este verificabil și devine obiectiv și legitim. Cercetarea cantitativă este utilă din punct de vedere științific, deoarece dezvoltă informații concrete și înglobează testarea ipotezelor de cercetare și/sau a teoriilor, identificarea unor relații între variabile și schițarea unei prognoze bazate pe rezultate veridice.[2] Adepții metodei cantitative caută frecvent corelații între variabile, dar, de obicei, au rețineri să treacă de la declarații de corelare la declarații cauzale din cauză că întreaga complexitate a vieții sociale face dificilă certitudinea deplină că o anumită variabilă este singura cauză a unui anumit fenomen.[3]

Cercetarea cantitativă s-a bazat pe realizarea unui chestionar, prin care să evidențiez nivelul culturii de securitate cibernetică a angajaților Spitalului Clinic Județean de Urgență Cluj-Napoca (SCJU Cluj). De asemenea, am studiat o parte din literatura de specialitate care abordează domeniul securității cibernetice. Cercetarea calitativă s-a bazat pe realizarea unui studiu de caz, în care am demonstrat faptul că atacurile cibernetice de tip ransomware lansate de grupările de criminalitate informatică sunt foarte periculoase pentru organizații, iar dezvoltarea culturii de securitate

[1] International Telecommunication Union (ITU-T), *Series X: Data networks, open system communications and security. Telecommunication security*, Overview of cybersecurity, ITU-T X.1205, aprilie 2008, p.2.
[2] Edward Barroga, Glafera Janet Matanguihan, „A Practical Guide to Writing Quantitative and Qualitative Research Questions and Hypotheses in Scholarly Articles", în *Journal of Korean Medical Science*, 12 aprilie 2022, disponibil la https://jkms.org/pdf/10.3346/jkms.2022.37.e121, accesat în 25 august 2023.
[3] Charles Ragin, Lisa Amoroso, *Constructing Social Research. The Unity and Diversity of Method*, Editura Thousand Oaks, London, 2011, p.4.

cibernetică a utilizatorilor finali/angajaților din cadrul instituțiilor medicale din România este o condiție esențială pentru a preveni materializarea unui atac de tip ransomware. Mixul metodologic cantitativ-calitativ constituie cea mai potrivită abordare a tematicii acestei lucrări. Principalul avantaj al acestei metode vizează reprezentativitatea datelor obținute. Acestea reprezintă cel mai bine opinia întregii populații investigate. O limită a metodei de cercetare o reprezintă agregarea opiniilor unor persoane cu experiențe diferite în ceea ce privește utilizarea echipamentelor informatice și securitatea cibernetică a acestora.

Având în vedere interesul ridicat al instituțiilor, companiilor, statelor și organizațiilor internaționale de a asigura securitatea cibernetică a infrastructurii de tehnologia informației și numărul redus al cercetărilor științifice din spațiul românesc care abordează chestiunea securității cibernetice în infrastructurile naționale și europene din sectorul sănătate, am optat pentru un aparat metodologic care mi-a permis îmbinarea eficientă a aspectelor teoretice și științifice din domeniul studii de securitate cu o cercetare empirică bazată pe studii de caz și analize de specialitate, realizate prin studierea surselor primare, secundare și terțiare. În scopul obținerii unor date relevante, am avut în vedere explorarea relațiilor cauzale și interdependența dintre riscurile, amenințările și fenomenele din spațiul cibernetic, realizarea de analize SWOT, utilizarea analizei structurale și comparative, instrumentar care a favorizat obiectivitatea științifică. Am considerat oportun ca o mare parte a acestei lucrări să se bazeze pe un fundament empiric consistent, care să sublinieze clar noutatea cercetării și contribuția personală adusă la dezvoltarea domeniilor studii de securitate și relații internaționale.

Pentru a atinge obiectivele de cercetare ale acestei lucrări am utilizat atât cărți de specialitate din domeniile securitate cibernetică, relații internaționale și studii de securitate, cât și articole științifice valoroase care abordează problematica securității infrastructurilor cibernetice critice și criminalitatea informatică.

Elementele de originalitate ale cercetări mele sunt reprezentate de expunerea unei potențiale matrice prin care s-ar putea identifica atacurile cibernetice și clasificarea acestora în funcție de intensitate și impact. În aceeași notă a caracterului de originalitate, studiul de față a prezentat „tabloul” unei diagnoze de securitate cibernetică a sistemelor informatice din cadrul Spitalului Clinic Județean de Urgență Cluj-Napoca, pe baza datelor și informațiilor colectate privind sistemele IT&C și rețeaua de calculatoare a instituției (au fost colectate doar date care nu sunt confidențiale pentru organizația menționată). În plus, am stabilit nivelul culturii de securitate cibernetică al angajaților SCJU Cluj-Napoca.

De asemenea, am realizat o analiză SWOT a modului de operare (modus operandi) a unei grupări de criminalitate cibernetică autohtone care a lansat atacuri cibernetice (cu impact minor) și

dorea afectarea infrastructurii IT&C a unor instituții medicale din România, prin desfășurarea unor atacuri de tip ransomware (atacuri cibernetice cu impact major). Gruparea aleasă a fost PentaGuard. Totodată, am evidențiat un modus operandi al hackerilor care lansează atacuri cibernetice de tip MitM (Man-in-the-Middle), deoarece rezultatele chestionarelor aplicate angajaților Spitalului Clinic Județean de Urgență Cluj-Napoca, au arătat că terminalele cibernetice ale acestor utilizatori sunt vulnerabile la atacurile de tip Man-in-the-Middle.

De asemenea, am definit cele trei tipuri de infrastructuri de pe teritoriul României (infrastructuri obișnuite, infrastructuri speciale și infrastructuri critice), urmărind să formulez definiții cât mai exhaustive, ceea ce nu s-a regăsit în literatura de specialitate aferentă domeniilor studii de securitate și relații internaționale.

În cadrul lucrării am demonstrat faptul că puterea cibernetică a unui actor statal se referă la capabilitățile sale de apărare cibernetică, dar și la capacitățile și capabilitățile ofensive necesare desfășurării de operații în rețelele de calculatoare ale adversarului, inclusiv spionaj cibernetic, capacitatea de a compromite rețelele de date și sistemele IT&C ale inamicului și de a prelua controlul de administrator asupra terminalelor cibernetice, prin rootkit-uri sau troieni. În plus, am realizat reprezentarea grafică a locului războiului cibernetic în gradația intenistății atacurilor cibernetice. În cadrul războiului cibernetic, un actor statal poate să afecteze securitatea națională a adversarului prin întreruperea pentru o perioadă de timp a funcționării unei componente a infrastructurii esențiale sau critice (de exemplu, sistemele informatice ale instituțiilor din sectorul sănătate).

Securitatea a devenit un ingredient necesar în foarte multe sectoare de activitate și a evoluat în ultimul deceniu ca un răspuns la riscurile și amenințările generate de globalizarea societății contemporane. Evoluția rapidă a tehnologiilor au adus în atenția specialiștilor, practicienilor dar și decidenților politici concepte precum: protecția infrastructurilor cibernetice critice, securitate fără frontiere, cloud computing, securitatea informațiilor electronice.[4]

În mediul academic, dezbaterile și discuțiile despre aceste dimensiuni/sectoare ale securității sunt numerose, iar orice perspectivă și cercetare științifică nouă determină noi descoperiri și implicații asupra securității indivizilor, comunităților umane și statelor. Acest fapt poate fi explicat prin natura și diversitatea riscurilor și amenințărilor de securitate. Cele cinci dimensiuni sau sectoare identificate de Barry Buzan au un rol analitic, urmând descompunerea „securității naționale a statelor" în elemente mai mici, de natură a o face mai ușor de discutat, în funcție de ceea ce o societate consideră că este periculos.[5] Securitatea națională a unui stat trebuie privită pe toate palierele sale:

4 Tiberiu Tănase (coord.), Șerban-Dan Predescu, Petru Ștețcu, *Managementul securității informațiilor - suport de curs*, Editura Concordia, Arad, 2022, p.86.

5 J Baylis, „International and global security", *The Globalization of World politics An introduction to international relations*, Sixth edition, Baylis, Smith, Owens (coord.), Oxford University, 2014, p.231.

apărarea militară a țării, securitatea energetică, securitatea economică, ordinea și siguranța publică sau securitatea cibernetică a infrastructurilor speciale și critice.

Secolul XXI se caracterizează prin implementarea securității cibernetice în agenda de securitate națională a statelor, fiind privită drept un pilon vital în menținerea status-quo-ului unui actor statal.[6] Securitatea națională a statelor tinde să fie privită drept o responsabilitate a guvernelor și depinde de politicile interne și externe, de capabilitățile militare, dar și de eficiența serviciile de intelligence în zona de desfășurare a acțiunilor informativ-operative și procesarea informațiilor, pentru obținerea produsului analitic de intelligence. Cu toate acestea, protecția și securitatea infrastructurilor critice ale unei țări trebuie privite drept o responsabilitate partajată între state, deoarece un singur guvern nu poate asigura în totalitate protecția necesară acestor categorii de infrastructuri.[7] În plus, atât susținerea angajamentului actorilor non-statali (firme, companii, instituții, organizații, indivizi) în asigurarea securității rețelelor proprii de calculatoare, cât și încercările pe plan național și internațional de a proteja spațiul cibernetic, au același nivel de importanță.[8]

Joseph Nye oferă o descriere cu privire la distribuția puterii între națiuni, pe care o analizează sub forma unui „joc de șah tridimensional complex". Cele trei table de șah sunt reprezentate de către un actor statal diferit, fiecare punând accentul pe o dimensiune diferită. În viziunea lui Joseph Nye, prima tablă de șah este reprezentată de dimensiunea militară, care este preponderent unipolară, fiind concentrată pe un singur pol de putere (SUA). Tabla de șah din mijloc este reprezentată de dimensiunea economică, care este multipolară, puterea fiind distribuită mai multor actori statali sau poli de putere (SUA, Uniunea Europeană, Japonia și China). Cea de a treia tablă de șah este reprezentată de dimensiunea relațiilor transnaționale, care a trecut de frontierele naționale ale statelor și a scăpat de controlul guvernamental, în această categorie încadrându-se actori statali de diferite tipuri, printre care și grupările de criminalitate cibernetică sau hackerii.[9]

Joseph Nye face, în cartea sa „Viitorul Puterii" (2011), câteva precizări și completări noi, față de ideile menționate cu un an în urmă, în lucrarea „Cyber Power". Apreciem că modificările aduse de autor se află în concordanță cu evoluțiile din mediul de securitate internațional specific secolului XXI. Nye subliniază ideea difuzării puterii, mai ales a „puterii cibernetice" către alți actori, în afară de statul națiune.[10] „Puterea cibernetică reprezintă capacitatea de a obține rezultatele așteptate, prin

6 Ionela Maria Ciolan „Defining cybersecurity as the security issue of the twenty first century. A constructivist approach", în The Public Administration and Social Policies Review, VI, 1(12), iunie 2014, p.122, disponibil la https://revad.uvvg.ro/files/nr12/8.Ionela_Ciolan.pdf, accesat în 22 iulie 2023.

7 J. Eriksson, G. Giacomello, „The Information Revolution, Security and International Relations: (IR)relevant Theory?", în International Political Science Review, 27(3), 2006, pp.221-244.

8 Ionela Maria Ciolan, op.cit., p.132.

9 Joseph Nye, „Cyber Power", Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, mai 2010, disponibil la https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf, accesat în 22 iulie 2023.

10 Joseph Nye, Viitorul puterii, Editura Polirom, Iași, 2012, p.113.

folosirea resurselor sistemelor informaționale interconectate din sectorul cibernetic."[11] Având în vedere cele menționate anterior, este necesar să actualizăm „jocul de șah tridimensional complex", introducând și conceptul de război cibernetic, definit de Paul Robinson drept „războiul purtat prin intermediul calculatoarelor și al Internetului. Include atât măsuri ofensive, destinate să producă pagube sistemelor informatice ale oponenților, cât și măsuri defensive, menite să protejeze propriile sisteme de atacuri ostile".[12] De asemenea, Joseph Nye consideră că cea mai vizibilă modificare are loc în domeniile de aplicare ale celui de al treilea nivel. În consecință, spațiul cibernetic devine din ce în ce mai relevant, aducând cu sine implicații asupra politicii internaționale.

Considerăm că puterea cibernetică a unui stat se referă la capabilitățile de apărare cibernetică, dar și la capacitățile și capabilitățile ofensive necesare desfășurării de operații în rețelele de calculatoare ale adversarului, inclusiv spionaj cibernetic, capacitatea de a compromite rețelele și sistemele IT&C ale inamicului și de a prelua controlul de administrator asupra dispozitivelor informatice sau sistemelor de calcul, prin rootkit-uri sau troieni. Puterea cibernetică este o resursă de securitate pentru state, alături de puterea politică, puterea militară, diplomatică, economico-financiară sau informațională. Capacitatea forțelor armate de a executa un ansamblu complex de acțiuni defensive și ofensive asupra sistemelor IT&C și rețelelor de date, reprezintă unul dintre determinanții puterii statelor.

Prin utilizarea suportului tehnic al tehnologiei informației și comunicațiilor are loc o schimbare pragmatică în configurarea relațiilor de putere dintre actorii non-statali și state, rezultând un război în spațiul realității virtuale (un război cibernetic) care poate avea posibile ținte infrastructurile critice ale statelor (sisteme de distribuție a energiei electrice, facilități industriale și ale industriei de apărare, comunicații guvernamentale, sistemul financiar-bancar sau serviciile medicale).[13]

Kenneth Waltz menționează faptul că interdependența este o relație între egali.[14] Atunci când părțile nu sunt egale în sfera cibernetică, poate exista un grad de dependență și, în același timp, de vulnerabilitate, din moment ce relația dintre actori nu este echilibrată.[15] Scepticismul și neîncrederea statelor sunt potențate de mai mulți factori. Unul dintre aceștia se referă la faptul că actorii statali dispun de capabilități diferite în ceea ce privește domeniul cibernetic. Unele state își concentrează eforturile și resursele economico-financiare în direcția dezvoltării, la nivelul forțelor armate, a unor capacități și capabilități de apărare cibernetică, precum și capabilități necesare pentru desfășurarea de

11 Ibidem, p.123.

12 Paul Robinson, Dicționar de securitate internațională, Editura CA Publishing, Cluj-Napoca, 2010, p.164.

13 Gheorghe Arădăvoaice, Valentin Stancu, Războaiele de azi și de mâine - agresiuni neconvenționale, Editura Militară, București, 1999, p.43.

14 Kenneth Waltz, Theory of International Politics, Editura Waveland Press, Long Grove, 2010, p.144.

15 Brandon Valeriano, Ryan C. Maness, Cyber war versus cyber realities: cyber conflict in the international system, Editura Oxford University Press, Oxford, 2015, p.13.

operații în rețelele de calculatoare ale unui potențial inamic. Cu toate că, o parte dintre atacurile cibernetice sunt lansate de către hackeri individuali și grupări de criminalitate cibernetică, există și atacuri sau operațiuni în spațiul cibernetic desfășurate de grupări de hackeri susținute de actori statali. În acest sens, pot fi oferite mai multe exemple: atacuri cibernetice care au ca țintă infrastructura critică a unor state, implicarea în unui actor statal în politica internă a altui stat, furtul de proprietate intelectuală sau sabotarea unei entități (cazul Coreea de Nord cu Sony Pinctures).[16] Deși, Coreea de Nord este o țară săracă din punct de vedere economic, aceasta dispune de capabilități și capacități cibernetice destul de sofisticate.[17]

Infrastructura de pe teritoriul României se încadrează în 3 clase: infrastructuri critice, infrastructuri speciale, infrastructuri obișnuite.[18]

În continuare, dorim să definim într-un mod cât mai exhaustiv cele 3 tipuri de infrastructură, astfel încât să evidențiem legăturile care se pot stabili între ele și caracteristicile funcționale ale fiecărui tip de infrastructură, în strânsă corelare cu zona de siguranță națională.

Considerăm că, infrastructurile obișnuite se referă la structuri, construcții, care asigură buna funcționare a unor sisteme de natură economică, financiară, socială, culturală, militară, administrativă. În categoria infrastructurilor obișnuite sunt încadrate acele sisteme și componente ale sistemelor care nu necesită măsuri deosebite de securitate și protecție. Aceste infrastructuri asigură menținerea unor funcții ale societății, fiind necesare oamenilor și comunităților. În cazul perturbării sau opririi funcționării acestora, pe o perioadă scurtă de timp, nu sunt afectate în mod semnificat procesele economice, sociale, politice, militare. În această categorie se încadrează școlile, bibliotecile, drumurile care nu au o importanță majoră pentru domeniul transporturilor civile sau militare (drumurile din mediul rural). Aceste infrastructuri pot deveni speciale sau critice, pentru o perioadă determinată de timp, în funcție de evoluțiile sociale, economice și militare din anumite regiuni sau zone ale țării.

Infrastructurile speciale pot avea un aport important în funcționalitatea unor sisteme sau procese economice, sociale, politice, militare, financiare. În cazul perturbării acestora, stabilitatea la nivel social și economic poate fi afectată, fără a pune în primejdie funcționarea de ansamblu a sistemelor și proceselor asimilate sectoarelor economic, social, militar, politic, informațional. Un aerodrom construit într-o localitate poate fi încadrat în această categorie în funcție de importanța sa în cadrul unui proces (transport comercial, militar), de vulnerabilitățile de securitate care sunt identificate sau de posibile amenințări care pot determina scoaterea sa din funcțiune pentru un timp

16 Richard Haass, Lumea în care trăim. O scurtă introducere, Editura Nemira, București, 2021, p.257.

17 Ibidem, p.258.

18 Grigore Alexandrescu, Gheorghe Văduva, Infrastructurile critice: pericole, amenințări la adresa acestora; sisteme de protecție, Editura Universității Naționale de Apărare „Carol I", București, 2006, p.6.

scurt. În funcție de consecințele pe care le-ar putea avea perturbarea sau oprirea funcționării unui subsistem, asupra funcționării proceselor și sistemelor, se va face și încadrarea în categoria infrastructurilor critice, pe o perioadă determinată sau nedeterminată.

Infrastructurile critice reprezintă un sistem sau un subsistem care este important pentru menținerea unor funcții vitale ale societății, perturbarea și/sau distrugerea lor fiind resimțită la nivel local, regional sau național, afectând semnificativ buna funcționare a proceselor sociale, financiare, economice, militare, unele avarii și disfuncții punând în primejdie chiar securitatea națională. Aceste infrastructuri necesită măsuri deosebite de securitate și protecție, deoarece perturbarea funcționării acestora chiar și pentru scurt timp poate să producă efecte negative la nivel social, economic, financiar, militar: aeroporturile internaționale, bazele militare strategice, rețeaua electrică națională, frontiera de stat, drumuri de mare viteză (autostrăzi, drumuri express), drumuri strategice din punct de vedere militar (facilitează deplasarea rapidă a forțelor armate și tehnicii militare), porturi maritime și fluviale importante (împreună cu infrastructura aferentă lor), hidrocentrale cu putere instalată de sute și mii de MW, termocentrale mari, de importanță regională (termocentralele Rovinari și Turceni sunt de importanță regională și pot fi încadrate în categoria infrastructuri critice), centrale atomoelectrice, depozite de muniții, carburant și armament, rețele telefonice naționale, relee, rețele de calculatoare (rețele metropolitane, rețele de arie largă), sisteme și servicii informatice, oleoducte, gazoducte, spitale de importanță regională.

BIBLIOGRAFIE SELECTIVĂ:

I. Documente oficiale din surse electronice:

1). „Executive Order EO 13010 Critical Infrastructure Protection, 15 iulie 1996, disponibil la https://fas.org/irp/ offdocs/eo13010.htm.

2). Hotărârea Guvernului nr. 585/2002, pentru aprobarea standardelor naționale de protecție a informațiilor clasificate în România, în Monitorul Oficial al României, Partea I, nr. 485 din 5 iulie 2002.

3). UNODC, „Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation”, http://www.unodc.org/documents/congress//Declaration/V1504151_English.pdf.

4). Declarația Summit-ului NATO din Țara Galilor, paragraful 72, disponibil la https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.
5). Cybercrime Convention Committee (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, Strasbourg, iulie 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.
6). Site-ul oficial al Administrației Prezidențiale: *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*, București, 2020, disponibil la https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.
7). Guvernul României, *Strategia de Securitate Cibernetică a României din 30 decembrie 2021, pentru perioada 2022-2027*, 3 ianuarie 2022, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235.

II. Legislație:

1). „Ordonanța de urgență nr. 61/2019 pentru modificarea și completarea Ordonanței de urgență a guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice", 30 august 2019, disponibil la https://lege5.ro/Gratuit/gm2deojsg4zq/ordonanta-de-urgenta-nr-61-2019-pentru-modificarea-si-completarea-ordonantei-de-urgenta-a-guvernului-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.
2). „Legea nr. 255/2018 pentru modificarea și completarea Ordonanței de urgență a guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice", 3 august 2018, disponibil la https://lege5.ro/Gratuit/gi4tamrrg44a/legea-nr-225-2018-pentru-modificarea-si-completarea-ordonantei-de-urgenta-a-guvernului-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.
3). „Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică", 23 mai 2013, disponibil la https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.
4). Prevenirea și combaterea criminalității informatice - Legea nr. 161/2003", disponibilă la https://lege5.ro/gratuit/hezdgobv/prevenirea-si-combaterea-criminalitatii-informatice-lege-161-2003?dp=giztimztg4ytk.

5). Regulamentului General european 2016/679 privind protecția datelor cu caracter personal (GDPR), articolul 32 - *Securitatea prelucrării*, disponibil la https://www.privacy-regulation.eu/ro/32.htm.
6). „Noul Cod Penal actualizat 2024 - Legea 286/2009", https://legeaz.net/noul-cod-penal/.
7). Portalul Legislativ al Ministerului Justiției: „Legea nr.58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative".

III. Rapoarte și buletive informative:

1). International Telecommunication Union (ITU-T), Series X: *Data networks, open system communications and security. Telecommunication security, Overview of cybersecurity,* ITU-T X.1205, aprilie 2008.
2). Check Point Research Team, „Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks", 5 ianuarie 2023, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks.
3). Site-ul oficial al Serviciului Român de Informații: *Protecția infrastructurilor critice,* disponibil la https://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf.
4). Serviciul Român de Informații, *Buletin Cyberint - semestrul 1 (2022)*, disponibil la https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2022-RO.pdf.
5). Serviciul Român de Informații, *Buletin special Cyberint în contextul COVID-19*, disponibil la https://www.sri.ro/assets/files/publicatii/buletin-special-covid-cyber-2020.pdf.
6). Serviciul Român de Informații, *Buletin Cyberint*, *nr.2 - 2021*, disponibil la https://www.sri.ro/assets/files/publicatii/buletin-cyber-nr2.pdf.
7). Site-ul oficial al Serviciului Român de Informații: *Ghid de bune practici pentru securitate cibernetică*, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf.
8). Centrul de Management și Transfer Tehnologic și Cognitiv, Universitatea Babeș-Bolyai, *QTSTRAT Newsletter*, nr. 1, decembrie 2021.
9). Centrul de Management și Transfer Tehnologic și Cognitiv, Universitatea Babeș-Bolyai, *QTSTRAT Newsletter*, nr. 3.
10). Centrul de Management și Transfer Tehnologic și Cognitiv, Universitatea Babeș-Bolyai, *QTSTRAT Newsletter*, nr. 5.

11). Secretariatul General al Consiliului Uniunii Europene, *EMPACT 2022 Results, Factsheets*, 2023, disponibil la https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf.
12). EU Agency for Criminal Justice Cooperation, *Annual Report 2022: Criminal Justice across borders*, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2022-en.pdf.
13). Site-ul oficial al EUROPOL: *The European Union Agency for Law Enforcement Cooperation*, Luxembourg: Publications Office of the European Union, 2022, disponibil la https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20in%20Brief.pdf.
14). Site-ul oficial al Consiliului Europei: „Council of Europe action against Cybercrime", disponibil la https://www.coe.int/en/web/portal/coe-action-against-cybercrime.
15). United Nations Office at Vienna, Centre for Social Development and Humanitarian Affairs, *International Review of Criminal Policy, Nos. 43 and 44, 1994, United Nations Manual on the prevention and control of computer-related crime,* disponibil la https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF.
16). Consiliul Uniunii Europene, *Cybersecurity: how the EU tackles cyber threats*, ultima actualizare 11 ianuarie 2023, https://www.consilium.europa.eu/en/policies/cybersecurity/.
17). Institute for Security and Technology, *Combating Ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, disponibil la https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
18). IBM Security, *Cost of a Data Breach - Report 2022*, iulie 2022, Statele Unite ale Americii, disponibil la https://www.ibm.com/downloads/cas/3R8N1DZJ.
19). Matt Ahlgren, „Peste 50 de statistici, fapte și tendințe în domeniul securității cibernetice pentru 2023", august 2023, https://www.websiterating.com/ro/research/cybersecurity-statistics-facts/.
20). The Engine Room, Internews, *Case study: Watering hole attacks*, iunie 2020, disponibil la https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-Watering-Hole-Junio-2020.pdf.

IV. Lucrări de specialitate (Cărți):

1). ABLON, Lillian, BOGART, Andy, *Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, Santa Monica, 2017.

2). ALEXANDRESCU, Grigore, VĂDUVA, Gheorghe, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare Carol I, București, 2006.
3). ARĂDĂVOAICE, Gheorghe, STANCU, Valentin, *Războaiele de azi și de mâine - agresiuni neconvenționale*, Editura Militară, București, 1999.
4). BARBU, Alida Monica Doriana, *Inteligența artificială: cum vor schimba AI, Deep Learning și robotica domeniul militar*, Editura Militară, București, 2023.
5). BAYLIS, John, SMITH, Steve, OWENS, Patricia (coord.), *The Globalization of World Politics: an introduction to international relations*, Sixth edition, Oxford University Press, Oxford, United Kingdom, 2014.
6). BLOKDYK, Gerardus, *SWOT Analysis - A Complete Guide*, Editura The Art of Service - SWOT Analysis Publishing, 2021.
7). CHAWKI, Mohamed, DARWISH, Ashraf, KHAN, Mohammad Ayoub, TYAGI, Sapna, *Cybercrime, Digital Forensics and Jurisdiction*, Studies in Computational Intelligence, Volume 593, Springer International Publishing, 2015.
8). CLARKE, Justin et all., *SQL Injection Attacks and Defense*, Editura Syngress Publishing, Burlington, 2009.
9). CURELEA, Mihai Bogdan, ȘTEȚCU, Petru, *Criminalistica*, Editura Concordia, Arad, 2023.
10). DEAC, Aron Liviu, IRIMIA, Ion, *Securitate și apărare națională - culegere de lecții*, Editura Academiei de Înalte Studii Militare, București, 1999.
11). ELISAN, Christopher C., *Advanced Malware Analysis*, McGraw-Hill Education, New York, 2015.
12). FINE, Lawrence, *The SWOT Analysis: Using your Strength to overcome Weaknesses, using Opportunities to overcome Threats*, Editura CreateSpace Independent Publishing Platform, Ediția 1, 2010.
13). FREEDMAN, Lawrence, *Viitorul războiului: o istorie*, Editura Litera, București, 2019.
14). FERENȚ, Darius-Antoniu, *Introducere în securitatea cibernetică*, Editura Limes, Florești, 2023.
15). GERCKE, Marco, International Telecommunication Union, *Understanding cybercrime: Phenomena, challenges and legal response*, Geneva, 2014.
16). GOODMAN, Marc, *X-Cyber: viitorul începe azi*, Editura RAO, București, 2016.
17). GOLDSTEIN, Joshua S., PEVEHOUSE, Jon C., *International Relations*, Tenth edition, Editura Pearson, 2014.
18). GRAHAM, James, HOWARD, Richard, OLSON, Ryan, *Cyber Security Essentials*, Editura CRC Press Taylor&Francis Group, New York, 2011.

19). GRIFFITHS, Martin (ed.), *International Relations Theory for the 21st Century: An Introduction*, Editura Routledge, Londra, New York, 2007.
20). HAASS, Richard, *Lumea în care trăim. O scurtă introducere*, Editura Nemira, București, 2021.
21). HIRST, Paul, *Război și putere în secolul XXI. Statul, conflictul militar și sistemul internațional*, Editura Antet, 2003.
22). HOFSTEDE, Geert, HOFSTEDE, Gert Jan, MINKOV, Michael, *Culturi și organizații: softul mental. Cooperarea interculturală și importanța ei pentru supraviețuire*, Editura Humanitas, București, 2012.
23). IONIȚĂ, Gheorghe-Iulian, *Infracțiunile din sfera criminalității informatice*, Editura Universul Juridic, București, 2018.
24). JENKINSON, Andrew, *Ransomware and Cybercrime*, CRC Press, Taylor&Francis Group, Londra, 2022.
25). KATZ, Jonathan, LINDELL, Yehuda, *Introduction to Modern Cryptography*, ediția a 2-a, Editura CRC Press, Taylor & Francis Group, 2015.
26). LUCAS, George, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*, Editura Oxford University Press, New York, 2017.
27). KEYTON, Joann, *Communication and Organizational culture: A Key to Understanding Work Experiences*, Sage Publications, Ediția 1, 2005.
28). LISKA, Allan, GALLO, Timothy, *Ransomware: Defending Against Digital Extortion*, Editura O'Reilly Media, Sebastopol, USA, 2017.
29). MANCI, Ioan, PREJA,Corneliu, *Introducere în studii de securitate și strategice*, Editura CA Publishing, Cluj-Napoca, 2014.
30). MEARSHEIMER, John, *The Tragedy of Great Power Politics*, Editura W.W. Norton & Company, London, 2014.
31). MELINESCU, Nicolae, *Noțiuni introductive pentru studiul relațiilor internaționale*, Editura CA Publishing, Cluj-Napoca, 2014.
32). MIROIU, Andrei, UNGUREANU, Radu-Sebastian, BIRO, Daniel, DÎRDALĂ, Lucian-Dumitru, TODEREAN, Olivia, *Manual de relații internaționale*, Editura Polirom, Iași, 2006.
33). NIEBUHR, Reinhold, *Moral Man and Immoral Society. A Study In Ethics and Politics*, Presbytherian Publishing Corporation, 2021.
34). POPA, Eliza-Tatiana, TĂNASE, Tiberiu, *Riscuri și amenințări ale mileniului III - Volumul 1*, Editura Concordia, Arad, 2022.
35). PREJA, Amos Corneliu, BOGDAN, Ioan, *Introducere în teoria generală a informației și studii de intelligence,* Editura CA Publishing, Cluj-Napoca, 2017.

36). ROBINSON, Paul, *Dicționar de securitate internațională*, Editura CA Publishing, Cluj-Napoca, 2010.
37). RYAN, Matthew, *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Editura Springer, Cham, Elveția, 2021.
38). SFETCU, Nicolae, *Beginner's Guide for Cybercrime Investigators*, Editura MultiMedia Publishing, București, 2014.
39). SFETCU, Nicolae, *Introducere în inteligența artificială*, Editura MultiMedia Publishing, București, 2021.
40). SFETCU, Nicolae, *Amenințările persistente avansate în securitatea cibernetică. Războiul cibernetic*, Editura MultiMedia Publishing, București, 2024.
41). SHIMONSKI, Robert, *AI in Healthcare: How Artificial Intelligence Is Changing IT Operations and Infrastructure Services*, Editura Wiley, 2021.
42). TĂNASE, Tiberiu, ȘTEȚCU, Petru, *Investigarea infracțiunilor informatice*, Editura Concordia, Arad, 2021.
43). TANCO, Alexandru (coord.), NERON, Mircea, ȘTEȚCU, Petru, *Prevenirea și combaterea infracționalității*, Editura Concordia, Arad, 2023.