



UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY

TRADITIO ET EXCELLENTIA



FACULTATEA DE
ISTORIE ȘI FILOSOFIE



ȘCOALA DOCTORALĂ DE
**Relații Internaționale și
Studii de Securitate**

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

TEZĂ DE DOCTORAT

Rezumat

CONDUCĂTOR DE DOCTORAT:

Prof. Univ. Dr. Ivan Adrian Liviu

STUDENT-DOCTORAND:

CLAUDIA-ALECSANDRA GABRIAN

**CLUJ-NAPOCA
2026**



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



FACULTATEA DE
ISTORIE ȘI FILOSOFIE



ȘCOALA DOCTORALĂ DE
**Relații Internaționale și
Studii de Securitate**

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

**GEOPOLITICA CYBERCRIME ȘI RECONFIGURAREA
ECOSISTEMULUI DE CRIMINALITATE CIBERNETICĂ DUPĂ
DECLANȘAREA RĂZBOIULUI RUSO-UCRAINEAN**

Domeniul de doctorat:

Relații Internaționale și Studii Europene

CONDUCĂTOR DE DOCTORAT:

Prof. Univ. Dr. Ivan Adrian Liviu

STUDENT-DOCTORAND:

CLAUDIA-ALECSANDRA GABRIAN

**CLUJ-NAPOCA
2026**

CUPRINS

LISTA ABBREVIERILOR

LISTA FIGURILOR

LISTA TABELELOR

INTRODUCERE..... 5

CAPITOLUL I. FUNDAMENTARE TEORETICĂ ȘI CONCEPTUALĂ:

GEOPOLITICA SPAȚIULUI CIBERNETIC.....Error! Bookmark not defined.

1.1. *Abordarea relațiilor internaționale în analiza spațiului cibernetic* .Error! Bookmark not defined.

1.1.1. De la interconectare globală la instrumentalizarea interdependenței Error! Bookmark not defined.

1.1.2. Realismul structural și Anarhia internațională Error! Bookmark not defined.

1.1.3. Depășirea constrângerilor geografice și maximizarea puterii relative Error! Bookmark not defined.

1.2. *Teoria Cyber-Geopoliticii și Dilema de Securitate în spațiul digital*Error! Bookmark not defined.

1.2.1. Spațiul cibernetic ca domeniu de conflict Error! Bookmark not defined.

1.2.2. Dilema de Securitate în era digitală și avantajul structural al ofensivei...Error! Bookmark not defined.

1.2.3. Limitările Teoriilor Relațiilor Internaționale în analiza spațiului cibernetic: De la Neorealism la Teoria Haosului.....Error! Bookmark not defined.

1.3. *Delimitări conceptuale și operaționalizare* Error! Bookmark not defined.

1.3.1. Reconceptualizarea „Cybercrime”: Din infracțiune financiară în act de război hibrid. Error! Bookmark not defined.

1.3.2. Tipologia infractorilor ciberneticici în spațiul cibernetic contemporan Error! Bookmark not defined.

1.3.3. Contractul social și profilul psihologic al criminalului cibernetic Error! Bookmark not defined.

1.4. *Doctrina Federației Ruse: Suveranitatea cibernetică și Militarizarea spațiului informațional* Error! Bookmark not defined.

1.4.1. Conceptul de Cyber-Sovereignty și RuNet.....Error! Bookmark not defined.

1.5. *Spațiul cibernetic ca domeniu emergent al competiției strategice și impactul asupra securității naționale*.....Error! Bookmark not defined.

1.5.1. Tipologia atacurilor ciberneticice în contextul războiului hibridError! Bookmark not defined.

1.5.2. Definirea și apariția atacului de tip ransomware .Error! Bookmark not defined.

CAPITOLUL II. ECOSISTEMUL DE CRIMINALITATE CIBERNETICĂ DIN FEDERAȚIA RUSĂ: CONVERGENȚA DINTRE PROFIT ȘI OBIECTIVE STRATEGICE Error! Bookmark not defined.

2.1. Paradigma de securitate a Federației Ruse și Suveranitatea Digitală.Error! Bookmark not defined.

2.1.1. De la protecție juridică la instrumentalizare: mecanisme de recrutare în spațiul cibernetic Error! Bookmark not defined.

2.1.2. Aplicarea selectivă ca mecanism de cooptare și gestiune a resurselor cibernetic Error! Bookmark not defined.

2.2. Infrastructura Financiară a Ecosistemului Infrațional: Exploatarea Sistemelor IABS, Criptomonedes și Mecanisme de Spălare a banilor Error! Bookmark not defined.

2.2.1 Ecosistemul criptomonedelor Error! Bookmark not defined.

2.2.2. Infrastructura operațională de pe Dark Web Error! Bookmark not defined.

2.2.3. Ecosistemul “underground” și forumurile de pe Dark Web Error! Bookmark not defined.

2.2.4. Brokerii de Acces Inițial și rolul lor în ecosistemul de criminalitate cibernetică Error! Bookmark not defined.

2.3. Dinamica Ecosistemului Infrațional în Contextul Invaziei din 24 Februarie 2022 Error! Bookmark not defined.

2.3.1. Schimbarea selecției țintelor.....Error! Bookmark not defined.

2.3.2. Eficiența și vulnerabilitățile modelului proxy.....Error! Bookmark not defined.

2.4. Automatizarea ofensivei: Integrarea Inteligenței Artificiale în ecosistemul Ransomware Error! Bookmark not defined.

2.4.1. Tranziția către Războiul de Nouă Generație pe flancul european.....Error! Bookmark not defined.

2.4.2. Doctrina Atacului Informațional Strategic: De la subversiune psihologică la blocare tehnică Error! Bookmark not defined.

CAPITOLUL III. ANALIZA COMPARATIVĂ A ECOSISTEMULUI RANSOMWARE: CAZUL CONTI ȘI BLACK BASTA Error! Bookmark not defined.

3.1. Continuitatea operațională a grupărilor ransomware Error! Bookmark not defined.

3.2. Gruparea ransomware Conti.....Error! Bookmark not defined.

3.2.1. Conti Leaks Error! Bookmark not defined.

3.3. Gruparea ransomware Black Basta Error! Bookmark not defined.

3.3.1. Black Basta Leaks Error! Bookmark not defined.

CAPITOLUL IV. ECOSISTEMUL RANSOMWARE ȘI EVOLUȚIA LUI.....Error! Bookmark not defined.

4.1. Analiza ecosistemului ransomware în 2025 Error! Bookmark not defined.

4.2. Evoluția ransomware în 2026 și perspective de viitor Error! Bookmark not defined.

4.2.1. Ransomware leaks în 2026.....	Error! Bookmark not defined.
4.3. <i>Cyber-Intelligence: un instrument esențial pentru îmbunătățirea securității naționale în era digitală</i>	Error! Bookmark not defined.
4.4. <i>Rolul instituțiilor internaționale în combaterea criminalității cibernetice</i>	Error! Bookmark not defined.
CONCLUZIILE LUCRĂRII	20
BIBLIOGRAFIE	29

INTRODUCERE

În prezent, spațiul cibernetic nu se mai limitează la o rețea globală de comunicații sau la un mediu destinat exclusiv companiilor și inovațiilor tehnologice. În arhitectura contemporană a relațiilor internaționale, acesta reprezintă unul dintre cele mai active, volatile și dificil de controlat domenii, devenind, în timp, scena unei competiții geopolitice între marile puteri. Această transformare a fost posibilă datorită caracterului descentralizat al internetului, care a redus importanța limitelor geografice în desfășurarea activităților din mediul cibernetic. Infractorii ciberneticici sunt printre principalii actori ai mediului digital care au contribuit la reconfigurarea echilibrului de putere, descentralizarea reprezentând pentru aceștia un avantaj semnificativ.

Acești infractori ciberneticici pot fi organizați în grupuri extinse sau restrânse de persoane, care dispun de competențe tehnice și capacități avansate de calcul. Capacitatea lor de influență poate fi comparată în mediul global de securitate, cu cea exercitată de un stat. Începând cu anul 2022, spațiul cibernetic a devenit un mediu dinamic și imprevizibil, iar criminalitatea informatică transnațională a evoluat dincolo de instrumentele clasice de gestionare a fenomenelor infracționale. Furtul de date și extorcarea nu mai reprezintă exclusiv infracțiuni financiare, ci constituie și probleme de securitate națională și mijloace de exercitare a influenței asimetrice în competiția dintre actorii statali.

Evoluția amenințărilor ciberneticice marchează o schimbare de paradigmă în desfășurarea conflictelor internaționale. De exemplu, în deceniile anterioare, o parte semnificativă a atacurilor ciberneticice erau desfășurate de indivizi sau grupuri restrânse, motivați de curiozitate sau obținerea unor câștiguri financiare ocazionale. În prezent, peisajul cibernetic este caracterizat de apariția unor organizații de criminalitate specializate în *ransomware*, care nu mai sunt motivate doar financiar și care se bazează pe rețele extinse de afiliați.

Grupările specializate în *ransomware* sunt structuri organizaționale complexe, dispun de resurse financiare semnificative și sunt specializate în diverse domenii, cu niveluri clare de ierarhizare. În timp, unele guverne au identificat posibilitatea de a obține avantaje strategice prin tolerarea activității acestora și au ales să le ignore sau să le permită să opereze discret, limitând riscul unor consecințe juridice sau diplomatice directe. În acest context, grupările au devenit exploatate indirect pentru promovarea unor interese statale. Ca urmare, s-a conturat așa-numita *zonă gri*, în care criminalitatea cibernetică se intersectează cu interesele geopolitice, iar infractorii ciberneticici acționează drept instrumente indirecte de influență.

Utilizarea rețelelor de criminalitate cibernetică drept intermediari poate oferi statelor avantaje geopolitice importante, întrucât acestea pot acționa fără o atribuire directă a responsabilității. Astfel, statele pot desfășura activități de sabotaj economic, furt de date

sensibile sau atacuri asupra infrastructurilor critice, fără a-și asuma în mod public responsabilitatea pentru aceste acțiuni. Dimensiunea cibernetică devine un spațiu în care activitățile ostile se desfășoară în paralel cu conflictele deschise, contribuind la influențarea și amplificarea acestora.

Relația dintre actorii statali și grupările de criminalitate cibernetică evidențiază o transformare a modalităților de exercitare a influenței în spațiul cibernetic. Statul nu mai acționează direct, ci poate recurge și la rețele informale, dificil de urmărit și de atribuit, care pot deveni parte a instrumentelor indirecte de exercitare a puterii. În acest context, capacitatea de a utiliza sau contracara aceste rețele poate constitui un element strategic important.

Într-o societate caracterizată de o digitalizare accelerată, activitățile convenționale au devenit tot mai interconectate cu spațiul cibernetic. Evoluția tehnologiei informației și comunicațiilor a adus beneficii considerabile, dar, în același timp, a expus fiecare sector al funcționării statului unor noi vulnerabilități. În prezent, protejarea datelor împotriva amenințărilor rău intenționate nu mai reprezintă doar o preocupare de natură tehnică, ci o necesitate fundamentală.

Codurile malițioase sunt într-o continuă evoluție, la fel ca atacurile cibernetice, care, de cele mai multe ori pot pătrunde în sisteme fără cunoștința operatorilor și pot obține acces neautorizat la resursele acestora. Aceste intruziuni sunt facilitate de tehnici tot mai sofisticate de inginerie socială, care exploatează nivelul insuficient de informare și conștientizare al utilizatorilor de internet, cu privire la natura și amploarea acestor amenințări.

Printre aceste amenințări, atacurile de tip *ransomware* au cunoscut o evoluție considerabilă, devenind unul dintre cele mai persistente forme de atac cibernetic care afectează securitatea globală în prezent. Din perspectiva atacatorilor ciberneticici, internetul a reprezentat principalul instrument pentru crearea unui ecosistem în care rețelele financiare să fie dezvoltate și utilizate pentru desfășurarea activităților pe canale private sau ascunse, inclusiv pe *dark web*. În cadrul forumurilor *underground*, acestora le-a fost facilitată anonimizarea tranzacțiilor, precum și evitarea mecanismelor tradiționale de monitorizare și control. Popularitatea monedelor digitale, precum *Bitcoin*, a oferit un avantaj considerabil atacatorilor, prin punerea la dispoziție a unei metode de plată pseudo-anonime, care le-a permis să își monetizeze activitățile de extorcere.

Grupările de criminalitate cibernetică au integrat în ultimii ani modele de afaceri sofisticate, sub denumirea de syndicate *Ransomware-as-a-service* (RaaS), cu scopul de a-și maximiza profiturile. În cadrul acestora, în schimbul unor sume de bani, persoane cu competențe tehnice de bază, pot închiria infrastructura pusă la dispoziție de grupare și pot participa activ la desfășurarea de atacuri, urmând ca un procent din suma obținută în urma plății răscumpărării să revină administratorilor. Această proliferare a capabilităților a modificat semnificativ structura ecosistemului de criminalitate cibernetică, influențând direct

modul în care sunt percepute și analizate în prezent aceste sindicate.

Revoluția informațională a contribuit la apariția unor noi tipologii de actori implicați în conflicte, precum și la diversificarea strategiilor adoptate de aceștia, influențând direct modul în care statele sunt afectate de atacurile cibernetice. În prezent, tehnologia este indispensabilă pentru funcționarea societății și poate influența aproape toate domeniile acesteia. Pentru atacatori, tehnologia poate reprezenta o vulnerabilitate pe care să o exploateze, astfel încât infrastructurile critice pot deveni obiective ale operațiunilor de sabotaj, în special în contextul desfășurării conflictelor armate. Legătura dintre război și criminalitatea cibernetică poate fi analizată prin prisma modului în care aceste grupări sunt implicate, direct sau indirect, în desfășurarea conflictelor.

Criminalitatea cibernetică, fie că este desfășurată de actori statali sau non-statali, s-a transformat într-o amenințare la adresa securității naționale, întrucât vizează sectoare critice, precum sănătatea, educația, sistemele financiare, sectorul energetic etc. Câștigurile obținute prin întreruperea serviciilor esențiale pot constitui un factor important de motivație pentru continuarea atacurilor cibernetice. Pentru a înțelege nivelul de complexitate al acestor grupări, este necesară analizarea modului în care sunt organizate. Acestea funcționează pe baza unor structuri organizaționale bine definite, în cadrul cărora fiecare membru îndeplinește un rol specific.

La fel ca orice altă amenințare cibernetică, ecosistemul *ransomware* evoluează constant și se adaptează la noile tehnologii, inclusiv prin utilizarea inteligenței artificiale (IA) pentru eficientizarea activităților infracționale. În prezent, modelele lingvistice de mari dimensiuni (*Large-Language-Models* - LLM) pot fi utilizate pentru identificarea potențialelor victime, redactarea notelor de răscumpărare și adaptarea acestora la limba și contextul cultural al victimei, cu scopul de a crește probabilitatea obținerii plății. Totuși, indiferent de nivelul de profitabilitate, competitivitate și organizare tehnică al acestor grupări, infractorii cibernetici pot să fie influențați de mediul geopolitic.

Invazia din Ucraina (*Україна*) a reprezentat un moment de reconfigurare a acestui ecosistem, deoarece au apărut noi loialități politice. Astfel, grupările de criminalitate cibernetică care înaintea conflictului urmăreau în principal obținerea unor câștiguri financiare, s-au divizat în tabere de susținere a beligeranților, conturându-se în acest context o tabără pro-rusă și una pro-ucraineană. Un exemplu este gruparea *ransomware Conti*, care a apărut în anul 2020 și care, la 25 februarie 2022 și-a exprimat public susținerea față de invazia Rusiei (*Россия*) în Ucraina (*Україна*), declarându-și sprijinul pentru Rusia (*Россия*). Aceasta a fost prima grupare *ransomware* care și-a exprimat public susținerea față de un actor statal, amenințând cu atacuri asupra infrastructurii critice a oricărei națiuni occidentale care ar fi intervenit împotriva Rusiei (*Россия*). Această poziționare a declanșat o divizare în cadrul grupării, iar afiliații ucraineni au reacționat prin divulgarea unor volume semnificative de

informații, inclusiv comunicații interne și elemente ale codului sursă, contribuind la dezintegrarea ulterioară a grupării.

Divizarea acestui ecosistem infracțional pe criterii geopolitice evidențiază faptul că actorii implicați nu mai acționează într-un spațiu complet separat de dinamica geopolitică internațională. Aceste evoluții au contribuit la o transformare semnificativă a criminalității cibernetice, care a ajuns să reflecte, în anumite situații, diviziunile geopolitice și ideologice generate de conflictele internaționale. În acest context, anumite grupări pot ajunge să fie utilizate ca instrumente indirecte în cadrul unor forme de război asimetric, cum este războiul dintre Rusia (*Россия*) și Ucraina (*Україна*).

Prezenta lucrare doctorală investighează un fenomen care a contribuit la transformarea arhitecturii de securitate globală: implicarea unor grupări de criminalitate cibernetică în conflicte armate, prin depășirea obiectivelor exclusiv financiare și asumarea unor poziționări geopolitice, inclusiv prin acțiuni desfășurate în sprijinul unor actori statali. Cercetarea analizează evoluția ecosistemului *ransomware* în perioada 2020-2026 și examinează modul în care invazia Federației Ruse (*Российская Федерация*) în Ucraina (*Україна*), declanșată la 24 februarie 2022, a contribuit la o schimbare semnificativă în dinamica conflictelor asimetrice. În acest context, gruparea *Conti* anterior orientată predominant către obținerea de profituri financiare, și-a manifestat poziționarea geopolitică și ar fi desfășurat activități compatibile cu interesele Federației Ruse (*Российская Федерация*), inclusiv prin forme de cooperare și aliniere strategică. Ipoteza generală a cercetării vizează transformarea unor grupări infracționale independente în entități digitale alinate strategic și subordonate intereselor Federației Ruse (*Российская Федерация*).

Din perspectivă istorică, grupările de criminalitate cibernetică și-au desfășurat activitatea preponderent în mod discret, evitând asumarea unor agende geopolitice, pentru a limita expunerea în fața autorităților și a serviciilor de informații. Cu toate acestea, conflictul ruso-ucrainean a evidențiat o schimbare în această abordare operațională, prin asumarea publică a unor poziționări politice a unor actori implicați în criminalitatea cibernetică, cât și prin publicarea unor manifeste politice. Această schimbare a generat necesitatea aprofundării fenomenului prin analiza factorilor care au determinat gruparea *Conti* să își exprime public susținerea față de Federația Rusă (*Российская Федерация*) în contextul acestui conflict.

Scopul tezei constă în analiza unui fenomen emergent în istoria criminalității cibernetice, reprezentat de implicarea și exprimarea publică a susținerii unei grupări de tip *ransomware* a conflictului militar declanșat de Federația Rusă (*Российская Федерация*) în Ucraina (*Україна*). Lucrarea își propune să analizeze dinamica ecosistemului *ransomware* pe o perioadă de șase ani, precum și evoluțiile ulterioare momentului în care gruparea *Conti* și-a exprimat public susținerea pentru Federația Rusă (*Российская Федерация*). În sprijinul acestei cercetări, sunt analizate trei grupări importante din ecosistemul de criminalitate

cibernetică de tip *ransomware*: *Conti*, *Black Basta* și *The Gentlemen*. Selectarea acestora se bazează pe continuitatea identificată între actorii implicați în aceste grupări, evidențiată în special prin informațiile și discuțiile divulgate în urma unor scurgeri de date (*leaks*). Analiza urmărește evoluția și migrarea unor actori dintr-o grupare către alta, precum și menținerea unor legături organizaționale și operaționale între aceste ecosisteme infracționale.

Gruparea *Conti* este analizată ca un caz relevant, întrucât a fost prima grupare *ransomware* care și-a exprimat public susținerea față de invazia Federației Ruse (*Российская Федерация*) în Ucraina (*Україна*). Această poziționare a fost urmată la scurt timp, de divulgarea comunicațiilor interne ale grupării, fapt care a evidențiat divizarea membrilor și afilierea ulterioară a unora dintre aceștia la alte grupări de criminalitate cibernetică. În complementaritate, cercetarea analizează cea de a doua grupare, *Black Basta*, identificată drept succesor operațional al sindicatului *Conti* și cea de a treia grupare *The Gentlemen*, având o continuitate operațională.

Justificarea selectării celor trei cazuri derivă din similaritatea evoluțiilor acestor grupări. La aproximativ trei ani de la invazia Federației Ruse (*Российская Федерация*) în Ucraina (*Україна*), *Black Basta* a fost, la rândul său, afectată de divulgarea unor informații interne, fapt care a facilitat realizarea unei analize comparative asupra continuității actorilor, a structurilor organizaționale și a vulnerabilităților informaționale ale grupărilor analizate. A treia grupare, *The Gentlemen*, a fost, de asemenea, afectată de divulgarea unor informații interne, acestea constituind o bază documentară relevantă pentru a analiza relațiile dintre grupările de criminalitate cibernetică și interesele statului rus.

Coroborarea informațiilor provenite din aceste scurgeri de date oferă elemente relevante pentru testarea ipotezei generale privind existența unor forme de cooperare sau de aliniere între grupările analizate și actori statali ruși. În acest sens, mesajele divulgate conțin informații referitoare la legături dintre membrii grupărilor de criminalitate cibernetică și structuri sau servicii de informații ale Federației Ruse (*Российская Федерация*), precum Serviciul Federal de Securitate al Federației Ruse (FSB) (*Федеральная служба безопасности Российской Федерации - ФСБ*).

În vederea realizării scopului propus, cercetarea urmărește două obiective majore, orientate spre identificarea și explicarea acestor transformări:

Obiectivul teoretic: Analiza caracterului de noutate al implicațiilor hibride în cadrul criminalității cibernetice asociate cu Federația Rusă (*Российская Федерация*). Lucrarea urmărește să argumenteze, prin prisma neorealismului ofensiv, faptul că mobilizarea unor grupări din ecosistemul *ransomware* în contextul invaziei din 2022 constituie un fenomen relevant pentru analiza modului în care actorii cibernetici pot deveni participanți asumați în conflictele interstatuale. În acest context, cercetarea examinează implicațiile acestei transformări asupra conceptului de „*stare de non-pace*” (*unpeace*).

Obiectivul empiric: Cartografierea și reprezentarea grafică a structurilor organizaționale și a evoluției actorilor implicați în grupările *Conti*, *Black Basta* și *The Gentlemen*. Cercetarea urmărește identificarea, reprezentarea și analiza ierarhiilor și rolurilor actorilor cibernetici, pe baza surselor primare și a comunicațiilor interne divulgate pe forumuri și alte platforme utilizate de comunitățile de criminalitate cibernetică. Analiza presupune examinarea și traducerea mesajelor redactate în limba rusă, precum și interpretarea contextului în care acestea au fost transmise și a conținutului acestora. Scopul fiind identificarea eventualelor legături între grupările *ransomware* analizate și actori sau structuri statale ruse. De asemenea, cercetarea urmărește identificarea continuității actorilor, a structurilor și a relațiilor operaționale dintre cele trei grupări și explicarea mecanismelor prin care s-au produs aceste tranziții.

Motivația științifică pentru selectarea acestei problematice privind ecosistemul criminalității cibernetice își are originea într-un moment de fractură sistemică, observat în timp real, reprezentat de evenimentul declanșat la 24 februarie 2022, respectiv invazia Federației Ruse (*Российская Федерация*) în Ucraina (*Україна*). La scurt timp după declanșarea invaziei, conducerea grupării *ransomware Conti*, considerată la acel moment una dintre cele mai active și influente grupări *ransomware* de criminalitate cibernetică la nivel global, a publicat o declarație de susținere a guvernului rus. Această poziționare a marcat începutul unei fragmentări interne a grupării, care a culminat cu divulgarea comunicațiilor interne de către unul dintre membrii săi, de origine ucraineană, care s-a opus public poziționării grupării. Divulgarea acestor mesaje interne a devenit cunoscută sub denumirea de *Conti Leaks* și a oferit acces la un volum semnificativ de informații privind structura organizațională, relațiile dintre membri și modul de funcționare al grupării.

La nivel internațional, literatura de specialitate dedicată fenomenului *ransomware* este vastă, fiind dominată, în mare parte, de analize de natură tehnică, axate pe examinarea caracteristicilor codului malițios, a tehnicilor și procedurilor utilizate de actorii cibernetici, precum și a mecanismelor de prevenire și diminuare a efectelor acestor atacuri. Tema abordată în prezenta lucrare extinde această perspectivă prin analiza relațiilor dintre membrii grupărilor *ransomware* și actori statali ruși, cu un accent particular asupra posibilelor conexiuni cu serviciile de informații ale Federației Ruse (*Российская Федерация*).

În contextul academic, cercetarea asupra ecosistemului criminalității cibernetice asociat cu zona de influență rusă în contextului războiului, este mai puțin dezvoltată. În acest mod, cercetarea își propune să își evidențieze contribuția originală prin următoarele elemente: analiza unui eveniment relevant pentru studiul securității cibernetice și examinarea comunicațiilor în limba rusă din arhivele *Conti Leaks*, *Black Basta Leaks* și *The Gentlemen Leaks*, în vederea identificării relațiilor dintre actorii cibernetici analizați și structurile statale ruse.

Pentru structurarea demersului analitic și evidențierea caracterului de noutate al fenomenului, lucrarea este concepută ca o cercetare calitativă, empirică și exploratorie, fundamentată pe un design bazat pe un studiu de caz multiplu și comparativ. Caracterul empiric al cercetării este susținut de utilizarea unor surse primare, constând în conversațiile dintre membrii grupărilor, extrase din arhivele *Conti Leaks*, *Black Basta Leaks* și *The Gentlemen*, precum și din discuțiile publicate pe forumuri de pe *Dark Web*. Traducerea mesajelor redactate în limba rusă a presupus, acolo unde a fost necesar, interpretarea argoului specific utilizat de infractorii cibernetici, facilitând analiza intențiilor, practicilor și strategiilor acestora. Un element de originalitate al cercetării îl constituie realizarea unor reprezentări vizuale de tip organigramă a actorilor menționați în materialele divulgate. Această reprezentare permite identificarea și vizualizarea structurilor interne, a ierarhiilor și a rolurilor atribuite actorilor în cadrul grupărilor analizate, precum și urmărirea evoluției acestora între grupările *Conti*, *Black Basta* și *The Gentlemen*.

Lucrarea construiește o punte explicativă între neorealism, analiza cadrului juridic și instituțional din Federația Rusă (*Российская Федерация*) prin conceptul de protecție informală numită *krysha* (*Крыша*) și metodele cercetării calitative în mediul digital. Având în vedere natura clandestină a actorilor analizați, abordarea metodologică a necesitat utilizarea unor instrumente adaptate mediilor digitale mai puțin accesibile publicului larg. Metoda principală de cercetare utilizată este netnografia (etnografia rețelelor), aplicată comunităților *online* asociate criminalității cibernetice, inclusiv forumurilor din *Dark Web* și canalelor de *Telegram* în limba rusă. Aplicarea acestei metode a presupus monitorizarea sistematică a activității acestor comunități, urmărirea interacțiunilor dintre membri, a postărilor și a mesajelor publicate, precum și observarea modificărilor comportamentale și organizaționale apărute în timp. Această abordare a permis identificarea unor tipare de interacțiune, a schimbărilor în poziționările membrilor și a modului în care evenimentele geopolitice au influențat dinamica internă a acestor comunități, în special în contextul invaziei.

Netnografia reprezintă o metodă de cercetare esențială pentru înțelegerea modului în care o comunitate orientată exclusiv spre profit s-a polarizat pe criterii geopolitice. Netnografia este completată structural de analiza de conținut retrospectivă, fiind aplicată asupra corpusului de date provenit din *Conti Leaks* și asupra seturilor de date asociate *Black Basta Leaks* și *The Gentlemen Leaks*. Prin traducerea și interpretarea argoului specific utilizat de membrii grupărilor, cercetarea urmărește identificarea relațiilor dintre aceștia și statul rus și analiza profilurilor motivaționale. Utilizarea acestui corpus de comunicații interne divulgate, permite analiza structurii organizaționale a grupărilor, inclusiv a rolurilor de conducere și a distribuirii responsabilităților. Rezultatele cercetării vor contribui la înțelegerea modului în care activitățile de criminalitate cibernetică pot afecta instituțiile publice, dar și cetățenii.

Designul cercetării acestei lucrări pornește de la necesitatea de a depăși simpla

descriere a incidentelor de tip *ransomware*, propunând o analiză aprofundată a mecanismelor de putere asimetrice care structurează relațiile dintre criminalitatea cibernetică și aparatul de stat al Federației Ruse (*Российская Федерация*). În contextul actual al relațiilor internaționale, caracterizat de o estompare a granițelor dintre acțiunile actorilor statali și cele ale actorilor non-statali, cercetarea analizează modul în care războiul ruso-ucrainean a influențat poziționarea și implicarea unor grupări de tip *ransomware* în susținerea invaziei.

Toate informațiile analizate sunt supuse unui proces riguros de verificare și coroborare empirică, prin raportarea acestora la surse primare și la informațiile disponibile în comunitățile interne divulgate, ale grupărilor analizate și ulterior confirmate și de rapoarte de securitate cibernetică și instituții cu atribuții în acest domeniu. În mod particular, designul cercetării este orientat către identificarea și analiza eventualelor relații dintre membrii grupărilor de tip *ransomware* și persoane asociate serviciilor de informații statului rus, precum și către examinarea mecanismelor prin care aceste relații s-ar putea reflecta în activitatea și poziționarea grupărilor analizate. În acest sens, cercetarea se concentrează asupra conceptelor de simbioză funcțională și instrumentalizare strategică, analizând modul în care relațiile dintre actorii ciberneticici și actorii statali pot depăși dimensiunea exclusiv financiară. Problema centrală nu rezidă în tranzacțiile monetare în sine, ci în posibilitatea externalizării unor forme de agresiune asimetrică către actori non-statali.

În acest context, întrebarea de cercetare a acestei lucrări este: *În ce mod a determinat invazia Federației Ruse în Ucraina transformarea ecosistemului infracțional de ransomware?*. Cercetarea pornește de la premisa că, în urma declanșării invaziei, o parte a ecosistemului *ransomware* nu a mai acționat exclusiv financiar, ci a manifestat și poziționări geopolitice, inclusiv prin exprimarea publică a susținerii față de una dintre părțile implicate în conflict, în acest caz, a agresorului. Această transformare poate fi analizată prin prisma relației dintre criminalitatea cibernetică, dinamica geopolitică și formele de război hibrid, precum și a implicațiilor sale asupra evaluării amenințărilor ciberneticice emergente.

Pentru cercetarea empirică, arhivele de comunicații interne divulgate reprezintă surse primare deosebit de relevante, întrucât permit examinarea directă și în detaliu a interacțiunilor dintre membrii grupărilor, a structurilor organizaționale și a practicilor operaționale ale acestora. Repetarea unui fenomen similar de expunere de mesaje interne la aproximativ trei ani distanță, în februarie 2025 și ulterior în mai 2026, oferă posibilitatea unei analize comparative și contribuie la consolidarea relevanței empirice a cercetării. În cadrul celor trei scurgeri de informații, pot fi identificate date privind identitatea unor membri asociați grupărilor, modul în care și-au menținut aliasurile și metodele de atac, chiar dacă au migrat de la o grupare la alta.

Relevanța acestui demers derivă din necesitatea de a analiza mecanismele prin care conceptul de negare plauzibilă poate funcționa în relația dintre actori statali și grupări

criminale cibernetice. În acest context, cercetarea examinează în ce măsură existența unor relații, forme de cooperare sau de tolerare între grupările analizate și actori sau structuri statale ruse poate contribui la conturarea unui model de criminalitate cibernetică asociată intereselor statale, cu implicații asupra arhitecturii contemporane a securității cibernetice globale.

Ipoteza 1: Declanșarea conflictului în 24 februarie 2022 a acționat ca un factor declanșator de divizare a ecosistemului ransomware rusofon, determinând tranziția de la un model de operare orientat exclusiv către obținerea de câștiguri financiare, la un model de susținere a intereselor geopolitice ale Federației Ruse.

Ipoteza 2: Colaborarea informală dintre membrii grupărilor de criminalitate cibernetică și membrii serviciilor de informații ruse funcționează ca un mecanism de reciprocitate condiționată, unde susținerea invaziei din Ucraina devine o premisă necesară pentru menținerea impunității operative în fața legii.

Selecția cazurilor studiate în cadrul prezentei cercetări urmează o logică teoretică fundamentată pe criteriile de selecție a cazurilor propuse în literatura metodologică de specialitate, inclusiv în lucrările lui Gerring și Yin. Focalizarea asupra fenomenului *ransomware*, și nu asupra altor forme de amenințare cibernetică, precum spionajul cibernetic, este justificată prin poziționarea acestuia la intersecția dintre economia subterană și dimensiunea securității naționale. Specificitatea ecosistemului *ransomware* constă, printre altele, în existența unor forme vizibile de comunicare și interacțiune publică, prin intermediul site-urilor de *leaks*, al canalelor de negociere și al forumurilor utilizate de actorii cibernetici. Aceste caracteristici au permis identificarea unor surse primare relevante pentru investigarea transformărilor produse în cadrul ecosistemului, inclusiv a modului în care motivațiile predominant financiare se pot intersecta cu poziționări geopolitice și ideologice.

Pentru a asigura o validitate internă ridicată a studiului de caz multiplu, grupările *Conti* și *Black Basta* sunt selectate pentru a analiza două stadii distincte ale evoluției ecosistemului de criminalitate cibernetică rus. În completare, cazul grupării *The Gentlemen* confirmă faptul că, deși grupările de criminalitate cibernetică pot să fie dizolvate, activitatea și continuitatea operațională a acestor membri pot fi menținute prin migrarea acestora către alte structuri infracționale. Cazul *Conti* este unul de referință pentru înțelegerea modului în care o structură organizațională complexă de criminalitate cibernetică a fost afectată de asumarea unei poziționări politice. Analiza grupării *Conti* este esențială deoarece oferă un set de date exfiltrate (*Conti Leaks*), provenite din comunicațiile interne ale grupării și divulgate în contextul invaziei ruso-ucrainene în februarie 2022. Prin analiza acestui caz, cercetarea urmărește să examineze relația dintre poziționarea politică a grupării, structura sa internă și eventualele forme de influență sau control exercitate de actori statali asupra acesteia.

Cazul *Black Basta* este selectat pentru a analiza continuitatea unor actori și a unor

practici operaționale asociate anterior grupării *Conti*, având foarte multe similarități. Acest caz permite observarea procesului de reorganizare a ecosistemului criminalității cibernetice și a modului în care anumite elemente organizaționale și operaționale au fost menținute sau transformate. La aproximativ trei ani de la exprimarea publică a susținerii părții ruse de către *Conti*, cea de a doua grupare, *Black Basta*, a fost la rândul său afectată de divulgarea comunicațiilor sale interne. Datele publicate oferă posibilitatea unei analizări complexe, comparative despre evoluția structurii reorganizate și asupra continuității operaționale și a riscurilor de expunere. Abordarea comparativă permite cercetării să depășească limitele unei analize singulare și să examineze evoluția sistemică, către forme mai descentralizate și adaptabile. Selecția cazurilor, este, prin urmare, orientată nu doar către explicarea unor evenimente individuale, ci și către analiza transformării sistemice a amenințării în contextul presiunilor geopolitice asociate statului rus.

O condiție fundamentală pentru asigurarea rigurozității metodologice este stabilirea unor repere temporale fixe, care să permită analiza evoluției fenomenului independent de volatilitatea evenimentelor externe. În acest sens, cercetarea este delimitată temporal pentru perioada 2020-2026, interval care permite urmărirea evoluției actorilor și a activităților desfășurate în cadrul comunităților de criminalitate cibernetică. Observația a vizat forumuri de criminalitate cibernetică din *Dark Web*, site-urile publice asociate grupărilor analizate, precum și canale de *Telegram* și *TOX* utilizate pentru comunicarea internă. În cadrul acestei perioade, anul 2021 reprezintă un reper contextual important prin publicarea de către Vladimir Putin (Владимир Владимирович Путин) a eseului „Об историческом единстве русских и украинцев” („Despre unitatea istorică a rușilor și ucrainenilor”), care a formulat o serie de argumente istorice și politice privind relația dintre Rusia (Россия) și Ucraina (Україна). În cadrul prezentei cercetări, acest document este analizat ca element al cadrului discursiv care a precedat invazia și nu ca o cauză directă a mobilizării actorilor criminali cibernetici. Ca reper operațional, *T0* este stabilit la 25 februarie 2022, data la care gruparea *Conti* și-a exprimat public susținerea față de guvernul rus, la o zi după declanșarea invaziei.

Delimitarea temporală permite structurarea analizei în mai multe etape. Prima etapă vizează perioada 2020–2022 și urmărește evoluția grupării *Conti* până la momentul poziționării sale publice și al divulgării ulterioare a comunicațiilor interne. A doua etapă urmărește perioada de reorganizare și continuitate a unor actori în cadrul ecosistemului *ransomware*, cu focalizare asupra grupării *Black Basta*. Un al doilea reper empiric îl constituie 11 februarie 2025, data la care au fost divulgate comunicațiile interne ale grupării *Black Basta*, acestea acoperind în principal perioada septembrie 2023–septembrie 2024. A treia etapă o reprezintă evaluarea post-divulgare și *The Gentlemen Leaks* din 13 mai 2026. Ultima etapă a cercetării urmărește evoluțiile ulterioare acestor evenimente până la sfârșitul perioadei de observație, în septembrie 2026. Această delimitare temporală permite utilizarea

intervalului ca parametru de control pentru comparația dintre cazuri, facilitând analiza continuității actorilor, a modificărilor organizaționale și a transformărilor apărute în activitatea grupărilor analizate. Astfel, cercetarea nu se limitează la analiza unor evenimente izolate, ci urmărește evoluția ecosistemului de criminalitate cibernetică pe parcursul unei perioade delimitate, în raport cu principalele momente de dizolvare și reorganizare identificate empiric.

Metodologia cercetării este una calitativă, empirică și exploratorie, fundamentată pe un design de tip studiu de caz multiplu și comparativ. Validitatea empirică a cercetării este susținută printr-o strategie de triangulare a datelor, utilizată pentru verificarea și coroborarea informațiilor provenite din surse și tipuri de date diferite. Această arhitectură metodologică permite diferențierea între datele statice, informațiile provenite din scurgeri de date (*leaks*) și datele referitoare la dinamica actuală a ecosistemului, fiecare categorie fiind analizată prin instrumente metodologice adecvate specificului său.

O componentă majoră a materialului empiric este reprezentată de seturile extinse de date exfiltrate din infrastructurile grupărilor analizate, cunoscute sub denumirea de *Conti Leaks*, *Black Basta Leaks* și *The Gentlemen Leaks*. Aceste arhive constituie surse primare ale cercetării și permit accesul direct la comunicațiile interne ale grupărilor. Analiza jurnalelor de conversații, disponibile în formate precum *Jabber* și *JSON*, precum și a documentelor și protocoalelor interne referitoare la organizarea și desfășurarea activităților, este realizată prin intermediul analizei retrospective calitative de conținut. Această metodă permite identificarea și interpretarea temelor recurente, a relațiilor dintre actori, a rolurilor organizaționale și a schimbărilor intervenite în cadrul grupărilor analizate. Această abordare permite analizarea, pe de o parte, a structurii grupării *Conti*, care nu mai era activă la momentul inițierii cercetării, și, pe de altă parte, a structurii *Black Basta* și *The Gentlemen*, a căror activitate a putut fi urmărită în perioada în care acestea erau operaționale. În cazul acestora, coroborarea informațiilor provenite din surse publice cu datele divulgate ulterior a oferit elemente empirice pentru verificarea ipotezei privind continuitatea unor actori proveniți din ecosistemul *Conti* în cadrul noii structuri.

În perioada 2022–2026, analiza mesajelor publicate pe forumurile asociate comunităților de criminalitate cibernetică și a rapoartelor de securitate cibernetică publicate de companii specializate a permis identificarea unor relații și continuități între actorii analizați. Ulterior, informațiile provenite din scurgerile de date au permis verificarea și coroborarea acestor conexiuni. Datele divulgate au oferit acces la informații privind mecanismele interne de recrutare, relațiile ierarhice și distribuția rolurilor, precum și la interacțiunile dintre membrii grupărilor și anumite persoane sau entități despre care există indicii privind conexiuni cu structuri sau servicii de informații ruse.

Tratarea acestor comunicații ca arhive digitale permite cercetării să păstreze un corpus

empiric fix și verificabil, asupra căruia pot fi aplicate proceduri sistematice de analiză și coroborare. În acest mod, datele provenite din comunicațiile divulgate pot fi comparate cu informațiile obținute prin observația netnografică și cu sursele secundare de securitate cibernetică, contribuind la reducerea riscului unor interpretări bazate exclusiv pe observații izolate. Spre deosebire de analiza comunicațiilor interne divulgate, netnografia este utilizată în cadrul acestei teze ca instrument de monitorizare a dinamicii ecosistemului de criminalitate cibernetică pe forumuri *underground*, precum *XSS*, *Exploit* și *RAMP*, în intervalul 2022–2026. Metoda este aplicată pentru analiza modului în care membrii comunităților interacționează, discută și colaborează, precum și pentru examinarea mesajelor publicate în spațiile accesibile membrilor acestor forumuri.

În calitate de observator non-participant, cercetarea a urmărit discuțiile publice și semi-publice dintre *Brokerii de Acces Inițial* (*Initial Access Brokers* – IABs) și operatorii de *ransomware*, precum și interacțiunile dintre persoanele implicate în recrutarea unor noi membri sau în publicarea de anunțuri și mesaje pe forumuri. Monitorizarea sistematică a acestor interacțiuni a permis constituirea unui corpus observațional bazat pe stilul de comunicare, tiparele de interacțiune, comportamentul și activitatea actorilor analizați.

Un obiectiv important al aplicării netnografiei îl constituie observarea mecanismelor de auto reglementare existente în cadrul acestor comunități. În acest sens, cercetarea analizează, spre exemplu, modul în care unii moderatori au impus, după declanșarea invaziei, restricții privind publicarea unor mesaje referitoare la entități din spațiul CSI (Comunitatea Statelor Independente), informații privind arestarea unor membri ai comunității sau opinii referitoare la desfășurarea războiului. Aceste reguli și intervenții ale moderatorilor oferă indicii cu privire la mecanismele interne de control, auto reglementare și menținere a normelor comunitare.

Distincția dintre analiza comunicațiilor divulgate ca documente istorice și monitorizarea forumurilor ca mediu netnografic permite cercetării să surprindă atât evoluția grupărilor analizate, cât și comportamentul și interacțiunile actorilor în perioada în care acestea își desfășurau activitatea. Coroborarea celor două perspective oferă o bază empirică mai amplă pentru analiza transformărilor organizaționale și geopolitice din cadrul ecosistemului de criminalitate cibernetică, depășind perspectiva unei simple analize tehnice a atacurilor. Selecția forumurilor analizate este justificată prin relevanța acestora pentru comunitățile de criminalitate cibernetică investigate și prin volumul și diversitatea informațiilor disponibile pentru perioada analizată.

Pentru a asigura rigoarea științifică a demersului și pentru a evita ambiguitățile identificate în evaluările anterioare, prezenta cercetare propune o schemă de operaționalizare a conceptelor centrale. În cadrul studiului de față, conceptul de „instrumentalizare strategică” este operaționalizat prin intermediul unor indicatori empirici observabili în datele colectate,

care permit identificarea și analiza formelor concrete prin care actorii criminali cibernetici pot fi integrați în atingerea unor obiective de natură geopolitică. În acest sens, conceptul de „trecere de la profit la patriotism” este deconstruit în două dimensiuni fundamentale: dimensiunea motivațională, referitoare la modificarea obiectivelor și motivațiilor actorilor, și dimensiunea operațională, referitoare la modificarea comportamentului și a activităților desfășurate de aceștia în contextul conflictului ruso-ucrainean.

În ceea ce privește prelucrarea și interpretarea datelor, cercetarea utilizează *Process Tracing* pentru a analiza nu doar existența unei asocieri temporale între război și transformările comportamentale ale grupărilor de criminalitate cibernetică, ci și mecanismele prin care această transformare s-a produs. Cercetarea urmărește reconstruirea succesiunii de evenimente și identificarea mecanismelor cauzale care pot explica relația dintre variabila independentă, reprezentată de presiunile normative și operaționale asociate statului rus, și variabila dependentă, reprezentată de transformarea comportamentului și a poziționării grupărilor de criminalitate cibernetică.

Aplicarea acestei metode presupune utilizarea unor teste de evidență riguroase, precum „testul dovezilor concludente” și „testul condițiilor necesare”. De exemplu, prin analiza chat-urilor *Conti Leaks*, se vor căuta dovezi ale unor interacțiuni specifice care funcționează ca un mecanism de aplicare a voinței statale, cum ar fi sarcini primite prin intermediari sau menționarea unor imunități garantate în schimbul unor atacuri specifice sau procese de voluntariat. Această metodă va permite să se afirme dacă schimbarea de comportament a grupărilor este rezultatul unei evoluții organice sau, așa cum susține ipoteza tezei, rezultatul unei asocierii unor membri cu guvernul rus.

Utilizarea metodei *Process Tracing* permite depășirea unei narațiuni strict descriptive și orientarea analizei către identificarea mecanismelor prin care transformările geopolitice și presiunile asociate mediului de securitate rus au putut influența deciziile și comportamentul actorilor criminali cibernetici. Această abordare răspunde necesității de a fundamenta concluziile cercetării pe o analiză sistematică a succesiunii evenimentelor, a relațiilor dintre actori și a mecanismelor cauzale identificate în cadrul corpusului empiric. În sinteză, arhitectura metodologică propusă, urmărește consolidarea validității interne a cercetării. Coroborarea surselor primare, a observațiilor netnografice și a surselor secundare permite construirea unui cadru analitic pentru examinarea reconfigurării ecosistemului de criminalitate cibernetică în contextul transformărilor geopolitice și al conflictului ruso-ucrainean.

Lucrarea este structurată în patru capitole fundamentale, construite într-o succesiune logică și progresivă, care urmărește dezvoltarea cadrului teoretic și conceptual, fundamentarea metodologică a cercetării și aplicarea acesteia asupra ecosistemului contemporan de criminalitate cibernetică de tip *ransomware*. Structura lucrării permite trecerea de la analiza teoriilor și conceptelor relevante pentru înțelegerea spațiului cibernetic și a transformărilor

produse în cadrul relațiilor internaționale, la definirea și justificarea designului metodologic, pentru ca ulterior să fie analizate empiric dinamica, structurile organizaționale și transformările comportamentale ale grupărilor *ransomware* investigate. În acest mod, cele patru capitole contribuie, în mod complementar, la construirea cadrului analitic necesar examinării relațiilor dintre criminalitatea cibernetică, transformările geopolitice și actorii statali implicați în conflictul ruso-ucrainean.

Capitolul I, intitulat „*Fundamentare Teoretică și Conceptuală: Geopolitica Spațiului Cibernetic*”, constituie cadrul de revizuire a literaturii de specialitate și bazele teoretice ale cercetării, analizând modul în care teoriile clasice ale Relațiilor Internaționale (precum Realismul Structural și Neorealismul Ofensiv) se adaptează anarhiei specifice mediului digital. În cadrul acestuia, spațiul cibernetic este conceptualizat ca un domeniu de conflict geopolitic în care dilema de securitate este exacerbată de avantajul structural al ofensivei și de diminuarea constrângerilor geografice. Totodată, capitolul analizează o reconceptualizare a criminalității cibernetice (*cybercrime*), reîncadrând-o din simplă infracțiune financiară privată într-un act de război hibrid desfășurat în „*zona gri*” a relațiilor internaționale. În final, este analizată *Doctrina Federației Ruse* (Доктрина Российской Федерации) privind suveranitatea cibernetică (*RuNet-(PyHem)*) și sistemul de protecție informală *Krysha* (Крыша), demonstrându-se modul în care *Kremlinul* (Кремль) militarizează spațiul informațional prin instrumentalizarea strategică și cooptarea actorilor de tip *proxy*.

Capitolul II, intitulat „*Ecosistemul de criminalitate cibernetică din Rusia: convergența dintre profit și obiective strategice*”, reprezintă tranziția de la cadrul teoretic la realitatea operativă a spațiului digital rus, investigând infrastructura tehnică, financiară și juridică ce susține agresiunea asimetrică. Capitolul analizează paradigma suveranității digitale a Federației Ruse (Российская Федерация), *RuNet* (PyHem) și mecanismul „*aplicării selective a legii*”, demonstrând cum impunitatea oferită de *articolul 61 din Constituția rusă* (Статья 61 Конституции Российской Федерации) și garanția informală de protecție (*Krysha-Krysha*) sunt condiționate de orientarea atacurilor exclusiv în afara *Comunității Statelor Independente* (CSI) (Содружество Независимых Государств). Sunt analizate canalele economiei subterane, de la ecosistemul de spălare a criptomonedelor și piețele *Dark Web* (RAMP, XSS, Exploit), până la rolul esențial al *Brokerilor de Acces Inițial* (IABs) în modelul *Access-as-a-Service*. Totodată, este examinată reconfigurarea sistemică generată de invazia din 24 februarie 2022, marcând tranziția de la oportunitatea financiară la mobilizarea patriotică și alinierea la *Războiul de Nouă Generație* (NGW) (Война следующего поколения).

Capitolul III, intitulat „*Analiza Comparativă a Ecosistemului Ransomware: Cazul Conti și Black Basta*”, constituie nucleul empiric al lucrării și explorează evoluția și reorganizarea sistemică a amenințării prin intermediul unui studiu de caz multiplu și

comparativ. Fundamentat pe aplicarea metodei *Process Tracing*, a netnografiei și pe cadrul teoretic al structurilor *dissipative* (*Ilya Prigogine-Илья Пригожин*), capitolul reconstruiește evenimentele de cauzalitate ce asociază presiunea geopolitică a *Kremlinului* (*Кремль*) de conduita subordonată a infractorilor cibernetici. Analiza urmărește tranziția de la modelul organizațional și ideologizat al sindicatului *Conti* — a cărui aliniere publică a declanșat divizarea internă și scurgerea *Conti Leaks* — către modelul descentralizat, adaptiv și rezilient al grupării *Black Basta* (*Black Basta Leaks*). Prin traducerea și decodificarea surselor primare în limba rusă, inclusiv a argoului *Fenya* (*Фени*), capitolul expune relațiile ierarhice, mecanismele de extorcare, rețelele financiare de spălare a criptomonedelor (*Garantex*, *Media Land*) și legăturile dintre liderii grupărilor și serviciile ruse de informații (FSB, GRU). Totodată, este regăsită originalitatea empirică a cercetării prin realizarea organigramelor operaționale ale sindicatelor și identificarea numelor reale ale operatorilor-cheie (precum *Oleg Nefedov -Олег Неведов- GG/Trump* sau *Vitaly Kovalev - Виталий Ковалев- Stern/Bentley*).

Capitolul IV, intitulat „*Ecosistemul ransomware și evoluția lui*”, finalizează demersul analitic prin radiografierea dinamicii prospective a amenințărilor în intervalul 2025–2026 și prin evaluarea impactului noilor tehnologii asupra securității naționale. Capitolul investighează consolidarea modelului *Ransomware-as-a-Service* (RaaS) și a dublei extorcări, analizându-se al treilea studiu de caz empiric din mai 2026 privind gruparea *The Gentlemen* (*The Gentlemen Leaks*). Analiza chat-urilor interne expune tranziția către rețele experimentate, formate din nuclee restrânse de operatori veterani și afiliați atrași de modele economice de redistribuire a profitului deosebit de agresive. Totodată, este explorat rolul disruptiv al inteligenței artificiale generative (*WormGPT*, *FraudGPT* sau prima tulpină bazată pe IA, *ProimptLock*) în automatizarea ingineriei sociale, depășirea barierelor lingvistice, generarea de cod malițios în timp real și analiza rapidă a datelor exfiltrate. În a doua parte, capitolul conceptualizează pilonii de *Cyber-Intelligence* (CYBINT, OSINT, SOCMINT) ca instrumente esențiale de anticipare și analiză strategică a atacurilor asimetrice. În final se evaluează mecanismele de cooperare internațională, rolul operațiunilor de *Active Disruption* (precum Operațiunea *Endgame* a *Europol*) și al cadrului de diplomatie cibernetică în contracararea impunității oferite de statele ce adăpostesc membrii ai sindicatelor de criminalitate cibernetică și le asigură sprijin operațional sau avantaje strategice.

CONCLUZIILE LUCRĂRII

Prezenta teză de doctorat a investigat un fenomen definitoriu care a redefinit arhitectura de securitate globală contemporană: momentul în care grupările de criminalitate cibernetică au renunțat la neutralitatea financiară și au participat activ și asumat la un război cinetic, acționând ca proxy ai unui actor statal. Cercetarea a demonstrat că spațiul cibernetic nu mai reprezintă doar o infrastructură neutră de comunicații, ci a devenit unul dintre cele mai volatile și active medii ale competiției geopolitice, reconfigurând echilibrul de putere între actorii statali și non-statali. Fenomenul ransomware a depășit granițele criminalității financiare tradiționale, transformându-se într-o problemă de securitate națională și un instrument esențial al războiului hibrid și asimetric.

Demersul empiric, fundamentat pe analiza netnografică și metoda Process Tracing aplicate pe surse primare (arhivele ContiLeaks, Black Basta Leaks), a validat întrebarea de cercetare, demonstrând faptic că statul rus a exploatat anarhia din spațiul cibernetic pentru a obține avantaje strategice. Răspunsul la această întrebare a evidențiat procesul prin care Kremlinul a creat o „zonă gri”, în care interesele criminale s-au intersectat cu obiectivele doctrinei militare ruse. Această zonă a permis Rusiei să externalizeze agresiunea asimetrică către proxy-uri cibernetică, menținând astfel un regim de negare plauzibilă pe scena internațională.

Transformarea a fost determinată de integrarea ecosistemului infracțional în strategia de confruntare informațională a Rusiei. Prin folosirea acestor grupări ca instrumente indirecte de putere, Rusia a vizat sectoare critice occidentale (sănătate, energie, logistică) pentru a produce sabotaj economic și subversiune psihologică, estompând complet linia de demarcație dintre pace și conflict deschis. Răspunsul la întrebarea de cercetare subliniază că atacatorii, pe fondul declanșării războiului, nu au mai urmărit exclusiv extorcarea, ci au sprijinit o stare de non-pace, menită să blocheze instituțiile țărilor care susțineau Ucraina.

Lucrarea a formulat și testat două ipoteze majore, ambele fiind confirmate de analiza empirică a conversațiilor interne și a dinamicilor structurale ale grupărilor studiate.

Validarea Ipotezei 1: Declanșarea conflictului în 24 februarie 2022 a acționat ca un factor declanșator de divizare a ecosistemului ransomware rusofon, determinând tranziția de la un model de operare orientat exclusiv către obținerea de câștiguri financiare la un model de susținere a intereselor geopolitice ale Federației Ruse. Această ipoteză a fost validată integral prin analiza de caz a grupării Conti. Războiul din Ucraina a acționat ca un punct de inflexiune sistemică, eliminând mitul independenței apolitice a criminalității cibernetică. În data de 25 februarie 2022, la doar o zi după invazie, conducerea grupării Conti a publicat pe blogul propriu o declarație în care își asuma sprijinul deplin pentru guvernul rus, amenințând cu atacuri distructive asupra infrastructurii critice a inamicilor care ar riposta. Această trecere

asumată de la profit la patriotism, a invalidat regula neutralității și a provocat imediat o fractură internă majoră. Divizarea ecosistemului pe criterii ideologice și naționaliste a fost demonstrată de fenomenul ContiLeaks: un cercetător cibernetic ucrainean a ripostat împotriva conducerii pro-ruse, publicând peste 170.000 de jurnale de chat interne și expunând arhitectura întregii grupări. Așadar, ipoteza se confirmă: ecosistemul cibernetic nu mai este unit doar de motivul economic, ci s-a fracturat organic în tabere de susținere a beligeranților, confirmând transformarea sa într-un instrument asimetric și ideologizat al războiului.

Validarea Ipotezei 2: Colaborarea informală dintre membrii grupărilor de criminalitate cibernetică și membrii serviciilor de informații ruse funcționează ca un mecanism de reciprocitate condiționată, unde susținerea invaziei din Ucraina devine o premisă necesară pentru menținerea impunității operative în fața legii. Ipoteza a fost validată empiric, evidențiindu-se funcționarea mecanismului mafiot de protecție, denumit *krysha* („acoperiș”). Statul rus garantează infractorilor ciberneticici impunitatea în fața extrădării, folosindu-se de Articolul 61 din Constituția Federației Ruse, și aplică în mod selectiv Articolele 272 și 273 din Codul Penal. Acest contract social informal prevede o protecție totală din partea Serviciului Federal de Securitate (FSB), atâta timp cât hackerii respectă regula strictă de a nu ataca ținte din Comunitatea Statelor Independente (CSI). Mai mult, chiar și atunci când au loc arestări interne (precum cazul grupării REvil), acestea servesc adesea ca mecanism de cooptare și recrutare forțată a specialiștilor în structurile de intelligence, statul naționalizând practic criminalitatea cibernetică.

Arhivele divulgate au oferit probe privind subordonarea și cooperarea dintre liderii grupărilor și FSB/GRU. În ContiLeaks, s-a descoperit că liderul Stern lucra pentru FSB, membrii operau din proximitatea sediilor FSB din Moscova și Sankt Petersburg și discutau despre solicitări venite din partea agențiilor de informații, inclusiv cooperarea cu grupările APT guvernamentale („urși” – APT29/Cozy Bear) și spionarea jurnaliștilor care investigau guvernul (ex. cazul Navalnîi). Similar, publicarea datelor Black Basta din 2025 a confirmat această continuitate a corupției sistemice: liderul Oleg Nefedov (GG/Tramp) a recunoscut explicit în mesageria TOX că a mituit ofițeri din Lubianka (FSB) și GRU pentru a beneficia de protecție. În momentul reținerii sale în Armenia, un „coridor verde” asigurat de persoane influente de la nivelul conducerii din Rusia a permis extragerea sa imediată la Moscova, potrivit informațiilor rezultate din conversațiile analizate, dovedind că impunitatea garantată de stat este complet integrată la cel mai înalt nivel politic.

O componentă fundamentală a cercetării a constatat în analiza evoluției structurale a ecosistemului de criminalitate cibernetică rusofon. Pentru a explica modul în care acest ecosistem a supraviețuit expunerilor masive de date (leaks) și sancțiunilor internaționale, lucrarea a aplicat conceptul structurilor disipative. Conform acestei perspective, syndicatele de criminalitate cibernetică funcționează ca sisteme complexe aflate departe de echilibru; în

momente de criză critică sau divizare (precum incidentul ContiLeaks generat de invazia Ucrainei), aceste sisteme nu se dezintegrează definitiv, ci se reorganizează în forme noi, mai flexibile și mai adaptive. Triangularea datelor din surse primare (ContiLeaks și Black Basta Leaks) a permis radiografierea acestei tranziții de la structuri monopoliste, semi-corporatizate, la rețele descentralizate și extrem de persistente.

Cercetarea a demonstrat că gruparea Conti a reprezentat apogeul maturizării organizaționale în ecosistemul ransomware. A depășit modelul tradițional al grupărilor restrânse de hackeri, Conti a funcționat după un model de afaceri corporatist complet integrat, capabil să genereze profituri anuale estimate la sute de milioane de dolari. Analiza conversațiilor interne a scos la iveală o organigramă rigidă și o diviziune clară a muncii: departamente de resurse umane (HR) care recrutau activ pe forumuri (precum headhunting.ru din Moscova), echipe de programatori (coderi), specialiști în pentesting, experți OSINT pentru profilarea victimelor și o echipă de negociatori (apelanți). Angajații beneficiau de salarii fixe (plătite în Bitcoin), evaluări de performanță, zile de concediu și bonusuri de performanță. Lideri precum Stern, Target, Tramp sau Mango gestionau bugete uriașe, coordonau zeci de afiliați și chiar intenționau să creeze propriile rețele sociale pe Dark Web (proiectul matrioska.ru) și platforme de schimb cripto (Bablo) pentru a face spălare de bani.

Mai mult, cercetarea a infirmat mitul hackerului izolat: membrii de la vârful Conti operau inclusiv din birouri fizice situate în Moscova sau Sankt Petersburg și călătoreau frecvent pentru întâlniri în Dubai. Deși au atins un succes financiar fără precedent, alinierea ideologică pro-rusă asumată în 25 februarie 2022 a generat o divizare internă, ducând la publicarea a peste 168.000 de mesaje interne și, în final, la închiderea oficială a brandului Conti în mai 2022. Închiderea nu a însemnat dispariția amenințării, demonstrând reziliența structurală a ecosistemului. Răspunsul la această criză a fost reorganizarea imediată sub noi identități. Apărută în aprilie 2022, la doar câteva săptămâni după publicarea de date Conti, gruparea Black Basta a fost identificată faptic ca fiind un succesor direct al acesteia. Cercetarea a validat această continuitate prin identificarea acelorași membri cheie care operau sub noi aliasuri. De exemplu, operatorul principal Tramp din Conti a condus Black Basta sub pseudonimul GG (identificat ulterior ca Oleg Nefedov), având peste 80.000 de mesaje de coordonare.

Black Basta a moștenit infrastructura operațională, tacticile de dublă extorcare, rețelele de spălare a banilor (ex. Garantex) și preferința pentru aceleași ținte critice din Occident, menținând totodată regula strictă de a nu ataca statele din CSI. Totuși, Black Basta a demonstrat o rafinare a tehnicilor de inginerie socială, utilizând atacuri de tip vishing (phishing vocal) și inginerie socială prin Microsoft Teams, pozând în echipe de help-desk pentru a convinge angajații să instaleze aplicații de acces la distanță precum AnyDesk. Deși Black Basta a încercat să își compartimenteze mai bine operațiunile pentru a evita soarta

Conti, ecosistemul infrațional a rămas vulnerabil la tensiunile interne, generând Black Basta Leaks în februarie 2025, când aproximativ 197.000 de mesaje au fost expuse, ducând din nou la expunerea liderilor și la arestări (inclusiv a lui Nefedov).

Un studiu de caz recent din 4 mai 2026 reflectă stadiul actual al evoluției ecosistemului: trecerea la structuri restrânse, ultra-specializate și extrem de agile. Apărută în mai 2025 în urma unei dispute financiare în cadrul grupării Qilin, operațiunea The Gentlemen marchează o nouă paradigmă în modelul Ransomware-as-a-Service (RaaS). Cercetarea relevă că infractorii cibernetici au învățat din vulnerabilitățile structurii Conti și s-au adaptat. The Gentlemen operează cu un nucleu restrâns de aproximativ nouă operatori, centrați în jurul administratorului zeta88 (hastalamuerte). Agilitatea acestui grup este demonstrată de viteza cu care acționează: zeta88 a construit panoul de administrare RaaS în doar trei zile, cu asistența inteligenței artificiale. Pentru a atrage cei mai experimentați afiliați din syndicatele rivale, The Gentlemen a modificat agresiv modelul economic, oferind afiliaților până la 97% din veniturile obținute din extorcarea datelor (fără criptare) și 90% pentru atacurile ransomware clasice. Tactic, au renunțat la achiziționarea constantă de vulnerabilități zero-day, preferând o abordare oportunistă: valorifică eficient ecosistemul subteran de acreditări furate (info stealers), scanând jurnalele pentru a accesa VPN-uri și portaluri corporative vulnerabile. Cazul The Gentlemen, ale căror date au fost de asemenea publicate în mai 2026, demonstrează fluiditatea absolută a pieței actuale: un simplu afiliat nemulțumit astăzi poate lansa și administra mâine un sindicat RaaS de top. Ecosistemul nu mai este controlat de câteva carteluri, ci de rețele interconectate, capabile să se dizolve și să se reorganizeze sub un nou brand, menținând un ritm constant de atac asupra infrastructurilor critice globale, inclusiv pe teritoriul României.

O altă concluzie majoră a cercetării vizează arhitectura logică a ecosistemului infrațional. Lucrarea a demonstrat că eficiența grupărilor de tip ransomware nu derivă exclusiv din codul malițios, ci dintr-o diviziune a muncii extrem de bine structurată și dintr-un lanț de aprovizionare complex (supply chain) care funcționează pe Dark Web. Războiul asimetric contemporan este industrializat prin intermediul modelului Access-as-a-Service și Ransomware-as-a-Service (RaaS). Cercetarea a evidențiat că Brokerii de Acces Inițial (IAB) au devenit esențiale în ofensiva cibernetică. Aceștia acționează ca intermediari specializați: compromit rețelele țintă prin phishing, forță brută sau exploatarea vulnerabilităților de rețea privată virtuală (VPN) și a protocolului de acces la distanță (RDP), dar nu criptează datele. În schimb, vând aceste accese sindicatelor RaaS pe forumuri exclusiviste de limbă rusă (RAMP, XSS, Exploit).

Dinamica observată arată o tranziție către relații business-to-business (B2B) și o integrare pe verticală. De exemplu, jurnalele ContiLeaks au arătat cum liderii Conti negociau direct procente din răscumpărare cu brokeri precum RDP Corp. Prin externalizarea intruziunii,

sindicatelor își comprimă timpul de execuție de la luni la doar câteva zile, limitând reacția instituțiilor de securitate. Din punct de vedere financiar, cercetarea concluzionează că grupările sunt total dependente de platforme specializate pentru spălarea veniturilor obținute din șantaj, folosind o triadă clasică: plasare, stratificare, integrare. Trecerea de la Bitcoin la monede cu nivel ridicat de anonimizare (precum Monero) și folosirea serviciilor de mixare (tumblers) demonstrează adaptarea la monitorizarea internațională.

Atât Conti, cât și Black Basta au utilizat platforma rusească Garantex (ulterior sancționată de SUA) pentru a spăla zeci de milioane de dolari. Un element de noutate surprins în teză este tendința de utilizare a Jetoanelor Nefungibile (NFT-uri) pentru spălarea sumelor, dar și dependența de „călăreți de bani” (drop-uri) recrutați prin Telegram (precum serviciul Laundromat) pentru conversia în monedă fiat. S-a demonstrat inclusiv intenția conducerii Conti, prin aliasul Mango și Stern, de a crea o rețea socială și de criptomonede proprie pe Dark Web (matrioska.ru/Bablo), pentru a controla întregul lanț de spălare a banilor și a se dezafilia de intermediarii vulnerabili la sancțiuni.

O altă concluzie are în vedere demonstrarea adaptării tehnologice profunde pe care ecosistemul a suferit-o în perioada 2025-2026: tranziția de la atacuri manuale la automatizarea ofensivei prin inteligența artificială. Teza validează faptul că inteligența artificială funcționează acum ca un multiplicator de forță asimetric în confruntarea informațională. Infracatorii cibernetici rusofoni au trecut de etapa utilizării modelelor comerciale legitime, precum ChatGPT și au dezvoltat propriile rețele de IA fără restricții etice. Cercetarea documentează apariția unor instrumente LLM underground, precum WormGPT, FraudGPT, DarkBERT sau ChaosGPT. Acestea permit generarea automată de cod malițios și scrierea unor campanii de phishing și spear-phishing corecte gramatical și contextual, anulând barierele lingvistice pentru hackerii ruși.

A fost observată inclusiv adaptarea directă a IA în grupările studiate. Black Basta și-a creat propriul chat-bot intern numit BlackBastaGPT, iar gruparea The Gentlemen folosește asistenți IA (precum DeepSeek sau Qwen) pentru redactarea de cod și planifică utilizarea IA pentru procesarea și analiza rapidă a volumelor uriașe de date exfiltrate, în scopul extorcării țintite. În plus, a fost identificat un punct de inflexiune lansarea în 2025 a primului ransomware bazat pe inteligență artificială, PromptLock, capabil să genereze scripturi malițioase în timp real, adaptându-se dinamic la mecanismele de apărare ale victimei.

În concordanță cu Doctrina Gherasimov privind războiul informațional-psihologic, IA este utilizată pentru a eroda încrederea societăților democratice. Utilizarea tehnologiilor deepfake (audio/video) și a clonării vocale (vishing) permite atacatorilor să simuleze identități adevărate. Așa cum s-a observat la Black Basta, gruparea a implementat tehnici de vishing prin Microsoft Teams, apelând angajații și dându-se drept personal de la help-desk (IT) pentru a-i convinge să descarce sarcina utilă. Integrarea IA automatizează etapa de inginerie socială,

acelerează masiv etapa de intruziune și modifică modelul de șantaj. Chatbot-urile IA sunt folosite acum inclusiv pentru a negocia direct cu victimele plata răscumpărării, menținând un nivel ridicat de presiune psihologică fără implicare emoțională sau efort uman direct din partea atacatorului. Aceste inovații indică faptul că, pentru Federația Rusă, IA reprezintă pilonul tranziției către războiul de nouă generație (NGW), un instrument ideal pentru colapsarea proceselor decizionale din statele NATO, evitând pragul cinetic al Articolului 5.

Deși arhitectura metodologică a acestei teze de doctorat a fost riguros fundamentată pe triangularea datelor, utilizând netnografia și metoda Process Tracing aplicate direct pe surse primare de tip *leaks*, cercetarea recunoaște existența unor limite obiective. Aceste limitări decurg în mod inherent din natura clandestină, puternic securizată și volatilă a ecosistemului de criminalitate cibernetică rusească investigat. În primul rând, o limitare a cercetării o constituie imposibilitatea analizei interacțiunilor desfășurate în mediul fizic (offline). Deși datele digitale au permis creionarea unei organigrame detaliate și a rețelelor de comunicare, o parte semnificativă a activităților și negocierilor strategice ale membrilor de nivel superior a avut loc față în față, în birourile fizice din Moscova și Sankt Petersburg sau în timpul călătoriilor acestora în locații precum Dubai,. Aceste întâlniri fizice influențează direct dinamica grupării și deciziile organizaționale, aspecte care nu pot fi captate integral doar prin analiza amprentei digitale.

În al doilea rând, persistă dificultatea structurală a atribuirii atacurilor și a probării ordinilor de stat. Mediul cibernetic se caracterizează prin anonimat și garantează actorilor statali avantajul tactic al negării plauzibile. Deși arhivele de mesaje interne probează asocieri clare și colaborări cu ofițeri ai FSB sau GRU, de exemplu, subordonarea liderilor *Stern* sau *Bentley*, estomparea intenționată a graniței dintre un atac oportunist și un sabotaj direct coordonat de Kremlin rămâne o barieră în analizele de securitate.

În al treilea rând, dependența cercetării de baze de date statice de tip Leaks (ContiLeaks și Black Basta Leaks) reprezintă o limitare temporală,. Deși aceste documente constituie o oportunitate unică pentru cercetare, ele reprezintă doar capturi cronologice (ex. 2020-2022 pentru Conti; 2023-2024 pentru Black Basta) ale unui ecosistem extrem de dinamic și complex. Grupările infracționale își modifică frecvent tacticile, tehnicile și procedurile (TTP) și se rebranduiesc rapid pentru a evita monitorizarea forțelor de ordine.

În al patrulea rând, accesul direct la membrii grupării prin mesaje în grupurile interne de Telegram, TOX sau pe forumurile rusofone, a fost limitat. Aceste persoane sunt foarte discrete și nu comunică informații cu persoane din exterior. Cu toate acestea, există cazuri în care membrii ai unor grupări au acordat interviuri cercetătorilor renumiți în analize de securitate cibernetică, însă membrii acestor grupări nu au fost intervievați în cadrul prezentei cercetări.

Transformarea accelerată a ecosistemului de criminalitate cibernetică și

interconectarea acestuia cu instrumentele geopolitice deschid multiple direcții de cercetare necesare pentru dezvoltarea viitoare a studiilor de securitate cibernetică. Analiza noilor grupări derivate și internaționalizarea fenomenului ransomware, reprezintă o direcție viitoare necesară. Cercetările viitoare ar trebui să analizeze dinamica unor grupări emergente și flexibile precum Akira, Royal, Qilin sau RansomHub, investigând modul în care afiliații migrează între aceste rețele. De asemenea, este necesară explorarea internaționalizării acestui model, întrucât previziunile indică faptul că actorii ransomware din afara Federației Ruse vor deveni numeric superiori celor autohtoni, divizând și mai mult arhitectura de securitate globală.

Evoluția LLM-urilor malițioase (precum WormGPT sau FraudGPT) și implementarea primului ransomware bazat pe inteligență artificială (PromptLock) reprezintă doar începutul. Direcțiile viitoare de cercetare trebuie să evalueze impactul pe care agenții IA autonomi îl vor avea în războiul hibrid, unde aceștia ar putea coordona simultan operațiuni de dezinformare (deepfake) împreună cu sabotajul infrastructurilor fizice (logistică, rețele energetice) pentru a genera colaps social. De asemenea, evoluția criptografiei post-cuantice necesită investigații strategice, deoarece utilizarea acesteia de către infractori va face decriptarea datelor imposibilă în absența achitării răscumpărării.

O altă direcție de cercetare vizează evaluarea eficienței instrumentelor de Diplomatie Cibernetică și a măsurilor de Active Disruption, deoarece demersurile viitoare ar trebui să analizeze eficacitatea acțiunilor transnaționale ale forțelor de ordine, cum a fost Operațiunea Endgame a Europol) asupra rezilienței rețelelor Dark Web,. Este vitală studierea impactului pe care instrumentarul diplomatic (precum EU Cyber Diplomacy Toolbox) și Convenția ONU împotriva criminalității cibernetice îl au în transformarea atribuirii tehnice în costuri și sancțiuni politice reale pentru statele care garantează imunitate grupurilor de hackeri.

O ultimă direcție de cercetare are în vedere monitorizarea celor mai persistente grupări de ransomware începând cu anul 2026. Ca în cazul Conti și Black Basta, grupările pot să fie și ele compromise și pot apărea online alte informații interne are oricăror alte grupări, așa cum s-a întâmplat cu The Gentleman în luna mai 2026. Astfel, studierea acestor grupări și analiza modului în care acestea operează, reprezintă o direcție de cercetare importantă.

În sinteză, prezenta teză de doctorat demonstrează faptul că spațiul cibernetic a depășit statutul de infrastructură tehnologică neutră, devenind principalul teatru de operațiuni asimetrice și competiție geopolitică al secolului XXI. Fenomenul ransomware, analizat istoric sub lupa criminologiei ca o simplă infracțiune financiară de extorcere, s-a transformat într-o problemă de securitate națională și într-un instrument al războiului hibrid. Cercetarea validează premisa conform căreia invazia Federației Ruse în Ucraina, declanșată la 24 februarie 2022, a acționat ca un punct de inflexiune sistemică. Acest eveniment a eliminat mitul independenței apolitice a criminalității cibernetice rusofone, determinând o fractură

ideologică care a forțat sindicatele de tip Ransomware-as-a-Service să abandoneze neutralitatea financiară în favoarea susținerii doctrinei a aparatului de stat rus.

Prin intermediul studiului de caz comparativ aplicat arhivelor exfiltrate (ContiLeaks și Black Basta Leaks), lucrarea a decriptat mecanismul de asociere prin care Kremlinul a naționalizat parțial criminalitatea cibernetică. Beneficiind de o protecție informală garantată de instituțiile de securitate rusești, de tip krysha (acoperiș), și de aplicarea selectivă a Codului Penal, acești infractori cibernetici au devenit proxy-uri strategici. Această externalizare a agresiunii permite Rusiei să proiecteze forță disruptivă împotriva infrastructurilor critice din statele occidentale, generând un impact socio-economic constant.

Complexitatea amenințării a fost amplificată structural prin industrializarea lanțului de intruziune. Brokerii de Acces Inițial (IAB) au transformat breșele de securitate într-o afacere tranzacționabilă, iar ecosistemele underground de spălare a criptomonedelor asigură circuitul capitalului ilicit. În plus, utilizarea noilor capacități de inteligență artificială transformă aceste grupări din simpli extorcatori în actori specializați în operațiuni de subversiune psihologică și manipulare decizională. Prin urmare, concluzia centrală a acestei teze subliniază că răspunsul la amenințarea ransomware nu se mai poate rezuma la consolidarea izolată a securității rețelelor. Destructurarea acestor sindicate necesită o cooperare internațională coerentă, cât și aplicarea diplomației cibernetice. Succesul pe termen mediu și lung, într-un mediu dominat de asimetrie și de doctrina Războiului de Nouă Generație, va depinde de capacitatea instituțiilor globale de a lupta împotriva ecosistemului de criminalitate cibernetică.

Prin urmare, toate aceste argumente și demonstrații empirice confirmă validitatea direcției de studiu asumate prin această teză de doctorat. Cercetarea a demonstrat faptul că peisajul digital nu mai poate fi separat de conflictele cinetice internaționale. Invazia din februarie 2022 a reprezentat un punct de inflexiune ce a determinat o reconfigurare profundă și o fragmentare ideologică a ecosistemului infracțional rusofon, infractorii fiind recrutați, asimilați sau tolerați pentru a transforma extorcerea cibernetică într-o armă proxy a statului. Astfel, lucrarea concluzionează că analiza securității cibernetice trebuie să depășească barierele tehnice sau criminologice tradiționale și să integreze fenomenul ransomware în studiile de geopolitică, aceasta reprezentând o abordare care să anticipeze și să neutralizeze amenințările care redefinesc în mod continuu granițele puterii și suveranității naționale în secolul XXI. Divizarea grupărilor de ransomware în tabere de susținere a beligeranților a reprezentat problema identificată în cadrul acestui ecosistem, dar și elementul de noutate pe care s-a bazat această lucrare. Analizarea, citirea și interpretarea discuțiilor în limba rusă dintre hackeri au oferit o perspectivă nouă asupra modului în care aceștia colaborează și interacționează, iar legătura dintre membrii grupărilor de ransomware și guvernul rus nu mai poate fi contestată.

Demersul analitic al prezentei teze de doctorat a plecat de la premisa că invazia Federației Ruse în Ucraina din 24 februarie 2022 a marcat o fractură sistemică definitivă, ce impune o reconfigurare profundă a modului în care înțelegem criminalitatea cibernetică în Relațiile Internaționale. Obiectivul fundamental al cercetării nu a fost o simplă cartografiere tehnică sau o cronică a atacurilor IT, ci demonstrarea unei schimbări calitative de ordin geopolitic: transformarea unor syndicate infracționale private în vectori de război hibrid, cooptați și instrumentalizați de un stat revizionist. Prin investigarea empirică riguroasă a datelor primare din arhivele *ContiLeaks*, *Black Basta Leaks* și *The Gentlemen Leaks*, lucrarea a analizat funcționarea invizibilă a „zonei gri”, demonstrând cum garanția de impunitate oferită prin sistemul informal *Krysha* a consolidat legătura dintre criminalitatea organizată și guvernul rus.

Analiza derulată confirmă faptul că războiul contemporan nu mai poate fi conceptualizat doar prin intermediul bătăliilor cinetice și al frontierelor terestre. Ransomware-ul s-a dovedit a fi cel mai eficient instrument de extorcare și vizare strategică sub pragul unui casus belli convențional, erodând distincțiile clasice din *Jus in bello* dintre spațiul civil și cel militar, dintre infracțiunea financiară privată și acțiunea asumată de stat.

Privind spre viitor, dinamica observată până în anii 2025–2026 indică faptul că ecosistemul de ransomware nu va dispărea în urma presiunilor internaționale, ci va continua să evolueze spre forme tot mai disipative, opace și reziliente. Apariția sindicatelor ultra-agile precum *The Gentlemen*, asociată cu proliferarea Inteligenței Artificiale Generative (de la modele underground de tip WormGPT până la tulpini autonome precum PromptLock), marchează începutul unei noi ere în care barierele tehnice de intrare scad, iar viteza de execuție a atacurilor asimetrice crește exponențial. Această accelerare tehnologică va amplifica starea de non-pace (unpeace) în spațiul digital, transformând amenințarea cibernetică într-o constantă existențială a politicii globale.

În final, această teză de doctorat demonstrează că înțelegerea metamorfozei ransomware-ului nu reprezintă doar un exercițiu academic de decodificare a trecutului recent, ci o grilă de lectură esențială pentru descifrarea noii ordini geopolitice, influențată de grupările de criminalitate cibernetică în continuă evoluție. Într-un mediu internațional caracterizat de anarhie digitală și competiție între marii actori, modul în care comunitatea internațională va reuși să înțeleagă, să deconspire și să contracareze această convergență dintre criminalitatea subterană și agenda de stat va defini însăși reziliența arhitecturii globale de securitate în deceniile ce vor urma.

BIBLIOGRAFIE

Bibliografie primară

Abaimov Stanislav, Martellini Maurizio, *Cyber Arms: Security in Cyberspace*, CRC Press, 2020, 395 pag.

Ackerman Pascal, *Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment*, ed. a II-a, Birmingham, Packt Publishing, 2021, 800 pag.

Aitel Dave, d'Antoine Sophia, Garwin Thomas, Roos Ian, Rostow Nicholas, Sherman Justin, Wagner Abraham, Margin Research, *Russia's Cyber Operations: A Threat to American National Security*, New York, 2022, 119 pag.

Alexandrou Alex, *Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*, Boca Raton, CRC Press / Taylor & Francis, 2021, 455 pag.

Arquilla John, Ronfeldt David, „Cyberwar is Coming!”, în: *Comparative Strategy*, vol. 12, nr. 2, 1993, pp. 141-165, https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf, accesat în data de 12.01.2023.

Austin Greg, *Cyber Policy and Economics in an Era of Uncertainty*, London, Routledge, 2014, pp. 45-52.

Bandura Albert, *Moral Disengagement: How People Do Harm and Live with Themselves*, New York, Worth Publishers, 2014, pp. 45-50.

Bandura Albert, *Social Learning Theory*, Englewood Cliffs, Prentice-Hall, 1977, pp. 22-26.

Barker Jessica, *Confident Cyber Security: The essential insights and how to protect from threats*, Londra, Kogan Page, 2023, 265 pag.

Bateman Jon, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Washington, D.C., Carnegie Endowment for International Peace, 2022, 78 pag.

Baylis John, Wirtz James J., Gray Colin S. (editori), *Strategy in the Contemporary World: An Introduction to Strategic Studies* (Sixth Edition), Oxford, Oxford University Press, 2019, 477 pag.

Bodungen Clint, *ChatGPT for Cybersecurity Cookbook: Learn practical generative AI recipes to supercharge your cybersecurity skills*, Birmingham, Packt Publishing, 2023, 372 pag.

Buchanan Ben, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Cambridge, Harvard University Press, 2020, pp. 107-111.

Butler Michael, Wakley Jacob G., *The Business of Hacking: Creating, Developing, and Maintaining an Effective Penetration Testing Team*, Boca Raton, CRC Press, 2024, 311 pag.

Buzan Barry, Wæver Ole, Wilde de Jaap, *Security: A New Framework for Analysis*, Boulder, Lynne Rienner Publishers, 1998, pp. 23-26.

Calder Alan, *The Cyber Security Handbook*, Ely, IT Governance Publishing, 2022, 361 pag.

Caruso Jeffrey, *Inside Cyber Warfare: Mapping the Cyber Underworld*, ed. a III-a, Sebastopol, O'Reilly Media, 2024, 249 pag.

Cyberint, *Israel-Hamas vs. Russia-Ukraine War: Cyber Warfare Insights*, Tel Aviv, Cyberint Technologies, 2024, 35 pag.

Dahj Jean Nestor M., *Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense*, Birmingham, Packt Publishing, 2022, 528 pag.

Dover Robert, Goodman Michael S., Hillebrand Claudia (eds.), *Routledge Companion to Intelligence Studies*, Londra, Routledge, 2013.

Dunn Cavelty Myriam, Wenger Andreas (ed.), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Londra, Routledge, 2022, 287 pag.

Edwards Jason, *Mastering Cybersecurity: Strategies, Technologies, and Best Practices*, San Francisco, No Starch Press, 2024, 790 pag.

Erendor Mehmet Emir, *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, Wilmington, Vernon Press, 2024, 233 pag.

Galeotti Mark, *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*, Policy Brief, European Council on Foreign Relations (ECFR), 2017.

GitHub, *Conti Ransomware Internal Jabber Chat Logs (DeepL Translated) – File: 185.25.51.173-20210409_en-US.json*, 2022, https://github.com/TheParmak/conti-leaks-englished/blob/master/english_chats/deepL_translated_jabber/2021/185.25.51.173-20210409_en-US.json, accesat în data de 02.03.2023.

Goșu Armand, *Războiul fără sfârșit: Cum a schimbat invadarea Ucrainei regulile jocului*, Iași, Polirom, 2026, 308 pag.

Graham James, Howard Richard, Olson Ryan (editori), *Cyber Security Essentials*, Boca Raton, CRC Press, 2011, 331 pag.

Gerring, J. (2017). *Case Study Research: Principles and Practices* (2nd ed.). Cambridge University Press.

Greenberg Andy, *Sandworm: A New Era of Cyber War and the Hunt for the Kremlin's Most Dangerous Hackers*, New York, Anchor Books, 2020, 379 pag.

Greenberg Andy, *Traces in the Dark: The Global Hunt for the Dark Web's Cybercriminals*, New York, Doubleday, 2022, 516 pag.

Grimes Roger A., *Ransomware Protection Playbook*, Hoboken, John Wiley & Sons, 2021, 323 pag.

Gritsenko Daria, *The Palgrave HandBook of Digital Russia Studies*, 2021, pp. 115-135,

<https://link.springer.com/book/10.1007/978-3-030-42855-6>, accesat în data de 04.06.2023.

Gururaj H. L., Janhavi V., Ambika V. (editori), *Social Engineering in Cybersecurity: Threats and Defenses*, Boca Raton, CRC Press, 2024, 241 pag.

Hillebrand Gregory D., Ault Bill, *Strategic Cyberspace Operations Primer*, Carlisle, U.S. Army War College, 2023, 221 pag.

Holt Thomas J., Bossler Adam M., Seigfried-Spellar Kathryn C., *Cybercrime and Digital Forensics: An Introduction*, New York, Routledge, 2022, 813 pag.

Howard Rick, *Cybersecurity First Principles: A Reboot of Strategy and Tactics*, Hoboken, John Wiley & Sons, 2023, 401 pag.

Janeja Vandana P., *Data Analytics for Cybersecurity*, Cambridge, Cambridge University Press, 2022, 207 pag.

Jenkinson Andrew, *Ransomware and Cybercrime*, Londra, Routledge, 2024, 199 pag.

Junta Interamericana de Defensa, *Cyber Defense Handbook: Guidelines for the design, planning, implementation and development of a military cyber defense*, Washington, D.C., Inter-American Defense Board, 2022, 101 pag.

Kaplan Jacob, *Crime by the Numbers: A Guide to Analyzing and Understanding Publicly Available Crime Data*, Philadelphia, University of Pennsylvania, 2023, 432 pag.

Karmakar Abhishek, *Certified blackhat: Methodology to unethical hacking*, Chandigarh, White Falcon Publishing, 2019, 135 pag.

Kaspersky, *Common TTPs of Modern Ransomware Groups*, Moscova, Kaspersky Lab, 2023, 137 pag.

KELA, *TELEGRAM: How a Messenger Turned Into a Cybercrime Ecosystem by 2023*, Tel Aviv, KELA, 2023, 59 pag.

Kello Lucas, *The Virtual Weapon and International Order*, New Haven, Yale University Press, 2017, pp. 60-65.

Keohane Robert O., Nye Joseph S., *Power and Interdependence*, 4th Edition, Boston, Longman, 2011, pp. 20-25.

Kestner Peter, *The Art of Cyber Warfare: Strategic and Tactical Approaches for Attack and Defense in the Digital Age*, New York, Springer, 2024, 237 pag.

Kuo Joshua M., Gibson Ross, *The Hidden Potential of DNS in Security*, Hoboken, John Wiley & Sons, 2024, 192 pag.

Lefebvre Henri, *The Production of Space*, trad. Donald Nicholson-Smith, Oxford, Blackwell Publishing, 1991, pp. 26-33.

Maglaras Leandros, Kantzavelou Ioanna, Ferrag Mohamed Amine (ed.), *Cyber Security of Critical Infrastructures*, Basel, MDPI, 2023, 318 pag.

Maleh Yassine, Alazab Mamoun, Tawalbeh Loai, Romdhani Imed (editori), *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*, New York, ACM Books /

Morgan & Claypool, 2022, 310 pag.

Martínez Roberto, *Incident Response with Threat Intelligence*, Birmingham, Packt Publishing, 2024, 468 pag.

Maurer Tim, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge, Cambridge University Press, 2018, pp. 22-26.

Maurice Chad, Thompson Jeremy, Copeland William, *The Foundations of Threat Hunting: Organize and design effective cyber threat hunts to meet business needs*, Birmingham, Packt Publishing, 2024, 246 pag.

Mearsheimer John J., *The Tragedy of Great Power Politics*, New York, W.W. Norton & Company, 2001, pp. 30-32.

Menzie Ross, *Hacking for Beginners: Comprehensive Guide on Hacking Websites, Smartphones, Wireless Networks, Conducting Social Engineering, Performing a Penetration Test, and Securing Your Network*, Chennai, Notion Press, 2022, 159 pag.

Millie Katie, *Cybersecurity Crash Course: Learn Fast, Protect Faster! Don't Be the Next Victim. Secure your computers, smartphones, and tablets*, Independently Published, 2023, 244 pag.

National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, Washington, D.C., The National Academies Press, 2014, 150 pag.

Nearchou Nearchos, *Combating Crime on the Dark Web: Learn how to access the dark web safely and not fall victim to cybercrime*, Birmingham, Packt Publishing, 2024, 138 pag.

New Strategic Concept, *Clans of Ukraine: Analyzing Links Between Key Groups of the Ukrainian Oligarchy and European and U.S. Families and Institutions*, București, New Strategic Concept, 2023, 71 pag.

Nye Joseph S., *Cyber Power*, Harvard University, Belfer Center for Science and International Affairs, 2010, pp. 3-5.

Palacín Valentina, *Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools*, Birmingham, Packt Publishing, 2021, 398 pag.

Pease Andrew, *Threat Hunting with Elastic Stack: Solve complex security challenges with integrated prevention, detection, and response*, Birmingham, Packt Publishing, 2021, 292 pag.

Prigogine Ilya, Stengers Isabelle, *Order Out of Chaos: Man's New Dialogue with Nature*, New York, Bantam Books, 1984, 349 pag.

Rains Tim, *Cybersecurity Threats, Malware Trends, and Strategies* (Second Edition), Birmingham, Packt Publishing, 2023, 585 pag.

RAND Europe, *Strategic Competition in the Age of AI*, Cambridge, RAND Corporation, 2024, 144 pag.

Recorded Future, *The Intelligence Handbook: A Roadmap for Building an Intelligence-Led Security Program* (Fourth Edition), Somerville, Recorded Future, 2022, 198 pag.

Rid Thomas, *Cyber War Will Not Take Place*, New York, Oxford University Press, 2013, pp. 11-15.

Roddie Megan, Deyalsingh Jason, Katz Gary J., *Practical Threat Detection Engineering: A hands-on guide to planning, developing, and validating detection capabilities*, Birmingham, Packt Publishing, 2023, 328 pag.

Roy Kaushik, *Artificial Intelligence, Ethics and the Future of Warfare*, Londra, Routledge, 2024, 299 pag.

Sandbu Marius, *Windows Ransomware Detection and Protection*, Birmingham, Packt Publishing, 2021, 290 pag.

Santos Henrique M. D., *Cybersecurity: A Practical Engineering Approach*, Cham, Springer, 2022, 341 pag.

Schneier Bruce, *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back*, New York, W. W. Norton & Company, 2023, 296 pag.

Sharma Sanjay, *Data Privacy and GDPR Handbook*, Hoboken, John Wiley & Sons, 2022, pp. 5-103, [https://cdn.oujdalibrary.com/books/614/614-data-privacy-and-gdpr-handbook-\(www.tawcer.com\).pdf](https://cdn.oujdalibrary.com/books/614/614-data-privacy-and-gdpr-handbook-(www.tawcer.com).pdf), accesat în data de 22.04.2023.

Shekokar Narendra M., Vasudevan Hari, Durbha Surya S., Michalas Antonis, Nagarhalli Tatwadarshi P. (editori), *Intelligent Approaches to Cyber Security*, Singapore, Springer, 2026, 210 pag.

Solanki Shivam R., Khublani Drupad K., *Generative Artificial Intelligence: Exploring the Power and Potential of Generative AI*, Boca Raton, CRC Press, 2024, 465 pag.

Soldatov Andrei, Borogan Irina, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, New York, PublicAffairs, 2015, pp. 210-215.

Spykman Nicholas J., *America's Strategy in World Politics: The United States and the Balance of Power*, New York, Harcourt, Brace and Company, 1942, p. 41

Stoddart Kristan, *Cyberwarfare: Threats to Critical Infrastructure*, Londra, Palgrave Macmillan, 2022, 586 pag.

Susskind Jamie, *Politica viitorului: Tehnologia digitală și societatea*, București, Editura Corint, 2019, 562 pag.

Sutton David, *Cybersecurity: The complete guide to cyber threats and protection* (Second Edition), Londra, BCS, The Chartered Institute for IT, 2023, 340 pag.

Suvorov Viktor, *Acvarium*, București, Editura Elit Comentator, 1993, 352 pag.

Tan Chang, *Cyberwarfare for Evasive Cyber Tactics*, Singapore, Springer, 2024, 342 pag.

United Nations Office on Drugs and Crime, *Digest of Cyber Organized Crime*, Viena, United Nations Office on Drugs and Crime, 2021, 144 pag.

Vander James W. Zanden, *Social psychology*, Random House, New York, 1987, 631 pag., https://archive.org/details/socialpsychology0000unse_h0e1, accesat în data de 05.04.2024.

Verma Abhishek, Kumar Jitendra, Gaur Hari Mohan, Singh Vrijendra, Balas Valentina Emilia (ed.), *Advances in Cyber Security and Intelligent Analytics*, Boca Raton, CRC Press, 2023, 310 pag.

Waltz Kenneth N. , *Theory of International Politics*, Reading, Addison-Wesley Publishing, 1979, pp. 111-114.

Watters Paul A., *Cybercrime and Cybersecurity*, Boca Raton, CRC Press, 2024, 183 pag.

Wendt Alexander , *Social Theory of International Politics*, Cambridge, Cambridge University Press, 1999, pp. 1-40.

Wilhoit Kyle, Opacki Joseph, *Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs*, Birmingham, Packt Publishing, 2022, 460 pag.

Wittkop Jeremy, *The Cybersecurity Playbook for Modern Enterprises*, Hoboken, John Wiley & Sons, 2024, 270 pag.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications.

Zimmerman Carson, *Ten Strategies of a World-Class Cybersecurity Operations Center*, Bedford, MITRE Corporation, 2014, 289 pag.

Zouave Erik, Bruce Marc, Colde Kajsa, Jaitner Margarita, Rodhe Ioana, Gustafsson Tommy, *Artificially Intelligent Cyberattacks*, Stockholm, Swedish Defence Research Agency (FOI), 2020, 50 pag.