TIPOLOGII DE INFRACTORI CIBERNETICI – ANALIZĂ CRIMINOLOGICĂ ȘI DE DREPT PENAL

(TYPOLOGIES OF CYBER CRIMINALS – CRIMINAL LAW AND CRIMINOLOGIC ANALYSIS)

Maxim DOBRINOIU*

Abstract

Studiul de față propune o analiză interdisciplinară a tipologiilor de infractori cibernetici, îmbinând perspectiva criminologică cu cea de drept penal substanțial. Pornind de la o premisă a studiilor în domeniu că nu există un profil unic al infractorului digital, cercetarea identifică și sistematizează principalele categorii de actori ai criminalității informatice în funcție de motivația (intrinsecă și extrinsecă), profilul psihologic, modul operațional și încadrarea juridică a faptelor comise. Analiza trece în revistă și tendințele ecosistemului criminal cibernetic, cu accent pe scăderea vârstei atacatorilor, evoluția factorilor favorizanți sau determinanți în comiterea de infracțiuni informatice, industrializarea atacurilor prin modelul Crime-as-a-Service și convergența dintre inteligența artificială și ingineria socială. Materialul realizează, totodată, și o evaluare critică a instrumentelor de prevenție și sancționare disponibile în dreptul penal român, oferind propuneri de îmbunătățire a mecanismelor juridice.

Cuvinte-cheie*: criminalitate informatică, tipologii de infractori cibernetici, criminologie, drept penal, hack value, Crime-as-a-Service, hacktivism, APT, amenințare din interior.*

Abstract

This study proposes an interdisciplinary analysis of cybercriminal typologies, combining criminological perspectives with those of substantive criminal law. Starting from the premise widely acknowledged in the literature that there is no single profile of the digital offender, the research identifies and systematizes the main categories of cybercrime actors based on their motivation (intrinsic and extrinsic), psychological profile, modus operandi, and the legal classification of the offenses committed. The analysis also examines current trends in the cybercriminal ecosystem, with a particular focus on the decreasing age of offenders, the evolution of facilitating and determining factors in the commission of cyber offenses, the industrialization of attacks through the Crime-as-a-Service model, and the convergence between artificial intelligence and social engineering techniques. Furthermore, the paper provides a critical assessment of the prevention and sanctioning mechanisms available under Romanian criminal law, offering proposals aimed at improving existing legal frameworks and enhancing the effectiveness of judicial responses to cybercrime.

*Associated Professor PhD., ”Nicolae Titulescu” University of Bucharest (Romania), Faculty of Law, Criminal Law Department.

Keywords: *cybercrime, cybercriminal typologies, criminology, criminal law, hack value, Crime-as-a-Service, hacktivism, advanced persistent threats (APT), insider threat.*

1. Introducere

Criminalitatea informatică reprezintă una dintre cele mai dinamice și complexe forme de manifestare a fenomenului infracțional contemporan[1]. Deși cadrul normativ internațional, edificat prin Convenția Consiliului Europei asupra criminalității informatice (Budapesta, 2001), continuat prin Directiva 2013/40/UE și consolidat prin Convenția Organizației Națiunilor Unite privind criminalitatea informatică (New York, 2025), oferă un fundament solid pentru incriminare și cooperare judiciară, înțelegerea fenomenului rămâne incompletă în lipsa unor analize criminologice privind esența acestor fapte și a autorilor.

Dreptul penal român incriminează infracțiunile contra siguranței și integrității sistemelor și datelor informatice în mai multe titluri din Codul penal, dar normele nu operează cu diferențieri în funcție de profilul subiectului activ. Cu toate acestea, motivația, nivelul de sofisticare tehnică și contextul operațional al infractorului influențează în mod direct atât gravitatea faptei, cât și periculozitatea infractorilor, elemente indispensabile unei strategi de individualizare a pedepsei.

Prezentul studiu își propune să răspundă la o întrebare fundamentală pentru criminologia cibernetică: cine sunt infractorii cibernetici și ce îi determină pe aceștia să acționeze? Demersul este structurat în jurul a trei axe complementare: profilul psihologic și comportamental al infractorilor, o tipologie operațională sistematizată după criterii multiple și, nu în ultimul rând, implicațiile de drept penal substanțial ale fiecărei categorii tipologice.

Se impune o precizare metodologică inițială: studiul nu are în vedere infractorii care doar utilizează sisteme informatice ca instrumente pentru săvârșirea unor infracțiuni „tradiționale” (de exemplu, înșelăciune prin intermediul internetului sau amenințare transmisă electronic). Analiza vizează exclusiv actorii pentru care tehnologia informatică constituie nu doar mijlocul, ci și obiectul material sau mediul esențial al activității infracționale.

2. Inexistența unui profil unic al infractorului cibernetic

Una dintre concluziile constante ale cercetărilor criminologice în domeniul criminalității informatice este aceea că nu se poate defini un profil unic al infractorului cibernetic[2]. Spre deosebire de anumite forme de criminalitate convențională, unde studiile au reușit să identifice tipare relativ stabile (de exemplu, corelarea dintre infracționalitatea violentă și anumite variabile socio-demografice), criminalitatea informatică se caracterizează printr-o eterogenitate accentuată[3].

Această eterogenitate se explică, în principal, prin diversitatea motivațiilor care stau la baza comportamentului infracțional digital, fie că este vorba despre aspecte financiare, ideologice, tehnic-exploratorii, militar sau economic-strategice sau pur distructive. Un eventual profilul al

[1] Thomas J. Holt, Adam M. Bossler, Cybercrime in Progress (Routledge 2016), p. 3 și UNODC, Comprehensive Study on Cybercrime (2013), disponibil online.
[2] Rutger Leukfeldt, Thomas Holt, The Human Factor of Cybercrime (Routledge 2019), p. 21.
[3] Raoul Chiesa, Stefano Ducci, Silvio Ciappi, Profiling Hackers (CRC Press 2009), p. 45.

infractorului cibernetic nu se poate construi individual, ci statistic, prin agregarea unor trăsături recurente observate sau întâlnite în cadrul unor categorii tipologice distincte. Este vorba, așadar, despre o criminologie a tendințelor, nu a certitudinilor deterministe.

Din perspectiva istoricului de viață, studiile arată că mulți infractori cibernetici încep activități tehnice la vârste fragede (12–20 de ani)[4], manifestă un interes precoce pentru programare sau jocuri online (gaming) și sunt frecvent autodidacți. Nu s-a identificat un tipar familial unic, iar analiza spețelor soluționate în justiție ne arată că aceștia provin atât din familii intacte, cât și din medii dezorganizate, cu variații semnificative inclusiv în planul statutului socio-economic.

Nivelul educațional variază de la autodidacți (marcați de dezinteresul pentru educația formală) la absolvenți ai unor programe de specialitate în electronică și tehnologia informației.

Socializarea acestora se realizează preponderent în comunități online (forumuri de specialitate, servere Discord, spații din Dark Web), iar cercurile de prieteni sunt mai degrabă virtuale decât fizice.

3. Profilul psihologic al infractorului cibernetic

3.1. Trăsături psihologice dominante

Cercetarea de specialitate a evidențiat un set de trăsături psihologice frecvent întâlnite la infractorii cibernetici, fără ca acestea să constituie un tipar predictiv validat științific în sens determinist.

Printre cele mai relevante aspecte observate se numără: atractivitatea pentru rezolvarea problemelor complexe (ceea ce în subcultura de hacking este denumit „hack value”), curiozitatea tehnică și orientarea spre provocarea intelectuală, motivația internă bazată pe ingeniozitate și demonstrarea competenței ori a abilităților (tehnice, de manipulare etc.), dorința de a afișa putere și interesul de poziționare în raport cu semenii ori cu autoritatea statală.

3.2. Modelul „Dark Triad” și relevanța sa criminologică

O contribuție semnificativă la înțelegerea profilului psihologic al infractorilor cibernetici provine din modelul „Dark Triad”[5], care identifică trei dimensiuni ale personalității frecvent corelate cu comportamentul deviant: machiavelismul, psihopatia și narcisismul[6].

Machiavelismul infractorilor cibernetici se manifestă adesea prin capacitatea extinsă de manipulare strategică și exercitarea nefastă a puterii (ex. coerciție), trăsătură relevantă, spre exemplu, în cazul atacurilor cibernetice asupra infrastructurilor critice (de exemplu, asupra rețelelor energetice).

Psihopatia, înțeleasă ca tendință de căutare a senzațiilor extreme și lipsă a empatiei, se regăsește în cazul atacurilor de tip ransomware îndreptate asupra spitalelor sau a altor organizații vulnerabile.

---

[4] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, disponibil online.
[5] Delroy L. Paulhus, Kevin M. Williams, „The Dark Triad of personality” (2002) 36 Journal of Research in Personality p. 556.
[6] Kathryn Seigfried-Spellar, Marcus K. Rogers, „Does the Dark Triad predict cyberbullying?” (2013) Computers in Human Behavior.

Narcisismul adaptativ, marcat preponderent de căutarea validării prin performanța tehnică, ar putea explica, într-o oarecare măsură, comportamentul atacatorilor care exploatează vulnerabilități (tehnice sau umane) pentru faimă sau recunoaștere în comunitățile sub-culturii „hacking".

3.3. Efectul dezinhibării online

Un factor esențial care amplifică comportamentul infracțional în spațiul digital este așa-numitul „efect al dezinhibării online"[7]. Anonimitatea, invizibilitatea (aparentă) și disocierea de consecințele directe ale acțiunilor proprii creează un context în care barierele morale și sociale sunt semnificativ diminuate[8]. Infractorul cibernetic nu își confruntă victima față în față, nu percepe suferința cauzată în mod direct și beneficiază de o senzație de invulnerabilitate și chiar impunitate conferite de mediul digital.

Din perspectivă criminologică, acest efect are o dublă relevanță. Pe de o parte, el facilitează trecerea la acțiune a persoanelor care, în mediul fizic, nu ar fi comis fapte antisociale. Pe de altă parte, el contribuie la raționalizarea comportamentului infracțional, alimentând justificări precum „testez securitatea" sau „ajut sistemul să devină mai sigur".

4. Motivația infracțională: factori intrinseci și extrinseci[9]

4.1. Motivații intrinseci

Motivațiile intrinseci ale infractorilor cibernetici sunt cele care provin din interiorul individului, fără o condiționare externă directă.

Principalele categorii identificate în literatură și în practica judiciară includ:

a) curiozitatea intelectuală și provocarea tehnică (ex. dorința de a rezolva probleme dificile, de a „sparge" un sistem pentru satisfacția cognitivă)

b) căutarea de senzații și asumarea riscului (thrill-seeking)

c) nevoia de statut, faimă sau recunoaștere în comunitățile „underground"

d) ideologia și convingerile (ex. în cazul hacktivismului, atacurilor motivate politic, religios sau social – posibil cyber-terorism ori „defacement", scurgeri de date din interiorul organizațiilor pentru o cauze determinate de motivațiile anterioare sau atacurile DDoS asupra țintelor politice)

e) răzbunarea sau resentimentul personal (acte comise din răzbunare față de actuali sau foști angajatori, foști parteneri, colaboratori sau chiar instituții percepute ca abuzive, aspecte întâlnite frecvent în cazurile de insider threat).

4.2. Motivații extrinseci

Motivațiile extrinseci sunt determinate de factori externi individului.

[7] John Suler, „The Online Disinhibition Effect" (2004) 7 CyberPsychology & Behavior p. 321.
[8] Ibidem.
[9] Rogers, Marcus K., A social learning theory and moral disengagement analysis of criminal computer behavior, 2001, International Journal of Cyber Criminology

Câștigul financiar direct constituie motivația dominantă la nivelul majorității grupurilor infracționale profesioniste, în cazul atacurilor prin ransomware, fraudelor financiare (ex. Frauda Directorul Executiv), copierea datelor asociate cardurilor (skimming, carding), vânzări de date (ex. credențiale de acces compromise) și spălare de bani.

O atenție aparte se manifestă în cazul monetizării serviciilor criminalității informatice, exemplificate în rapoartele oficiale drept Crime-as-a-Service (CaaS)[10], în care infractorii își transformă competențele tehnice în oportunități de obținere a veniturilor (ilicite), unii actori cibernetici funcționând pur și simplu ca prestatori „for-hire" sau „on demand" (la comandă).

Coerciția sau manipularea (inclusiv prin trafic de persoane sau acte de exploatare) constituie motivații distincte, remarcându-se situații în care persoane vulnerabile sunt constrânse, induse în eroare ori determinate să coopereze la comiterea de infracțiuni informatice.

Nu în ultimul rând, actele de „sponsorizare" din partea unor entități statale sau non-statale se disting din ce în ce mai evident în ecosistemul infracțional cibernetic, această formă particulară de implicare (din perspectiva dreptului penal substanțial – instigare, complicitate) fiind aptă să determine rezoluții infracționale specifice, motivate strategic, geopolitic sau de obținerea de informații clasificate ori protejate prin drepturi de proprietate intelectuală (intelligence) ori de perturbarea funcționării infrastructurilor critice ale unui stat țintă.

4.3. Conceptul de „hack value"

Un concept esențial pentru înțelegerea motivației intrinseci este acela de „hack value", definit ca valoarea internă a unui actor cibernetic de a reuși o performanță tehnică remarcabilă[11]. Este vorba despre un criteriu estetic (ex. creativitate, eleganță, demonstrație de putere cognitivă) și despre afișarea propriei autosuficiențe.

În absența eticii, acest concept poate raționaliza încălcarea legii, infractorul percepând fapta nu ca pe o infracțiune, ci ca pe o performanță intelectuală demnă de admirație.

5. Tipologia operațională a infractorilor cibernetici

Pe baza criteriilor combinate ale motivației, nivelului de sofisticare tehnică a acțiunilor întreprinse, modului operațional și obiectivelor urmărite, se pot distinge următoarele categorii tipologice principale de infractori cibernetici:

5.1. White hats (hackeri etici)

Hackerii etici acționează cu consimțământul proprietarilor de sisteme, în cadrul unor programe de testare autorizată (ex. teste de penetrare) sau de raportare a vulnerabilităților (bug bounty).

Din punct de vedere penal, activitatea lor nu constituie infracțiune atâta vreme cât se desfășoară în limitele consimțământului acordat (ex. Scope of Work).

[10] Europol, IOCTA 2024

[11] Pekka Himanen, The Hacker Ethic and the Spirit of the Information Age (Random House 2001), p. 7.

Relevanța lor tipologică rezidă în faptul că aceleași instrumente utilizate în scop comercial autorizat sau de cercetare științifică (etic) pot fi folosite abuziv de alte categorii de actori.

5.2. Grey hats (actori din zona gri moral-juridică)

Actorii din această categorie operează în zona de limită dintre legalitate și ilegalitate. Ei pot efectua operațiuni aparent legale, dar scopul acestora și metodologiile folosite le plasează inclusiv în sfera ilicitului penal (ex. scanări de vulnerabilități fără consimțământ, divulgarea necoordonată a rezultatelor cercetării de securitate, intervenții unor website-uri etc.).

Din perspectiva dreptului penal român, astfel de activități pot întruni elementele constitutive ale infracțiunilor de acces ilegal la un sistem informatic (art. 360 C.pen.), alterarea integrității datelor informatice (art. 362 C.pen.), perturbarea funcționării sistemelor informatice (art. 363 C.pen.), transferul neautorizat de date informatice (art. 364 C.pen.) ori operațiuni ilegale cu dispozitive sau programe informatice (art. 365 C.pen.), chiar și în absența unei intenții vădit păgubitoare la adresa țintelor.

Riscul principal asociat acestei categorii este cel de migrare către zona „black hat".

5.3. Black hats (infractori cibernetici convenționali, actori de amenințare)

Black hats sunt infractorii care acționează intenționat ilegal, frecvent cu motivație financiară.

Operațiunile lor includ: atacuri de tip ransomware (inclusiv modelul RaaS – Ransomware-as-a-Service, care presupune criptarea datelor victimelor și, după caz, exfiltrarea acestor date, urmate de șantaj multiplu), distribuție de malware, furt și comercializare de date personale, web skimming, fraude informatice de tip phishing sau BEC (Business Email Compromise), carding și preluare neautorizată de conturi (account takeover).

În dreptul penal român, aceste fapte se încadrează în infracțiunile prevăzute de art. 360–365 C.pen., cu posibilitatea concursului de infracțiuni, fiind atrasă tipicitatea unor infracțiuni conexe: frauda informatică (art. 249 C.pen.), fals informatic (art. 325 C.pen.), efectuarea de operațiuni financiare în mod ilegal (art. 250 C.pen.) și chiar a unor infracțiuni „tradiționale" (ex. șantaj – art. 207 C.pen.).

5.4. Brokeri de acces, traficanți de informații și mercenari cibernetici

Această categorie cuprinde actorii motivați preponderent economico-financiar, care operează în ecosistemul CaaS:

- intermediari de acces inițial („initial access brokers"- IAB) - sunt actorii de amenințare care vând credențiale și metode de acces la sisteme deja compromise
- afiliați ai rețelelor specializate în Ransomware-as-a-Service (RaaS)
- furnizori de malware-as-a-service
- operatori de digital skimming
- persoane implicate în spălarea banilor prin criptomonede (money mules)

Profesionalizarea acestor piețe, semnalată atât de EUROPOL, cât și de ENISA, demonstrează că infracționalitatea cibernetică a atins un nivel de industrializare comparabil cu modelele de afaceri legitime.

În aceeași categorie se încadrează și hackerii mercenari (hacker-for-hire) sau așa-numiții PSOA (Private Sector Offensive Actors), care oferă servicii ofensive comerciale: dezvoltare de exploit-uri, personalizare de malware, servicii de intruziune contractată. Activitatea acestora ridică probleme juridice complexe, întrucât se situează la intersecția dintre sfera privată și cea statal-ofensivă.

5.5. Hacktiviștii, cyber-extremiștii și teroriștii cibernetici

Hacktiviștii acționează sub motivații preponderent ideologice[12] (politice sau religioase) ori revendicativ sociale. Arsenalul lor include atacuri de tip DDoS (ex. perturbarea funcționării infrastructurilor critice), alterarea conținutului website-urilor guvernamentale, exfiltrări și publicări de date clasificate, confidențiale sau informații personale pentru „denunțare publică" (doxxing) și campanii de dezinformare.

Autoritățile de aplicare a legii și organizații precum ENISA și Europol raportează o creștere a campaniilor cu caracter geopolitic, în contextul conflictelor armate în desfășurare și al tensiunilor internaționale.

Cyber-extremiștii și cyber-teroriștii merg mai departe, urmărind perturbarea gravă ori chiar distrugerea infrastructurilor critice, propagarea materialelor cu conținut fundamentalist sau extremist, recrutarea de adepți sau afiliați, precum și sprijinirea cu informații ori coordonarea de operațiuni ofensive offline.

Deși resursele lor sunt adesea limitate, riscurile devin semnificative atunci când se conectează cu actori mai bine dotați tehnic sau cu grupuri APT.

5.6. Grupurile APT (Advanced Persistent Threat)

Grupurile APT (Advanced Persistent Threat) reprezintă echipe specializate de actori cibernetici susținuți (juridic, financiar, tehnologic, logistic) de entități statale sau non-statale ori afiliați ai unor astfel de entități (angajați, contractori), care operează în mediul IT&C pentru atingerea unor obiective strategice:

- spionaj cibernetic (exfiltrare de date sensibile)
- acces ilegal persistent la sisteme sau infrastructuri informatice (backdoors)
- interceptarea fluxurilor de comunicații
- compromiterea lanțurilor de aprovizionare (supply-chain)
- sabotarea/perturbarea sistemelor operaționale industriale (OT/ICS)

Motivația este eminamente geopolitică (poziționare, influențare) și strategică (avantaj competitiv pe anumite zone politico-economice) și indirect comercială (obținerea de beneficii pe termen lung).

[12] Tim Jordan, Paul Taylor, Hacktivism and Cyberwars (Routledge 2004), p. 67.

În dreptul penal, activitatea grupurilor APT ridică anumite probleme în ceea ce privește atribuirea – adică se manifestă o dificultate semnificativă în ceea ce privește capacitatea statelor sau organizațiilor afectate de a demonstra legătura dintre o anumită grupare APT și un anumit stat sau o anumită entitate de tip „sponsor", aspecte care influențează atât competența jurisdicțională, cât și aplicarea mecanismelor de cooperare judiciară internațională.

5.7. Insider threats (amenințările din interior)

Persoanele din interiorul organizațiilor, fie acestea răuvoitoare ori neglijente, se constituie într-o categorie distinctă, caracterizată prin faptul că autorul beneficiază deja de acces legitim la sistemele și datele organizației.

Practica arată că motivația lor combină o serie de factori intrinseci, precum stresul profesional, hărțuirea sau bullying-ul la locul de muncă, nemulțumirea față de organizație sau deciziile managementului etc. suprapuși peste o bună oportunitate de a acționa.

Acest lucru face ca prevenirea să necesite abordarea unei alte strategii de „apărare" (protecție), prin măsuri organizatorice și tehnice specifice. Activitatea tipică a actorilor de amenințare din interior include:

- exfiltrări de date clasificate, confidențiale sau cu caracter personal
- utilizarea privilegiilor legitime pentru acces neautorizat în alte platforme sau sisteme ale organizației și executarea de mișcări laterale
- sabotajul intern (modificarea, ștergerea sau distrugerea intenționată sau accidentală a datelor, restricționarea accesului la aceste date și/sau perturbarea funcționării sistemelor sau rețelelor organizației)
- facilitarea accesului extern (credential sharing) – pentru alți actori de amenințare (hackeri, spioni cibernetici, traficanți de informații, grupări APT etc.)

5.8. Infractorii juvenili și actorii cu nivel redus de competență tehnică

Rapoartele EUROPOL și ENISA semnalează un fenomen îngrijorător, și anume cel al scăderii vârstei infractorilor la momentul intrării pe piața criminalității cibernetice. Tinerii sunt din ce în ce mai îndemânatici și performează în utilizarea de instrumente (aplicații, echipamente, cunoștințe) specifice, precum kit-uri de Phishing prefabricate, malware bazat pe șabloane, servicii „DDoS-for-hire" și tehnici de inginerie socială pentru preluarea de conturi.

Deși nivelul inițial de sofisticare al operațiunilor executate este redus, acești actori sunt capabili să scaleze rapid și se pot adapta mediilor țintă, iar pe măsură ce dobândesc competențe, se integrează mult mai bine în rețelele infracționale.

Din perspectivă penală, această categorie ridică probleme specifice legate de răspunderea penală și de aplicarea măsurilor educative. Spre exemplu, considerăm total depășite măsuri educative neprivative de libertate precum: „stagiul de formare civică" (art. 117 C.pen.), „supravegherea" (art. 118 C.pen.), „consemnarea la sfârșit de săptămână" (art. 119 C.pen.) ori „asistare zilnică" (art. 120 C.pen.) în lipsa altor mecanisme sau obligații legale care să le restricționeze acestora accesul la echipamente de telecomunicații ori racordarea la rețele (ex. internet), pe durata respectivelor măsuri.

5.9. Actorii specializați în manipulare informațională (DaaS)

O categorie emergentă, amplificată inclusiv de progresele inteligenței artificiale generative, este cea a furnizorilor de servicii de tip „Disinformation-as-a-Service" (DaaS). Acești actori de amenințare utilizează noi tipuri de instrumente, precum „deepfakes", „voice cloning", campanii de inginerie socială țintită (Spear Phishing) și operațiuni de influență pentru manipulare în scop politic sau financiar.

Încadrarea lor juridico-penală reprezintă o provocare pentru agențiile de aplicare a legii, întrucât faptele acestora pot îmbrăca forme care depășesc tiparele tradiționale ale infracțiunilor informatice.

6. Încadrarea juridico-penală și individualizarea sancțiunilor

6.1. Cadrul incriminator din Codul penal român

Titlul VII al Părții speciale a Codului penal român cuprinde infracțiunile contra siguranței și integrității sistemelor și datelor informatice: accesul ilegal la un sistem informatic (art. 360), interceptarea ilegală a unei transmisii de date informatice (art. 361), alterarea integrității datelor informatice (art. 362), perturbarea funcționării sistemelor informatice (art. 363), transferul neautorizat de date informatice (art. 364) și operațiunile ilegale cu dispozitive sau programe informatice (art. 365). Falsul informatic (art. 325) și frauda informatică (art. 249) completează arsenalul incriminator. Acestora li se adaugă și alte infracțiuni contra patrimoniului (ex. furtul în scop de folosință – art. 230 alin. 2 C.pen., efectuarea de operațiuni financiare în mod fraudulos – art. 250 C.pen.), de fals (ex. falsificarea de titluri de credit sau instrumente de plată – art. 311 alin. 2 C.pen.) sau contra conviețuirii sociale (ex. pornografia infantilă – art. 374 C.pen.)

Tipologia operațională a infractorilor cibernetici are o relevanță directă pentru individualizarea judiciară a pedepsei. Astfel, un actor APT care compromite infrastructuri critice prezintă un grad de pericol social fundamental diferit de cel al unui tânăr autodidact care utilizează un kit de Phishing prefabricat. Cauzele de atenuare sau de agravare, care oferă informații valoroase privind gravitatea faptelor sau periculozitatea făptuitorilor, sunt în mod evident completate cu elemente specifice care țin de motivația, scopul urmărit, mijloacele utilizate și consecințele produse, fiind necesar a fi evaluate diferențiat și interdisciplinar.

6.2. Interzicerea accesului la sisteme informatice ca sancțiune penală

O problemă *de lege lata* și *de lege ferenda* cu relevanță directă pentru tema tipologiilor de infractori cibernetici este cea a interzicerii accesului suspectului, inculpatului sau condamnatului la sisteme, aplicații, rețele, platforme și dispozitive electronice.

Codul penal român nu prevede (în cuprinsul art. 66 C.pen.) posibilitatea aplicării pedepsei complementare a interzicerii dreptului de a comunica prin internet sau prin orice altă rețea de comunicații electronice.

Această măsură de restricționare a accesului suspectului, inculpatului sau condamnatului ori persoanei căreia i se aplică o măsură educativă ridică însă probleme juridice și practice semnificative, care trebuie evaluate prin prisma unor principii fundamentale. Astfel:

În primul rând, măsura trebuie să fie tehnic aplicabilă – adică să existe mecanisme reale de implementare și monitorizare a respectării.

În al doilea rând, ea trebuie să fie temporară, nu permanentă.

În al treilea rând, o astfel de obligație trebuie să fie necesară și proporțională, în raport cu gravitatea faptei și periculozitatea infractorului.

Nu în ultimă instanță, o atare restricție nu trebuie să afecteze reintegrarea socială a condamnatului. Într-o societate în care accesul la internet a devenit o condiție a exercitării majorității drepturilor civile, o interdicție excesivă poate produce efecte contrare reintegrării.

Aceeași analiză trebuie extinsă și către alte categorii de sancțiuni penale: măsuri de siguranță, pedepse accesorii, măsuri educative neprivative de libertate (pentru minori) și măsuri de control în mediul penitenciar. Fiecare dintre acestea presupune o evaluare specifică a proporționalității și a fezabilității tehnice.

7. Tendințe emergente (2025–2026)

Peisajul amenințărilor cibernetice se află într-o continuă transformare, iar fenomenul criminal asociat prezintă semnele unei evoluții periculoase. În acest context, câteva tendințe emergente merită a fi semnalate în perspectiva perioadei următoare:

În primul rând, **scăderea vârstei autorilor infracțiunilor informatice**: barierele de intrare în ecosistemul infracțional digital sunt din ce în ce mai scăzute, iar tineri fără competențe tehnice avansate pot accesa instrumente ofensive prefabricate, cu impact major asupra țintelor.

În al doilea rând, **democratizarea instrumentelor ofensive prin modelul CaaS și prin utilizarea inteligenței artificiale generative (GenAI)**. „Deepfakes", „voice cloning" și instrumente bazate pe Modele de Limbaje Largi (LLM) transformă semnificativ capacitățile actorilor de amenințare, inclusiv ale celor cu nivel redus de competență tehnică, potențându-le acestora „agresivitatea virtuală".

În al treilea rând, **convergența tehnologică între OSINT (Open Source Intelligence), inteligența artificială și ingineria socială** permite o eficiență sporită atât în inducerea în eroare a victimelor, cât și în dezvoltarea de noi instrumente malware, mai sofisticate și mai dificil de detectat.

Nu în ultimul rând, **creșterea importanței hacktivismului geopolitic și a actorilor statali** și angajarea acestora în executarea de operațiuni tipice de război hibrid, campanii de spionaj cibernetic și perturbarea / distrugerea infrastructurilor critice configurează un peisaj al amenințărilor în care granița dintre infracțiunea de drept comun și actul de agresiune statală, consfințit de dreptul internațional, devine din ce în ce mai difuză.

8. Prevenție și control

Analiza tipologiilor de infractori cibernetici permite statelor formularea unor direcții de acțiune preventivă diferențiate. Educația timpurie și crearea de canale legale de exprimare a competențelor tehnice, cum ar fi: competiții CTF (Capture the Flag), programe de „bug bounty"

etc. pot orienta tinerii / persoanele cu aptitudini tehnice către alternative legale și etice de cercetare în securitate cibernetică.

Detectarea timpurie a indicatorilor psihosociali (ex. dispreț al adresa legii ori la adresa autorității publice, predispoziția pentru încălcarea legii ori a regulilor de securitate) ori a indicatori de risc profesional asociați angajaților (pentru prevenirea insider threats) poate reduce riscul de trecere de la manifestarea intelectivă la cea de voință și apoi acțiune.

Cooperarea mai strânsă între instituțiile din educație, organizațiile din industria IT și autoritățile competente în supravegherea spațiului cibernetic național civil este esențială, alături de programele de reintegrare (a celor care au săvârșit deja infracțiuni informatice) și de promovarea unei reale culturi a eticii și comportamentului digital.

Pe plan normativ, Directiva NIS2, transpusă la nivel național prin OUG nr. 155/2024, aprobată cu modificări și completări prin Legea nr. 124/2025), consacră la nivel european, dar și național, cerințe sporite de securitate cibernetică, de raportare a incidentelor și de divulgare coordonată a vulnerabilităților.

Al Doilea Protocol Adițional al Convenției CoE asupra criminalității informatice (Budapesta) consolidează mecanismele de cooperare judiciară internațională și de acces la probele electronice. Regulamentul GDPR nr. 679/2016 vine să completeze cadrul de protecție a datelor personale, cu relevanță directă pentru faptele de exfiltrare și comercializare a datelor, iar noua Convenție ONU asupra criminalității informatice (New York, 2025) obligă statele semnatare să adopte de urgență cele mai adecvate măsuri de drept substanțial penal și procesual penal pentru a combate fenomenul.

9. Concluzii

Criminalitatea informatică nu este doar o abatere de la lege, ci și o distorsiune a relației omului cu tehnologia. În spatele fiecărui cod malițios și în spatele fiecărei acțiuni agresive în mediul virtual se află o motivație umană, iar înțelegerea acestei motivații constituie premisa oricărei strategii eficiente de prevenire și combatere a acestui tip particular de infracționalitate.

Studiul de față a demonstrat că infractorii cibernetici nu formează o categorie omogenă, ci un spectru larg de actori diferențiați prin motivație, competență tehnică, mod operațional și obiective urmărite. Tipologiile identificate, de la „hackeri etici” la grupuri APT și de la insideri (actori interni de amenințare) la furnizori de DaaS, reflectă tocmai complexitatea unui fenomen aflat în continuă evoluție.

Din perspectiva dreptului penal substanțial, această eterogenitate impune o individualizare judiciară atentă, care să țină seama nu doar de fapta comisă, ci și de profilul autorului, de motivația care l-a determinat să acționeze și de contextul operațional în care s-a desfășurat activitatea infracțională. Instrumentele de sancționare trebuie, astfel, adaptate specificului criminalității digitale, cu respectarea principiilor legalității, proporționalității, fezabilității tehnice și reintegrării sociale.

În concluzie, aspectele tratate în acest studiu impun o analiză interdisciplinară care să conducă în final la o actualizare a cadrului normativ și instituțional prin care statul răspunde eficient și efectiv noilor amenințări ale spațiului cibernetic și tipologiilor diferite de actori agresivi.

Practică demonstrează faptul că infractorii cibernetici nu se nasc în cod binar, ci apar din neînțelegeri, nevoi ori dintr-un sens creat de alții pentru ei. Prezentul studiu vine să arate că a înțelege această realitate este primul pas către un răspuns penal și criminologic adecvat.

Referințe bibliografice:

I. Acte normative

- Codul penal român (Legea nr. 286/2009), publicat în Monitorul Oficial nr. 510 din 24 iulie 2009, cu modificările și completările ulterioare.
- OUG nr. 155/2024, aprobată cu modificări și completări prin Legea nr. 124/2025 (de transpunere a Directivei 2022/2555).
- Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României.
- Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta), adoptată la 23 noiembrie 2001, ratificată de România prin Legea nr. 64/2004.
- Al Doilea Protocol Adițional la Convenția de la Budapesta privind cooperarea consolidată și divulgarea probelor electronice, adoptat la 12 mai 2022.
- Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice.
- Directiva (UE) 2022/2555 (NIS2) a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune.
- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (GDPR).
- Convenția ONU privind criminalitatea informatică (New York, 2025)

II. Rapoarte instituționale

- ENISA, Threat Landscape, rapoartele anuale 2023–2024, disponibile la: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
- EUROPOL, Internet Organised Crime Threat Assessment (IOCTA), rapoartele anuale 2023–2024, disponibile la: https://www.europol.europa.eu/publications-events
- UNODC, Comprehensive Study on Cybercrime, 2013 (actualizat periodic), disponibil la: https://www.unodc.org/unodc/en/cybercrime

III. Surse doctrinare recomandate

Internaționale

- Paulhus, Delroy L.; Williams, Kevin M., *The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy*, 2002, Journal of Research in Personality, DOI: https://doi.org/10.1016/S0092-6566(02)00505-6
- Seigfried-Spellar, Kathryn C.; Rogers, Marcus K., *Does the Dark Triad predict cyberbullying?*, 2013, Computers in Human Behavior, DOI: https://doi.org/10.1016/j.chb.2013.01.022
- Rogers, Marcus K., *A social learning theory and moral disengagement analysis of criminal computer behavior*, 2001, International Journal of Cyber Criminology

- Holt, Thomas J.; Bossler, Adam M., *Cybercrime in Progress*, 2016, Routledge, ISBN: 9781138930020
- Chiesa, R.; Ducci, S.; Ciappi, S., *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, 2009, CRC Press
- Leukfeldt, Rutger; Holt, Thomas, The Human Factor of Cybercrime, 2019, Routledge
- Pekka Himanen, *The Hacker Ethic and the Spirit of the Information Age*, 2001, Random House

Internă

- Dobrinoiu, Maxim, *Infracțiuni în domeniul informatic*, Ed. CH Beck, 2006
- Zlati, George, *Tratat de criminalitate informatică*, Ed. Solomon, 2020
- Moise, Adrian Cristian, *Dimensiunea criminologică a criminalității în cyberspațiu*, Ed. CH Beck, 2015