

EFECTELE CRIMINALITĂȚII CIBERNETICE ASUPRA SECURITĂȚII NAȚIONALE A REPUBLICII MOLDOVA⁴⁹

THE EFFECTS OF CYBERCRIME ON NATIONAL SECURITY OF THE REPUBLIC OF MOLDOVA

Marcel BENCHECI, *doctor, cercetător științific coordonator*,
Institutul de Cercetări Juridice, Politice și Sociologice
al Universității de Stat din Moldova,
e-mail: marcelbencheci@mail.ru,
ORCID: 0000-0002-6619-5299

Nicolae PANFILII, *doctorand*,
Universitatea Liberă Internațională din Moldova,
e-mail: n.panfilii22@gmail.com,
ORCID: 0009-0002-3640-6849

Diana HÎRBU, *doctor, conferențiar universitar*,
Universitatea de Stat din Moldova
ORCID: 0000-0002-7867-1731

Summary

Ensuring the informational security and cyber protection of the Republic of Moldova is a state obligation. The situation that has arisen recently in the post-Soviet space, including audiovisual informational resources from the Russian Federation, has begun to have a particularly negative impact on the observance of human rights, state security, and the consolidation of the status of a sovereign, independent, and integral state.

The effects of cybercrime on national security derive from the way technology is used by hostile elements and malicious individuals. Currently, cybercrime is no longer significant beyond the fields of IT risk management and law enforcement.

Keywords: *cybercrime, Republic of Moldova, information security, national security, state.*

Garantarea securității informaționale și a protecției cibernetice în Republica Moldova reprezintă o responsabilitate a statului. Recent, situația din spațiul post-sovietic, inclusiv influența resurselor informaționale audiovizuale din Federația Rusă, a început să afecteze negativ respectarea drepturilor omului, securitatea națională și consolidarea statutului de stat suveran, independent și unitar.

Impactul criminalității informatice asupra securității naționale depinde de modul în care tehnologia este folosită de elemente ostile și persoane cu intenții rele. În prezent, criminalitatea informatică nu mai are o relevanță majoră în afara domeniilor de management al riscului IT și al aplicării legii. Responsabilitatea statului de a asigura securitatea cetățenilor săi nu se poate limita doar la spațiul cibernetic; în plus, în acest domeniu, manifestările practice ale unei astfel de responsabilități trebuie definite ca parte a unui proces politic democratic, bazat pe date factuale solide [1].

Estimările financiare privind amploarea daunelor cauzate de criminalitatea informatică datează încă din anii 1990, când companiile de securitate au început să conducă cercetări în acest domeniu și să publice numeroase rapoarte. Există zeci de evaluări diferite provenite din sectoarele comerciale și guvernamentale din Statele Unite, Anglia și alte țări dezvoltate [2, p. 16-17]. Un raport FBI a estimat daunele aduse afacerilor americane în 2005 la 65 de miliarde de dolari [3, p. 10]. În 2009, secretarul de Comerț al SUA, Gary Locke a susținut că daunele anuale aduse companiilor americane, ca urmare a contrafacerii și pirateriei (adică, utilizarea ilegală a codurilor de calculator) erau de aproximativ 200-250 de miliarde de dolari [4]. În anul 2011, potrivit unui raport al unei companii britanice, s-au estimat daunele la 27 de miliarde de lire sterline anual: prejudiciul anual pentru cetățenii britanici a fost estimată la 3,1 miliarde de lire sterline, pentru sectorul de afaceri la 21

⁴⁹ Articolul este elaborat în cadrul subprogramului 01.05.01 **Securitatea națională a Republicii Moldova în contextul aderării la Uniunea Europeană: abordări juridice, politologice și sociologice**, realizat de Institutul de Cercetări Juridice, Politice și Sociologice al Universității de Stat din Moldova.

de miliarde de lire sterline și pentru guvern la 2,2 miliarde de lire sterline [5]. Un alt raport recent al Symantec, un important furnizor global de software pentru securitatea computerelor, a estimat daunele directe cauzate de criminalitatea cibernetică la 114 miliarde de dolari anual în 24 de națiuni [6]. Alte estimări vorbesc de sute de miliarde de dolari anual. Raportul din 2021 al Biroului Federal de Investigații [7, p. 3] privind criminalitatea pe Internet a menționat pierderi legate de criminalitatea cibernetică de 7 miliarde de dolari, dublu față de pierderile raportate în 2019 [8].

Totuși, criminalitatea informatică nu este doar o problemă economică. Aceasta implică și aspecte semnificative de securitate națională. În timp ce infractorii ciberneticici învață unii de la alții, grupurile de hackeri susținute de state învață și ele de la infractorii ciberneticici și viceversa. Infrastructura criminalității informatice și chiar infractorii ciberneticici înșiși au fost cooptați de guverne în trecut, existând dovezi că statele ar putea achiziționa instrumente din subteranul infractorilor ciberneticici. De asemenea, securitatea națională și-a crescut profilul și importanța datorită abordărilor paralele prin care pot avea loc atacurile. Atacurile fizice nu mai sunt singura metodă de subminare sau compromitere a securității unei națiuni. Rețelele digitale interconectate moderne oferă o abordare aproape paralelă, care, în anumite circumstanțe, este mai puțin costisitoare, mai discretă și mai dăunătoare decât atacurile fizice tradiționale.

Legătura dintre criminalitatea informatică și securitatea națională a devenit tot mai evidentă, pe măsură ce tehnologia a crescut capacitatea infractorilor de a provoca daune și anxietate atât asupra indivizilor, cât și asupra infrastructurii critice a unei națiuni, subminând resursele sale vitale. Astfel, a apărut o nouă abordare a modalităților emergente pentru a trata probleme vechi, precum asigurarea securității naționale, utilizând în unele cazuri modificările legislative existente. Pe măsură ce factorii de decizie continuă să abordeze numeroasele provocări de securitate prezentate de lumea digitală interconectată de astăzi, care este în mod inerent internațională, s-a dezvoltat o schimbare a practicilor în comun între autoritățile de aplicare a legii și agențiile de informații și securitate.

În consecință, conceptul de securitate națională s-a schimbat semnificativ în ultimii ani. Au trecut vremurile când principalele amenințări de securitate ale unei țări erau de natură teritorială și strict militară. Acum, țările nu mai văd o invazie fizică sau militară ca principala amenințare la adresa securității interne și externe, ci se concentrează pe probleme precum sănătatea publică, economia națională și coeziunea socială [9]. Distanța și izolarea odinioară au oferit țărilor precum Noua Zeelandă posibilitatea relativ scăzută de atac fizic și sunt acum aproape irelevante [10]. Un anumit tip de infracțiune care exemplifică această nouă capacitate de atac este cel al criminalității informatice. Definită în general ca o infracțiune în care „*calculatoarele și Internetul joacă un rol central în infracțiune, și nu unul incidental*” [11], criminalitatea informatică caracterizează globalizarea prin scară, viteză și cogniție [12].

Activitățile ciberneticice cresc într-un ritm rapid, permițând conexiuni aproape instantanee. Rafinamentul acestor activități a atins niveluri fără precedent, reprezentând o amenințare serioasă pentru societate. Percepția asupra duratei activităților s-a schimbat semnificativ datorită avansării rapide a tehnologiei ciberneticice. Grupările criminale răspund presiunii exercitate de forțele de ordine, reorganizându-și operațiunile și atrăgând o nouă generație de programatori și experți ciberneticici. Ideea că lumea este un loc mai mic a influențat modul în care țările privesc securitatea.

Într-o lume globalizată și dependentă de tehnologia cibernetică, țările și indivizii pot fi atacați oricând și de oriunde, în diverse moduri și cu o viteză uluitoare. Acești factori, împreună cu costurile relativ scăzute ale criminalității informatice, ilustrează de ce aceasta reprezintă probabil o amenințare directă la adresa securității naționale. Guvernul, infrastructura, proprietatea intelectuală și informațiile personale sunt toate potențial amenințate. Aceste amenințări sunt critice pentru securitatea națională datorită potențialului lor de a perturba semnificativ sau de a afecta funcționarea societății unui stat. Este deosebit de îngrijorător faptul că aceste amenințări nu provin doar de la alte state cu resurse semnificative, ci și de la indivizi rău intenționați care au nevoie doar de cunoștințe și acces la un computer pentru a reprezenta o amenințare potențială.

Una dintre problemele esențiale în dezbateră privind considerarea criminalității ciberneticice drept o amenințare la adresa securității naționale este clasificarea acesteia. Criminalitatea informatică, asemănătoare criminalității transnaționale, include o varietate de infracțiuni, dintre care nu toate sunt văzute ca potențiale amenințări la securitatea națională. Deși criminalitatea informatică acoperă în general infracțiuni comise cu ajutorul sau prin intermediul sistemelor informatice, cum ar fi exploatarea copiilor, fraudă, spălarea banilor, „hacktivismul”, spionajul și terorismul, în Republica Moldova definiția este în general destul de largă pentru autoritățile care se ocupă de acest fenomen.

Într-un mod interesant, Grabosky P. [9] distinge între criminalitatea informatică organizată și cea neorganizată în contextul securității naționale, sugerând că amenințarea nu este determinată în mod exclusiv de organizație, ci mai degrabă de scopurile sau motivațiile grupurilor respective. De asemenea, se argumentează că împărțirea infracțiunilor informatice în grupuri bazate pe motivație ajută la gestionarea acestora mai eficient.

Prin clasificarea infracțiunilor informatice în categorii distincte, se poate atribui unui grup sau departament guvernamental responsabilitatea de a aborda aceste infracțiuni, utilizând specialiști cu expertiză adecvată în domeniul respectiv.

Cu toate acestea, pentru a clasifica și a răspunde în mod corespunzător la infracțiunile informatice, motivația din spatele crimei trebuie cunoscută și înțeleasă [2]. De exemplu, sabotarea sistemelor de control și supraveghere ale unei centrale nucleare ar putea fi realizată de „hacktiviști” care protestează împotriva utilizării energiei nucleare, sau poate fi opera teroriștilor care încearcă să afecteze infrastructura critică. De asemenea, poate fi un act de sabotaj economic, cum ar fi spionajul realizat de o companie energetică rivală pentru a obține un avantaj pe piață. Deși este evident beneficiul de a avea grupuri specializate în combaterea acestor infracțiuni informatice, delimitarea precisă a acestor grupuri criminale poate fi extrem de dificilă, în special atunci când motivațiile nu sunt clar definite pentru analiză, și mai ales când făptuitorul nu poate fi identificat sau refuză să își asume responsabilitatea.

Republica Moldova nu este complet imună la atacurile și infracțiunile informatice. Un atac cibernetic direcționat cu succes ar putea perturba serviciile critice, ar putea afecta negativ economia și ar putea reprezenta o amenințare potențială la adresa securității naționale. Este evident că Guvernul Republicii Moldova este expus la criminalitatea informatică și este vulnerabil la astfel de atacuri, cu mai multe incidente în care site-uri din țară au fost vizate, cum ar fi încercările de blocare a serverelor Aeroportului Chișinău, Ministerului de Externe și Agenției Naționale pentru Reglementare în Energetică [13]. În urma acestor incidente, autoritățile le recomandă prestatorilor de servicii să-și consolideze securitatea cibernetică.

Un alt exemplu relevant este incidentul din seara zilei de 17 decembrie 2023, când serviciile și resursele de informare guvernamentale au fost inaccesibile timp de peste o oră, între orele 21:18 și 22:23. În această perioadă, site-urile guvernamentale din Republica Moldova nu au putut fi accesate de utilizatorii internaționali ai Internetului și de către toți utilizatorii operatorilor naționali (consumatori MD-IX). Cu toate acestea, disponibilitatea nu a fost afectată pentru utilizatorii din rețelele RTAAP furnizate de STISC instituțiilor guvernamentale. În același context, Președinția Republicii Moldova a raportat compromiterea serverului său de poștă electronică, descoperită la data de 10 august 2022 [14].

Observăm și investigațiile inițiate de către Serviciul de Informații și Securitate în colaborare cu Procuratura municipiului Chișinău, Oficiul Principal, pentru contracararea activității unui hacker specializat în criminalitate informatică în scopuri profitabile. Un tânăr în vârstă de 29 de ani a încercat ilegal să se autentifice pe sistemele informaționale guvernamentale aparținând I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” folosind metoda brute-force. În cadrul anchetei penale, au fost efectuate percheziții în locațiile unde opera individul, confiscându-se servere, unități de stocare și echipamente suplimentare pentru asigurarea funcționării continue (un generator, doisprezece UPS-uri profesionale, un stabilizator), precum și trei calculatoare de birou utilizate pentru gestionarea activității criminale.

Cele mai recente statistici privind criminalitatea pentru Republica Moldova au categorii precum: art. 177 din Codul penal, art. 178 din Codul penal, art. 260¹ din Codul penal, art. 260² din Codul penal, art. 260³ din Codul penal, art. 260⁵ din Codul penal, art. 260⁶ din Codul penal, art. 261 din Codul penal, art. 261¹ din Codul penal și art. 301¹ din Codul penal (a se vedea *Anexa 1*). Astfel, Procuratura Republicii Moldova a raportat recent că a existat o descreștere a numărului cauzelor penale pornite în baza art. 177 din Codul penal, însă aceste cauze penale constituie în continuare un raport semnificativ de 53,9% din totalul cauzelor penale pornite pe fapte de crimă cibernetică pentru anul 2023. Un alt aspect relevant este redat în *Anexa 2* și anume scăderea numărului cauzelor penale privind infracțiunea de *Fals informatic*, însă s-a majorat neesențial numărul de cauze penale privind *Fraudă informatică* [15]. Cauzele penale cu privire la investigarea infracțiunilor informatice constituie circa 60% din totalul cauzelor penale pornite pe fapte de crimă cibernetică. Numărul acestora a scăzut semnificativ și este redat în tabelul din *Anexa 3*. Totodată, este relevant de indicat principalii indicatori ai activității organelor de urmărire penală în domeniul pe parcursul perioadei de raport conform *Anexei 4*.

În urma analizei datelor menționate, se observă unele discrepanțe în raportarea infracțiunilor informatice și inițierea dosarelor, rămânând mai multe probleme nerezolvate. În primul rând, una dintre cauzele numărului redus de dosare este faptul că victimele ar putea să nu raporteze deloc infracțiunea. În al doilea rând, acestea pot raporta incidentul, dar nu către poliție sau procuratură. În al treilea rând, entitățile la care se raportează incidentul pot să nu transmită informațiile către poliție. În al patrulea rând, chiar dacă incidentele sunt raportate la poliție, acestea pot să nu fie încadrate juridic ca infracțiuni informatice. Drept urmare, oamenii nu abordează serios criminalitatea informatică și nu o consideră o infracțiune reală din cauza naturii sale virtuale. De exemplu, dacă o persoană contactează banca pentru o tranzacție suspectă în cont, pe cine va suna când e-mailul său a fost piratat? Furnizorul de e-mail? Aceste probleme pot crea o reprezentare eronată a incidenței criminalității informatice nu doar în Republica Moldova, ci la nivel global, dacă mecanismele de raportare nu pot centraliza diferitele date legate de activitățile ciberneticе.

Rapoartele privind scăderea criminalității generale pot avea consecințe neintenționate pentru Republica Moldova dacă se ignoră importanța criminalității cibernetice. Această problemă evidențiază faptul că infracțiunile informatice nu sunt tratate la fel ca infracțiunile fizice, așa cum demonstrează atacurile cibernetice menționate, care nu au declanșat investigații sau urmăriri penale din partea poliției. Dacă autoritățile nu inițiază raportări precise, resursele necesare pentru prevenirea infracțiunilor informatice și pentru creșterea rezilienței vor fi probabil irosite. Situația actuală este potențial periculoasă, deoarece evaluările naționale ale amenințărilor din Republica Moldova nu se bazează pe statistici exacte sau complete. În cazul unui atac cibernetic semnificativ, Republica Moldova ar putea fi nepregătită. Prin urmare, sunt necesare statistici colectate printr-un mecanism de raportare cuprinzător și precis pentru a determina dacă criminalitatea informatică are potențialul de a afecta securitatea națională a Republicii Moldova, influențând capacitatea țării și a cetățenilor săi de a funcționa normal. Neraportarea, raportarea greșită sau incapacitatea de a înregistra cu exactitate datele despre criminalitatea informatică afectează capacitatea autorităților de a combate această problemă eficient. Resursele și cercetările necesare provin din capacitatea agențiilor și a guvernului de a justifica necesitatea acestora. Dacă criminalitatea informatică nu este raportată și înregistrată corect și complet într-un mod centralizat (așa cum se întâmplă cu majoritatea celorlalte infracțiuni), guvernul va avea dificultăți în a prezice impactul asupra afacerilor și mijloacelor din Republica Moldova, afectând astfel planificarea resurselor pentru apărare și rezistență. Așa cum considerăm, un eșec de a planifica înseamnă un plan de a eșua.

O altă problemă esențială care apare în dezbaterile privind dacă criminalitatea informatică reprezintă o amenințare directă la adresa securității naționale a Republicii Moldova este capacitatea statului de a colecta statistici precise despre incidența acestor infracțiuni, precum și de a urmări penal și a pedepsi făptașii. Tabansky [1] și Burton [16] menționează despre alegerea unei persoane să folosească spațiul cibernetic pentru mijloace ilegale în detrimentul comiterii fizice a infracțiunii. Ei susțin că alegerea este evidentă; spațiul cibernetic poate oferi viteză, anonimat, operare de la distanță și posibilitatea ca infracțiunea să nu fie raportată și, prin urmare, un risc redus de reținere și urmărire penală. Cu toate acestea, comiterea efectivă a infracțiunii este probabil să fie mai lentă și să necesite prezența reală într-o locație. Prin urmare, potențialul ca cineva de a recunoaște individul crește șansa ca infracțiunea să fie raportată, sugerând că șansa de reținere este mare.

Criminologia clasică sugerează că infracțiunea este rezultatul unei decizii raționale, iar în luarea acestei decizii, folosim aceeași logică: dacă există certitudinea pedepsei, decizia rațională este de a nu comite infracțiunea. Dintr-o perspectivă criminologică, este mai rațional să comiți o infracțiune informatică decât una fizică, deoarece pedeapsa nu este atât de sigură. Această idee este susținută și de Tabansky [1], „*răspunsurile statului nu au ținut pasul cu ritmul schimbărilor tehnologice în spațiul cibernetic*” [1, p. 120]. Dacă o infracțiune fizică ar declanșa o investigație a poliției, o infracțiune informatică ar putea să nu fie raportată sau, chiar dacă ar fi, ancheta ar putea fi complicată de faptul că infracțiunea a avut loc într-o altă țară unde nu există posibilități de extrădare sau Republica Moldova nu are jurisdicție. Astfel, criminalitatea informatică reprezintă o amenințare directă la adresa securității naționale a Republicii Moldova, având potențialul de a distruge infrastructura, de a afecta economia prin pierderea proprietății intelectuale, a secretelor comerciale sau a informațiilor sensibile din punct de vedere comercial și de a perturba sau dăuna viețile și mijloacele de trai ale cetățenilor moldoveni.

Republica Moldova, fiind atât relativ mică, cât și izolată geografic, depinde în mare măsură de tehnologiile care permit conectarea globală a persoanelor și întreprinderilor, aspect reflectat probabil în exporturi și investiții. Deși anterior Republica Moldova beneficia de o securitate națională fizică datorită izolării sale geografice, aceasta nu mai poate fi considerată îndepărtată sau izolată, deoarece implicarea sa internațională și conexiunile globale au creat condițiile pentru a fi o țintă pentru infractorii cibernetici. Atât Statele Unite, cât și Regatul Unit consideră criminalitatea informatică drept o amenințare de prim nivel, la egalitate cu terorismul, iar Forumul Economic Mondial a clasat criminalitatea cibernetică drept cea mai mare amenințare la adresa infrastructurii globale în 2012 [17].

Criminalitatea informatică nu are doar potențialul de a afecta securitatea națională a Republicii Moldova prin economia sa, ci și prin capacitatea de a provoca daune și perturbări activităților zilnice, cum ar fi atacurile de tip Denial of Service asupra infrastructurilor guvernamentale. Aceste infracțiuni informatice nu sunt doar perturbatoare, ci și amenință încrederea în afaceri.

Deși Republica Moldova nu primește în prezent atenția globală acordată marilor puteri, ea este indisolubil legată de propriile angajamente, ceea ce face ca preocupările de securitate să fie la fel de importante. Țara noastră este, de asemenea, dependentă de lumea cibernetică, la fel ca orice altă națiune, arătând că sistemele și rețelele informatice care susțin toate sectoarele esențiale ale vieții de zi cu zi au o complexitate similară cu amenințarea teroristă mai largă: sunt internaționale și multifacetate.

Criminalitatea informatică este legată direct de securitatea națională, deoarece amenință sistemele informatice, rețelele și infrastructura care susțin viața cotidiană în Republica Moldova. Cel mai convingător

argument pentru care criminalitatea cibernetică reprezintă o amenințare la adresa securității naționale este potențialul de câștiguri mari. De exemplu, între septembrie 2011 și septembrie 2012, criminalitatea informatică a costat Noua Zeelandă aproximativ 625 de milioane de dolari. Această cifră, afectată de inconsistențele în raportarea statistică, poate reprezenta doar o mică parte din activitatea totală, existând multe alte cazuri de criminalitate informatică neraportate. De asemenea, s-a afirmat că criminalitatea informatică în Noua Zeelandă depășește piața neagră a diferitelor narcotice [18].

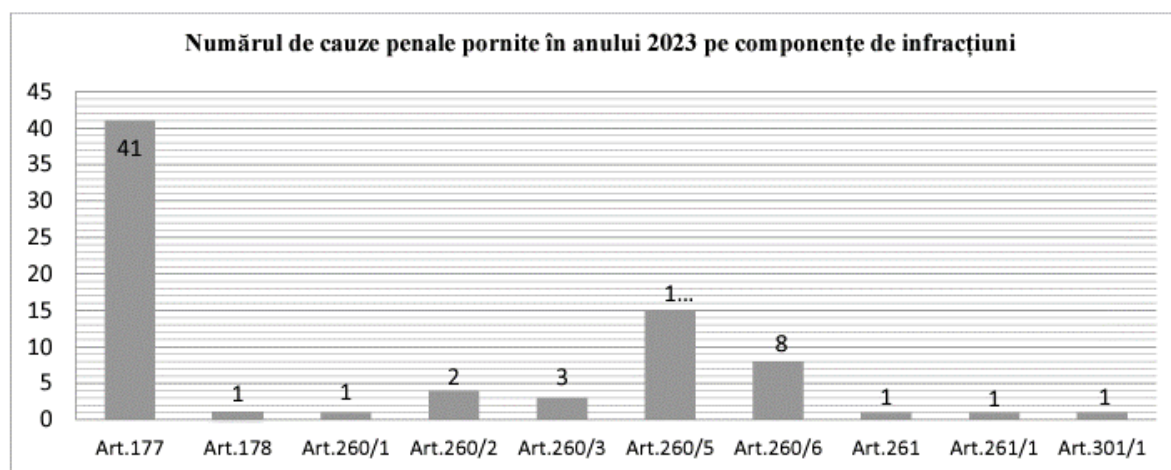
Deși criminalitatea informatică este considerată o amenințare la adresa securității naționale a Republicii Moldova datorită vitezei, anonimatului, costurilor scăzute de operare și capacității de a destabiliza economia și infrastructura critică, există riscul de a supraseduciza această problemă. Acest lucru ar putea determina statul să revindă drepturi speciale pentru a combate problema prin orice mijloace necesare. Criminalitatea informatică este fluidă și adaptabilă, ceea ce necesită ca guvernele, inclusiv cel al Republicii Moldova, să fie la fel de flexibile și adaptabile, fără a încălca libertățile civile excesiv.

Concluzii: Perspectiva Republicii Moldova nu diferă de cea a altor țări. Problemele prezentate de criminalitatea informatică trebuie abordate în mod combinat de structurile statului, care trebuie să promoveze o mai mare claritate în raportarea infracțiunilor cibernetice și a problemelor actuale.

Este clar că criminalitatea informatică reprezintă un exemplu perfect de estompăre a graniței dintre amenințările interne și externe la adresa securității naționale. Astfel, departamentele guvernamentale trebuie să depășească abordarea exclusiv internă sau externă și să adopte o combinație a celor două. Datorită schimbărilor aduse de amenințarea criminalității cibernetice, cerințele de securitate națională necesită vigilență constantă și revizuirea continuă a politicilor și legislației pentru a combate creșterea activităților criminalității cibernetice.

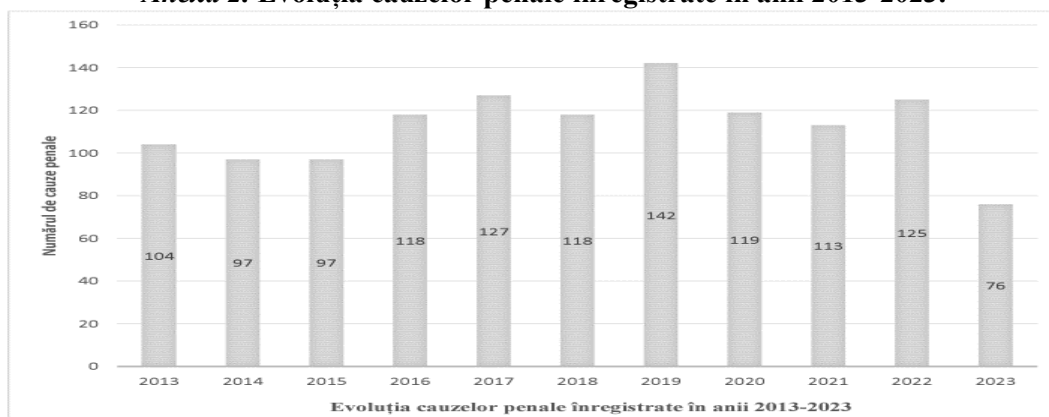
Complexitatea criminalității informatice reprezintă o provocare majoră pentru securitatea națională. De la spionajul cibernetic sponsorizat de stat la grupurile independente de hackeri, motivele din spatele atacurilor cibernetice sunt diverse. Aceste atacuri țintesc infrastructura critică, bazele de date guvernamentale sensibile și chiar sistemele electorale, subminând astfel structura de securitate a unei națiuni. Furtul de informații clasificate și întreruperea serviciilor esențiale prin mijloace cibernetice pot afecta capacitatea unei națiuni de a răspunde eficient la amenințările interne și externe. Pe lângă compromiterea datelor sensibile, criminalitatea informatică provoacă daune economice severe. Furtul de proprietate intelectuală, fraudă online și atacurile ransomware asupra întreprinderilor nu doar destabilizează economia, ci și împiedică progresele tehnologice esențiale pentru dezvoltarea națională. Impactul financiar al criminalității cibernetice se extinde în diverse sectoare, afectând atât întreprinderile mici, cât și marile corporații, subminând astfel rezistența economică a unei națiuni.

Anexa 1. Numărul de cauze penale pornite în anul 2023 pe componente de infracțiuni.



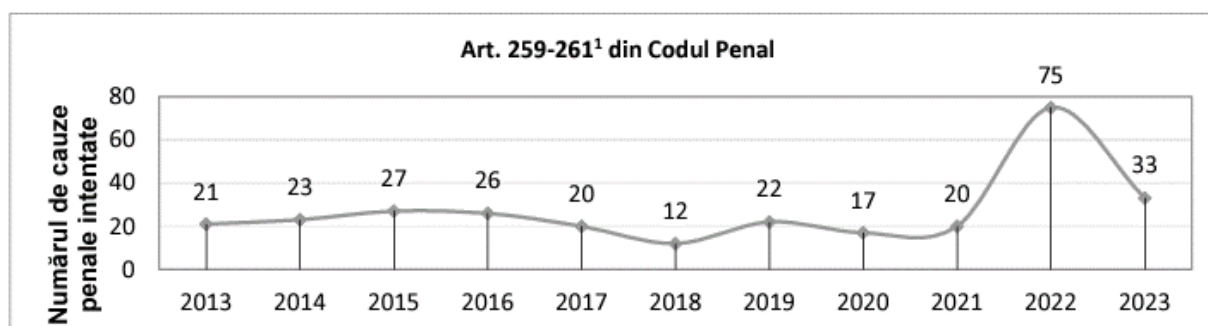
Sursa: Raportul privind activitatea Procuraturii pentru anul 2023.

Anexa 2. Evoluția cauzelor penale înregistrate în anii 2013-2023.



Sursa: Raportul privind activitatea Procuraturii pentru anul 2023.

Anexa 3. Numărul de cauze penale intentate pe anii 2013-2023.



Sursa: Raportul privind activitatea Procuraturii pentru anul 2023.

Anexa 4. Numărul de cauze penale în perioada anului 2023.

Numărul de cauze penale în perioada de activitate - 2023		
Pornite		76
Transmise după competență		14
Clasate		20
Conexate		5
Suspendată urmărirea penală	Persoana anunțată în căutare	4
	Nu este identificată persoana	14
Trimise în judecată		25
Suspendate condiționat		-
Fără soluții		97

Sursa: Raportul privind activitatea Procuraturii pentru anul 2023.

REFERINȚE BIBLIOGRAFICE

1. TABANSKY, L. *Cybercrime: A National Security Issue?*. În: Military and Strategic Affairs, vol. 4, nr. 3, Decembrie 2012. pp. 117-136. Disponibil la: https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/MASA4-3Engd_Tabansky.pdf [Accesat: 21.08.2024].
2. *Public and Private Entities Face Challenges in Addressing Cyber Threats*. GAO-07-705-Cybercrime Report. Iunie 2007, pp. 16-17. Disponibil la: <http://www.gao.gov/assets/270/262608.pdf>. [Accesat: 11.08.2024].
3. „The 2005 FBI Computer Crime Survey”. Federal Bureau of Investigation, USA. 19 p. Disponibil la: <http://www.wheresthepaper.org/FBIccs2005.pdf> [Accesat: 09.03.2024].

4. HATHAWAY, M. E. *Falling Prey to Cybercrime: Implications for Business and the Economy*. Cap. 6. În: *Securing Cyberspace: A New Domain for National Security*. Queenstown: Aspen Institute, Februarie 2012.
5. Oficiul pentru Securitate Cibernetică și Asigurare Informațională al Oficiului Cabinetului Regatului Unit și Detica. *The Cost of Cyber Crime*. 2011. 32 p. Disponibil la: <https://assets.publishing.service.gov.uk/media/5a79c9bc40f0b66d161ae26d/the-cost-of-cyber-crime-full-report.pdf> [Accesat: 21.07.2024].
6. *Norton Study Calculates Cost of Global Cybercrime: \$114 Billion Annually*. Disponibil la: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02. [Accesat: 17.08.2024].
7. Federal Bureau of Investigation. Internet crime report 2021. Disponibil la: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [Accesat: 16.08.2024].
8. HANDLER, S.; ROWLEY, L. The 5x5—Cybercrime and national security. Disponibil la: <https://www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/> [Accesat: 04.07.2024].
9. GRABOSKY, P. *Organized Crime and National Security*. În: *Challenges for Criminology and Criminal Justice*. Seoul. 2014. p. 19-30.
10. BURTON, J. *Small states and cyber security: The case of New Zealand*. În: *Political Science*, nr. 65 (2), 2013. pp. 216-238.
11. BIRCHFIELD, R. *Cyber threats and data privacy*. În: *Management*, 2013. p. 46-51.
12. BURKE, RH. *An Introduction to Criminological Theory*. În: *Oxon*, 2009. Anglia: Taylor & Francis.
13. CARȚÎN, S. Atac cibernetic asupra site-urilor din Republica Moldova. Disponibil la: <https://tvrmdova.md/article/1b68e425e462a815/atac-cibernetic-asupra-site-urilor-din-republica-moldova.html> [Accesat: 06.08.2024].
14. SAVA, C. Atac cibernetic la președinția Republicii Moldova. Disponibil la: <https://tvrmdova.md/article/f94a8e1f0b38fa1c/atac-cibernetic-la-presedintia-republicii-moldova.html> [Accesat: 21.08.2024].
15. Ordinul Procurorului General interimar nr. 19/3 din 28.02.2024 privind aprobarea Raportului de activitate al Procuraturii pentru anul 2023.
16. BURTON, J. *Small states and cyber security: The case of New Zealand*. În: *Political Science*, nr. 65 (2), 2013. pp. 216-238.
17. Hotărârea nr. 930/2021 privind aprobarea Strategiei naționale împotriva criminalității organizate 2021-2024. În: *Monitorul Oficial al României, Partea 1*, nr. 898 din 20.09.2021.
18. GRIFFIN, P. *The crime online*. În: *Listener*, nr. 52. 2012.