Protejarea spațiului informațional

Analiza Strategiei Securității Informaționale (2019-2024) și prezentarea recomandărilor pentru noua Strategie

PISA
Platforma pentru Inițiative de Securitate și Apărare
DCAF
Geneva Centre for Security Sector Governance
Sweden
Sverige

CENTRUL DE LA GENEVA PENTRU GUVERNAREA SECTORULUI DE SECURITATE (DCAF)

PLATFORMA PENTRU INIȚIATIVE DE SECURITATE ȘI APĂRARE (PISA)

PROTEJAREA SPAȚIULUI INFORMAȚIONAL: **Analiza Strategiei Securității Informaționale (2019-2024) și prezentarea recomandărilor pentru noua Strategie**

AUTORI:
Sanda SANDU, Rodica PANȚA, Sergiu BOZIANU, Elena MÂRZAC, Danu MARIN

CHIȘINĂU 2025

Studiul a fost elaborat în cadrul proiectului „Consolidarea securității informaționale în Republica Moldova. Analiză și consultare”, implementat de Platforma pentru Inițiative de Securitate și Apărare (PISA) și susținut de Centrul de la Geneva pentru Guvernarea Sectorului de Securitate (DCAF), ca parte a proiectului „Consolidarea Guvernării Sectorului de Securitate în Moldova”, finanțat de Suedia.

Ne exprimăm înalta consideraţie şi toată gratitudinea noastră pentru toate instituțiile care ne-au acordat suport în elaborarea acestui Studiu prin completarea chestionarelor sau participare la interviurile organizate în cadrul proiectului.

CUPRINS

INTRODUCERE

Într-o lume în care granițele dintre realitate și lumea virtuală sunt neclare, spațiul informațional devine o adevărată linie invizibilă ce ne unește, ne modelează și, uneori, ne divizează. Ne aflăm simultan în două lumi - cea fizică, palpabilă și definită de interacțiuni directe, și cea online, fluidă și imprevizibilă, unde informația circulă fără limite. În această lume digitală, fiecare clic, fiecare postare și fiecare știre contribuie la construirea percepției noastre despre realitate. Este un spațiu al oportunităților, dar și al riscurilor emergente sau nemaiîntâlnite.

Spațiul informațional este, astăzi, câmpul de luptă al ideilor. Manipularea informațională nu mai este doar un fenomen izolat, ci o strategie sofisticată aplicată de actori statali și non-statali. În aceste lumi paralele, manipularea informațională reprezintă una dintre cele mai mari amenințări, având puterea de a distorsiona realitatea, de a influența procesele democratice și de a submina încrederea în instituțiile fundamentale ale statului.

Strategia Securității Informaționale are scopul să protejeze spațiul informațional, iar aceasta are un impact asupra fiecărei persoane, de la elevul/eleva care își caută sursele pentru un proiect școlar, părintele care încearcă să distingă între știri reale și false, jurnalista care luptă să aducă adevărul în lumină la fiecare dintre noi, cei care, fără să ne dăm seama, purtăm o luptă zilnică pentru a discerne realitatea, adevărul sau minciuna. Într-o lume în care informația ne definește deciziile, protejarea acestui spațiu devine o misiune pentru noi toți.

Implementarea Strategiei Securității Informaționale a Republicii Moldova pentru anii 2019-2024 a adus rezultate semnificative în consolidarea capacităților instituționale și legislative privind protecția informației și combaterea amenințărilor cibernetice. Printre realizările palpabile pentru cetățeni se numără sporirea securității în spațiul online și implementarea campaniilor de informare împotriva dezinformării. Totuși, există lacune în ceea ce privește adaptarea rapidă la noile forme de propagandă și război hibrid, precum și în educația cetățenilor privind utilizarea responsabilă a informației. Eforturile recente ale autorităților au crescut reziliența cetățenilor față de aceste amenințări, însă mai sunt necesare acțiuni pentru a combate complexitatea fenomenelor de dezinformare și influență externă.

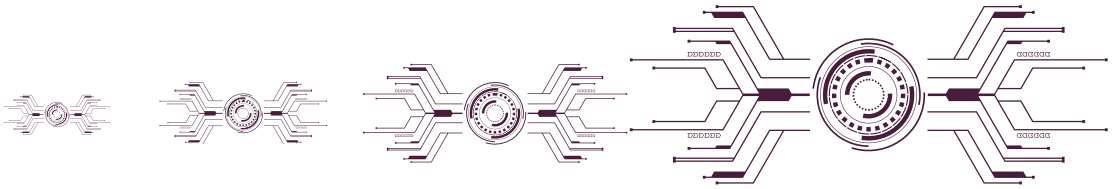
Acest document își propune să analizeze implementarea Strategiei de Securitate Informațională a Republicii Moldova în perioada 2019-2024. Printre realizările semnificative se numără consolidarea cadrului legislativ prin adoptarea Legii nr. 48/2023 privind Securitatea Cibernetică, crearea structurilor de răspuns la incidente precum CERT Gov MD și lansarea unor campanii de educare privind protecția datelor cu caracter personal. De asemenea, s-a înregistrat o îmbunătățire a cooperării internaționale, în special prin

parteneriate cu UE, NATO și alte organizații regionale, cu scopul de a întări reziliența cibernetică, informațională și combaterea amenințărilor hibride.

Cu toate acestea, procesul de implementare a întâmpinat multiple provocări sistemice. Printre cele mai acute probleme se numără lipsa specialiștilor calificați, infrastructura învechită și resursele financiare limitate. Coordonarea deficitară între instituțiile responsabile de securitatea informațională, precum SIS, MAI, Procuratura Generală, a încetinit realizarea unor obiective strategice esențiale. De asemenea, dezinformarea și manipularea informațională rămân amenințări constante, amplificate de campaniile externe menite să submineze stabilitatea democratică, în special în perioade electorale și în contextul referendumului privind aderarea la UE.

Pentru a răspunde acestor provocări, noua Strategie de Securitate Informațională trebuie să includă măsuri concrete pentru dezvoltarea capacităților instituționale, combaterea dezinformării, modernizarea infrastructurii critice și consolidarea cooperării internaționale. De asemenea, noua Strategie trebuie să conțină o componentă dedicată reglementării social media și educației informaționale pentru a crește reziliența cetățenilor în fața manipulărilor externe și interne.

CONTEXT



Securitatea informațională a Moldovei este strâns legată atât de capacitatea statului de a comunica eficient cu cetățenii săi, cât și de nivelul de informare și educație mediatică a populației. Într-o lume în care fluxul informațional este mai intens ca oricând, nivelul de informare al publicului crește, dar încrederea în sursele de știri rămâne fragilă. Studiile arată că tot mai mulți cetățeni din Moldova se simt bine informați, percepția de părtinire și influența politică continuă să erodeze satisfacția față de media și sursele de informare oficiale. În același timp, digitalizarea și extinderea în viața cotidiană a conținutului generat de inteligența artificială aduc oportunități, dar și riscuri semnificative de natură informațională și societală. Capacitatea cetățenilor de a recunoaște dezinformarea se îmbunătățește treptat, însă complexitatea peisajului mediatic, dominat tot mai mult de rețele sociale și conținut AI, ridică noi provocări pentru securitatea informațională și educația media.

Strategia de Securitate Informațională a Republicii Moldova pentru anii 2019-2024 a fost concepută să răspundă provocărilor tot mai complexe din spațiul informațional național, având în vedere avansarea tehnologică și riscurile asociate manipulării informaționale. În cadrul Strategiei au fost abordate riscurile generate de atacurile hibride, dezinformare, criminalitate informatică și coordonarea deficitară între instituțiile naționale. Structurată pe patru piloni principali, Strategia a vizat protejarea spațiului informațional-cibernetic, securizarea spațiului mediatic, consolidarea capacităților operaționale și îmbunătățirea cooperării naționale și internaționale.

1) Pilonul I: „Asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice";

2) Pilonul II: „Asigurarea securității spațiului informațional-mediatic";

3) Pilonul III: „Consolidarea capacităților operaționale";

4) Pilonul IV: „Eficientizarea procesului de coordonare internă și cooperare internațională în domeniul securității informaționale"

Asigurarea securității spațiului informațional-mediatic în Republica Moldova este o prioritate pentru stabilitatea națională, în contextul provocărilor multiple generate de războiul informațional, propaganda și dezinformarea externă.

Potrivit Strategiei Securității Informaționale 2019-2024, acest domeniu vizează protejarea spațiului mediatic național de influențele externe nocive, mai ales în timpul evenimentelor politice majore, când campaniile de dezinformare sunt amplificate pentru a influența opinia publică și procesele decizionale.Analizând implementarea Strategiei Securității Informaționale a Republicii Moldova 2019-2024, putem observa câteva realizări și lacune majore. Pe partea realizărilor, s-a reușit consolidarea cadrului legal și instituțional pentru combaterea criminalității informatice și sporirea rezilienței la atacurile cibernetice. Crearea CERT-urilor (Centre de Răspuns la Incidente de Securitate Cibernetică) la nivel național și guvernamental a reprezentat un pas important, alături de eforturile de conștientizare și educare a cetățenilor privind riscurile din spațiul cibernetic. De asemenea, a fost recunoscută necesitatea protecției infrastructurilor critice și implementarea măsurilor de prevenire și reacție la incidentele cibernetice.

Totuși, au existat și lacune semnificative. În primul rând, lipsa unui sistem integrat de management al securității cibernetice la nivel național a împiedicat o coordonare eficientă a resurselor și răspunsului la riscuri. De asemenea, lipsa de specialiști calificați și insuficienta finanțare pentru pregătirea și salarizarea acestora au redus capacitatea instituțiilor publice de a face față provocărilor emergente. Problemele legate de coordonarea între sectorul public și cel privat, și lipsa unor audituri cuprinzătoare de securitate cibernetică au fost, de asemenea, evidențiate ca bariere majore.

În timp ce s-au realizat progrese importante în asigurarea securității informaționale, persistă provocări considerabile care trebuie abordate în cadrul unei noi strategii. Acestea includ o mai bună coordonare instituțională, dezvoltarea capacităților operaționale și crearea unui sistem eficient de management al securității cibernetice

Realizările de până acum includ recunoașterea vulnerabilităților spațiului informațional și necesitatea creării unui cadru legislativ și instituțional pentru combaterea propagandei și a informării manipulatorii. De asemenea, s-a subliniat importanța cooperării cu societatea civilă și implicarea acesteia în monitorizarea și contracararea dezinformării.

Analizând modul în care a fost implementată Strategia Securității Informaționale am depistat 3 puncte-cheie care au reprezentat obiective de bază și sunt repere pentru Strategia următoare.

ASIGURAREA SECURITĂȚII SPAȚIULUI INFORMAȚIONAL MEDIATIC

Asigurarea securității spațiului informațional mediatic în Republica Moldova este importantă pentru menținerea stabilității interne și prevenirea interferențelor externe în procesele politice și sociale. Noua strategie de securitate informațională ar trebui să prioritizeze combaterea propagandei externe și a campaniilor de dezinformare printr-o abordare holistică, care să includă atât măsuri tehnice, cât și strategii de comunicare eficientă. În contextul unui mediu

informațional tot mai dominat de influențe străine, este necesară implementarea unor mecanisme proactive de monitorizare și răspuns la incidentele din acest spațiu.

Pentru a proteja spațiul mediatic, este necesară o colaborare consolidată între instituțiile statului, sectorul privat și societatea civilă. Crearea unei platforme naționale dedicată monitorizării și combaterii dezinformării ar facilita detectarea rapidă a atacurilor și coordonarea răspunsului la nivel național. Această platformă ar putea, de asemenea, să ofere resurse educative pentru public, crescând reziliența informațională a cetățenilor prin creșterea gândirii critice.

Un alt aspect important al securității spațiului informațional este coordonarea cu partenerii internaționali. Republica Moldova ar trebui să își intensifice cooperarea cu organizațiile regionale și globale pentru a accesa tehnologii avansate de monitorizare și a învăța din experiențele altor state în combaterea amenințărilor hibride. Aceasta va ajuta la protejarea integrității informaționale a țării și la prevenirea escaladării campaniilor de dezinformare.

Noua Strategie trebuie să asigure și controlul mai riguros al surselor de informare interne, pentru a preveni utilizarea platformelor media locale în răspândirea propagandei străine. Stabilirea unor standarde clare privind transparența și responsabilitatea în mass-media este importantă pentru a contracara influențele maligne, asigurând astfel o informare corectă și obiectivă a cetățenilor.

DEZVOLTAREA CAPACITĂȚILOR DE REACȚIE ÎN CAZUL UNOR AMENINȚĂRI HIBRIDE DE SECURITATE

Amenințările hibride combină tactici tradiționale de război cu tehnici moderne de atacuri cibernetice, propagandă și dezinformare, creând un mediu complex și dificil de gestionat. Noua strategie de securitate informațională trebuie să abordeze în mod prioritar dezvoltarea capacităților de reacție la astfel de amenințări, prin întărirea capacităților instituționale și crearea unor proceduri clare de răspuns rapid. Republica Moldova trebuie să își îmbunătățească mecanismele de detectare timpurie a acestor amenințări și să dezvolte echipe de intervenție specializate în analizarea și combaterea războiului hibrid.

Un aspect esențial se referă la formarea și dotarea echipelor de răspuns cibernetic și a altor structuri guvernamentale care să poată răspunde prompt și eficient la atacurile de acest tip. Colaborarea între instituțiile de securitate națională, cum ar fi Serviciul de Informații și Securitate și Ministerul Apărării, va fi cheie pentru a asigura o apărare integrată. Mai mult, trebuie dezvoltate exerciții comune cu aliați internaționali pentru a testa și îmbunătăți capacitățile de reacție în situații reale. În plus, este necesară consolidarea legăturilor între domeniul securității informaționale și cel cibernetic, pentru a preveni și contracara atacurile care vizează infrastructurile critice și sistemele de guvernare digitală.

Aceasta include crearea unor protocoale de alertare rapidă și mecanisme de coordonare între entitățile publice și private care gestionează astfel de infrastructuri.De asemenea, implementarea unor politici de reziliență cibernetică, inclusiv introducerea standardelor de securitate pentru sectorul public și privat, va fi o componentă-cheie. Reziliența în fața amenințărilor hibride presupune nu doar detectarea și răspunsul la atacuri, ci și capacitatea de a se recupera rapid din astfel de incidente și de a preveni repetarea acestora.

MONITORIZAREA SPAȚIULUI INFORMAȚIONAL ȘI DEPISTAREA ACȚIUNILOR DE DEZINFORMARE ȘI DE INFORMARE MANIPULATORIE DIN EXTERIORUL ȘI INTERIORUL ȚĂRII

Unul dintre pilonii principali ai strategiei de securitate informațională este monitorizarea continuă a spațiului informațional pentru detectarea acțiunilor de dezinformare atât din exterior, cât și din interior. FIMI ar trebui să integreze surse diverse de date, inclusiv din media tradițională, social media și surse online, pentru a oferi o imagine completă a spațiului informațional. Acest sistem ar permite monitorizarea activă a actorilor externi, dar și a grupurilor interne care desfășoară campanii de dezinformare.

Prin colaborarea cu instituții de specialitate, cum ar fi agențiile de informații, instituțiile academice și societatea civilă, sistemul FIMI poate dezvolta algoritmi și metode de analiză avansate pentru a detecta tiparele de dezinformare și a preveni răspândirea acestora. Pe lângă monitorizare și detectare, sistemul ar putea genera rapoarte periodice și alerte care să ajute la elaborarea politicilor și la luarea deciziilor rapide în fața amenințărilor emergente.

Un alt element important este crearea unei baze naționale de date cu incidente de dezinformare, care să fie accesibilă instituțiilor guvernamentale și partenerilor privați implicați în securitatea informațională. Aceasta ar permite un răspuns coordonat și rapid la orice acțiuni care ar putea submina stabilitatea și securitatea națională.

CAPITOLUL I: EVALUAREA IMPLEMENTĂRII STRATEGIEI DE SECURITATE INFORMAȚIONALĂ ÎN PERIOADA 2019-2024

1.1 Realizările în implementarea Strategiei de Securitate Informațională

Strategia Securității Informaționale a Republicii Moldova pentru perioada 2019-2024 a fost concepută să răspundă provocărilor actuale în ceea ce privește criminalitatea cibernetică, vulnerabilitățile infrastructurilor digitale și impactul dezinformării. În continuare, prezentăm principalele realizări în cadrul acesteia.

Printre cele mai importante realizări la nivel național menționăm crearea:

Consolidarea cadrului instituțional și al cooperării între instituții și agenții guvernamentale

Consiliului coordonator pentru asigurarea securității informaționale (CSASI)

cu o reprezentare pe cele patru paliere: cibernetic, operațional, mediatic și civic-privat, a cărui funcție de bază este promovarea și coordonarea măsurilor de punere în aplicare a politicilor de securitate informațională și cibernetică într-o societate democratică, în funcție de dezvoltarea tehnologiei, raporturilor juridice și de altă natură din sectorul informațional atât la nivel național, cât și internațional [1].

Consiliului coordonator în domeniul securității cibernetice [2]

care este un organ colegial fără personalitate juridică a cărui funcție de bază este promovarea și coordonarea, la nivel strategic și operațional, a politicilor în domeniul securității cibernetice. Consiliul urmează să exercite un rol-cheie în coordonarea elaborării și implementării Strategiei naționale de securitate cibernetică și a altor documente de politici și de planificare în domeniul securității cibernetice.

De asemenea, instituirea Agenției pentru Securitate Cibernetică [3], autoritate administrativă subordonată Ministerul Dezvoltării Economice și Digitalizării ce are misiunea de a implementa politica de stat în domeniul securității cibernetice, pentru asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii, esențiale pentru funcționarea societății și a statului [4].

În aceeași ordine de idei, instituției Publice Serviciul Tehnologia Informației și Securitatea Cibernetică i s-a conferit rolul de Centru guvernamental de reacție la incidente de securitate cibernetică (CERT Gov), iar cu suportul Serviciului de Informații și Securitate au fost create

CERT – urile departamentale - subdiviziuni de securitate pentru tehnologia informației în cadrul a 22 entități/instituții de stat în domenii, precum sectorul energetic, servicii de transport, sănătate, comunicații și sectorul financiar. Centrele au fost echipate cu tehnologie avansată pentru identificarea și soluționarea rapidă a vulnerabilităților, monitorizarea traficului de date și a incidentelor cibernetice. Aceste modificări instituționale au dus la crearea unui sistem național integrat pentru gestionarea riscurilor cibernetice și la consolidarea cooperării dintre SIS, Serviciul Tehnologia Informației și Securitatea Cibernetică și Agenția de Guvernare Electronică [5]. În rezultat, în cadrul celui de-al doilea tur al alegerilor prezidențiale, sistemul cibernetic a rezistat în pofida unui atac cibernetic Ddos asupra site-ului voteaza.md [6].

În ceea ce privește comunicarea strategic, aceasta este abordată ca o componentă esențială în asigurarea securității informaționale a Republicii Moldova, mai ales în contextul provocărilor hibride și a dezinformării. Strategiaşsi-a propus să dezvoltare mecanisme de comunicare strategică pentru realizarea intereselor naționale și anume crearea unei platforme informaționale de comunicare strategică care să conțină informații despre incidentele de securitate informațională, ghiduri de comunicare strategică și tentative de dezinformare. În acest sens a fost planificat acordarea politicilor de comunicare internă la platformele externe ale structurilor de securitate, apărare și ordine publică, dezvoltarea unor politici de comunicare strategică pentru consolidarea securității informaționale și promovarea intereselor naționale.

Plus, a fost evidențiată importanța implicarea societății civile și a experților în monitorizarea securității informaționale, crearea unui consiliu al societății civile pentru evaluarea și implicarea în asigurarea securității informaționale. În ceea ce privește combaterea dezinformării au fost propuse stabilirea unor ghiduri de comunicare strategică care să contracareze tentativele de manipulare, implementarea unor politici care să reglementeze activitatea mass-mediei digitale pentru a preveni propaganda și manipularea informațională.Aceste elemente evidențiază faptul că dezvoltarea și implementarea comunicării strategice reprezintă un pilon fundamental pentru securitatea informationala a statului, reziliența societății și protecția intereselor naționale.

În acest sens, o realizare importantă este crearea Centrului pentru Comunicare Strategică și Combatere a Dezinformării [7], care reprezintă o etapă incipientă de instituționalizare a comunicării strategice în Republica Moldova. În conformitate cu legislația în vigoare, activitatea Centrului este axată pe prevenirea propagandei și a manipulării informaționale în spațiul public și realizarea campaniilor de informare și cooperare internațională pentru contracararea fenomenelor de dezinformare.

Remarcăm câteva realizări în cadrul instituțiilor: crearea și operaționalizarea Centrului de Reacții Cibernetice din cadrul Armatei Naționale (ce facilitează implementarea măsurilor pentru protecția infrastructurii cibernetice a sectorului militar, în special în ceea ce privește

securitatea comunicațiilor speciale și protejarea informațiilor clasificate), restructurarea subdiviziunilor din cadrul Procuraturii, în anul 2022, și separarea tehnologiilor informaționale de combatere a crimelor cibernetice prin crearea Secției combaterea crimelor cibernetice, crearea Serviciului specializat de investigare a crimelor informatice în cadrul Direcției de poliție a municipiului Chișinău și crearea rețelei naționale de investigatori responsabili de domeniul prevenirii şi combaterii infracțiunilor informatice şi celor conexe, inclusiv de exploatare sexuală și abuz asupra copiilor prin Internet.

Îmbunătățirea cadrului legislativ și normativ

În perioada 2019-2024 au fost adoptate mai multe legi și reglementări care au drept scop să stabilească standarde de securitate cibernetică în toate instituțiile publice și în sectorul privat, inclusiv racordarea la prevederile Directivei NIS2 și, implicit, a unor elemente esențiale ale Directivei NIS1 [8]. Printre cele mai importante menționăm:

Adoptarea Legii nr. 48/2023 *privind securitatea cibernetică,*

care stabilește cadrul normativ primar în domeniul securității cibernetice, urmează să între în vigoare pe 1 ianuarie 2025. Legea are ca scop asigurarea securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private,
în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice.

Adoptarea Legii nr. 58/2024 *pentru modificarea unor acte normative,*

în vederea aducerii cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică, prin ajustarea normelor cuprinse în actele legislative sectoriale care reglementează activitatea viitorilor furnizori de servicii, precum și a normelor juridice, având un caracter conex normelor ce asigură direct aplicarea legislației armonizate.

Aprobarea Hotărârii Guvernului nr. 671/2023 privind dezvoltarea profesională în domeniul securității cibernetice

cibernetice și înființarea Institutului Național de Inovații în Securitatea Cibernetică „Cybercor” din cadrul UTM, care va asigura dezvoltarea abilităților în domeniul securității cibernetice a personalului din autoritățile publice, a studenților, profesioniștilor în securitatea cibernetică și a altor persoane interesate din sectorul public și privat, prin programe de instruire, perfecționare și exerciții de antrenament. Această inițiativă se aliniază demersurilor UE privind Cyber Skills Academy, prin care se urmărește reducerea deficitului de talente în securitatea cibernetică, consolidarea forței de muncă în acest domeniu și stimularea competitivității și rezilienței la nivelul UE.

Adoptarea Legii 195/2024 *privind protecția datelor cu caracter personal,*

care va intra în vigoare din 23.08.2026, care instituie: la art. 25, obligația operatorului de a asigura protecția datelor cu caracter personal, începând cu momentul conceperii și în mod implicit, și la art. 33, obligația raportării incidentelor de securitate în termen de cel mult 72 de ore și măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor efecte negative.

Elaborarea proiectul de lege de modificare a Codului penal care la 19.05.2023

În vederea armonizării legislației naționale cu Directiva 2011/92/UE a Parlamentului European și a Consiliului din 13 decembrie 2011, privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile, în anul 2023, de către Procuratura Generală în parteneriat cu C.I. „La Strada" a fost elaborat proiectul de lege de modificare a Codului penal care la 19.05.2023 a fost remis Ministerului Justiției ca autoritate care promovează proiectele de modificare a legii. Acest proiect ține să îmbunătățească răspunsul autorităților naționale la cazurile de exploatare a copiilor cu utilizarea tehnologiilor online.

Semnarea Ordinului comun dintre Ministerul Afacerilor Interne și Ministerul Educației și Cercetării cu privire la realizarea măsurilor de prevenire a riscurilor în mediul online a tinerilor.

Modificarea Legii nr. 20/2009 *privind prevenirea și combaterea criminalității informatice [9]*

Realizările substanțiale în dezvoltarea cadrului normativ în domeniul securității cibernetice sunt evidențiate și în clasamentele internaționale, inclusiv Indicele național de securitate cibernetică (NCSI), elaborat de e-Governance Academy, și Indicele global de securitate cibernetică (GCI), realizat de Uniunea Internațională a Telecomunicațiilor (ITU). NCSI, care atribuie Republicii Moldova poziția 8 în versiunea cea mai recentă a clasamentului (31 iulie 2024), evaluează cu valori maxime (100%) progresul Republicii Moldova în ceea ce privește politicile naționale, activitatea de cercetare-dezvoltare, analiza amenințărilor cibernetice și creșterea nivelului de conștientizare a protecția datelor cu caracter personal și combaterea criminalității cibernetice.

Alte domenii evaluate sunt: educația în domeniul securității cibernetice (90%), protecția infrastructurii informatice critice (50%), răspunsul la incidente cibernetice (79%) și apărarea cibernetică (33%) (Figura 1).

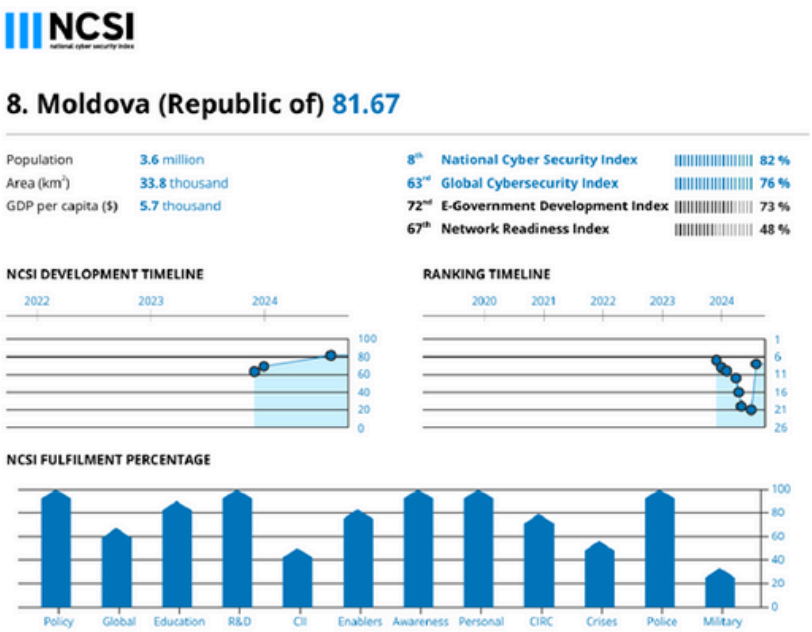


Figura 1. Poziția Republicii Moldova în clasamentul internațional *Indicele național de securitate cibernetică (NCSI)* Sursa: ncsi.ega.ee/country/md/?pdfReport=1 (accesat 24.09.2024)

Totodată, Republica Moldova a obținut un punctaj general de 65.09 în Indicele Global al Securității Cibernetice publicat de ITU, numărându-se printre statele care au demonstrat un angajament de bază în domeniul securității cibernetice prin acțiuni guvernamentale ce cuprind evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate într-un număr moderat de piloni sau indicatori (țările din categoria *T3 Establishing*). Astfel, eforturile Republicii Moldova în domeniul dezvoltării cadrului legal și normativ au acumulat un punctaj de 18,28 din 20 de puncte posibile, măsurile organizaționale au fost apreciate cu un scor de 15,51, iar măsurile de cooperare – 16,58. Cu toate acestea, există deficiențe semnificative în ceea ce privește măsurile tehnice (6,68/20) și dezvoltarea capacităților (8,04/20) ***(Figura 2).***

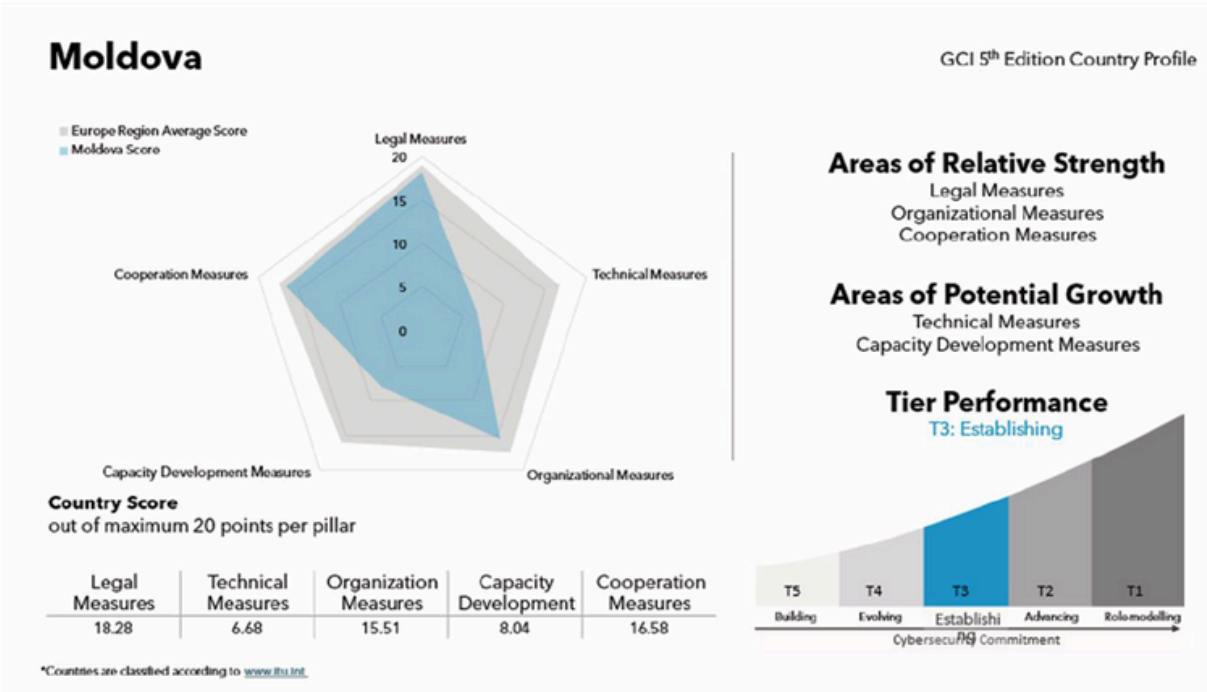


Figura 2. Scorul Republicii Moldova în clasamentul Indicele Global al Securității Cibernetice
Sursa: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Colaborarea internațională și importanța parteneriatelor în consolidarea securității informaționale și cibernetice

Republica Moldova a participat la inițiative regionale și internaționale, cum ar fi programele Uniunii Europene privind securitatea cibernetică și a dezvoltat parteneriate cu organizații globale pentru transferul de cunoștințe și resurse, care au contribuit la modernizarea capacităților locale în domeniul securității cibernetice și informaționale. Totodată, au fost **consolidate parteneriatele internaționale** atât la nivel multilateral prin colaborarea în domeniul apărării cibernetice cu NATO și Uniunea Europeană și extinderea cooperării cu Uniunea Europeană prin crearea Misiunii de Parteneriat a UE (EUPM), în conformitate cu Decizia (PESC) 2023/855 în cadrul politicii de securitate și apărare comună a UE. EUPM Moldova își propune să contribuie la îmbunătățirea rezilienței sectorului de securitate al Republicii Moldova în domeniul gestionării crizelor și al amenințărilor hibride, inclusiv în ceea ce privește securitatea cibernetică și contracararea acțiunilor străine de manipulare a informațiilor și a ingerințelor străine.

EUPM are două sarcini principale: consolidarea structurilor de gestionare a crizelor și consolidarea rezilienței la amenințările hibride [10]. La nivel bilateral, menționăm dezvoltarea colaborării cu Republica Italiană în domeniul securității, cu accent pe combaterea amenințărilor cibernetice, consolidarea parteneriatului cu Ucraina pentru combaterea criminalității organizate, inclusiv a infracțiunilor informatice și intensificarea cooperării cu Turkmenistanul în lupta împotriva criminalității organizate, cu accent pe prevenirea și combaterea infracțiunilor informatice.

În scopul aplicării mai eficiente a Strategiei au fost organizate campanii de sensibilizare și formare profesională pentru angajații din domeniul public și privat, care au sporit conștientizarea asupra riscurilor cibernetice și a măsurilor de prevenire. De exemplu, Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova (CNPDCP) a instruit 11.739 de persoane prin intermediul a cel puțin 190 de activități de instruire, scopul fiind sporirea gradului de percepție a angajaților asupra inovațiilor legislative privind protecția datelor cu caracter personal (evaluarea impactului, consultarea prealabilă, persoana responsabilă cu protecția datelor, transferul transfrontalier al datelor cu caracter personal), precum și asupra asigurării aplicării corecte a prevederilor legale din domeniu în activitatea pe care o desfășoară.

Rezultate mai modeste remarcăm în domeniul combaterii dezinformării și educației digitale. În pofida implementării diverselor programe naționale pentru educarea populației cu privire laidentificarea știrilor false și a manipulării informaționale, utilizarea securizată a tehnologiei și monitorizării mass-media și rețelelor sociale în scopul prevenirii propagării mesajelor care amenință securitatea națională, dezinformarea continuă să fie o amenințarea gravă la adresa securității naționale, lucru confirmat de prezența excesivă a narațiunilor false în timpul campaniei electorale și rezultatele referendumului constituțional. În conformitate cu Raportul OSCE, acestea au fostmarcate de îngrijorări privind interferența străină ilegală și eforturile active de dezinformare, care auavut un impact asupra integrității procesului electoral [11].

Strategia Securității Informaționale a Republicii Moldova 2019-2024 a realizat progrese semnificative în consolidarea cadrului instituțional și normativ, combaterea criminalității cibernetice și contracararea dezinformării. Printre realizările majore se numără crearea Consiliilor pentru securitatea informațională și cibernetică a Agenției pentru Securitate Cibernetică și a Centrului pentru Comunicare Strategică și Combaterea Dezinformării, implementarea CERT-urilor departamentale, adoptarea unor legi importante, precum Legea securității cibernetice și cea privind protecția datelor personale, racordate la standardele europene. De asemenea, inițiativele din domeniul educației digitale, crearea Centrului „Cybercor” și parteneriatele internaționale, inclusiv colaborarea cu UE și NATO, au contribuit la consolidarea rezilienței cibernetice. Totuși, dezinformarea și educația digitală rămân provocări semnificative, evidențiindu-se necesitatea unei abordări mai ample pentru a contracara amenințările hibride și a îmbunătăți securitatea informațională.

1.2. Provocări și impedimente în implementarea Strategiei de Securitate Informațională în perioada 2019-2024

Implementarea Strategiei de Securitate Informațională a Republicii Moldova în perioada 2019-2024 a reflectat o serie de eforturi semnificative, dar și multiple provocări sistemice. În continuare, prezentăm o analiză a progreselor și obstacolelor întâmpinate de instituțiile-cheie, precum și a contextului de securitate informațională în fața războiului hibrid și a evenimentelor electorale critice din 2024.

Strategia a fost fundamentată pe necesitatea unui cadru legislativ solid pentru securitatea cibernetică și cea informațională. Adoptarea Legii nr. 48/2023 privind securitatea cibernetică reprezintă un pas înainte în clarificarea responsabilităților instituționale și implementarea măsurilor de protecție. De asemenea, crearea unor structuri precum CERT Gov MD și inițiativele de instruire pentru protecția datelor cu caracter personal au oferit un cadru operațional îmbunătățit. Cu toate acestea, implementarea acestor măsuri a fost marcată de întârzieri și de o aplicare neuniformă între diferite instituții.

Combaterea dezinformării și a propagandei online reprezintă o provocare majoră, mai ales în contextul alegerilor prezidențiale și al referendumului privind aderarea la UE. Societatea civilă, experții, Consiliul Audiovizualului au remarcat ineficiența activităților desfășurate și lipsa unei strategii integrate pentru contracararea campaniilor de dezinformare. Această situație amplifică riscurile de polarizare socială și de subminare a proceselor democratice.

Resursele umane

Una dintre cele mai mari provocări sistemice este lipsa specialiștilor calificați în securitate cibernetică și informațională. Instituțiile publice, precum Ministerul Afacerilor Interne și Inspectoratul General al Poliției, au raportat o migrație constantă a experților IT către sectorul privat din cauza salariilor necompetitive.

Această situație a condus la o capacitate redusă de reacție în fața atacurilor cibernetice și a necesitat investiții urgente în formare profesională și retenția personalului. Deficitul de specialiști în securitate cibernetică constituie o barieră constantă în implementarea eficientă a strategiei. Lipsa resurselor umane calificate în instituțiile guvernamentale și sectorul privat împiedică dezvoltarea unor soluții robuste de protecție.

Exodul experților către sectorul privat, care oferă salarii mai competitive, agravează această problemă și reduce capacitatea instituțiilor de a răspunde rapid și eficient la amenințările cibernetice, dar și afectează grav capacitatea instituțiilor de a combate criminalitatea informatică. Această migrație constantă reduce numărul experților disponibili pentru investigarea infracțiunilor cibernetice și limitează eficiența măsurilor de prevenire.

Coordonarea instituțională

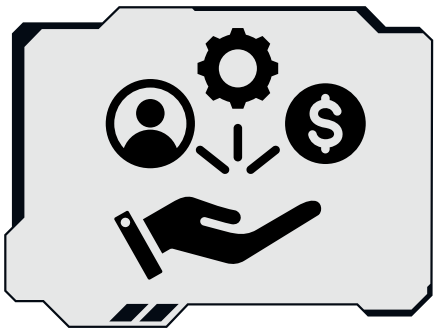
Cooperarea interinstituțională insuficientă afectează schimbul de informații și coordonarea în gestionarea incidentelor de securitate. În absența unei platforme centralizate pentru raportarea și analizarea incidentelor asupra securității informaționale, instituțiile nu reușesc să acționeze concertat. Această deficiență lasă infrastructurile critice vulnerabile în fața atacurilor tot mai sofisticate. Coordonarea între instituțiile responsabile de securitatea informațională rămâne un obstacol major. Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației și Ministerul Apărării au evidențiat lipsa unei platforme eficiente de schimb de informații și dificultățile în definirea clară a responsabilităților. Aceste lacune au dus la întârzieri în implementarea unor măsuri esențiale și la o reacție incoerentă în fața incidentelor de securitate.

Lipsa unei coordonări eficiente între instituțiile responsabile a încetinit implementarea acțiunilor planificate. Ambiguitatea în competențe și responsabilități pentru anumite acțiuni a dus la întârzieri în îndeplinirea obiectivelor strategice. Un exemplu ar fi Crearea Centrului Național de Reacție la Incidente de Securitate Cibernetică (CERT Național) a fost realizată doar parțial până în 2023.

Resurse financiare

Resursele financiare insuficiente au afectat majoritatea instituțiilor implicate în implementarea Strategiei. Ministerul Afacerilor Interne și Procuratura Generală au raportat constrângeri bugetare care au limitat achizițiile de echipamente și investițiile în infrastructură. Fără finanțare adecvată, eforturile de consolidare a securității informaționale sunt compromise. Multe instituții au semnalat insuficiența echipamentelor și a infrastructurii tehnologice necesare pentru protejarea rețelelor și a datelor sensibile. Ministerul Apărării și Procuratura Generală au subliniat nevoia urgentă de modernizare a infrastructurii critice și a

softurilor specializate pentru investigarea infracțiunilor cibernetice. Fără aceste investiții, instituțiile rămân vulnerabile la atacuri cibernetice și la război hibrid.



Insuficiența resurselor financiare limitează dezvoltarea capacităților necesare pentru reacția la incidente cibernetice. Bugetele reduse afectează achiziția de echipamente moderne și dezvoltarea infrastructurii necesare pentru protejarea datelor și investigarea infracțiunilor informatice.

Totodată, insuficiența echipamentelor și softurilor specializate limitează capacitatea de detectare și răspuns la atacuri cibernetice. Lipsa unei infrastructuri moderne afectează eficiența măsurilor de protecție și încetinește reacția la incidente.Bugetele limitate alocate pentru securitatea informațională împiedică dezvoltarea capacităților necesare pentru combaterea criminalității cibernetice. Fără resurse financiare adecvate, instituția nu poate achiziționa tehnologia necesară pentru investigarea eficientă a infracțiunilor informatice. Resursele limitate pentru analiza și prevenirea amenințărilor hibride îngreunează protejarea spațiului informațional al țării. SIS necesită o infrastructură modernizată și o forță de muncă bine instruită pentru a face față complexității amenințărilor actuale.

Cooperarea internațională

Republica Moldova este expusă constant la amenințări hibride, inclusiv atacuri cibernetice coordonate și campanii de manipulare informațională din surse externe, în special din partea Rusiei. Ministerul Dezvoltării Economice și Digitalizării a semnalat nevoia de consolidare a cooperării internaționale pentru a face față acestor amenințări. În lipsa unei strategii coordonate, războiul hibrid continuă să submineze stabilitatea națională.

Cooperarea internațională limitată a fost un alt impediment în implementarea Strategiei. Deși au fost stabilite parteneriate cu organizații precum NATO și UE, colaborarea efectivă și schimbul de bune practici sunt încă la un nivel insuficient. Această situație limitează accesul Moldovei la resurse și expertiză internațională necesare pentru consolidarea securității cibernetice.

Educație și informare

Nivelul scăzut de educație în securitate cibernetică și informațională reduce reziliența populației în fața amenințărilor. Inspectoratul General al Poliției și Procuratura Generală au subliniat importanța campaniilor de educare și conștientizare publică. Lipsa unor astfel de inițiative favorizează succesul campaniilor de phishing, fraude online și dezinformare.

Evaluarea implementării Strategiei de Securitate Informațională 2019-2024 subliniază necesitatea urgentă de a elabora o nouă strategie care să abordeze provocările sistemice. Aceasta trebuie să includă măsuri concrete pentru modernizarea infrastructurii, formarea specialiștilor, combaterea dezinformării și consolidarea cooperării internaționale. Doar printr-o abordare integrată și bine coordonată, Republica Moldova poate face față amenințărilor informaționale actuale și viitoare.

Tabel: Indicatori și evaluarea implementării SSI

INDICATOR	STARE IMPLEMENTARE	PROVOCĂRI IDENTIFICATE	RECOMANDĂRI
Crearea CERT Național	Parțial Realizat	Întârzieri în coordonarea interinstituțională și resurse limitate	Operaționalizarea CERT Național și consolidarea coordonării
Adoptarea cadrului legislativ pentru securitate cibernetică	Realizat	Adoptare întârziată, implementare parțială	Implementarea completă a legislației adoptate
Monitorizarea și combaterea dezinformării	Parțial Realizat	Lipsa unei strategii integrate și resurse insuficiente	Dezvoltarea unei strategii naționale anti-dezinformare
Capacități instituționale în combaterea criminalității informatice	Parțial Realizat	Deficit de personal și infrastructură învechită	Investiții în infrastructură și formare continuă
Protecția infrastructurilor critice naționale	În Proces de Realizare	Resurse financiare și tehnologice insuficiente	Alocarea de fonduri suplimentare pentru protecția infrastructurilor
Formarea specialiștilor în securitate cibernetică	Parțial Realizat	Exodul specialiștilor și lipsa programelor de formare	Lansarea de programe naționale de formare
Cooperare internațională în domeniul securității informaționale	Parțial Realizat	Cooperare internațională limitată	Consolidarea parteneriatelor cu UE și NATO
Campanii de educare și conștientizare publică	Parțial Realizat	Nivel scăzut de cultură în securitate cibernetică	Campanii naționale de conștientizare și educație

Implicarea insuficientă a tuturor actorilor din domeniul securității informaționale afectează colaborarea și coordonarea eforturilor. Lipsa unui angajament comun din partea tuturor instituțiilor reduce eficiența măsurilor de combatere a criminalității cibernetice. Coordonarea dificilă a activităților interinstituționale reprezintă un obstacol semnificativ în implementarea strategiei. Lipsa unui mecanism clar de cooperare între SIS și alte instituții afectează gestionarea eficientă a amenințărilor hibride și a campaniilor de dezinformare.

Evaluarea tendințelor pe social media și comunicarea de criză

Securitatea informațională a Republicii Moldova este profund afectată de războiul hibrid, care combină dezinformarea, propaganda și atacurile cibernetice pentru a destabiliza țara. Aceste tactici sunt utilizate pentru a amplifica diviziunile sociale, a eroda încrederea în instituțiile statului și a influența opinia publică în favoarea unor interese externe. Campaniile de dezinformare, adesea orchestrate prin rețele sociale și canale media afiliate, promovează narative false despre neutralitatea țării, identitatea națională și relațiile cu partenerii occidentali. În acest context, capacitatea Moldovei de a detecta și combate amenințările hibride este esențială pentru protejarea suveranității și stabilității naționale.

Studiile arată că nivelul de informare al populației despre evenimentele actuale este în creștere, de la 55% în 2018 la 63% în 2024, conform sondajelor de opinie [12]. Cu toate acestea, satisfacția față de media rămâne scăzută, peste jumătate exprimând nemulțumire, din cauza percepției de părtinire și influenței politice asupra surselor de știri. În acest context, este foarte importantă capacitatea publicului de recunoaștere a dezinformării și manipulării mediatice. Conform studiului din cadrul proiectului Media-M despre analiza percepției media în Moldova, 87-92% recunosc importanța distincției între știrile factuale și propagandă [13]. Totuși, puțini cetățeni au încredere că sursele lor de informație sunt cu adevărat independente, sondajele arată că doar 15-18% sunt siguri de obiectivitatea media, considerând că media este puternic politizată, ceea ce afectează încrederea generală [14].

Lipsa de încredere este legată și de schimbarea obiceiurilor de consum media. Conform datelor publice, televiziunea rămâne sursa principală de știri, deși utilizarea sa este în scădere pe măsură ce platformele online câștigă popularitate. Rețelele sociale, site-urile și canalele YouTube au devenit mai des folosite ca surse de informare [15]. O importantă distincție este consumul media în funcție de mediul de reședință și categoria de vârstă – tinerii și locuitorii din mediul urban preferă sursele online, în timp ce populația mai în vârstă și cea din mediul rural se bazează mai mult pe media tradițională. Utilizarea internetului ca sursă de informare, devine din ce în ce mai răspândită, populația utilizând un mix de surse online de informare, precum agregatoare de noutăți și știri prin rețelele sociale. La moment, cea mai utilizată dintre rețelele sociale este Facebook, care joacă rolul unei platforme de discuții politice. În același timp, crește rolul aplicațiilor de mesagerie, precum Telegram, WhatsApp și Viber, și a platformelor Instagram și TikTok utilizate preponderent de tineri.

O altă provocare emergentă este creșterea conținutului generat de inteligența artificială (AI) care are un impact semnificativ asupra securității informaționale, crescând riscurile de dezinformare în masa prin generarea de text, imagini și video deep-fake. Acest lucru este deosebit de periculos în contexte politice, economice și sociale, unde narativele false pot influența opinia publică și destabiliza societatea. În mai multe studii a fost notat că oamenii au o capacitate redusă de a identifica și distinge conținutul generat de AI. Studiile arată că oamenii întâmpină dificultăți în identificarea textului generat de AI. De exemplu, participanții au identificat corect textul scris de oameni în 67% din cazuri, în timp ce textul generat de AI a fost identificat incorect ca fiind uman în 54% din cazuri [16]. O altă provocare este recunoașterea imaginilor, studiile constatând că indivizii au clasificat greșit imaginile generate de AI ca fiind fotografii reale în 38.7% din cazuri [17]. Cu îmbunătățirea modelelor AI, această problemă poate deveni și mai gravă, dacă nu vor fi îmbunătățite aspectele legale și de educație ale populației.

Lipsa mecanismelor eficiente de informare a populației

Noile tehnologii au avut un impact profund asupra consumului media și a modului în care populația Republicii Moldova accesează informațiile, mai ales în contextul securității informaționale. În primul rând, cetățenii au un acces mai rapid și diversificat la informații prin platforme social media și aplicații de comunicare precum WhatsApp, Telegram (Vezi Anexa 1, Studiul de caz), Viber etc. În al doilea rând, platformele media moderne sunt însoțite de un risc mai mare de dezinformare și manipulare, iar depistarea acestora este mai provocatoare pentru că a crescut nivelul de descentralizare și anonimitate.

Așadar, persoanele fizice s-au regăsit într-o nouă postură, pe lângă consumul de date realizat prin aceste metode moderne, aceștia au devenit în consecință și utilizatori activi în distribuirea și răspândirea acestor informații. Astfel, pe lângă toate aspectele pozitive pe care le oferă soluțiile software și platformele din online, în obținerea accesului la informații, mai nou, facilitățile tehnologiilor informaționale sunt utilizate de unele grupări cu interese mai puțin legale, în vederea diseminării unor falsuri, mesaje distorsionate, transfer de imagine - care duc, în esență, la manipularea și distorsionarea opiniei publice.

Aceste provocări cel mai mult lovesc în credibilitatea față de acțiunile sau inacțiunile Statului, care de regulă pot fi compromise cu ușurință prin utilizarea acestor canale de comunicare pentru a promova conținut defăimător sau fals. În acest sens, regula generală dictează că este cu atât mai ușor să manipulezi și să diseminezi conținut denaturat cu cât este mai puțin alfabetizată digital populația.

Cu regret, constatăm că la moment, Statul nu a valorificat potențialul acestor tehnologii informaționale pentru a pune la dispoziție persoanelor fizice căi moderne de informare și comunicare, prin intermediul cărora să fie distribuite pozițiile oficiale ale autorităților publice.

Deci, la moment, lipsesc mecanisme certe prin care să poată fi distinsă o informație oficială din prima sursă de celelalte informații, care adesea sunt denaturate și trunchiate de pozițiile oficiale, inclusiv lipsește mecanismul de identificare a cazurilor de falsificare sau distorsionare a acestor comunicări, dar și eventualele măsuri de constrângere.

Mai mult ca atât, lipsesc mecanisme concrete de informare a societății în situații de criză, sau în situații specifice, care ar determina instituțiile și persoanele responsabile, perioada de reacție, periodicitate, canalele de legătură, mijloacele de comunicare și alte particularități care să permită să se mențină un dialog cu societatea și să se mențină o informare corectă și la timp.

Este necesar, în regim prioritar, să fie dezvoltate strategiile corespunzătoare privind comunicarea autorităților publice a pozițiilor oficiale și determinarea rolurilor entităților vizate, în mod special fiind creionat aportul mass-media, a formatorilor de opinie și a persoanelor cointeresate să determine conduita și trasabilitatea fluxurilor informaționale.

1.3. Constatări și concluzii privind implementarea Strategiei Securității Informaționale în Republica Moldova

Implementarea Strategiei de Securitate Informațională 2019-2024 a evidențiat progrese semnificative în consolidarea cadrului instituțional și legislativ pentru protejarea spațiului informațional al Republicii Moldova. Crearea unor structuri, precum Consiliul Coordonator pentru Asigurarea Securității Informaționale și Consiliul pentru Securitate Cibernetică a facilitat o mai bună coordonare strategică și operațională între instituțiile-cheie. De asemenea, înființarea Agenției pentru Securitate Cibernetică și dezvoltarea centrelor de reacție la incidente cibernetice (CERT Gov MD și CERT-urile departamentale) au întărit capacitatea națională de prevenire și răspuns la atacurile cibernetice. Aceste măsuri au dus la o creștere a rezilienței cibernetice, demonstrată prin gestionarea eficientă a atacurilor DDoS în timpul proceselor electorale, protejând astfel infrastructura digitală critică a statului.

Totuși, implementarea Strategiei a fost afectată de deficiențe sistemice care au limitat eficiența măsurilor adoptate. Una dintre principalele provocări a fost lipsa specialiștilor calificați în securitate informațională și cibernetică, generată de migrarea acestora către sectorul privat din cauza salariilor necompetitive din instituțiile publice. Această situație a redus capacitatea instituțiilor de a detecta și combate amenințările informaționale complexe. În plus, insuficiența resurselor financiare și tehnologice a împiedicat modernizarea infrastructurii critice și achiziționarea de echipamente necesare pentru protejarea rețelelor și datelor sensibile. Coordonarea interinstituțională a fost, de asemenea, fragmentată, ceea ce a dus la întârzieri în implementarea unor măsuri esențiale, cum ar fi operaționalizarea completă a CERT Național.

O altă provocare majoră a fost combaterea dezinformării și manipulării informaționale, mai ales în contextul alegerilor prezidențiale din 2024 și al referendumului privind aderarea la UE. Deși au fost inițiate campanii de educare și conștientizare, acestea nu au fost suficient de ample sau bine coordonate pentru a combate eficient narațiunile false și propaganda externă. Centrul pentru Comunicare Strategică și Combatere a Dezinformării reprezintă un început promițător, dar este necesară consolidarea acestuia prin alocarea de resurse adecvate și stabilirea unor parteneriate cu platformele de social media pentru identificarea și eliminarea rapidă a conținutului manipulator. Pentru a contracara aceste amenințări este esențială o strategie integrată care să includă educație media, reglementări clare pentru platformele digitale și campanii continue de informare publică.

Evaluarea implementării Strategiei de Securitate Informațională 2019-2024 subliniază necesitatea urgentă de a elabora o nouă strategie care să abordeze provocările sistemice. Aceasta trebuie să includă măsuri concrete pentru modernizarea infrastructurii, formarea specialiștilor, combaterea dezinformării și consolidarea cooperării internaționale. Doar printr-o abordare integrată și bine coordonată, Republica Moldova poate face față amenințărilor informaționale actuale și viitoare.

CAPITOLUL II: VIZIUNEA PENTRU NOUA STRATEGIE. PREZENTAREA COMPONENTELOR-CHEIE PENTRU NOUA STRATEGIE A SECURITĂȚII INFORMAȚIONALE

2.1. Prezentarea componentelor-cheie pentru noua strategie a securității informaționale

Noua Strategie de Securitate Informațională trebuie să ofere un cadru cuprinzător și integrat pentru protejarea spațiului informațional național. În contextul avansării rapide a tehnologiilor digitale, al intensificării războiului hibrid și al provocărilor geopolitice, Strategia trebuie să consolideze reziliența instituțională, informațională și socială. Noua Strategie trebuie să consolideze eforturile naționale privind combaterea dezinformării, protejarea proceselor democratice, cooperarea interinstituțională și educația informațională. În continuare, vă prezentăm o serie de priorități care trebuie să se regăsească în noua SSI.

Combaterea dezinformării și propagandei

Combaterea dezinformării trebuie să fie o prioritate pentru noua Strategie, având în vedere campaniile tot mai sofisticate care vizează destabilizarea societății și subminarea încrederii în instituțiile democratice. În acest context, menționăm rolul Centrului StratCom și de Combatere a Dezinformării în monitorizarea spațiului informațional, identificarea rapidă a narațiunilor false și elaborarea de narative eficiente. Centrul va continua să colaboreze cu instituțiile media, societatea civilă și partenerii internaționali pentru a asigura o abordare coordonată și eficientă.

Implementarea unei strategii clare de combatere a dezinformării va permite identificarea timpurie a campaniilor de manipulare și neutralizarea acestora înainte de a produce efecte negative. Creșterea transparenței și responsabilității platformelor de social media va contribui la reducerea răspândirii dezinformării.

De asemenea, implementarea campaniilor naționale de educare va ajuta cetățenii să recunoască și să evite conținutul manipulator, consolidând astfel reziliența societății.

Securizarea spațiului informațional național

Protejarea spațiului informațional național necesită implementarea unor măsuri coordonate pentru a preveni manipularea informațiilor și a asigura integritatea comunicării publice. Aceasta presupune monitorizarea continuă a platformelor de știri, a rețelelor sociale și a surselor externe, identificând și blocând încercările de a influența opinia publică prin intermediul știrilor false. Instituțiile responsabile trebuie să dezvolte sisteme eficiente pentru identificarea și analizarea amenințărilor informaționale.

Un aspect important reprezintă vulnerabilitatea mass-media (Legea presei Nr. LP243/1994 din 26.10.1994 este practic caducă), astfel, este necesară adaptarea cadrului legal național la cel al UE, precum:

Regulamentul privind libertatea mass-media,

adoptat în 2024, stabilește norme clare pentru a asigura pluralismul și independența mass-media în Uniunea Europeană. Acesta protejează instituțiile de presă împotriva interferențelor politice, economice și externe, asigurând condiții echitabile pentru jurnaliști și companii media. De asemenea, regulamentul prevede măsuri pentru transparența proprietății media și pentru alocarea echitabilă a publicității publice, consolidând astfel încrederea cetățenilor în informațiile prezentate de surse oficiale și independente [18].

Regulamentul anti SLAPP,

este o inițiativă europeană menită să combată procesele abuzive intentate împotriva jurnaliștilor, activiștilor și apărătorilor drepturilor civile pentru a-i intimida și reduce la tăcere. Această propunere oferă măsuri de protecție, inclusiv posibilitatea de a respinge rapid procesele nefondate și de a solicita despăgubiri pentru abuzul de procedură. Regulamentul promovează un mediu sigur pentru libertatea de exprimare și dezbaterea publică, prevenind utilizarea sistemului juridic pentru a suprima dreptul la informare și participare democratică [19].

Un spațiu informațional protejat va permite cetățenilor să acceseze informații corecte și echilibrate, promovând astfel o dezbatere publică sănătoasă. Cooperarea între instituțiile statului și sectorul privat va facilita schimbul de date și implementarea unor măsuri proactive de apărare. De asemenea, crearea unui cadru legal clar pentru sancționarea manipulării informaționale va contribui la descurajarea actorilor rău-intenționați.

Tehnologii noi emergente și avansarea sofisticării FIMI

În contextul geopolitic actual, manipularea și interferența informațiilor străine FIMI reprezintă o amenințare semnificativă pentru securitatea informațională și stabilitatea democratică a statelor. FIMI se referă la acțiuni deliberate întreprinse de actori străini pentru a manipula informațiile și a interfera în procesele sociale, politice și economice ale altor țări. Avansul tehnologiilor noi emergente a dus la sofisticarea fără precedent a metodelor de manipulare informațională, facilitând operațiuni complexe și greu de detectat.

Progresele în inteligența artificială au permis crearea de deepfake-uri extrem de realiste care pot fi folosite pentru a manipula opinia publică, a discredita lideri politici sau a semăna confuzie în societate. Actorii străini utilizează aceste tehnologii pentru a crea videoclipuri, imagini și înregistrări audio falsificate, distribuindu-le pe rețelele sociale pentru a influența procesele democratice, cum ar fi alegerile.

Actorii străini folosesc boți automatizați pentru a distribui masiv conținut manipulator pe rețelele sociale. Acești boți pot simula comportamentul utilizatorilor reali, creând o impresie falsă de consens public și influențând tendințele online. Campaniile coordonate de boți pot fi folosite pentru a amplifica narațiuni false și pentru a destabiliza societățile țintă.

Actorii străini dispun acum de instrumente sofisticate pentru a manipula informațiile și a interfera în procesele democratice. Pentru a răspunde acestor amenințări, Republica Moldova trebuie să adopte o strategie proactivă și integrată, care să includă tehnologii avansate de detecție, reglementări clare, prevederi privind sancționarea, inclusiv cu posibilitatea includerii interdicțiilor de a desfășura o activitate similară pentru o anumită perioadă de timp. În continuare, prezentăm unele recomandări-cheie:

RECOMANDĂRI - CHEIE

Soluții tehnologice bazate pe inteligență artificială pentru detectarea conținutului falsificat (deepfake-uri) înainte ca acesta să fie răspândit. Integrarea acestor instrumente în platformele de *social media* și în instituțiile responsabile de securitatea informațională poate preveni diseminarea conținutului manipulator.

Extinderea colaborării cu Uniunea Europeană, NATO și alte organizații internaționale pentru schimbul de bune practici și tehnologii de combatere a FIMI. Participarea la exerciții comune și la inițiative de răspuns rapid împotriva manipulării informaționale.

Elaborarea unor reglementări care să definească și să sancționeze în mod clar manipularea informațională realizată de actori străini. Aceste reglementări trebuie să includă măsuri punitive, cum ar fi amenzi, blocarea conținutului și interdicția temporară de desfășurare a activităților similare pentru cei implicați.

Impunerea obligației platformelor sociale de a identifica și elimina conturile false și campaniile coordonate de dezinformare. Obligații suplimentare pentru a asigura transparența algoritmilor de recomandare și publicarea rapoartelor periodice privind măsurile anti-FIMI.

Dezvoltarea unor programe de instruire continuă pentru personalul din instituțiile publice, în special pentru cei din domeniul securității naționale și al comunicațiilor. Acești specialiști trebuie să fie pregătiți pentru a identifica și combate amenințările FIMI.

Coordonare și reglementare social media

Social media joacă un rol tot mai important în formarea opiniei publice, diseminarea informațiilor și influențarea proceselor democratice. În contextul actual, platformele de social media sunt adesea exploatate pentru răspândirea dezinformării, propagandei și a altor forme de manipulare informațională. Noua strategie trebuie să includă o componentă dedicată social media, care să abordeze reglementarea, monitorizarea și stabilirea de parteneriate cu platformele digitale pentru securizarea spațiului informațional.

Este necesară dezvoltarea unui cadru legal clar pentru a responsabiliza platformele sociale în combaterea dezinformării și a conținutului nociv. Aceasta implică introducerea unor obligații pentru platforme de a identifica și elimina conținutul manipulator, de a transparentiza algoritmii de recomandare și de a colabora activ cu autoritățile naționale pentru investigarea campaniilor de influență. Totodată, stabilirea de memorandumuri de cooperare între Guvern și marile platforme digitale va facilita schimbul de informații și va permite reacții rapide în cazul campaniilor de dezinformare.

În Republica Moldova portalurile web la nivel național ".md" nu publică datele de identificare ale proprietarului domeniului, ceea ce duce la imposibilitatea contracarării cazurilor de defăimare, injurie, calomnie și prelucrare ilegală a datelor cu caracter personal. O recomandare de îmbunătățire a situației ar fi modificarea cadrului legal privind Legea nr. 241/2007 privind comunicațiile electronice, pentru a determina expres obligația deținătorilor portalurilor web, de a publica datele de identificare ale proprietarilor, gestionarilor acestora, deoarece la moment, aceste informații sunt mascate, iar consumatorii de informații, inclusiv persoanele care sunt calomniate, înjurate sau ale căror date sunt prelucrate ilegal, nu pot:

- Înainta acțiunea în instanța de judecată conform art. 166 din Codul de procedură civilă pentru a ataca în ordine de defăimare/calomniere și distribuirea informațiilor false;
- Autoritățile publice cu competențe de a sancționa calomnia sau prelucrarea ilegală a datelor cu caracter personal etc., NU pot identifica și responsabiliza acești deținători de portaluri, deoarece obținerea acestor informații poate fi realizată doar în ordine penală nu și în ordine contravențională.

În continuare, vă prezentăm o serie de recomandări:

Introducerea unor reglementări care să impună platformelor sociale măsuri stricte pentru eliminarea dezinformării și transparență în raportarea incidentelor. Aceste reglementări ar trebui să includă sancțiuni pentru nerespectarea obligațiilor.

Crearea unor parteneriate între instituțiile guvernamentale și platformele sociale pentru a facilita identificarea și combaterea campaniilor de influență. Colaborarea cu echipele de moderare ale platformelor poate accelera procesul de eliminare a conținutului fals și a conturilor implicate în manipulare.

Solicitarea platformelor să ofere transparență cu privire la algoritmii de recomandare și modul în care aceștia pot fi folosiți pentru amplificarea dezinformării. Înțelegerea acestor mecanisme va permite autorităților să dezvolte contramăsuri eficiente.

Implementarea unor campanii de conștientizare și educație care să-i învețe pe cetățeni să recunoască manipularea informațională pe social media. Aceste campanii pot include ghiduri de identificare a știrilor false și tehnici de verificare a surselor.

Protejarea proceselor electorale și democratice

În contextul alegerilor prezidențiale și al referendumurilor, protejarea proceselor democratice devine esențială. Noua Strategie trebuie să includă măsuri specifice pentru detectarea și combaterea dezinformării în timpul campaniilor electorale. Aceasta presupune colaborarea între Comisia Electorală Centrală, instituțiile de securitate și societatea civilă pentru a monitoriza spațiul informațional și a identifica narațiunile false care vizează candidații și instituțiile democratice.

Implementarea unor mecanisme de alertă timpurie va permite reacții rapide în fața tentativelor de manipulare a opiniei publice. De asemenea, instituțiile trebuie să comunice transparent cu cetățenii pentru a combate zvonurile și pentru a asigura încrederea în procesul electoral. Educația privind alfabetizarea media și gândirea critică va contribui la consolidarea încrederii cetățenilor în alegeri și în instituțiile democratice.

Educație și conștientizare informațională

Educația în domeniul securității informaționale este fundamentală pentru creșterea rezilienței societății. Noua Strategie trebuie să promoveze programe de alfabetizare media și educație digitală în școli, universități și în rândul populației generale. Aceste programe vor dezvolta abilități critice de analiză a informațiilor și vor ajuta cetățenii să identifice știrile false și manipularea informațională.

Campaniile naționale de conștientizare trebuie să fie accesibile și adaptate diferitelor segmente ale populației. Promovarea unor mesaje clare și exemple practice de recunoaștere a dezinformării vor contribui la o societate mai informată și mai rezilientă.

Implicarea instituțiilor de stat, a societății civile și a mediului privat în aceste campanii va asigura o acoperire largă și eficiență sporită.

Colaborare interinstituțională pentru securitatea informațională

Coordonarea eficientă între instituțiile responsabile este esențială pentru implementarea unei strategii de succes. Noua Strategie trebuie să stabilească mecanisme clare de cooperare și schimb de informații între SIS, MAI, Procuratura Generală, Consiliul Audiovizualului și alte entități relevante. Crearea unui Comitet interinstituțional permanent pentru securitatea informațională va facilita luarea rapidă a deciziilor și implementarea măsurilor necesare.

Lipsa unei coordonări eficiente a fost o problemă sistemică în implementarea strategiei anterioare. Prin îmbunătățirea colaborării și stabilirea unor responsabilități clare, instituțiile vor putea reacționa prompt și coerent la amenințările informaționale. Platformele comune de raportare și analiza incidentelor vor contribui la o mai bună gestionare a crizelor și la eliminarea redundanțelor.

Protecția datelor și confidențialitatea informațiilor

Protejarea datelor cu caracter personal este un pilon esențial al securității informaționale. Noua Strategie trebuie să includă măsuri stricte pentru asigurarea confidențialității datelor în sectorul public și privat. Aceasta presupune adoptarea de standarde internaționale de protecție a datelor, audituri periodice și sancțiuni clare pentru încălcarea legislației în domeniu.

Implementarea unor mecanisme eficiente de raportare și gestionare a incidentelor va reduce riscul de scurgeri de date și va consolida încrederea cetățenilor. O cooperare strânsă între Centrul Național pentru Protecția Datelor cu Caracter Personal și instituțiile publice va facilita aplicarea unitară a legislației și va asigura respectarea drepturilor fundamentale ale cetățenilor.

Gestionarea crizelor informaționale

Noua Strategie trebuie să includă un plan național de răspuns la crize informaționale, care să detalieze scenarii de intervenție și responsabilități clare pentru fiecare instituție implicată. Acest plan va permite gestionarea rapidă a situațiilor de urgență și va asigura o comunicare eficientă cu publicul în momente critice.

Implementarea unor exerciții de simulare a crizelor va pregăti instituțiile pentru scenarii reale și va identifica vulnerabilitățile procesului de comunicare. Un răspuns coordonat și transparent în timpul crizelor informaționale va reduce impactul negativ al dezinformării și va consolida încrederea populației în autorități.

2.2. Asigurarea securității informaționale din perspectiva drepturilor fundamentale ale persoanei

Reieșind din situația de nesiguranță creată la hotarele Republicii Moldova, în ultimii 2 ani, autoritățile publice au venit cu mai multe inițiative în vederea modificării cadrului legal, pentru a fortifica activitatea instituțiilor responsabile de securitatea statului și ale altor instituții din domeniul polițienesc, dar și din domeniul administrativ.

Astfel, efortul de bază a fost îndreptat spre crearea cadrului legal necesar pentru a permite instituțiilor responsabile de a utiliza metode moderne de colectare, stocare, utilizare a informațiilor, pentru a realiza eficient și echidistant obiectivele urmărite, inclusiv pentru a valorifica procedeele și mijloacele noi din punct de vedere a tehnologiilor informaționale. Mai mult, alinierea cadrului legal a fost necesară și din perspectiva digitalizării resurselor informaționale de stat și a platformei de schimb de date Mconnect.

Aşadar, printre cele mai intruzive proiecte de lege în raport cu dreptul la viața privată în legătură cu prelucrarea datelor cu caracter personal, pot fi menționate următoarele:

Legea nr. 59/2012 privind activitatea specială de investigație: principalele modificări s-au referit la realizarea măsurilor speciale de investigație în afara urmăririi penale, specificarea unor noi măsuri speciale de investigații, modificarea modului de dispunere a măsurilor speciale de investigație și reducerea nivelului de autorizare pentru unele dintre aceste activități;

Legea nr. 179/2023 privind activitatea contrainformativă și activitatea informativă externă: a investit Serviciul de Informații și Securitate cu competențe noi, care au lărgit esențial arealul de dispoziție, dar și a activitățile specifice de investigare, au fost determinate noi procedee de investigare, colectare, stocare și utilizare a informațiilor;

Legea nr. 619/1995 privind organele securității statului: Centrul Național Anticorupție a fost investit, inclusiv în calitate de autoritate publică, cu atribuții de asigurare a securității statului;

Totodată, ca o contrabalanță în raport cu fortificarea măsurilor intruzive admise prin lege către autoritățile publice responsabile de asigurarea ordinii publice, a securității statului și a altor activități administrative, precum și asigurarea unui control eficient din partea societății civile, dar și a cetățeanului, au fost elaborate 2 legi noi:

Legea nr. 148/2023 privind accesul la informațiile de interes public: chiar dacă elaborarea noului cadru legal a fost argumentat ca fiind o necesitate de a întări dreptul de acces la informațiile de interes public, pentru a responsabiliza autoritățile publice în oferirea unui acces mai lărgit și mai calitativ la date, precum creșterea numărului de furnizori de informații, determinarea obligației de a publica din oficiu (proactiv) anumite informații de interes public, restrângerea termenului de examinare a cererilor de acces la informație, reducerea cerințelor pentru aspectele de formă și procedură privind cererile de acces la informație. Într-un final, prevederile art. 8 alin. (2) din această lege, au invalidat în totalitate efortul reflectat pentru anumite categorii de informații, prin determinarea expresă că accesul la informațiile atribuite la secret de stat este limitat, ceea ce presupune că odată ce informațiile au fost secretizate, indiferent de faptul dacă se referă la informații de interes public sau de interes personal (datele cu caracter personal), accesul la aceste informații nu este permis. Mai mult, prevederile acestei legi nu determină o perioadă limită de restricționare a accesului, modalitatea de contestare și autoritățile responsabile, inclusiv generează situații de incertitudine și riscuri pentru libertatea de exprimare și, în special, pentru activitatea jurnaliștilor de investigație, dar și a surselor de informații jurnalistice, or, prevederile acestei legi, nu oferă nici o posibilitate legală de a determina cazurile în care datele atribuite la secret de stat să poată fi publicate spre acces public nerestricționat.

Legea nr. 195/2024 privind protecția datelor cu caracter personal: deși această lege a avut obiectivul de a alinia cadrul legal național la cel european, în special transpunerea REGULAMENTULUI (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 și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), potrivit căruia, persoanele fizice să dispună de mai multe drepturi și de un control efectiv asupra propriilor date cu caracter personal, și în cazul acestei legi, care reprezintă unul dintre principalele instrumente ale cetățeanului de a contracara/combate eventualele abuzuri în privința dreptului fundamental la viața privată din partea autorităților și instituțiilor publice, conform art. 2 alin. (2) lit. a) din această lege, activitățile atribuite la secret de stat, au fost excluse în totalitate de la regimul juridic al acestei legi.

Așadar, prin includerea acestor prevederi în Legea nr. 195/2024, aceasta în loc să ridice gradul de protecție al persoanei în ceea ce privește operațiunile de prelucrare a datelor cu caracter personal efectuate de către autoritățile și instituțiile publice care au dreptul de a atribui informația la secret de stat, această lege a regresat, oferind un nivel de protecție mai jos decât cel prevăzut de Legea nr.133/2011 privind protecția datelor cu caracter personal. Mai mult, aceste derogări sunt nejustificate și contrare prevederilor art. 23 din GDPR, dar și art. 11 din Convenția nr. 108 modernizată pentru protecția persoanelor față de prelucrarea datelor cu caracter personal, care determină expres că nu se permite nici o excepție de la prevederile acestui Capitol, cu excepția prevederilor articolului 5 alin. (4), art. 7 alin. (2), art. 8 alin. (1) și art. 9, în cazul în care o astfel de excepție este prevăzută de lege, respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică. Mai simplu spus, este contrar Convenției excluderea în totalitate de la cadrul legal privind protecția datelor a oricăror operațiuni de prelucrare a datelor, inclusiv cele atribuite la secret de stat, totodată, Convenția permițând

pentru cazurile de protecție a securității naționale de a se stabili în cadrul legal național, derogări specifice și limitative, în conformitate cu limitele prevăzute de Convenție.

O altă interferență nejustificată, reprezintă și derogările prevăzute la art. 2 alin. (2) lit. c) din Legea nr. 195/2024, conform cărora, regimul juridic de protecție prevăzut de această lege nu se aplică autorităților competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor ori al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. Aceste derogări au fost justificate de către Ministerul Justiției prin faptul că aceste prelucrări de date vor face obiectul de reglementare al unei noi legi opozabile exclusiv instituțiilor de aplicare a legii din sectorul polițienesc, lege, care va transpune prevederile DIRECTIVEI (UE) 2016/680 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului. Cu părere de rău, la moment, nu există un proiect de lege similar celui reflectat de Ministerul Justiției.

Un declin evident în ceea ce privește asigurarea drepturilor fundamentale la viața privată, rezultă din informațiile oficiale prezentate în raportul de activitate al Centrului Național pentru Protecția Datelor cu Caracter Personal pentru anul 2023 , în care au fost prezentate informațiile comparative pentru anii 2021 – 2023 prin accesările efectuate de unele autorități publice prin intermediul SIA ,,Acces-Web" și COI (Common Object Interfaces) și pentru anul 2022 – 2023, prin intermediul platformei de interoperabilitate (Mconnect).

Conform acestor date, relevăm o îngrijorare majoră cu privire la conformitatea utilizării informațiilor cu caracter personal în scopurile polițienești, de asigurare a securității statului și scopurilor administrative, or, la o populație de circa 2,4 milioane (conform informațiilor oficiale prezentate de Biroul Național de Statistică), autoritățile statului au efectuat zeci de milioane de accesări. Mai mult ca atât, vedem o creștere exponențială a numărului de accesări de date:

- **Ministerul Afacerilor Interne, de la 13 milioane de accesări în 2021, la 26 milioane de accesări în 2023 prin intermediul SIA ,,Acces-Web" și COI și + 3 milioane prin Mconnect, în total aproximativ 29 milioane, ceea ce înseamnă că aproximativ de 12 ori mai mult a fost verificat fiecare locuitor al Republicii Moldova;**
- **Serviciul Fiscal de Stat, de la 3 milioane de accesări în 2021, la 9 milioane de accesări în 2023 prin intermediul SIA ,,Acces-Web" și COI și + 15 milioane prin Mconnect, în total circa 24 milioane de accesări, asta ar însemna verificarea fiecărui locuitor al Republicii Moldova de circa 10 ori mai mult.**
- **În cazul Serviciului de Informații și Securitate, Centrului Național Anticorupție, Serviciul Vamal, Ministerul Apărării, observăm niște cifre mult mai modeste, totodată constatându-se fie o creștere neesențială, fie menținerea aproximativă a aceluiași număr de accesări. Singura instituție care a demonstrat o scădere clară a numărului de accesări este Procuratura Generală, instituție care și așa nu era prea mult vizată de cazuri de încălcare a dreptului la viața privată.**

2.3 Bune practici la nivelul UE care pot fi implementate la nivel național

În contextul actual al intensificării amenințărilor informaționale și al manipulării coordonate din surse externe, Uniunea Europeană a dezvoltat o serie de bune practici și strategii eficiente pentru a proteja spațiul informațional și a consolida reziliența societății. Aceste măsuri includ tehnologii avansate de detecție a dezinformării, reglementări clare pentru combaterea manipulării informaționale, colaborări internaționale și inițiative educaționale pentru alfabetizarea media. Implementarea acestor bune practici la nivel național poate oferi Republicii Moldova instrumentele necesare pentru a face față provocărilor tot mai complexe din domeniul securității informaționale, protejând astfel democrația, instituțiile și cetățenii împotriva interferențelor externe și a campaniilor de dezinformare.

Pachetul de măsuri privind Spațiul Digital (Digital Services Act și Digital Markets Act, 2022)

Elemente-cheie:

- Responsabilizarea platformelor mari de social media. Obligația platformelor de a elimina rapid conținutul ilegal și dezinformarea și de a oferi transparență privind algoritmii.
- Măsuri pentru protejarea utilizatorilor de conținut înșelător și practici comerciale neloiale.
- Platformele trebuie să ofere rapoarte periodice privind acțiunile de combatere a dezinformării și să fie supuse unor audituri independente.

Planul de Acțiune împotriva Dezinformării (2018, Actualizat 2021)

Elemente-cheie:

- Sistemul Rapid de Alertă (Rapid Alert System - RAS). Un mecanism pentru schimbul rapid de informații între statele membre și instituțiile UE privind campaniile de dezinformare în timp real.
- Codul de Conduită privind Dezinformarea. Colaborarea cu platformele online pentru eliminarea conținutului fals și a conturilor false, promovând transparență și responsabilitate.
- Crearea echipelor specializate (East StratCom Task Force): monitorizarea și expunerea narațiunilor de dezinformare, cu accent pe propaganda rusă în Europa de Est.

Combaterea dezinformării și a manipulării și interferențelor cu informații străine [20]

În cadrul Planului de acțiuni pentru democrație europeană, UE și-a intensificat eforturile de a răspunde acestui peisaj de amenințări în evoluție atât pe plan intern, cât și internațional. Aceasta se bazează pe activitatea existentă a UE și este ferm înrădăcinată în valorile și principiile europene. Protejează libertatea de exprimare și dreptul oamenilor de a accesa conținut legal.

Acțiunile-cheie în acest domeniu includ:

- cooperarea consolidată, bazându-se pe rețelele existente pentru a coordona acțiunile UE ca răspuns la valul tot mai mare de campanii de dezinformare;
- un set de instrumente consolidate al UE pentru a contracara manipularea și interferența informațiilor străine (FIMI) [21];
- asigurarea unei mai mari responsabilități a platformelor online pentru a preveni răspândirea dezinformării printr-un cod de practici consolidat privind dezinformarea, stabilirea unui cadru de coreglementare, în conformitate cu Legea privind serviciile digitale.

Asigurarea unei mai mari responsabilități a platformelor online

Ca urmare a orientărilor adoptate de Comisie în 2021, cu privire la modul de consolidare al Codului existent de practică al UE privind dezinformarea [22], în iunie 2022 a fost semnat un nou Cod, care reunește atât platformele online majore, cât și cele specializate, industria publicității online, cercetarea și societatea civilă, precum și verificatorii de fapte. Codul stabilește o gamă largă de angajamente, de la demonetizare la transparență și la accesul de date. Important, Codul vine cu un cadru solid de monitorizare și un Centru de transparență pentru a asigura o transparență și responsabilitate sporite.

De asemenea, stabilește un cadru de coreglementare în conformitate cu Digital Services Act (DSA) [23], care obligă platformele online foarte mari și motoarele de căutare să evalueze în mod regulat riscurile sistemice pe care serviciile lor le pot prezenta pentru societate, inclusiv riscul ca serviciile lor să fie utilizate abuziv ca un instrument pentru campanii de dezinformare.

CONCLUZII

Implementarea Strategiei de Securitate Informațională 2019-2024 a adus progrese importante în consolidarea cadrului legislativ și instituțional al Republicii Moldova, însă persistă provocări semnificative. Crearea unor entități, precum CERT Gov MD, adoptarea Legii nr. 48/2023 privind securitatea cibernetică și dezvoltarea structurilor de reacție cibernetică, reprezintă pași valoroși pentru securizarea spațiului informațional. Implementarea Strategiei Securității Informaționale a determinat reducerea semnificativă a vulnerabilităților în infrastructura critică și a numărului de atacuri cibernetice asupra instituțiilor de stat, îmbunătățirea gradului de conștientizare al populației cu privire la amenințările cibernetice și manipulările informaționale și a creat un sistem integrat de securitate informațională care poate răspunde provocărilor emergente. Totuși, lipsa specialiștilor calificați, infrastructura învechită, coordonarea deficitară între instituții și resursele financiare insuficiente au limitat eficiența strategiei. În contextul amenințărilor hibride și al avansării tehnologice, este necesară o abordare mult mai integrată și flexibilă pentru a proteja procesele democratice și stabilitatea socială.

Unul dintre obstacolele majore întâmpinate a fost deficitul de resurse umane calificate în domeniul securității informaționale și cibernetice. Lipsa specialiștilor a dus la o capacitate redusă de a identifica și răspunde prompt la atacurile informaționale și cibernetice. Exodul de talente către sectorul privat, în condițiile unor salarii necompetitive în sectorul public, a agravat această situație. De asemenea, infrastructura tehnologică învechită a limitat capacitatea instituțiilor de a dezvolta soluții eficiente pentru detectarea și prevenirea dezinformării și a interferențelor străine.

În plus, coordonarea deficitară între instituțiile responsabile a afectat implementarea unitară a strategiei. Deși există entități precum SIS, MAI, Procuratura Generală și Consiliul Audiovizualului, lipsa unui mecanism centralizat de comunicare și colaborare a dus la întârzieri în reacție și la duplicarea eforturilor. Această fragmentare a redus eficiența răspunsului național la campaniile de manipulare informațională și la atacurile hibride. Este esențială o mai bună clarificare a responsabilităților și o structură de cooperare interinstituțională bine definită pentru a asigura o protecție coerentă a spațiului informațional.

De asemenea, dezinformarea și manipularea informațională rămân amenințări constante, în special în perioade electorale și în contextul geopolitic actual. Actorii străini utilizează tehnologii avansate, cum ar fi inteligența artificială pentru crearea de deep fake-uri și boți automatizați pentru amplificarea narațiunilor false. Strategia a evidențiat aceste riscuri, însă măsurile pentru combaterea lor au fost insuficient implementate. Lipsa unor parteneriate solide cu platformele de social media și a unor mecanisme rapide de detectare și eliminare a conținutului fals a permis perpetuarea acestor amenințări.

Amenințările hibride, cum ar fi dezinformarea, atacurile cibernetice și influențele politice externe, reprezintă riscuri majore pentru Republica Moldova. Comunicarea strategică este vitală pentru monitorizarea mediului informațional, crearea unei narațiuni naționale pozitive și educarea publicului. Este necesară dezvoltraea capacităților de detectarea timpurie a manipulărilor informaționale, crearea unor campanii naționale educaționale pentru reziliența societală de către institutiile statului; dezvoltarea colaborării intersectoriale între guvern, societatea civilă și mass-media. Comunicarea strategică în Republica Moldova este încă în fază incipientă, cu progrese realizate în ultimii ani. Crearea unor structuri precum Centrul pentru Comunicare Strategică și Combaterea Dezinformării (2023) reprezintă pași importanți, însă insuficienți pentru o abordare sistemică și integrată. Provocări identificate precum lipsa unui cadru centralizat și a unei coordonări interinstituționale,resurse umane și financiare limitate, absența unei narațiuni naționale coerente care să unifice mesajele, instruire insuficientă a personalului implicat în comunicarea strategică, necesită existența unei mentalitatii comune de comunicare strategica și o voință politică puternică pentru institutionalizarea acesteia la toate nivelele.

RECOMANDĂRI

Pentru a răspunde acestor provocări, se recomandă modernizarea infrastructurii tehnologice. Aceasta se poate realiza prin investiții în echipamente și software avansate pentru detectarea și prevenirea atacurilor cibernetice. Totodată, formarea și retenția specialiștilor trebuie să fie o prioritate pentru instituțiile guvernamentale. Ministerul Educației și Cercetării ar trebui să introducă programe educaționale de securitate cibernetică în curriculumul școlar și universitar, iar Guvernul trebuie să ofere salarii competitive pentru specialiștii din sectorul public.

În domeniul combaterii dezinformării și propagandei, Centrul pentru Comunicare Strategică și Combatere a Dezinformării trebuie să joace un rol central. Acest Centru ar trebui să colaboreze activ cu platformele de social media pentru a identifica rapid și elimina conținutul manipulator. Se recomandă stabilirea de parteneriate între SIS și platformele digitale pentru a asigura transparența algoritmilor și pentru a monitoriza mai eficient narațiunile false. De asemenea, societatea civilă trebuie implicată în campanii de educație media și alfabetizare digitală, oferind cetățenilor instrumentele necesare pentru a recunoaște și respinge dezinformarea.

Pentru o coordonare eficientă, propunem coordonarea schimbului de informații și răspunsul la incidente în timp real. În ceea ce privește cooperarea internațională, Guvernul Republicii Moldova trebuie să consolideze parteneriatele cu UE și NATO pentru a beneficia de expertiză și resurse în domeniul securității informaționale. Implementarea bunelor practici europene, precum Regulamentul privind libertatea mass-media și inițiativele anti-SLAPP, poate contribui la protejarea presei independente și a dreptului la informare.

În continuare, propunem o serie de recomandări pentru a asigura securitatea spațiului informațional:

1 **OPERAȚIONALIZAREA CONSILIULUI COORDONATOR AL SECURITĂȚII INFORMAȚIONALE:**

Consiliul trebuie să funcționeze ca un organism central pentru schimbul rapid de informații și luarea deciziilor strategice. Consiliul are rolul de a elabora și implementa politici unitare, de a asigura monitorizarea constantă a spațiului informațional și de a coordona răspunsul în situații de criză. Prin întâlniri regulate, simulări și rapoarte de progres, acest consiliu ar facilita o reacție promptă și eficientă la amenințările hibride și dezinformare, evitând astfel duplicarea eforturilor și asigurând o viziune coerentă și integrată la nivel național. Recomandăm utilizarea platformei Consiliului Coordonator și crearea activităților proactive.

2 DEZVOLTAREA COMPETENȚELOR SPECIALIȘTILOR ÎN DOMENIUL SECURITĂȚII INFORMAȚIONALE ȘI CIBERNETICE

este esențială pentru a face față provocărilor tot mai sofisticate din spațiul digital. Instituții, precum Ministerul Educației și Cercetării și Ministerul Dezvoltării Economice și Digitalizării trebuie să colaboreze pentru a introduce programe educaționale specializate în securitate cibernetică în școli, universități și centre de formare profesională. De asemenea, este necesar să se ofere training-uri continue și certificări internaționale pentru personalul din instituțiile publice și private. Oferirea de stimulente financiare și oportunități de carieră atractive în sectorul public poate contribui la retenția specialiștilor și la reducerea exodului de talente. Parteneriatele cu organizații internaționale și schimburile de experiență pot ajuta la creșterea nivelului de pregătire și la aplicarea celor mai bune practici internaționale.

3 SINCRONIZAREA ACTIVITĂȚILOR DINTRE AUTORITĂȚILE PUBLICE ȘI SECTORUL PRIVAT

Pentru o securitate informațională eficientă, este necesară sincronizarea activităților dintre autoritățile publice și sectorul privat. Instituțiile statului, operatorii de infrastructură critică și companiile din domeniul IT trebuie să colaboreze prin crearea unor platforme comune de schimb de informații și bune practici. Această colaborare poate include partajarea de date despre amenințări, desfășurarea de exerciții comune de simulare a atacurilor cibernetice și dezvoltarea unor protocoale standardizate de răspuns la incidente. La nivel internațional, Republica Moldova trebuie să intensifice cooperarea cu organizații, precum UE, NATO, INTERPOL și țările partenere pentru a beneficia de resurse, instruire și expertiză. Această abordare va facilita reacții coordonate în fața atacurilor hibride și va întări reziliența națională în fața amenințărilor transfrontaliere.

4 INSTITUȚIILE NAȚIONALE, PRECUM SIS ȘI CONSILIUL AUDIOVIZUALULUI, SĂ STABILEASCĂ PARTENERIATE ACTIVE CU PLATFORMELE DIGITALE

Dezinformarea răspândită pe platformele de socializare reprezintă una dintre principalele amenințări la adresa securității informaționale. Este imperativ ca instituțiile naționale, precum SIS și Consiliul Audiovizualului, să stabilească parteneriate active cu platformele digitale (Facebook, Twitter, YouTube, TikTok) pentru a identifica și elimina rapid conținutul manipulator. Aceste colaborări ar trebui să includă crearea unor mecanisme de raportare rapidă, partajarea datelor privind sursele de dezinformare și implementarea de algoritmi care să detecteze automat conținutul fals. De asemenea, este necesară promovarea transparenței algoritmilor de recomandare și impunerea unor obligații de responsabilitate pentru platformele sociale. Educația publicului despre recunoașterea dezinformării trebuie să completeze aceste eforturi, pentru a construi o reziliență pe termen lung în fața manipulării informaționale.

5 EVALUAREA CONTINUĂ A RISCURILOR ȘI AMENINȚĂRILOR DIN SPAȚIUL INFORMAȚIONAL

Evaluarea continuă a riscurilor și amenințărilor din spațiul informațional este esențială pentru anticiparea și prevenirea atacurilor. Instituții, precum SIS, MAI și CERT Gov MD, trebuie să dezvolte un sistem integrat de monitorizare și analiză în timp real a spațiului informațional. Acest sistem ar trebui să includă tehnologii avansate de inteligență artificială pentru detectarea tendințelor și identificarea rapidă a campaniilor de manipulare. Rapoartele periodice de evaluare a riscurilor trebuie să fie comunicate către factorii de decizie și către publicul larg pentru a asigura transparență și informare corectă. În plus, organizarea de exerciții de simulare a incidentelor poate ajuta la testarea capacității de răspuns și la identificarea vulnerabilităților existente.

6 ADAPTAREA CADRULUI NORMATIV LA NOILE REALITĂȚI TEHNOLOGICE ȘI LA DINAMICA DE SECURITATE REGIONALĂ

Adaptarea cadrului normativ la noile realități tehnologice și la dinamica de securitate regională este esențială pentru protejarea eficientă a spațiului informațional. Instituțiile legislative și de reglementare, precum Parlamentul, SIS și Ministerul Justiției, trebuie să efectueze evaluări periodice ale legislației existente pentru a identifica lacunele și pentru a actualiza reglementările în funcție de noile amenințări, inclusiv cele generate de inteligența artificială și platformele de social media. Este necesară introducerea unor prevederi clare pentru responsabilizarea platformelor digitale, reglementarea deep fake-urilor și combaterea campaniilor de manipulare coordonată. De asemenea, armonizarea legislației naționale cu reglementările europene, precum Regulamentul privind libertatea mass-media și Directiva anti-SLAPP, va consolida protecția spațiului informațional și va sprijini integrarea Moldovei în structurile europene de securitate.

7 CREAREA UNUI CADRU NAȚIONAL CENTRALIZAT PENTRU COMUNICAREA STRATEGICA

Crearea unui cadru național centralizat pentru comunicarea strategica cu roluri și responsabilități clar definite pentru toate instituțiile implicate. Aceasta include transformarea structurilor actuale din fiecare minister sau instituție într-o unitate StratCom standardizată, bazată pe o structură comună cu functii de planificare și evaluare a mediului informațional.

8 CONSOLIDAREA EDUCAȚIEI MEDIA ȘI A ALFABETIZĂRII DIGITALE

Consolidarea educației media și a alfabetizării digitale, se recomandă continuarea eforturilor pentru creșterea competențelor media ale cetățenilor, în special pentru identificarea dezinformării și manipulării media. Parteneriatele cu ONG-uri, organizații media și instituții de învățământ ar putea susține campanii de conștientizare și programe de educație media, vizând atât tinerii, cât și persoanele în vârstă.

9 ÎMBUNĂTĂȚIREA SIGURANȚEI ONLINE

Îmbunătățirea siguranței online, având în vedere riscurile asociate rețelelor sociale, inițiativele de educație publică ar trebui să abordeze modul de identificare și evitare a dezinformării și a conținutului manipulator. Promovarea canalelor oficiale și a surselor verificate de informații pe rețelele sociale.

10 ÎMBUNĂTĂȚIREA LEGISLAȚIEI ȘI A REGLEMENTĂRILOR ÎN DOMENIUL SOCIAL MEDIA ȘI INTELIGENȚĂ ARTIFICIALĂ

Îmbunătățirea legislației și a reglementărilor în domeniul social media și inteligență artificială. Deși legislația națională este bine dezvoltată în domeniul media tradiționale, în Moldova lipsesc instrumente clare de monitorizare și intervenție în canale de comunicare online. De asemenea, este nevoie de nevoie de reglementări care să impună etichetarea clară a conținutului generat de AI, în special în publicitate și știri, pentru a permite utilizatorilor să recunoască imediat conținutul artificial. Un rol important în acest sens este ajustarea la standardele UE din domeniu media, digital și AI.

11 IMPLEMENTAREA PROGRAMELOR DE ALFABETIZARE MEDIA LA NIVEL NAȚIONAL

Implementarea programelor de alfabetizare media la nivel național, asigurând o acoperire completă și unitară. Organizarea de campanii educaționale menite să sporească reziliența cetățenilor, axate pe dezvoltarea competențelor de alfabetizare digitală și încurajarea implicării active a societății civile.

12 ORGANIZAREA CAMPANIILOR DE CONȘTIENTIZARE PUBLICĂ, PRIN CARE SĂ SE EXPLICE RISCURILE ȘI SEMNELE CONȚINUTULUI GENERAT DE AI

Organizarea campaniilor de conștientizare publică, prin care să se explice riscurile și semnele conținutului generat de AI, poate ajuta la educarea publicului. Acestea pot include tutoriale, ghiduri vizuale și sesiuni interactive pentru a demonstra cum se identifică conținutul fals. De asemenea, se recomandă instruirea diferitor grupuri de cetățeni în folosirea instrumentelor de detectare AI, precum Originality.AI.

13 NECESITĂȚI PENTRU A CREȘTE GRADUL DE SIGURANȚĂ AL PERSOANELOR ÎN CONFORMITATE CU ACȚIUNILE INSTITUȚIILOR STATULUI

1. Modificarea art. 8 alin. (1) și abrogarea alin. (2) din Legea nr. 148/2023 privind accesul la informațiile de interes public, pentru a determina clar limitele restricționării accesului la informațiile de interes public care au fost atribuite la secret de stat, mai ales atunci când sunt comise încălcări, abuzuri, accesări ilegale, pentru a se păstra un control efectiv din partea societății civile, a jurnaliștilor și a simplului cetățean;
2. Abrogarea art. 2 lit. a) din Legea nr. 195/2024 privind protecția datelor cu caracter personal, cu includerea unor prevederi specifice, în corespundere cu restrângerile stabilite la art. 23 din aceeași lege, pentru a determina derogări și excepții adecvate și proporționale activității organelor din domeniul asigurării securității naționale, în corespundere cu cerințele Convenției modernizate pentru protecția persoanelor față de prelucrarea datelor cu caracter personal dar și a cadrului legal;
3. Elaborarea unei noi legi prin care să fie transpusă DIRECTIVA (UE) 2016/680 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;
4. Determinarea unor criterii specifice de raportare pentru organele responsabile de asigurarea securității statului, dar și a altor autorități publice, inclusiv criteriile de verificare și control ale organelor de supraveghere, precum Comisia securitate națională, apărare și ordine publică și Comisia drepturile omului și relații interetnice, Avocatul Poporului și Centrul Național pentru Protecția Datelor cu Caracter Personal, Procuratura Generală;
5. Includerea unui mecanism cert cu privire la reflectarea în Mcabinet a operațiunilor de prelucrare a datelor cu caracter personal efectuate de către autoritățile publice din sectorul polițienesc și a securității statului, deoarece la moment, astfel de informații nu se afișează ,,numquam”.

BIBLIOGRAFIE

[1] Hotărârea Guvernului RM nr, 467 din 06 iulie 2022 cu privire la crearea Consiliului coordonator pentru asigurarea securității informaționale. https://gov.md/sites/default/files/document/attachments/subiect-11-nu-259-mei-2020.pdf
[2] Hotărârii Guvernului nr. 333/2024 cu privire la instituirea, organizarea și funcționarea, Consiliului coordonator în domeniul securității cibernetice. https://www.legis.md/cautare/getResults?doc_id=143430&lang=ro
[3] Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică. https://cancelaria.gov.md/sites/default/files/document/attachments/nu-856-mded-2023.pdf
[4] Legea nr. 48/2023 privind securitatea cibernetică. https://www.legis.md/cautare/getResults?doc_id=136732&lang=ro
[5] Agenția de Guvernare Electronic - responsabilă pentru implementarea politicilor în domeniile de modernizare a serviciilor guvernamentale, și transformarea digitală a guvernării, gestionează platforma și servicii electronice guvernamentale (MConnect, MPass, MSign, MPay etc). De asemenea, AGE are și responsabilități ce țin de asigurarea securității informației în autoritățile și instituțiile din sectorul public în procesul de e-Transformare a guvernării.
[6] Incident de securitate cibernetică remediat de STISC. https://stisc.gov.md/ro/comunicate-de-presa/incident-de-securitate-cibernetica-remediat-de-stisc
[7] L E G E privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și modificarea unor acte normative
[8] Directivă NIS (Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune) și are drept scop creșterea nivelului de pregătire a statelor UE pentru a face față la incidentele de securitate informatică și respectiv creșterea gradului de încredere a cetățenilor în Piața Digitală Unică;
Directiva NIS2 este legislația la nivelul UE privind securitatea cibernetică. Acesta prevede măsuri juridice pentru a stimula nivelul general de securitate cibernetică în UE.
[9] Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice. https://gov.md/sites/default/files/document/attachments/nu-104-mai-2023_0.pdf
[10] Misiunea de parteneriat a UE în Republica Moldova (EUPM Moldova). https://eur-lex.europa.eu/RO/legal-content/summary/eu-partnership-mission-in-moldova-eupm-moldova.html
[11] Alegerile și Referendumul din Republica Moldova, Considerate Eficiente și Competitive de către Observatorii Internaționali, în Ciuda Tentativelor de Subminare a Integrității. https://www.oscepa.org/en/documents/election-observation/election-observation-statements/moldova/press-releases-16/5096-2024-presidential-rom/file
[12] Date compilate din Barometrul de Opinie Publica 2020-2024
[13] Media-M Project (2022) Assessment of Public Perception of Media and Media Skills in the Republic of Moldova. https://internews.md/wp-content/uploads/2023/08/Report_In-depth-analysis-of-the-3-surveys-to-evaluate-media-perceptions-and-skills-among-Moldovan-citizens_ENG_final.pdf
[14] Media-M Project (2022) Assessment of Public Perception of Media and Media Skills in the Republic of Moldova. https://internews.md/wp-content/uploads/2023/08/Report_In-depth-analysis-of-the-3-surveys-to-evaluate-media-perceptions-and-skills-among-Moldovan-citizens_ENG_final.pdf
[15] International Republic Institute (2024) National Poll of Moldova, May-June 2024
[16] Debora Weber-Wulff et.al. (2023) Testing of Detection Tools for AI-Generated Text. https://doi.org/10.48550/arXiv.2306.15666
[17] Zeyu Lu et.al. (2023) Seeing is not always believing: Benchmarking Human and Model Perception of AI-Generated Images. https://doi.org/10.48550/arXiv.2304.13023
[18] Regulamentul (UE) 2024/1083 al Parlamentului European și al Consiliului din 11 aprilie 2024 de stabilire a unui cadru comun pentru serviciile mass-media în cadrul pieței interne și de modificare a Directivei 2010/13/UE (Regulamentul european privind libertatea mass-mediei). https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32024R1083
[19] Propunere de DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI privind protecția persoanelor implicate în acțiuni de mobilizare publică împotriva procedurilor judiciare vădit nefondate sau abuzive („Acțiuni strategice în justiție împotriva mobilizării publice”). https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52022PC0177
[20] Protecting democracy. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en
[21] FIMI: towards a European redefinition of foreign interference. https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/
[22]https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan/strengthened-eu-code-practice-disinformation_en
[23] The Digital Services Act. Ensuring a safe and accountable online environment
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

ANEXE

Anexa 1:

Studiu de caz: Impactul Telegram asupra securității informaționale și comunicării în timpul crizelor

Utilizarea Telegram a avut un impact semnificativ asupra războiului din Ucraina. Aplicația Telegram, cunoscută pentru confidențialitate și capacitatea de a gestiona grupuri mari de comunicare, a devenit un instrument esențial în peisajul digital al conflictului. Trei aspecte-cheie ale Telegramului îl fac o provocare pentru securitatea informațională a statului, în special dacă acesta este într-un război hibrid, și anume, fluxul descentralizat de informație, acces ușor la un public larg și capacitatea creatorilor și utilizatorilor de a rămâne anonimi utilizând acest serviciu.
Impactul Telegram asupra războiului din Ucraina are patru provocări-cheie pentru dezvoltarea politicilor naționale de securitate informațională și cibernetică:

Actualizări în timp real despre război: atât partea ucraineană, cât și cea rusă utilizează Telegram pentru a posta actualizări regulate despre mișcările de trupe, operațiunile militare și numărul victimelor. Canalele oficiale ale autorităților militare și guvernamentale oferă actualizări în timp real, modelând percepția publică și moralul de pe ambele părți. Una dintre provocările-cheie în cadrul Telegram sunt scurgerile de date strategice și tactice, precum și comunicarea eronată a autorităților cu cetățenii.

Războiul informațional și propaganda: Telegram a devenit un câmp de luptă pentru propagandă, prin distribuirea narativelor pentru a influența opinia publică. Acestea includ deseori imagini și videoclipuri manipulate și rapoarte părtinitoare care urmăresc să influențeze sentimentul internațional și moralul intern. Războiul psihologic: ambele tabere folosesc Telegram pentru a răspândi tactici psihologice, cum ar fi postarea pierderilor inamice, victoriilor și actualizărilor care vizează demoralizarea adversarului. Capacitatea Telegram de a ajunge la grupuri țintă, inclusiv tineri și oameni din zonele de conflict, îi amplifică impactul în războiul psihologic. Provocarea-cheie în acest context este lipsa de moderare a conținutului pe Telegram, care facilitează răspândirea materialelor nesupravegheate. Până în prezent nu exista un mecanism guvernamental eficient pentru managementul influenserilor din Telegram și a conținutului pe care aceștia îl promovează.

Instrument de mobilizare: Telegram a facilitat, de asemenea, strângerea de fonduri și recrutarea, inclusiv apeluri pentru voluntari internaționali care să se alăture forțelor ucrainene și distribuirea de link-uri pentru donații în sprijinul eforturilor de apărare ale Ucrainei. Canalele Telegram distribuie linkuri către site-uri de crowdfunding, mobilizând astfel susținerea internațională pentru conflict. În acest context, Telegram poate fi utilizat ca un instrument important pentru comunicare strategică cu populația, în același timp,

capacitatea de mobilizare prin Telegram poate fi utilizată pentru a eroda suveranitatea națională și unitatea socială a populației ce prezintă o provocare majoră pentru stat din cauza anonimității canalelor și a utilizatorilor.

Recomandări privind utilizarea și gestionarea Telegram

- Moderarea conținutului: una dintre provocările principale ale Telegram este gestionarea dezinformării și a conținutului extremist. Lipsa unei moderări stricte a conținutului a dus la răspândirea rapidă a informațiilor neverificate și a discursului de ură. Experții sugerează că Telegram ar putea implementa sisteme mai robuste de verificare a conținutului, posibil incluzând verificarea bazată pe inteligență artificială și sisteme de semnalizare de către utilizatori, pentru a ajuta la monitorizarea și controlul dezinformării.
- Reglementări îmbunătățite de confidențialitate: se recomandă crearea unor reglementări de confidențialitate mai stricte, care să protejeze utilizatorii de exploatare, asigurând în același timp că platforma nu devine un refugiu pentru activități dăunătoare. Echilibrarea confidențialității utilizatorilor cu responsabilitatea ar putea implica colaborarea cu Telegram pentru a asigura utilizarea legală, în special în zonele de conflict.
- Parteneriate cu organizații de verificare a informațiilor: colaborarea cu organizații independente de verificare a informațiilor pentru a marca informațiile potențial înșelătoare și pentru a oferi surse verificate utilizatorilor. Această colaborare ar putea contribui la construirea unui spațiu mai credibil pentru utilizatorii care caută actualizări factuale pe subiecte sensibile.