

ROLUL CULTURII DE SECURITATE ÎN CONSOLIDAREA REZILIENȚEI INFORMAȚIONALE A SERVICIILOR DE INFORMAȚII

Tatiana BUSUNCIAN¹⁹

Abstract. *The influence of security culture on strengthening the information resilience of intelligence services in the context of hybrid threats refers to the process of identifying, assessing, and managing threats, disinformation, and cyberattacks targeting information networks. Such threats or risks may originate from a wide range of sources, including strategic management errors, accidents, and natural disasters. Information security threats and data-related risks, together with the strategies for managing and mitigating them, have become a key priority for intelligence services. Consequently, security culture is examined as a foundation of information security and defense, with emphasis on leadership, education, and organizational behavior. Resilience is presented as a strategic necessity, structured across technical, operational, human, and organizational dimensions. The interdependence between the two concepts is demonstrated through examples and practical recommendations. Therefore, a risk and hybrid-threat management plan includes strategies for strengthening capabilities and identifying control mechanisms for hybrid threats, highlighting the importance of continuous evaluation and interdisciplinary research in the field of security.*

Keywords: *Security culture, information resilience, intelligence services, hybrid threats, security policies.*

Introducere

Într-un context geopolitic și tehnologic marcat de volatilitate, complexitate și interdependență informațională crescândă, serviciile de informații sunt confruntate cu imperativul consolidării rezilienței informaționale înțeleasă ca un ansamblu de capacități instituționale integrate, orientate spre prevenirea, identificarea timpurie și gestionarea adaptivă a distorsiunilor informaționale și a riscurilor asociate pierderii, compromiterii sau manipulării datelor sensibile. Această abordare conceptualizează reziliența informațională ca un sistem adaptativ complex, în care procesele tehnologice, normative și culturale interacționează pentru a asigura continuitatea funcțională și credibilitatea instituțională în fața amenințărilor informaționale.

În această perspectivă, cultura de securitate se afirmă drept un pilon strategic al eficienței organizaționale, întrucât configurează sistemul de valori, comportamente și atitudini profesionale care determină modul în care personalul percepe, protejează și utilizează informația într-un mediu operațional dinamic și vulnerabil.

Actualitatea temei privind rolul culturii de securitate în consolidarea rezilienței informaționale a serviciilor de informații este determinată de transformările majore ale

¹⁹ Associate Professor, PhD in Political Sciences, The Faculty of International Relations, Political Sciences and Public Administration, Moldova State University. Director, Pro Marshall Center of the Republic of Moldova, Chisinau, Republic of Moldova. e-mail: busuncian@gmail.com; promarshall@europe.com

mediului internațional de securitate, caracterizat astăzi printr-un grad ridicat de volatilitate, complexitate și interdependență informațională.

Noile circumstanțe internaționale impun reguli și abordări inovatoare în domeniul securității globale. Redefinirea arhitecturii de securitate după prăbușirea ordinii bipolare a generat multiple provocări – nu doar de natură practică, ci și conceptuală – privind modul în care statele, instituțiile și actorii internaționali gestionează riscurile emergente. Într-un asemenea context, schimbarea mediului de securitate și reducerea tensiunilor internaționale trebuie să devină priorități pe agendele strategice ale tuturor statelor europene și democrațiilor occidentale. Fără o abordare coerentă și colaborativă a acestor provocări, nu se poate vorbi despre o Europă modernă, sigură și pașnică, capabilă să răspundă exigențelor secolului XXI.

În același timp, amplificarea amenințărilor informaționale – manifestate prin atacuri cibernetice, dezinformare și manipulare mediatică – transformă spațiul informațional într-un veritabil câmp de confruntare geopolitică. Serviciile de informații sunt, prin urmare, chemate să-și consolideze capacitatea instituțională de anticipare, adaptare și reacție, printr-o integrare coerentă a dimensiunilor tehnologice, organizaționale și culturale ale securității.

În acest cadru, cultura de securitate dobândește o importanță strategică, reprezentând fundamentul pe care se construiește reziliența informațională. Ea modelează percepțiile, valorile și comportamentele profesionale, definind modul în care personalul instituțional se raportează la riscuri și responsabilități. Astfel, cultura de securitate nu mai poate fi percepută ca un element secundar al managementului organizațional, ci ca un pilon esențial al stabilității și adaptabilității instituționale în fața amenințărilor hibride contemporane.

Totodată, progresul tehnologic accelerat – manifestat prin digitalizare, inteligență artificială și automatizarea proceselor analitice – impune o reevaluare a paradigmatelor tradiționale de protecție a informației și o valorizare crescută a resursei umane instruite, etice și responsabile. În acest sens, cultura de securitate devine nu doar o componentă a guvernantei informaționale, ci și un catalizator al rezilienței democratice, contribuind la consolidarea unei Europe capabile să protejeze pacea, stabilitatea și valorile sale fundamentale. Astfel, în această lume în continuă mișcare, este din ce în ce mai greu să navigăm printr-un prezent atât de complex și fragmentat, care este o provocare constantă.

Drept urmare este imposibil să anticipăm viitorul și, mai mult, să îi intuim consecințele directe și indirecte. Fluxul de informații devine din ce în ce mai abundent și din ce în ce mai necesar. Practic, informația întrunește deja atributele esențiale de motor și materie primă a societății noastre.

Protejarea informațiilor extrem de sensibile și a infrastructurii critice este cel mai important aspect al securității interne. Societățile moderne depind de acestea pentru a funcționa bine. Protecția datelor și disponibilitatea non-stop a sistemelor de comunicații au devenit probleme de supraviețuire în secolul XXI.

În afirmația fostului secretar american al apărării Donald Rumsfeld, informația este măsura tuturor lucrurilor care poate provoca îngrijorare și neliniște. În opinia acestuia incertitudinea este o constantă în lumea noastră dominată de informație. Pornind de la celebra frază a lui Donald Rumsfeld, „Nu știm ce nu știm”, autorul recunoaște că ne-

cunoscutul și imprevizibilul (întâmplarea și hazardul) pot afecta orice sistem, oricât de complex ar fi. Totuși, un indicator esențial al capacității instituționale și sociale îl constituie, conform autorului, abilitatea de a implementa soluții orientate spre consolidarea securității, dintre care educația și cultura de securitate joacă un rol central. Acestea sunt conceptualizate drept factori protectivi fundamentali împotriva riscurilor și incertitudinilor, acționând ca un „scut” care sprijină luarea deciziilor raționale și fundamentate în raport cu securitatea informațională și organizațională. Prin integrarea acestor elemente în valorile, comportamentele și atitudinile membrilor unei organizații sau ale societății, se consolidează stabilitatea și reziliența sistemică, oferind cadrul necesar pentru gestionarea eficientă a amenințărilor și vulnerabilităților. Deși nu este posibilă eliminarea tuturor riscurilor, cunoașterea, educația și promovarea unei culturi a securității permit dezvoltarea unei capacități adaptive de protecție, care facilitează anticiparea, prevenirea și gestionarea eficientă a situațiilor critice. Astfel, educația și cultura de securitate devin vectori strategici ai stabilității și siguranței organizaționale și sociale, reprezentând fundamentul unei abordări proactive și responsabile în fața provocărilor contemporane (Cum ne apara ... 2017).

Cultura de securitate poate fi definită drept suma cunoștințelor și a informațiilor referitoare la valorile și necesitățile naționale de securitate, a căror cunoaștere atrage dezvoltarea și promovarea unor comportamente necesare apărării individuale sau statale în fața pericolelor interne sau externe. Pentru apărarea securității, fie ea națională sau globală, este nevoie și de o puternică popularizare a culturii de securitate. Conceptul de cultură de securitate, a apărut în jurul anilor ,70 în literatura de specialitate și a suportat modificări constante în încercările teoreticienilor de a oferi o definiție cât mai complexă și corectă în contextul noilor tipuri de amenințări și vulnerabilități la nivel de individ, de comunitate, de țară, de regiune și global.

În opinia cercetătoarelor Alexandra Raluca Albescu și Georgiana-Cristina Perețeanu de la institutul național de cercetare-dezvoltare în informatică, cultura de securitate reprezintă abordarea instituțională modernă care promovează: problematica securității; cunoașterea tipurilor de urgențe politice, militare, economice, sociale și de mediu; totalitatea noțiunilor, ideilor și informațiilor disponibile cetățenilor unui stat cu privire la valori, interese și necesități naționale de securitate; modalitatea de cultivare a unor atitudini, motivații și comportamente necesare apărării și protecției individuale, de comunitate și de stat față de vulnerabilități, riscuri, amenințări, pericole sau eventuale atacuri (Albescu, 2019).

Determinarea culturii de securitate mai poate fi considerată drept o totalitate a valorilor, normelor, atitudinilor și acțiunilor care condiționează înțelegerea și asimilarea, la nivelul societății, a conceptului de securitate națională și a celor derivate (securitate individuală, colectivă, informațională, etc.).

Rolul culturii de securitate în societate are o importanță imensă și beneficii multiple, cum ar fi creșterea rezilienței societale. Oamenii conștienți de riscuri și pregătiți să acționeze sunt un scut eficient împotriva amenințărilor hibride și a tentativelor de subminare a statului. Un suport public pentru instituțiile de securitate aduce beneficii prin educarea unei societăți care înțelege și respectă rolul instituțiilor de apărare și ordine publică, le oferă legitimitate și sprijinul necesar pentru a-și îndeplini misiunea. Totodată, o cultură de securitate proactivă se concentrează pe prevenție prin educație și informare,

transformând cetățenii în parteneri activi în protejarea valorilor naționale. Prin promovarea unor valori și obiective comune de securitate, cultura de securitate contribuie la consolidarea coeziunii sociale și la depășirea diviziunilor interne (Calangea, 2017).

Cultura de securitate nu este un concept abstract, ci o realitate palpabilă care se manifestă în acțiunile și atitudinile de zi cu zi ale fiecărui cetățean. Dezvoltarea și consolidarea ei reprezintă o prioritate strategică pentru orice stat care dorește să-și asigure stabilitatea și prosperitatea pe termen lung. Prin educație, transparență și implicare, o societate își poate transforma cetățenii din simpli spectatori în actori responsabili ai propriei securități, construind astfel un viitor mai sigur și mai rezilient. Prin urmare, de o importanță primordială este cooperarea pentru realizarea securității, care este un bun al tuturor, care se obține prin efort sporit, prin interconectare și creare de canale eficiente de comunicare la nivel intern, cât și extern.

Orice simplă provocare sau abatere în respectarea sistemului de valori și concepte proprii unei culturi organizaționale a serviciilor/comunităților de informații, poate avea impact foarte mare asupra performanței profesionale, a imaginii serviciilor/comunităților și chiar asupra procesului decizional în formularea strategiilor și politicilor de securitate. În acest context, cultura și educația de securitate reprezintă un ansamblu de măsuri și norme de conduită care trebuie adaptate permanent mediului social în care trăim. Prin ruperea de realitatea socială în care își desfășoară activitatea, cultura organizațională de intelligence riscă să devină rigidă (Cultura de Securitate in intelligence..).

Adoptarea unei atitudini contrainformative proactive și defensive în cadrul serviciilor/comunităților de informații reflectă capacitatea personală de inovare a angajaților/membrilor acesteia, precum și o modalitate de a-și exprima considerația pentru valori și concepte organizaționale specifice.

În cadrul unei abordări defensive, este esențial să luăm în considerare două dimensiuni principale. Prima se referă la cadrul instituțional, care include normele și procedurile stabilite ce ghidează acțiunea. A doua componentă o reprezintă poziția socială a fiecărui individ, care este modelată de dinamica unei societăți aflate într-o perpetuă transformare.

Apartinând unui serviciu/comunități de informații, angajatorul/colaboratorul dezvoltă o serie de mecanisme psihologice specifice. Acest scut defensiv, esențial în interacțiunile sociale, se manifestă prin:

- discreția profesională, capacitatea de a menține secretul asupra afilierii la organizație;
- discernământul emoțional, abilitatea de a diferenția între autenticitatea și simularea sentimentelor interlocutorului;
- controlul emoțiilor, acțiunea de a-și canaliza emoțiile (pozitive sau negative) pentru a consolida un climat organizațional bazat pe securitate și protecție. Astfel, caracteristicile menționate reflectă o adaptare psihologică la cerințele specifice ale domeniului, unde inteligența emoțională este la fel de importantă ca cea cognitivă.

La începutul secolului al XXI-lea, mediul de securitate internațional înregistrează ca principale amenințări terorismul, crima organizată, criminalitatea economico-financiară și corupția, realități pe care reprezentanții societății civile trebuie să le cunoască, pentru a contribui împreună cu instituțiile statului la prevenirea și combaterea acestora.

Corupția reprezintă o amenințare globală la adresa securității, un fenomen care subminează dezvoltarea oricărei națiuni și erodează încrederea cetățenilor în instituțiile statului. Acest flagel afectează profund funcționarea statului, creând vulnerabilități sistemice care subminează stabilitatea instituțională, inclusiv generează vulnerabilități sistemice, afectează economia prin pierderi semnificative și limitează potențialul de creștere și progres al unei țări.

Pe termen lung, fenomenul corupției reprezintă o provocare de securitate internațională de prim rang, având un impact profund asupra mecanismelor unei economii de piață funcționale. Acesta erodează principiile concurenței loiale, descurajează investițiile străine directe și compromite respectarea drepturilor fundamentale ale omului, inclusiv accesul egal la oportunități și resurse. Astfel, educația și cultura de securitate constituie necesități ale unei noi apărări colective, dar care nu mai este realizată doar de către stat (ca entitate politico-administrativă), ci și de către cetățeni prin societatea civilă. Reprezentanții societății civile se pot implica activ în acțiuni de educație preventivă și de gestiune a noii realități de securitate, democrație conectată la valori euroatlantice.

Reziliența informațională – obiectiv strategic al serviciilor de informații. Pentru studiul de față este importantă abordarea rezilienței informaționale, care prin definiția sa reprezintă capacitatea unei organizații de a se adapta și a continua să funcționeze în fața amenințărilor, atacurilor sau incidentelor cibernetice.

Reziliența informațională este un fenomen relativ nou și important pentru contextul unui stat, cât și pentru cultura politică a unei societăți. Mulți cercetători și experți susțin că reziliența informațională este necesar să fie înțeleasă drept o abilitate a statului de a-și proteja spațiul său informațional. Analiza lucrărilor axate pe problematica rezilienței informaționale este foarte vastă dar mulți cercetători și experți limitează această problematică doar la spațiul virtual și la securitatea informațională pe când această are un spectru mai larg și reprezintă un bun public, care este în responsabilitatea statului de a fi protejată de interferențe externe și interne.

În contextul actual al Republicii Moldova, reziliența informațională reprezintă capacitatea instituțiilor și a societății de a preveni, detecta, răspunde și recupera rapid în fața amenințărilor informaționale, inclusiv dezinformării, manipulării și atacurilor cibernetice. Aceasta implică un ansamblu de măsuri instituționale, educaționale și tehnologice menite să protejeze securitatea națională și integritatea democratică.

O contribuție relevantă la dezvoltarea diverselor aspecte ale rezilienței informaționale a Republicii Moldova au adus cercetătorii V. Juc, V. Moraru, M. Benchechi, A. Peru, D. Hîrbu, L. Guștiuc, N. Albu și alții care în studiile lor reflectă aspecte ce țin de politica externă și securitatea națională, colaborarea în domeniul securității, interesele geopolitice, propagandă și dezinformare, securitatea în contextul integrării europene, securitatea umană etc. Cu o viziune asupra dezvoltării rezilienței informaționale vine Aurelia Peru, care din perspectiva practicilor confruntărilor geopolitice consideră că dezinformarea și propaganda, au devenit instrumente esențiale pentru opinia publică și pentru subminarea stabilității în statele-țintă. De asemenea, dezinformarea afectează direct credibilitatea guvernanților, deoarece scopul principal al unui atac informațional din exterior este de a compromite imaginea autorităților și derutarea cetățenilor (Peru-Balan, 2024).

La deschiderea conferinței științifico-practică internațională: ”Consolidarea rezilienței sociale prin valorificarea capitalului uman în contextul aderării Republicii Moldova și a Ucrainei la Uniunea Europeană” din octombrie 2024, Victor Juc a subliniat importanța modernizării instituționale și alinierea la standardele europene, care este crucială în consolidarea rezilienței sociale și instituționale. Astfel, aceasta implică nu doar apărarea fizică și politică, ci și capacitatea de a rezista la dezinformare și manipulare, care pot submina democrația și credibilitatea statului. Dezvoltarea durabilă, educația și o societate incluzivă sunt considerate elemente-cheie în fortificarea acestei reziliențe. Prin urmare, reziliența informațională este un pilon fundamental pentru ca Republica Moldova să devină un actor responsabil și activ în securitatea regională, nu doar un simplu beneficiar al acesteia. Astfel, analiza rezilienței informaționale se axează pe capacitatea Republicii Moldova de a-și proteja societatea și instituțiile de amenințările externe și interne, în special în contextul politic tensionat și al aspirațiilor de integrare europeană (Consolidarea rezilienței., 2024).

În articolul, ”Efectele criminalității cibernetice asupra securității naționale a Republicii Moldova” (Bencheci, Panfili, Hîrbu, 2024), autorii detaliază modul în care criminalitatea cibernetică, pe lângă pierderile economice, afectează direct securitatea națională. Se subliniază că aceste atacuri pot destabiliza infrastructura critică, submina încrederea în instituțiile statului și pot fi folosite ca instrumente de război hibrid, punând în pericol suveranitatea și stabilitatea Republicii Moldova. Un aspect cheie abordat este dimensiunea transnațională a criminalității cibernetice, care necesită o colaborare internațională intensă și o adaptare constantă a capacităților naționale de apărare. Autorii subliniază că atacurile cibernetice nu sunt doar infracțiuni ordinare, ci pot fi acțiuni ale unor actori statali sau non-statali, având obiective politice și strategice.

Potrivit unui raport al Institutului pentru Politici și Reforme Europene (IPRE), reziliența informațională este esențială pentru protejarea proceselor democratice și a valorilor fundamentale ale statului, în special în fața amenințărilor hibride și a campaniilor de dezinformare externe (Doroftei, 2024).

De asemenea, un studiu realizat de experții din cadrul Centrului de Informare și Documentare privind NATO în parteneriat cu Oficiul de Legătură NATO din Republica Moldova și Institutul de Cercetări Juridice, Politice și Sociologice subliniază importanța dezvoltării unei culturi a securității și a educației media pentru consolidarea rezilienței informaționale a cetățenilor (Mârzac, Albu, Panța, 2022).

În acest sens, autoritățile naționale, inclusiv Serviciul de Informații și Securitate al Republicii Moldova, au elaborat strategii și politici pentru combaterea dezinformării și protejarea spațiului informațional național. Printre acestea se numără înființarea Centrului pentru Comunicare Strategică și Combaterea Dezinformării, care are rolul de a coordona eforturile interinstituționale în domeniul securității informaționale (Mârzac, Sandu, 2022).

Astfel, Serviciul de Informații și Securitate (SIS) al Republicii Moldova a identificat în perioada 2022–2023 o creștere a tentativelor de imixtiune externă în afacerile interne ale țării, inclusiv în procesele electorale. Aceste activități subliniază importanța consolidării rezilienței informaționale ca obiectiv strategic național (Raport SIS, 2024).

Un studiu recent apărut, ”Democrația sub asediu. Provocări la adresa securității naționale și contracararea amenințărilor hibride în Republica Moldova” (PISA, 2025),

evidențiază vulnerabilități existente, tactici utilizate și măsuri de răspuns adoptate, oferind o imagine de ansamblu asupra contextului național de securitate. În studiu este analizat modul în care cultura de securitate, înțeleasă ca ansamblu de valori, norme, practici instituționale și nivel de conștientizare în domeniul securității, poate contribui la consolidarea rezilienței informaționale a Serviciului de Informații și Securitate din Republica Moldova. În contextul amplificării amenințărilor hibride și a presiunilor exercitate asupra democrației și securității naționale, este investigată importanța formării unei culturi organizaționale orientate spre prevenție, adaptabilitate și cooperare interinstituțională. Studiul abordează dimensiunile practice ale dezvoltării rezilienței informaționale prin instruirea personalului, gestionarea eficientă a resurselor informaționale, protecția împotriva campaniilor de dezinformare și consolidarea încrederii publice în sistemul național de securitate.

Interdependența dintre cultura de securitate și reziliența informațională

În contextul Republicii Moldova și al aspirațiilor sale europene, dezvoltarea unei culturi de securitate este esențială pentru consolidarea rezilienței informaționale a societății. Serviciile/comunitățile de informații au un rol crucial în acest proces, acestea contribuie la reziliența informațională prin informare și educație. Aceasta se manifestă prin organizarea de campanii publice, lecții deschise în instituțiile de învățământ superior și parteneriate cu societatea civilă pentru a sensibiliza publicul larg cu privire la riscurile dezinformării și manipulării. Acest lucru le permite cetățenilor să dezvolte o gândire critică și să discearnă informațiile false. Analiză strategică și avertizare timpurie se axează pe monitorizarea spațiului informațional și identificarea amenințărilor hibride și a campaniilor de dezinformare. Prin furnizarea de analize pertinente și avertizări timpurii către factorii de decizie, serviciile/comunitățile de informații contribuie la adoptarea de măsuri proactive de contracarare. Colaborarea interinstituțională contribuie la consolidarea cooperării cu alte instituții de stat, cum ar fi mass-media, pentru a echilibra promovarea politicii de securitate națională și a stimula un mediu informațional sănătos. O astfel de colaborare permite crearea unui sistem de avertizare timpurie eficient (Consolidarea rezilienței sociale, 2024).

Procesul de aderare a Republicii Moldova și a Ucrainei la Uniunea Europeană subliniază nevoia de a alinia standardele naționale la cele europene, inclusiv în domeniul securității informaționale și cibernetice.

În contextul aderării la Uniunea Europeană, Republica Moldova trebuie să adopte și să implementeze standardele europene în domeniul securității informaționale. Aceste standarde includ protecția infrastructurilor critice, combaterea dezinformării și a atacurilor cibernetice, precum și promovarea unei culturi a securității în rândul cetățenilor și instituțiilor. Uniunea Europeană sprijină Republica Moldova în acest proces prin diverse inițiative, inclusiv prin desfășurarea Echipei de Răspuns Rapid în domeniul Hibrid, care oferă asistență în fața riscurilor și amenințărilor hibride, inclusiv dezinformarea, atacurile cibernetice și ingerințele în procesele interne.

În acest context, Rezoluția Parlamentului European din 10 septembrie 2025 referitoare la întărirea rezilienței Republicii Moldova în fața amenințărilor hibride și a ingerințelor răuvoitoare ale Federației Ruse reprezintă un pas important în consolidarea relațiilor dintre Uniunea Europeană și Republica Moldova (Parlamentul European, 2025).

Rezoluția Parlamentului European din 10 septembrie 2025 se concentrează pe întărirea rezilienței Republicii Moldova în fața amenințărilor hibride și a ingerințelor răuvoitoare ale Federației Ruse. Documentul evidențiază intensificarea dezinformării, atacurilor cibernetice și manipulărilor politice ca strategii de destabilizare a regiunii. Prin măsurile propuse, se urmărește întărirea rezilienței Republicii Moldova în fața amenințărilor hibride și a ingerințelor externe. Aceste acțiuni fac parte dintr-o strategie mai largă de influență, similare cu cele observate în Ucraina și Georgia, și amenință stabilitatea politică, securitatea informațională și integritatea democratică a Republicii Moldova.

În contextul aderării Republicii Moldova la Uniunea Europeană, reprezintă un instrument strategic pentru Republica Moldova, care nu doar că întărește reziliența în fața amenințărilor hibride și ingerințelor externe, dar și susține procesul de integrare europeană și consolidarea securității naționale pe termen lung.

Pe de altă parte, procesul de aderare a Republicii Moldova la Uniunea Europeană reprezintă o transformare profundă și multidimensională a statului și societății prin:

- Armonizarea cadrului legal: Republica Moldova a adoptat Legea nr. 48/2023 privind securitatea cibernetică, aliniindu-se la standardele UE. Acest cadru legal modernizează instituțiile și asigură o mai bună protecție a infrastructurii critice.
- Creșterea capacității instituționale: cooperarea cu NATO și UE, prin programe precum Parteneriatul pentru Pace, contribuie la dezvoltarea capacităților de supraveghere și la consolidarea sistemului național de apărare. Această colaborare este esențială pentru a face față noilor provocări de securitate.
- Sprijin pentru mass-media și societatea civilă: UE susține inițiative care vizează fortificarea rezilienței informaționale, inclusiv prin finanțarea organizațiilor societății civile și a mass-mediei independente. Serviciile de informații pot beneficia de aceste parteneriate pentru a-și amplifica eforturile de combatere a dezinformării.

Serviciul de Informații și Securitate a Republicii Moldova a promovat activ conceptul de cultură de securitate prin campania națională „Educație de securitate” (SIS, Cultura dsesecuritate..). Publicațiile și rapoartele instituției, cum ar fi Raportul de monitorizare și evaluare a implementării Strategiei securității informaționale (SIS, Raport de evaluare, 2022), conțin informații valoroase despre rolul său în consolidarea rezilienței informaționale a societății.

Strategii pentru consolidarea culturii de securitate și a rezilienței informaționale

Pentru a aborda eficient securitatea informațională, este necesară o schimbare de paradigmă. Această schimbare nu este necesară doar din cauza amenințărilor actuale, ci și pentru a crea mecanisme eficiente de avertizare timpurie și reziliență sporită. Un astfel de cadru ar permite o cooperare internațională proactivă, participativă și transparentă, consolidând astfel un mediu cibernetic stabil și sigur. Prin aceste măsuri, putem asigura o dezvoltare durabilă și pașnică a spațiului cibernetic global. Această presupunere constituie mai mult decât prevenirea atacurilor. O organizație pregătită se concentrează pe abilitatea de a absorbi șocul și de a se recupera rapid, menținând în același timp integritatea și disponibilitatea datelor și sistemelor. De asemenea, aceasta le permite

profesioniștilor și cercetătorilor să analizeze fenomenul de exploatare ce se extinde asupra unei organizații reziliente care nu doar supraviețuiește unui atac, ci își revine, adesea, devinind mai puternică prin lecțiile învățate din incidentele precedente și din incidentele altor organizații/țări.

Prin urmare, noțiunile principale a rezilienței informaționale sunt prevenirea, detectarea și recuperarea. Pentru a ține pasul cu prevenirea atacurilor se iau măsuri proactive care includ implementarea de firewall-uri, sisteme de detectare a intruziunilor și criptarea datelor. Sigur o parte esențială a protecției este educația și cultura angajaților privind riscurile informaționale.

Ce ține de detectarea timpurie în minimizarea daunelor este crucială. Acțiunile imediate întreprinse după ce un incident este detectat și elaborarea unui plan de răspuns bine definit ajută la izolarea atacului, la minimizarea impactului și la oprirea propagării acestuia.

Recuperarea este noțiune care ține de procesul de restabilire a operațiunilor după un incident. Aceasta include restaurarea datelor din copii de rezervă, repararea sistemelor afectate/distruse și în unele situații reconstruirea infrastructurii, ceea ce constituie un proces foarte costisitor și complex, care poate implica nu doar resurse financiare considerabil, ci și o planificare minuțioasă, expertiză tehnică specializată și un effort substanțial de coordonare a echipelor.

În raportul de analiză prospectivă strategică din 2020, intitulat „Drumul de parcurs către o Europă mai rezilientă”, sunt analizate concluziile preliminare ale crizei COVID-19. Acest raport de asemenea explică modul în care gândirea strategică poate consolida reziliența pe termen lung a Europei. Raportul analizează reziliența UE pe patru dimensiuni principale: socioeconomică cu descrierea cum își revin societățile și economiile după șocuri; geopolitică privind capacitatea UE de a-și menține stabilitatea într-un context global dinamic; ecologică, adaptarea la provocările climatice și de mediu și digitală, cu privire la asigurarea rezilienței infrastructurii și a sistemelor digitale în fața amenințărilor (Comisia Europeană).

În concluzie, în contextul mai larg al aderării la UE, rolul culturii de securitate și al rezilienței informaționale este fundamental pentru consolidarea rezilienței societale. Serviciile/comunitățile de informații, prin acțiuni de educație, analiză strategică și colaborare interinstituțională, sunt actori-cheie în acest proces. Integrarea europeană servește drept catalizator pentru modernizarea și alinierea Republicii Moldova la standardele internaționale în domeniu, sporind astfel capacitatea de a face față amenințărilor informaționale.

Eforturile recente ale autorităților moldovenești și ale instituțiilor relevante, demonstrează concret de ce reziliența informațională nu este doar un concept teoretic, ci o necesitate practică, vitală pentru securitatea națională. Serviciile/comunitățile de informații trebuie să fie capabile să detecteze și să contracareze astfel de riscuri.

O cultură de securitate solidă în cadrul serviciilor/comunităților de informații este esențială. Aceasta include nu doar expertiza tehnică, ci și o mentalitate proactivă, o conștientizare constantă a riscurilor și o etică a securității. Fără o astfel de cultură, chiar și cele mai avansate sisteme de apărare pot fi vulnerabile la erori umane sau la atacuri de inginerie socială.

Amenințările cibernetice au un caracter hibrid. Acest lucru justifică extinderea rolului serviciilor/comunităților de informații de la colectarea de date clasice la monitorizarea constantă a spațiului cibernetic, colaborarea cu experții IT și educarea populației cu privire la riscuri. Astfel, serviciile de informații devin piloni ai rezilienței societale.

Prin inițiative de educație mediatică, campanii de conștientizare și consolidarea colaborării internaționale, Republica Moldova poate îmbunătăți semnificativ capacitatea cetățenilor de a identifica și contracara dezinformarea. În același timp, dezvoltarea unui sistem de monitorizare eficient al fluxurilor de informație și întărirea parteneriatelor cu organizațiile de fact-checking sunt esențiale pentru asigurarea unei informări corecte și echilibrate. Promovarea unei culturi a verificării faptelor și a responsabilității în consumul de informație va contribui nu doar la protejarea democrației, dar și la creșterea încrederii publicului în sursele de informație.

BIBLIOGRAFIE

- Albescu A. R., Perețeanu G.C., (2019), Cultura de securitate cibernetică în România. *Romanian Journal of Information Technology and Automatic Control*, Vol. 29, No. 4, 75-84, 2019, pag. 75-84.
- Analiza prospectivă strategică. https://commission.europa.eu/strategy-and-policy/strategic-foresight_ro (accesat la 12.11.2025)
- Bencheci M., Hîrbu D., Panfilii N., (2024), Efectele criminalității cibernetice asupra securității naționale a Republicii Moldova. CZU: 343.53:004:355.1. Materialele conferința științifico-practică internațională: ”Consolidarea rezilienței sociale prin valorificarea capitalului uman în contextul aderării Republicii Moldova și a Ucrainei la Uniunea Europeană”, 17-18 octombrie 2024, USM, Chișinău, 2024, pag. 395-401
- Calangea Claudia (2017), *Cultura de securitate. Surse și resurse*. Intelligence, București, 2017. <https://intelligence.sri.ro/cultura-de-securitate-surse-si-resurse/> (accesat la 12.11.2025)
- Cultura de securitate în intelligence. <https://intelligence.sri.ro/cultura-de-securitate-organizatia-de-intelligence/> (accesat la 12.11.2025)
- Cultura de securitate promovată prin informare și educație <https://sis.md/ro/content/cultura-de-securitate-promovata-prin-informare-si-educaiie> (accesat la 12.11.2025)
- Cum ne apără cultura de securitate. Intelligence, ICI București, 2017. <https://intelligence.sri.ro/cum-ne-apara-cultura-de-securitate/> (accesat la 12.11.2025)
- Democrația sub asediu. Provocări la adresa securității naționale și contracararea amenințărilor hibride în Republica Moldova. Studiu realizat de PISA în cadrul proiectului DCAF – Consolidarea guvernării sectorului de securitate în Moldova, finanțat de Suedia. Chișinău, 2025. <https://pisa.md/wp-content/uploads/2025/09/SUMAR.-Democratia-sub-asediu.-Provocari-la-adresa-securitatii-nationale-si-contracararea-amenintarilor-hibride-in-Republica-Moldova.pdf> (accesat la 12.11.2025)
- Doroftei Alina (2024), *Reziliența informațională la firul ierbii în Republica Moldova - o abordare*. Institutul pentru Politici și Reforme Europene Notă Analitică, Nr. 6/2024., p. 2.
- Fraudele electorale constatate în cadrul alegerilor prezidențiale și a referendumului republican. Imixtiunea externă în procesele electorale din Republica Moldova. Raport instituțional al Serviciului de Informații și Securitate al RM. https://sis.md/sites/default/files/comunicate/fisiere/Raport_SIS_Public_Interferenta_in_procesul_electoral.pdf (accesat la 12.11.2025)
- Legea nr. 48/2023 privind securitatea cibernetică. Publicată în Monitorul Oficial Nr. 151-153 din 28.04.2023
- https://www.legis.md/cautare/getResults?doc_id=136732&lang=ro (accesat la 12.11.2025)

- Mârzac E., Albu N., Panța R. (2022), *Reziliența în atenția securității*. Concepte, procese, necesități. Chișinău: USM, 2022, pp. 55-77
- Mârzac E., Sandu S. (2022), *Comunicarea strategică– instrument de fortificare a rezilienței informaționale*. Reziliența în atenția securității. Concepte, procese, necesități. Chișinău: USM, 2022, p. 56
- Materialele conferința științifico-practică internațională: ”Consolidarea rezilienței sociale prin valorificarea capitalului uman în contextul aderării Republicii Moldova și a Ucrainei la Uniunea Europeană”, 17-18 octombrie 2024, USM, Chișinău, 2024
- Materialele conferinței științifico-practică internațională: ”Consolidarea rezilienței sociale prin valorificarea capitalului uman în contextul aderării Republicii Moldova și a Ucrainei la Uniunea Europeană”, 17-18 octombrie 2024, USM, Chișinău, 2024
- Peru-Balan Aurelia (2024), *Narative propagandiste și dezinformare: reziliența informațională a Republicii Moldova*. Articolul este elaborat în cadrul subprogramului 01.05.01 Securitatea națională a Republicii Moldova în contextul aderării la Uniunea Europeană: abordări juridice, politologice și sociologice, realizat de Institutul de Cercetări Juridice, Politice și Sociologice al Universității de Stat din Moldova, pag. 245-255
- Raportul de monitorizare și evaluare a implementării Strategiei securității informaționale pentru anii 2019-2024 (perioada de raportare: 2022)
- Rezoluția Parlamentului European din 10 septembrie 2025 referitoare la întărirea rezilienței Republicii Moldova în fața amenințărilor hibride și a ingerințelor răuvoitoare ale Rusiei. https://www.europarl.europa.eu/doceo/document/TA-10-2025-0191_RO.html (accesat la 12.11.2025)