**UNIVERSITATEA DE STAT DIN MOLDOVA**

**FACULTATEA RELAȚII INTERNAȚIONALE, ȘTIINȚE POLITICE ȘI ADMINISTRATIVE**

**DEPARTAMENTUL RELAȚII INTERNAȚIONALE**

**CARAMAN IANA**

**COLUN ARINA**

**COJOCARU LOREDANA**

**SECURITATEA INFORMAȚIONALĂ ȘI ACTIVITATEA SERVICIILOR DE INFORMAȚII ÎN CONTEXTUL GLOBALIZĂRII**

**REFERAT**

Autorii: \_\_\_\_\_\_\_\_\_\_\_\_

Conducător științific: \_\_\_\_\_\_\_\_\_\_\_\_

**Ilașciuc Andrei,** **lector universitar**

**CHIȘINĂU, 2021**

**CUPRINS**

**INTRODUCERE.....................................................................................................3**

1. **ASPECTE TEORETICE ALE SECURITĂȚII INFORMAȚIONALE.......5**
2. **ACTIVITATEA SERVICIILOR DE INFORMAȚII ÎN CONTEXTUL GLOBALIZĂRII.............................................................................................11**
3. **ASIGURAREA SECURITĂȚII INFORMAȚIONALE ÎN REPUBLICA MOLDOVA......................................................................................................17**

**CONCLUZII..........................................................................................................22**

**BIBLIOGRAFIE...................................................................................................24**

**INTRODUCERE**

Sfera informațională, ca factor de organizare a societății contemporane, are o influență activă asupra componentelor politice, economice, sociale, de apărare, diplomatice și tehnologice ale securității statului. În cea mai mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul de informații. În noul context de securitate, informații de securitate și cooperare internațională a serviciilor de informații au sarcina de a identifica și de a sprijini oportunități care vizează atingerea informațiilor intereselor naționale/internaționale și de a afirma valorile de securitate. Serviciile de informații au responsabilitatea de a conlucra la programe comune ce țin de dezvoltarea unei cooperări mai eficiente, pentru a crește transparența instituțională, pentru a promova o deschidere eficientă către sectorul civil de către agențiile de informații, prin conectarea la cele mai recente preocupări ale instituțiilor universitare, postuniversitare de învățământ în domeniul securității și apărării internaționale, promovând dialogul și înțelegerea între popoarele lumii. Astfel de instituții stau la baza formării elitei în cadrul serviciilor de informații.

Mediul complex de securitate, viteza cu care au loc evenimentele, precum luarea deciziilor strategice sunt indicatori ai necesității unei noi formule de informații, capabile să genereze cunoștințe strategice, bazate pe rețele de inovare" și "grupuri de cunoștințe". Cadrul de cooperare, care se manifestă pe arena internațională în domeniul securității informațiilor organizațiilor internaționale, ar putea fi construit pe baza și timpul mai scurt dedicat formulelor integrate, un amestec al cooperării între organizațiile internaționale ar putea fi construit, un set de instrumente de comunicare împărtășite de toți actorii care vizează stabilirea si urmărirea priorităților, dezvoltarea mecanismelor de platforme de răspuns rapid și analiză, alocând în mod deliberat timpul necesar acestor eforturi, precum și consolidarea rețelelor de încredere reciprocă.

Sistemele informatice și de comunicații ale unui stat, precum și datele gestionate de acestea, sunt tot mai dependente de spațiul cibernetic. Totodată, mediul cibernetic găzduiește elementele de manifestare ale lumii reale, începând cu multiple comunități de interes și rețele umane ce se manifestă în mediul virtual. Dincolo de beneficiile evidente pe care acest mediu le are în facilitarea tuturor aspectelor existenței umane de la cele economice, financiare, sociale, culturale și până la cele politice și militare, acesta facilitează și o serie de riscuri specifice, în special în absența unor măsuri de securitate adecvate. Atât entitățile statale, cât și cele non-statale (la o scară care le pune aproape pe picior de egalitate cu agențiile guvernamentale în acest cadru), în baza propriilor interese, pot recurge la agresiuni cibernetice împotriva competitorilor sau opozanților. Astfel de atacuri cibernetice pot fi îndreptate împotriva sistemelor de tehnologia informației și de comunicații, care fie reprezintă infrastructuri critice în sine (de exemplu telecomunicațiile și rețeaua Internet), fie sunt esențiale pentru buna funcționare a celorlalte infrastructuri critice ale statului (de exemplu infrastructura de transport aerian, feroviar și rutier, sistemele de aprovizionare cu energie, gaze, petrol și apă, serviciile medicale, sistemul financiar-bancar etc.).

Prevenirea, apărarea și limitarea efectelor unor astfel de atacuri implică eforturi multidisciplinare, acțiuni complexe și procese decizionale ce necesită o informare corectă, completă și oportună cu privire la caracteristicile atacului cibernetic, vectorii purtători ai amenințării și actorii agresori. Ca în orice alt tip de proces decizional, recurgerea la produsele de Inteligență cu diferite grade de complexitate este o opțiune firească, indiferent dacă facem trimitere la entități publice sau private. Rolul Inteligenței raportat la orice sistem de referință este cel de a colecta, analiza și produce informații menite să furnizeze evaluări complete, exacte, oportune și relevante cu privire la amenințări, în vederea fundamentării deciziilor factorilor de răspundere.

Din această perspectivă, și abordarea problematicii Inteligenței în domeniul cibernetic comportă o serie de nuanțe, în funcție de sistemul de referință. La rândul ei, fiecare disciplină de culegere a informațiilor din spectrul Inteligenței se raportează la aspecte specifice în ce privește obiectivele operaționale și modalitatea de manifestare în fiecare dintre etapele ciclului Inteligenței - direcțioare, colectare, procesare și producție, diseminare raportate la definirea cerințelor de informații, tipul de date colectate, metodologia de colectare, resursele implicate/senzorii utilizați, modul de procesare a datelor și informațiilor primare, diseminarea produselor de Inteligență, caracterul acestora și asigurarea conexiunii inverse.

**1. ASPECTE TEORETICE ALE SECURITĂȚII INFORMAȚIONALE**

Istoria securității informaționale începe cu securitatea computerelor. Nevoia de securitate computerizată – adică nevoia de a securiza locațiile fizice, hardware-ul și software-ul împotriva amenințărilor – a apărut în timpul celui de-al Doilea Război Mondial, când primele mainframe, dezvoltate pentru a ajuta calculele pentru spargerea codului de comunicație au fost date în folosință. Au fost implementate mai multe niveluri de securitate pentru a proteja aceste mainframe și pentru a menține integritatea datelor lor. Accesul în locurile militare sensibile, de exemplu, a fost controlat prin intermediul insignelor, cheilor și recunoașterea facială a personalului autorizat de către agenții de securitate. Nevoia tot mai mare de a menține securitatea națională a condus în cele din urmă la garanții mai complexe și mai sofisticate din punct de vedere tehnologic pentru securitatea computerelor.

În primii ani, securitatea informațională a fost un proces simplu, compus în principal din securitate fizică și scheme simple de clasificare a documentelor. Principalele amenințări la adresa securității au fost furtul fizic al echipamentelor, spionajul împotriva sistemelor și sabotajul. Una dintre primele probleme de securitate documentate care nu se încadrau în aceste categorii a avut loc la începutul anilor 1960, când un administrator de sistem lucra la un MOTD (mesajul zilei), iar un alt administrator edita fișierul cu parole. O eroare a software-ului a amestecat cele două fișiere, iar întregul fișier a fost tipărit pe fiecare fișier de ieșire.

În timpul Războiului Rece, mult mai multe mainframe au fost transpuse online pentru a îndeplini sarcini mai complexe și mai sofisticate. A devenit necesar să se permită acestor mainframe să comunice printr-un proces mai puțin complicat decât trimiterea de benzi magnetice între centrele de calculatoare. Ca răspuns la această nevoie, Agenția pentru Proiecte de Cercetare Avansată (ARPA) a Departamentului de Apărare a început să examineze fezabilitatea unui sistem redundant de comunicații în rețea pentru a sprijini schimbul de informații al armatei. Larry Roberts, cunoscut drept fondatorul Internetului, a dezvoltat proiectul – care a fost numit ARPANET – încă de la început. ARPANET este predecesorul Internetului.

În următorul deceniu, ARPANET a devenit popular și utilizat pe scară largă, iar potențialul de utilizare greșită a crescut. În decembrie 1973, Robert M. Bob Metcalfe, care este creditat odată cu dezvoltarea Ethernet, unul dintre cele mai populare protocoale de rețea, a identificat probleme fundamentale cu securitatea ARPANET. Site-urile individuale nu aveau suficiente controale și măsuri de protecție pentru a proteja datele utilizatorilor de la distanță. Au existat alte probleme: vulnerabilitatea structurii și formatelor parolelor; lipsa procedurilor de siguranță pentru conexiunile dial-up; și identificarea utilizatorului și autorizarea inexistentă la sistem. Numerele de telefon au fost distribuite pe scară largă și mediatizate în mod deschis pe pereții cabinelor telefonice, oferind hackerilor acces ușor la ARPANET. Din cauza gamei și frecvenței încălcărilor securității computerelor și a exploziei numărului de gazde și utilizatori pe ARPANET, securitatea rețelei a fost denumită insecuritate în rețea. În 1978, un studiu celebru intitulat „Analiza de protecție: Raport final" a fost publicat. Acesta s-a concentrat pe un proiect întreprins de ARPA pentru a descoperi vulnerabilitățile securității sistemului de operare.

Mișcarea către securitate care a depășit protejarea fizică a locațiilor au început cu o singură lucrare sponsorizată de Departamentul Apărării, Raportul Rand R-609, care a încercat să definească multiplele controale și mecanisme necesare pentru protecția unui sistem informatic pe mai multe niveluri. Documentul a fost clasat timp de aproape zece ani și este acum considerat a fi lucrarea care a început studiul securității computerelor. Securitatea sistemelor care partajează resurse în cadrul Departamentului Apărării a fost adusă în atenția cercetătorilor în primăvara și vara anului 1967. La acea vreme, sistemele erau achiziționate într-un ritm rapid și securizarea lor era o preocupare presantă atât pentru furnizorii militari, cât și pentru domeniul apărării.

În general, securitatea este „calitatea sau starea de a fi în siguranță – a fi liber de pericol.” Cu alte cuvinte, protecția împotriva adversarilor – de cei care ar face rău, intenționat sau altfel – este obiectivul. Securitatea națională, de exemplu , este un sistem multistrat care protejează suveranitatea unui stat, activele sale, resursele și oamenii săi. Atingerea nivelului adecvat de securitate pentru o organizație necesită, de asemenea, un sistem cu mai multe fațete.

O organizație de succes ar trebui să aibă următoarele straturi multiple de securitate existentă pentru a-și proteja operațiunile:

* Securitate fizică, pentru a proteja obiectele fizice, împotriva accesului neautorizat și a utilizării greșite;
* Securitatea personalului, pentru a proteja persoana sau grupul de persoane care sunt autorizate să acceseze organizația și operațiunile sale;
* Securitatea operațiunilor, pentru a proteja detaliile unei anumite operațiuni sau a unei serii de activități;
* Securitatea comunicațiilor, pentru a proteja mediile de comunicații, tehnologia și conținutul;
* Securitatea rețelelor, pentru a proteja componentele de rețea, conexiunile și conținutul;
* Securitatea informațiilor, pentru a proteja confidențialitatea, integritatea și disponibilitatea activelor informaționale, indiferent dacă sunt stocate, procesate sau transmise. Se realizează prin aplicarea politicilor, educației, formării și conștientizării și tehnologiei.

Comitetul pentru Sisteme Naționale de Securitate (CNSS) definește securitatea informațională ca fiind protecția informațiilor și a elementelor sale critice, inclusiv sistemele și hardware-ul care utilizează, stochează și transmit acele informații. Modelul CNSS de securitate a informațiilor a evoluat dintr-un concept dezvoltat de industria de securitate informatică numit triunghiul CIA. Acesta a fost standardul industriei pentru securitatea computerelor de la dezvoltarea mainframe-ului. Se bazează pe cele trei caracteristici ale informațiilor care îi conferă valoare organizațiilor: confidențialitate, integritate și disponibilitate. Securitatea acestor trei caracteristici ale informațiilor este la fel de importantă astăzi precum a fost întotdeauna, dar modelul triunghiului CIA nu mai abordează în mod adecvat mediul în continuă schimbare. Amenințările la adresa confidențialității, integrității și disponibilității informațiilor au evoluat într-o colecție vastă de evenimente, inclusiv daune accidentale sau intenționate, distrugere, furt, modificări neintenționate sau neautorizate sau alte utilizări greșite. Acest nou mediu de multe amenințări în continuă evoluție a determinat dezvoltarea unui model mai robust care abordează complexitățile mediului actual de securitate a informațiilor.

Există o serie de termeni și concepte care sunt esențiale pentru orice discuție despre securitatea informațională:

* Acces: capacitatea unui subiect sau obiect de a utiliza, manipula, modifica sau afecta un alt subiect sau obiect. Utilizatorii autorizați au acces legal la un sistem, în timp ce hackerii au acces ilegal la un sistem. Controalele de acces reglează această abilitate.
* Activ: resursa organizațională care este protejată. Un activ poate fi logic, cum ar fi un site Web, informații sau date; sau un bun poate fi fizic, cum ar fi o persoană, un sistem informatic sau un alt obiect tangibil. Activele, și în special activele informaționale, sunt în centrul eforturilor de securitate; acestea sunt ceea ce aceste eforturi încearcă să protejeze.
* Atac: un act intenționat sau neintenționat care poate provoca daune sau compromite în alt mod informațiile și/sau sistemele care le susțin. Atacurile pot fi active sau pasive, intenționate sau neintenționate și directe sau indirecte. Când cineva citește întâmplător informații sensibile care nu sunt destinate utilizării sale este un atac pasiv. Un hacker care încearcă să pătrundă într-un sistem informațional este un atac intenționat. O lovitură de fulger care provoacă un incendiu într-o clădire este un atac neintenționat. Un atac direct este un hacker care folosește un computer personal pentru a pătrunde într-un sistem. Un atac indirect este un hacker care compromite un sistem și îl folosește pentru a ataca alte sisteme, de exemplu, ca parte a unei rețele bot. Acest grup de computere compromise, care rulează software-ul ales de atacator, poate funcționa autonom sau sub controlul direct al atacatorului pentru a ataca sistemele și a fura informații despre utilizator sau a conduce atacuri distribuite de refuzare a serviciului. Atacurile directe provin din amenințarea însăși. Atacurile indirecte provin dintr-un sistem sau o resursă compromisă care funcționează defectuos sau funcționează sub controlul unei amenințări.
* Control, salvgardare sau contramăsuri: mecanisme, politici sau proceduri de securitate care pot contracara cu succes atacurile, pot reduce riscurile, pot rezolva vulnerabilități și, în alt mod, pot îmbunătăți securitatea în cadrul unei organizații.
* Exploatare: O tehnică folosită pentru a compromite un sistem. Agenții de amenințare pot încerca să exploateze un sistem sau un alt bun de informare folosindu-l ilegal pentru câștigul lor personal. Sau, un exploit poate fi un proces documentat pentru a profita de o vulnerabilitate sau expunere, de obicei în software, care este fie inerent software-ului, fie este creat de atacator. Exploit-urile folosesc instrumentele software existente sau componentele software personalizate.
* Expunere: o stare de expunere. În securitatea informațională, expunerea există atunci când este prezentă o vulnerabilitate cunoscută de atacator.
* Pierdere: O singură instanță a unui activ de informații care suferă daune sau modificări sau dezvăluiri neintenționate sau neautorizate. Atunci când informațiile unei organizații sunt furate, aceasta a suferit o pierdere.
* Profil de protecție sau poziție de securitate: întregul set de controale și garanții, inclusiv politici, educație, formare și conștientizare tehnologice, pe care organizația le implementează (sau nu reușește să implementeze) pentru a proteja activul. Termenii sunt uneori folosiți interschimbabil cu termenul program de securitate, deși programul de securitate cuprinde adesea aspecte manageriale ale securității, inclusiv planificarea, personalul și programele subordonate.
* Risc: Probabilitatea ca ceva nedorit să se întâmple. Organizațiile trebuie să minimizeze riscurile pentru a se potrivi cu apetitul lor pentru risc - cantitatea și natura riscului pe care organizația este dispusă să-l accepte.
* Subiecte și obiecte: Un computer poate fi fie subiectul unui atac - o entitate agent folosită pentru a conduce atacul - fie obiectul unui atac - entitatea țintă. Un computer poate fi atât subiectul, cât și obiectul unui atac, atunci când, de exemplu, este compromis de un atac (obiect), iar apoi este folosit pentru a ataca alte sisteme (subiect).
* Amenințare: O categorie de obiecte, persoane sau alte entități care prezintă un pericol pentru un bun. Amenințările sunt întotdeauna prezente și pot fi intenționate sau nedirecționate. De exemplu, hackerii amenință în mod intenționat sistemele de informații neprotejate, în timp ce furtunile severe amenință întâmplător clădirile și conținutul acestora.
* Agent de amenințare: Instanța specifică sau o componentă a unei amenințări. De exemplu, toți hackerii din lume prezintă o amenințare colectivă, în timp ce Kevin Mitnick, care a fost condamnat pentru piratare în sistemele telefonice, este un agent specific de amenințare.
* Vulnerabilitate: O slăbiciune sau defecțiune a unui sistem sau mecanism de protecție care îl deschide spre atac sau deteriorare. Câteva exemple de vulnerabilități sunt o defecțiune a unui pachet software, un port de sistem neprotejat și o ușă deblocată. Unele vulnerabilități bine-cunoscute au fost examinate, documentate și publicate; altele rămân latente (sau nedescoperite).

Valoarea informaţiei provine din caracteristicile pe care le posedă. Când o caracteristică a informației se modifică, valoarea respectivei informații fie crește, fie, mai frecvent, scade. Unele caracteristici afectează valoarea informațiilor pentru utilizatori mai mult decât o fac altele. Acest lucru poate depinde de circumstanțe; de exemplu, actualitatea informațiilor poate fi un factor critic, deoarece informațiile își pierd mult din valoare atunci când sunt livrate prea târziu.

Deși profesioniștii în securitatea informațiilor și utilizatorii finali împărtășesc o înțelegere a caracteristicilor informațiilor, pot apărea tensiuni atunci când nevoia de a securiza informațiile de amenințări intră în conflict cu nevoia utilizatorilor finali de acces nestingherit la informații. De exemplu, utilizatorii finali pot percepe o întârziere de o zecime de secundă în calcularea datelor ca fiind o supărare inutilă. Cu toate acestea, profesioniștii în securitatea informațiilor pot percepe acea zecime de secundă ca o întârziere minoră care permite o sarcină importantă, cum ar fi criptarea datelor.

Un sistem informatic este mult mai mult decât hardware de calculator; este întregul set de software, hardware, date, oameni, proceduri și rețele care fac posibilă utilizarea resurselor informaționale în organizație. Aceste șase componente critice permit introducerea, procesarea, ieșirea și stocarea informațiilor. Fiecare dintre aceste componente are propriile sale puncte forte și puncte slabe, precum și propriile caracteristici și utilizări. Fiecare componentă a sistemului informațional are și propriile cerințe de securitate.

Chiar și cu cea mai bună planificare și implementare, este imposibil să obții o securitate perfectă a informațiilor. Securitatea informației nu poate fi absolută: este un proces, nu un scop. Este posibil să faci un sistem disponibil oricui, oriunde, oricând, prin orice mijloc. Cu toate acestea, un astfel de acces nerestricționat reprezintă un pericol pentru securitatea informațiilor. Pe de altă parte, un sistem informatic complet sigur nu ar permite accesul nimănui. De exemplu, atunci când a fost provocat să obțină o certificare de securitate la nivel TCSEC C-2 pentru sistemul său de operare Windows, Microsoft a trebuit să elimine toate componentele de rețea și să opereze computerul doar de la consola dintr-o cameră securizată.[[1]](#footnote-1)

Pentru a atinge echilibrul - adică pentru a opera un sistem informatic care să satisfacă utilizatorul și profesionistul în securitate - nivelul de securitate trebuie să permită acces rezonabil, dar să protejeze împotriva amenințărilor.

Din cauza preocupărilor și problemelor de securitate de astăzi, un sistem informatic sau un departament de prelucrare a datelor se pot înrădăcina prea mult în managementul și protecția sistemelor. Un dezechilibru poate apărea atunci când nevoile utilizatorului final sunt subminate de o concentrare prea mare pe protejarea și administrarea sistemelor informaționale. Atât tehnologiile de securitate a informațiilor, cât și utilizatorii finali trebuie să recunoască faptul că ambele grupuri împărtășesc aceleași obiective generale ale organizației - pentru a se asigura că datele sunt disponibile când, unde și cum sunt necesare, oricărui sistem, în special un program de securitate a informațiilor, funcționează la nivelul așteptărilor în mediul în continuă schimbare în care este plasat.

**2. ACTIVITATEA SERVICIILOR DE INFORMAȚII ÎN CONTEXTUL GLOBALIZĂRII**

Globalizarea este un proces cu efecte multiple în toate domeniile existențiale, efecte a căror înțelegere este necesară deoarece schimbă fundamentele analitice cu care ne-am obişnuit, modificând percepții, comportamente și atitudini într-o largă varietate de opțiuni și cauzalități, ce pot fi traduse în beneficii sau dezavantaje. Modalitățile de cuantificare ale acestora diferă, la rândul lor, în funcție de interesele, obiectivele și cultura organizațională a instituțiilor care le abordează.

Globalizarea întruneşte poziții opuse ale suporterilor care o văd ca factor pozitiv de presiune în favoarea politicilor democratice și a economiei de piață, cu rezultate directe în ce privește o populație globală cu standarde de viață superioare și ale criticilor care consideră că globalizarea serveşte doar interesele corporațiilor transnaționale, subminează democrația, accelerează degradarea mediului înconjurător, impune omogenitatea culturală și duce la escaladarea stărilor de conflict. În plan filozofic, perspectiva realistă asupra globalizării apreciază că modalitatea în care aceasta influențează aspectele sociale, economice, culturale etc. modifică în mod critic sistemul internațional actual, în care statele sunt principalii actori în competiția pentru putere și influență, în timp ce curentul idealist privește acest proces ca fază superioară a evoluției sistemului internațional, în care actorii non-statali intră în competiție cu statele.

La nivel global, asimetriile generatoare de dezechilibre se regăsesc în multiple domenii de activitate. În economie, concentrarea progresului tehnic și tehnologic în țările dezvoltate, ca sursă principală a creșterii lor economice, vulnerabilitatea macroeconomică ridicată a țărilor în curs de dezvoltare la șocurile externe, precum și contrastul dintre gradul înalt de mobilitate a capitalului și mobilitatea internațională a muncii, în special forța de muncă necalificată, pot constitui surse de instabilitate (criză economică și socială) și produc situații de risc la adresa securității. Gestionarea economicului este puternic subordonată factorului politic, reverberațiile dezechilibrelor de natură economică găsindu-și o putermică reprezentare în stabilitatea și coeziunea comunităților.

Totodată, globalizarea reduce capacitatea statelor de a menține monopolul asupra informației și puterii, accentuează permeabilitatea granițelor și permite actorilor nonstatali să acumuleze capital. Organizațiile societății civile se dezvoltă și încep să acționeze global, fără intermedierea guvernelor naționale pe care le concurează ca reprezentate legitime în promovarea intereselor comunităților, mai puțin interesate de expresia politică, cât de acțiuni concrete care să le sprijine dezvoltarea și bunăstarea. Pentru a contracara această influență, sistemele politice naționale trebuie să dea dovadă de flexibilitate și să iși dezvolte capacități de acțiune coordonată/ integrată, să redevină exponente ale intereselor maselor largi (promovând o formă avansată, modernă, a modelului statului social) și să evite alienarea funcțională (înțelegând prin aceasta aservirea și subordonarea energiei politice unor scopuri pur clientelare).

Din definiția globalizării nu trebuie eliminată dimensiunea militară, care, în ultimii ani, s-a manifestat în special prin lupta împotriva terorismului și fenomenelor de insurgență, mai mult sau mai puțin asociate acestuia. În contextul globalizării, această interconectare și „afiliere" este un argument necesar și suficient pentru a putea afima că securitatea unei zone date este inseparabilă de securitatea globală. Cu toate formele tradiționale de luptă împotriva pericolelor și amenințărilor la adresa securității internaționale, alianțele militare sunt încă necesare eliminării factorilor și surselor de insecuritate ce se globalizează, simpla proiecție a puterii militare a statelor nu mai este suficientă. Conflictul, de orice natură, capătă noi caracteristici, suferind dezvoltări cărora statele și instituțiile internaționale nu sunt pe deplin pregătite să le facă față, dar la care reacționează printr-un adaptativ ad-hoc.

Putem afirma că, prin dimensiunile sale de manifestare, globalizarea crează germenii unor presiuni ce influențează mediul internațional de securitate, dar și modul în care percepția securității se reflectă la nivelul experiențelor de securitate fizică și spirituală ale fiecărui individ. În ansamblu, globalizarea conduce la o nouă structură internațională, divizată între acele țări care sunt integrate în economia globală și cele care fie sunt lăsate în urmă, fie se opun normelor unei noi ordini globale. Peisajul securității la nivel politico-militar este completat de trendurile globale privind creșterea populației, inegalitățile în dezvoltarea economică, urbanizarea, pandemiile, dezvoltările în domeniul biotehnologiei, aspectele ecologice și încălzirea globalā, scarcitatea resurselor, etc.

În acest context, principala provocare a perioadei post-război rece este, cu certitudine, reașezarea coordonatelor echilibrului de putere (în sens multidimensional) la nivel global. Perioada „unipolarității" (SUA ca principal agent de putere la nivel global) a constituit doar segmentul de tranziție care a reliefat nevoia de reformă în înțelegerea noilor repere ale interdependențelor dintre actorii arenei internaționale. Noua arhitectură de securitate se manifestă ca un teren competițional în care se redefinesc sisteme de referință, repere relaționale și niveluri de ambiție, în virtutea unor seturi de valori și interese mai mult sau mai puțin diferite, dar care poziționează statele în raport cu principalele entități "subiecte" și "obiecte" ale scenei relațiilor internaționale. Statele se definesc, din această perspectivă, ca puteri (tradiționale/ emergente) atribut dat de potențialul politic, economic, militar.

Din punct de vedere al solidității și maturității conceptuale, nivelul de referință fundamental îl constituie securitatea națională, pornind de la premiza atenției pe care statele o acordă balanței puterii și concurenței cu competitorii direcți (în cursa pentru resurse, influență, prezervarea valorilor, promovarea intereselor). La acest nivel, factorii generatori de crize politico-militare sunt bine conturați și se raportează la vulnerabilități și amenințări interne sau externe la adresa structurii și funcționalității sistemului statal manifestate paşnic sau prin recurgere la violență. Făcând o comparație între perioada războiului rece și etapa actuală distingem o dezvoltare și diversificare semnificativă a acestora în special în contextul globalizării, fapt ce antrenează nevoia de adaptare a instrumentelor de cunoaștere, a proceselor decizionale și a elementelor de suport (incluzând aici și spectrul Inteligenței). Statul îşi prezervă statutul de principal reper ca sistem de securitate la care se raportează ființa umană atunci când işi evaluează existența și perspectivele. Prin mecanismele complexe dezvoltate în timp, statul – într-o formulă a sa ideală - este garantul securităii fizice și demnității cetățenilor, promovând premizele bunăstării și asigurând libertatea individuală de exprimare și alegere.

Strategia de securitate națională îşi definește scopul ca vizând "atât prevenirea și contracararea pericolelor generate de mediul internațional, cât și garantarea stării de securitate internă, în ansamblul său, a siguranței personale și securității comunităților", cerințe raportate la aspecte privind: securitatea individuală, securitatea energetică și alimentară, securitatea transporturilor și a infrastructurii, securitatea sănătății publice, sanitară, ecologică și culturală, securitatea financiară, informatică și informațională.

Pe de altă parte, în condițiile în care resortul principal al globalizării rezidă în dezvoltarea economică, aspecte ca: accesul la resurse, securitatea căilor de transport, dezvoltarea capacităților de producție, asigurarea forței de muncă adecvate (nivel de calificare în balanță cu costul acesteia), găsirea și prezervarea de noi piețe de desfacere, transferul de bunăstare, pierderea exclusivităților, accesul la informație, duc la reconsiderarea distribuției rolurilor ierarhice ale statelor în sistemul relațiilor internaționale. Faptul că majoritatea manifestărilor violente pornesc de la motivații de natură etnico- religioasă teritorială și/sau ideologică, iar o relativă reducere a violenței militare este asociată cu creșterea violenței politice, economice și tehnologice reprezintă un argument în plus că toate aceste aspecte trebuie avute în vedere în cadrul analizelor stării de securitate. Procesul repoziționării statelor pe scena relațiilor politice internaționale are o puternică semnificație în plan intern. Dobândirea unor avantaje economice strategice, asigurarea unui nivel decisiv de influență în evoluția unor procese vitale, controlul procesualităților sistemice, prezervarea securității naționale (și reflectarea propriei securități la nivel regional și global), ca obiective ale politicilor internaționale, toate se reflectă în politica internă. Proiectarea acestor interese nu se poate rezuma însă strict la teritoriul național, situație în care echilibrul obținut ar fi unul precar, supus contagiunii vecinătăților și conexiunilor insecurizante. Securitatea fiecărei națiuni trebuie concepută în context mult mai larg, care acceptă anumite ierarhii și dinamici multidimensionale, dar nu și compromisuri care să alieneze spiritul "contractului social" pe care apartenența la o formă de organizare statală o presupune. Alianțele și aliații sunt esențiali în a gestiona aspectele de securitate ale globalizării, atât din perspectiva resurselor, cât și a succesului acestei intreprinderi.

În acest sens, dorim să subliniem predilecția pe care abordarea analitică a problemelor de securitate o are privind sistemele teritoriale regionale, în care abordarea individuală a problemelor de securitate ale unei națiuni ar fi lipsită de realism fără corelarea cu aspectele similare ale vecinătăților. Barry Buzan denumeşte aceste sistem teritorial "complex de securitate", în care interacțiunile militare, politice, economice, socio-culturale transced facilitate de realități geopolitice legăturile funcționale cu alte state, sub "cupola" globalizări. Dezvoltarea, la nivel global, a unui mare număr de organizații și agenții internaționale indică o atenție crescută a statelor cu privire la viața economică și socială a popoarelor. Sprijinul pe care statele și-l acordă bilateral sau multilateral capătă o importanță aparte, securitatea socială depășind tot mai mult barierele naționale, cunoscând succesiuni graduale ale dezvoltării către limite teritoriale regionale. Pe de altă parte, disfuncțiile interne sau cele de relaționare externă ale statelor se traduc în tensiuni care pot evolua în stări de criză sau chiar conflicte armate. Aceste distorsiuni ale stării de normalitate reclamă intervenția sistemelor de securitate configurate tocmai în vederea diminuării riscurilor identificate, de aici reieșind rolul pe care organizațiile internaționale interguvernamentale îl au în domeniul securității.

Organismele internaționale au un rol aparte în procesul de evaluare continuă a situației de securitate la nivel regional și global, prin analiza și reconsiderarea permanentă a priorităților de securitate regională și globală și adaptarea conceptelor de securitate în raport cu noile evoluții din toate domeniile de referință. În NATO, din perspectiva interesului pentru domeniul Inteligenței, sunt recunoscuți o serie de factori cheie ce își pun amprenta asupra dezvoltării acestei capabilități ca necesitate pentru asigurarea superiorității decizionale în caz de risc de securitate în oricare dintre domeniile: terorismul, statele ostile (în mod direct sau prin intermediari), statele fragile (sau în colaps), amenințările hibride, globalizarea (prin nucleele de instabilitate pe care le provoacă și caracterul transnațional al amenințărilor), fenomenele de mediu (dezastre naturale asociate cu urgențe umanitare și instabilitate) și proliferarea rachetelor balistice, a armamentului nuclear și a altor arme de distrugere în masă.

Începutul secolului XXI este dedicat eforturilor de a dezvolta forme de cooperare și politici de securitate care să răspundă globalizării insecurității, conștientizând, totodată, că globalizarea nu elimină preocupările geopolitice tradiționale. Pozițiile divergente, dar și nevoia atingerii une arii de consens, sunt puternic vizibile în cadrul forumurilor și summiturilor unde se întrunesc lideri-cheie ai planetei; aceștia sunt provocați să depășească sfera intereselor strict naționale (presiunile politice și sociale interne) și să adopte un limbaj politic global (o soluție de compromis), în care să încadreze propriile priorități. În acest sens, este evident că o capacitate adecvată de control și gestiune a securității presupune previziune, anticipare; orice politică de acțiune trebuie să se bazeze pe predicții logice, coerente, plauzibile.

Doctrina britanică evaluează o serie de factori care afectează capabilitatea Inteligenței în mediul operațional contemporan. O primă particularitate o reprezintă faptul că palierele tactic, operațional și strategic sunt permeabile în ce privește accesul la informație și relevanța acesteia. Operatorii care îşi desfășoară activitatea la nivel tactic pot oricând obține informații de importanță strategică. Pe de altă parte, elementele de sprijin și coordonare din afara teatrului de operații (reach-back) permit forțelor dislocate accesarea de expertiză și servicii suplimentare din centre sau organizații aflate la depărtare (Inteligența strategică).

Capacitatea de a influența mediul operațional, tradusă în abilitatea de păstra inițiativa și controlul, permite atingerea efectelor dorite prin diferite mijloace de putere, "soft" sau "hard" ,iar produsele de Inteligență fundamentează opțiunile factorilor de decizie. Mecanismele de angajare în domeniul culegerii de informații depăşesc referința paradigmei clasice a securității, în virtutea căreia serviciile de Inteligență, în efortul lor de a promova interesele naționale, urmăreau exclusiv penetrarea până la cel mai înalt nivel a instituțiilor străine în vederea determinării intențiilor și capabilităților acestora. În plan global, s-a produs o mutație a intereselor dinspre zona geopolitică spre cea geoeconomică, abilitatea statului constând acum în gestionarea cunoașterii la nivel strategic pentru sectorul administrației publice, al economiei, al educației, al cercetării și al bunăstării sociale. Bineînțeles, acest fapt nu exclude importanța sectorului de securitate și apărare, însă abordarea acestor aspecte suferă o mutație.

Reducerea resurselor în acest sector în favoarea celor emergente se poate baza pe cooperare și punerea în comun a resurselor. Colectarea și diseminarea informațiilor, raportat la conceptul extins al securității naționale ia în considerare nivelul de percepție a amenințărilor și răspunsul politic la acestea (folosirea forței militare sau a amenințării cu forța, agresiune asimetrică) pentru impunerea voinței sau apărarea intereselor naționale. În aceste condiții, managementul și exploatarea informației devine decisivă în ce privește maximizarea potențialului fluxului de informații, în baza unor principii solide și eficiente ale sistemului de diseminare.

Alte probleme identificate în efortul de colectare țin atât de factorii calitativi (credibilitatea sursei și veridicitatea informației, pregătirea și experiența personalului, nivelul de actualizare a tehnologiilor, proceduri, managementul informației), cât și de cei cantitativi (acoperirea efectivă în timp și spațiu a domeniului informațional, capabilități de culegere, rețele de colaborare). În acest cadru, consolidarea culturii de securitate în rândul populației devine o necesitate. Aceasta duce la conștientizarea riscurilor și responsabilizarea actorilor societății civile, cu ecou în acțiunea civică, dar și în ce privește asigurarea cadrului interdisciplinar și pan-regional al schimbului de informații.

**3. ASIGURAREA SECURITĂȚII INFORMAȚIONALE ÎN REPUBLICA MOLDOVA**

Tehnologiile informaționale, resursele de informare şi sistemele de comunicare electronică, au devenit parte indispensabilă a tuturor domeniilor de activitate a persoanei, societății și statului. Prin dezvoltarea accelerată, tehnologiile informaţionale contribuie la transformări sociale de esenţă, fiind generatorul apariţiei şi consolidării societăţii informaţionale, de nivel naţional, regional şi internaţional, ce depăşesc cadrul juridic al frontierelor de stat sau comunităţi de state. Spaţiul informaţional a devenit un domeniu vital de activitate pentru stat, economie, ştiinţă, societate şi individ, un spaţiu nou de reglementare a drepturilor şi libertăţilor fundamentale ale omului, cu implicare directă şi indirectă asupra mecanismelor de asigurare a politicilor de securitate şi apărare naţională într-o societate democratică.

Etapa actuală de dezvoltare a Republicii Moldova, ca stat suveran, independent, democrat și de drept, se caracterizează prin dezvoltarea și răspândirea rapidă a tehnologiilor informaționale, prin rolul sporit al domeniului informational ce include totalitatea informației, infrastructurii informaționale și de telecomunicații, a subiecților care efectuează colectarea, formarea, răspândirea și utilizarea informației sistemului ce reglementează relații sociale apărute în acest sens. Pe parcursul ultimului deceniu, Republica Moldova a realizat mai multe strategii, programe şi politici de ţară, pentru dezvoltarea societăţii informaţionale la nivel naţional, în conformitate cu recomandările forurilor europene şi internaţionale din domeniul tehnologiilor informaționale și comunicaţiilor electronice, drepturilor şi libertăţilor fundamentale ale omului în mediul on-line şi off-line.

Potrivit Raportului anual cu privire la monitorizarea evoluției societății informaționale la nivel mondial „Measuring the Information Society 2017”, lansat de Uniunea Internațională a Telecomunicațiilor, Republica Moldova este plasată pe locul 59 din 176 de state incluse în clasament. La nivel european, Republica Moldova a avansat față de media globală și din regiune, fiind printre primele 10 state cu cele mai dinamice evoluții la nivel mondial. Sunt implementate sau în proces continuu de dezvoltare peste 21 de programe şi proiecte on-line de infrastructură şi servicii publice digitale, lansate strategii sectoriale în domeniul tehnologiei informației şi politici de modernizare tehnologică a guvernării.

Interacțiunea tehnologiilor informaţionale, cu diversitatea conţinutului informaţional pe de o parte şi fuziunea reţelelor de comunicare publică şi socială, cu sistemele electronice guvernamentale, de cealaltă parte, contribuie la o extindere şi sinergie a spaţiului informaţional, cu domeniile centrale de securitate şi apărare naţională, responsabile de asigurarea suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

Republica Moldova, în calitate de parte integrantă a spațiului European, parcurge un process de tranziție, către o societate de tip informațional. Potrivit prevederilor Acordului de Asociere între Republica Moldova, pe de o parte, și Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de altă parte, sunt stabilite priorități de încurajare și promovare a punerii în aplicare a instrumentelor tehnologiilor informației și comunicațiilor pentru o mai bună guvernare, e-learning și cercetare, servicii publice de asistență medicală, digitizarea patrimoniului cultural, dezvoltarea conținutului digital și a comerțului electronic, precum și îmbunătățirea nivelului de securitate a datelor cu caracter personal și a protejării confidențialității în comunicațiile electronice.

Pentru Republica Moldova, securitatea informațională este un domeniu relativ nou. Legislația naţională în vigoare nu stipulează nicio prevedere privind securitatea informaţională. În conformitate cu decretul prezidenţial nr. 374-IV din 22.12.2005, două comisii naţionale, formate din înalţi demnitari de stat, urmau să elaboreze Concepţia securităţii naţionale. Documentul respectiv trebuia să substituie Concepţia adoptată prin hotărârea Parlamentului nr. 445-XIII din 5.05.1995. Însă nici în documentul elaborat în 2005 printre pericolele estimate la adresa Republicii Moldova nu s-a regăsit influenţa mediatică din exterior sau lipsa controlului asupra spaţiului informaţional în unele teritorii ale ţării.

Într-o societate modernă, în care mediul online facilitează comiterea infracțiunilor cibernetice, importanța și necesitatea protecției intereselor societății și a statului de frecventele amenințări la adresa securității informaționale, sunt primordiale pentru Serviciul Tehnologia Informației și Securitatea Cibernetică – pilonul de bază în vederea creării și dezvoltării unei societăți informaționale avansate și protejate.

Instituția Publică "Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC) a fost creată în anul 2018 prin reorganizarea Întreprinderii de Stat „Centrul de Telecomunicații Speciale” și absorbția Întreprinderea de Stat „Centrul Informațional Agricol”, conform Hotărârii Guvernului Nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.[[2]](#footnote-2) În calitate de operator al serviciilor electronice guvernamentale, STISC are misiunea de a asigura administrarea, menținerea și dezvoltarea infrastructurii de tehnologie a informației, Sistemului de telecomunicaţii al autorităţilor administraţiei publice, ca parte a reţelei de comunicaţii speciale și a sistemelor informaționale de stat, gestionarea infrastructurii unice a cheii publice a Guvernului, precum și implementarea politicii statului în domeniul securității cibernetice.

La sfârșitul anului 2019, conform Hotărârii Guvernului Nr. 425 din 30.08.2019 cu privire la reorganizarea prin fuziune a Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” și a Întreprinderii de Stat „MoldData”[[3]](#footnote-3), toate bunurile Întreprinderii de Stat „MoldData” proprietate a statului, au fost transmise Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” în conformitate cu Regulamentul cu privire la modul de transmitere a bunurilor proprietate publică, aprobat prin Hotărârea Guvernului nr. 901/2015. Domeniile de competență ale Serviciului sunt următoarele[[4]](#footnote-4):

1. Administrarea infrastructurii de tehnologie a informației și a Sistemului de telecomunicaţii al autorităţilor administraţiei publice ca parte a reţelei de comunicaţii speciale;
2. Administrarea și menținerea sistemelor informaționale de stat;
3. Securitate cibernetică;
4. Gestionarea infrastructurii unice a cheii publice (PKI) a Guvernului;
5. Implementarea tehnologiilor informaționale în sectorul public.

În vederea asigurării unui sistem de protecție și dezvoltare a spațiului informațional în condițiile globalizării și liberei circulații a informațiilor, a fost adoptată Strategia de Securitate informațională pentru anii 2019-2024. Strategia prezintă o evaluare a situației actuale în domeniul securității informaționale, enumeră performanțele înregistrate și punctează noi tendințe de dezvoltare a societății informaționale, acestea constituind obiective de preocupare majoră a STISC-ului. Complexul de acțiuni, conform scopului și obiectivelor specificate sunt compartimentate pe patru piloni:

1. Pilonul I – Asigurarea securității spațiului informational-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.

Rolul Serviciului Tehnologia Informației și Securitate Cibernetică este de a asigura protecție în spațiul informational prin realizarea acțiunilor de consolidare a capacităților de apărare cibernetică și de combatere a criminalității informatice. Printre acțiunile de bază ale STISC-ului prevăzute în Planul de acțiuni, se enumeră următoarele:

* + Sistematizarea, analiza și evaluarea datelor statistice la capitolul securității cibernetice;
  + Determinarea politicii privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale;
  + Dezvoltarea capacităților de reziliență cibernetică și ridicarea nivelului de cultură în TIC;
  + Desfășurarea acțiunilor de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile securității cibernetice;
  + Desfășurarea exercițiilor și antrenamentelor de consolidare a capacităților de reacție la atacuri cibernetice, inclusive blocarea atacurilor cibernetice simulate;
  + Organizarea și efectuarea atelierelor de lucru în domeniul securității cibernetice.

Principalele documente de politici existente la momentul elaborării prezentei Strategii, valabile până în anul 2020, tangențiale dimensiunii securității informaționale, care urmează să transpună la nivel național modelul European de dezvoltare a societății informaționale sunt: Strategia națională de dezvoltare a societății informaționale Moldova Digitală 2020 și Programul național de Securitate cibernetică a Republicii Moldova pentru anii 2016-2020. Până în prezent, la nivel național nu au fost efectuate procese de audit complexe de Securitate cibernetică, nu există studii sau rapoarte care ar reflecta în detalii situația privind criminalitatea informatică, cât și numărul victimelor și prejudiciilor economice ale materializării acestora.

Una dintre problemele de bază este lipsa unui sistem integrat de management al securității cibernetice, în cadrul căruia să se efectueze coordonat planificarea și utilizarea resurselor disponibile, identificarea vulnerabilităților și riscurilor în urma auditului de Securitate cibernetică, a intervențiilor necesare pentru diminuarea imactului dăunător al criminalității, atacurilor și incidentelor cibernetice asupra dezvoltării sigure a societății informationale. O altă problemă majoră este lipsa unei entități, la nivel național, de tip CERT (Centru de reacție la incidente de securitate cibernetică) responsabilă pentru prevenirea și reacția la incidente din domeniul securității cibernetice, prin coordonarea, planificarea și utilizarea resurselor disponibile, identificarea vulnerabilităților și riscurilor în urma auditului de securitate cibernetică, a intervențiilor necesare pentru diminuarea impactului dăunător al criminalității, atacurile și incidentele cibernetice asupra dezvoltării sigure a societății informaționale. Lipsa unui sistem integrat de management al securității cibernetice la nivel național, generează și lipsa datelor complete, veritabile, actualizate și structurate, ceea ce, la rândul său, creează obstacole în identificarea de soluții optime.

Asigurarea prevenirii riscurilor și combaterii amenințărilor în adresa securității informaționale este una din sarcinile de bază ale statului, implementate prin instituțiile sale de drept, astfel fiind determinate următoarele probleme care necesită a fi abordate la nivel național:

* + Insuficiența specialiștilor calificați în domeniul tehnologiilor informaționale și nivelul redus de salarizare în special în sectorul public;
  + Lipsa programelor de instruire specializate dedicate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, specialiștilor și experiților judiciari în domeniu din cadrul structurilor de aplicare a legii precum și celor dedicate personalului ethnic din cadrul instituțiiilor publice în domeniul securității cibernetice;
  + Dotarea insuficientă cu echipament și soft-uri specializate dedicate investigării infracțiunilor informatice;
  + Finanțarea redusă pentru participarea specialiștilor la proiecte și evenimentele internaționale de consolidare a capacităților și schimbului de bune practici.[[5]](#footnote-5)

Asigurarea securității informaționale a statului constituie o prioritate pentru securitatea națională, fiind un obiectiv statuat în mai multe acte legislative și normative ale Republicii Moldova și necesită o finanțare suficientă. Necesitatea stringentă a protejării securității spațiului informațional național este conștientizată atât la nivelul autorităților publice, cât și reprezintă un deziderat al societății civile. La etapa actuală, propaganda, dezinformarea și informarea manipulatoare sunt extrem de dinamice, iar resursele alocate în acest scop de către terți, depășesc cu mult capabilitățile de răspuns și combatere a fenomenului dat ale Republicii Moldova. Pentru a face față provocărilor, Republica Moldova beneficiază de suportul Uniunii Europene, care pentru următorii ani și-a majorat bugetul pentru combaterea propagandei și a dezinformării, un accent separate fiind plasat și pe statele membre ale Parteneriatului Estic.

**CONCLUZII**

Tehnologiile informaţionale generează modificări a dimensiunii de informare şi comunicare, care se transformă într-un ritm accelerat într-o platformă multimedia, fiind dezvoltate noi componente şi mijloace de comunicare on-line şi off-line, iar libera circulaţie a informaţiilor şi ideilor la nivel local, regional şi global, devin un imperativ pentru crearea şi promovarea unei societăţi informate într-un stat democratic şi de drept.

Tendinţele de dezvoltare continuă a interacțiunii dimensiunii tehnologice cu dimensiunea de informare, în toate formele de structură şi funcţionare, de natură individuală, publică, privată sau de stat, de factură naţională sau globală, conduce la apariţia unei noi configuraţii de comunicare şi schimb de date pe domeniile publice și private de care depinde nivelul şi starea sectorială sau generală de securitate.

Pe lângă beneficiile incontestabile a tehnologiei moderne, spaţiul informaţional este supus unui șir de vulnerabilități, riscuri şi ameninţări de securitate, facilitând competiţia injustă, confruntarea şi spionajul, dezinformarea şi propaganda, terorismul şi criminalitatea, iar încălcările de confidenţialitate duc la răspândirea de noi forme de ură şi incitare la violenţă, în special pe motive de gen, rasă, naţionalitate, origine etnică, limbă, religie, apartenenţă politică sau pe orice alt criteriu care rămân subestimate şi rareori remediate sau contracarate.

Dezvoltarea infrastructurii informaționale, în curs de globalizare, în care se includ și structurile mediatice generează posibilități de comunicare din ce în ce mai sofisticate. Noțiunea de război clasic cedează terenul războiului informațional, care deja are mai multe forme/dimensiuni de manifestare: război psihologic, război imagologic, război de comandă-control, război electronic.

Domeniile politic, economic, social și militar sunt ținte ale războiului informațional care tinde, în mod special, influențarea proceselor decizionale. În aceste condiții, asigurarea securității informaționale este esențială pentru a întări discernământul social, atașamentul și interesul societății. Asigurarea securității informaționale este necesară și pentru contracararea supra-comunicării și abuzului informațional, care duc la noncomunicare și pseudo-comunicare, elemente ce generează rupturi sociale și dezechilibre în societatea civilă.

Propagarea informaţiei, fără a ține seama de limitele frontierelor naţionale, pe lângă efectele evident benefice, poate duce la sporirea capabilităţii de influenţă din partea actorilor străini guvernamentali sau neguvernamentali cu resurse suficiente.

Crimele cibernetice, spionajul, propaganda, diversiunea şi exploatarea excesivă a datelor cu caracter personal prin reţelele de comunicații electronice, sunt utilizate ca instrumente de bază la toate etapele de concepere a unei amenințări hibride de securitate şi cheamă la un răspuns colectiv şi reglementat, bazat pe mecanisme şi acţiuni coordonate, de implementare a politicilor din domeniu, asistenţă tehnică şi legală din perspectiva imperativelor de securitate, orientat la crearea unui mediu informaţional favorabil şi sigur pentru cetăţean, pentru mediul de afaceri de orice nivel şi pentru stat.

În cadrul societății informaționale, a estima puterea și viabilitatea sistemului de securitate națională fără a lua în considerare sistemele informaționale și modul de exploatare a informației (colectarea, protecția, transportul, managementul și îngrădirea accesului la informație) reprezintă un risc major, deoarece centrul de greutate al acțiunilor tinde să se deplaseze dinspre dimensiunea materială spre cea informațională. Pe de o parte, utilizarea tehnologiei informației oferă o creștere semnificativă a puterii și viabilității sistemului de securitate națională, iar pe de altă parte reprezintă un factor de risc în situația neprotejării infrastructurii informaționale.

Riscurile din spațiul cibernetic sunt proporționale cu gradul de informatizare a societății, iar combaterea fenomenului de criminalitate cibernetică trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi. Mediul virtual facilitează comiterea infracțiunilor, pune la dispoziţia conduitei criminale atât un nou obiect (informaţia conţinută şi procesată de sistemele informatice), cât şi un nou instrument. Acesta oferă un repertoriu vast de tehnici şi strategii de săvârșire a infracţiunilor, generând tendințe noi de infracţiuni.

Totodată, natura globală a sistemelor informaţionale şi a reţelelor de comunicaţii electronice, precum şi natura transnaţională a criminalităţii informatice necesită o coordonare strânsă între toate instituţiile responsabile atât la nivelul naţional, cît şi la nivel global.

**BIBLIOGRAFIE**

BARBA L. Securitatea spațiului informational – componentă a securității statului. Institutul Integrare Europeană și Științe Politice al AȘM. p. 86-90

COSMOIU, Florin (2013) Cyber threats a Romanian p. de BEAUPRÉ, Adrien, HELLBERG, Natasha (2012) Developing Cyber Threat Intelligence.or not failing in battle, Intru-Shun.ca Inc., AtISecCon

Documentul sinteză al SRI privind prioritățile strategice pe termen mediu ale ordonatorilor principali de credite pentru anul 2013 și perspectiva 2014-2016, <http://discutii.mfinante.ro/static/10/Mfp/proiect_buget2013/SRLpdf> (vizitat: 28.11.2021)

Financial Services Information Sharing and Analysis Center/ FS-ISAC (2013) Evolution and Revolution of Cyber Threat Intelligence, <http://www.nymissa.org/wp-content/uploads/2013/02/FSISAC-EVOLUTION-CYBER-THREAT-INTEL-201303020-final-santized.pdf> (vizitat: 28.11.2021)

Guvernul României, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a Romániei și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, publicat in Monitorul Oficial, Partea I nr. 296 din 23.05.2013 6. H.G. 494 /11 Mai 2011

HATNEANU D. O., VIDAICU M. Securitatea națională și accesul la informație în Republica Moldova. Raport de compatibilitate a legislației Republicii Moldova cu principiile globale privind securitatea națională și dreptul la informare. Institutul de Politici Publice. Chișinău. 2005.

Hotărârea Guvernului nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat. Disponibil: <https://www.legis.md/cautare/getResults?doc_id=119166&lang=ro> (vizitat: 28.11.2021)

Hotărârea Guvernului Nr. 425 din 30.08.2019 cu privire la reorganizarea prin fuziune a Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” și a Întreprinderii de Stat „MoldData”. Disponibil: <https://www.legis.md/cautare/getResults?doc_id=116725&lang=ro> (vizitat: 28.11.2021)

Intelligence and National Security Alliance/ INSA (2011) Cyber intelligence: Setting the landscape for an emerging discipline, [http://www.insaonline.org/d/a/Resources Cyber\_Intelligence.aspx](http://www.insaonline.org/d/a/Resources%20Cyber_Intelligence.aspx) (vizitat: 28.11.2021)

Intelligence and National Security Alliance (2014) Strategic Cyber Intelligence is Essential to Business Security, [http://www.insaonline.org/i/fipr/2014/03.27.14 StrategicCyber.aspx](http://www.insaonline.org/i/fipr/2014/03.27.14%20StrategicCyber.aspx) (vizitat: 28.11.2021)

Klimburg, Alexander (Ed.) (2012) National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn LEE, Robert M. (2014a)

Securitatea Informațională 2013. Conferință Internațională. Ediția a X-a Jubiliară. Laboratorul de Securitate Informațională al ASEM. Chișinău. 2013.

Serviciul Tehnicologia Informației și Securitatea Cibernetică. Direcții de activitate. Disponibil: <https://stisc.gov.md/ro/directii-de-activitate> [vizitat: 28.11.2021]

Strategia Securității Informaționale a Republicii Moldova pentru anii 2018-2023. Disponibil: <https://gov.md/sites/default/files/document/attachments/intr23_86.pdf> (vizitat: 28.11.2021)

WHITMAN, Michael E.; MATTORD, Herbert J. Principles of information security. Cengage learning, 2011.

1. WHITMAN, Michael E.; MATTORD, Herbert J. Principles of information security. Cengage learning, 2011. [↑](#footnote-ref-1)
2. Hotărârea Guvernului nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat. Disponibil: <https://www.legis.md/cautare/getResults?doc_id=119166&lang=ro> (vizitat: 28.11.2021). [↑](#footnote-ref-2)
3. Hotărârea Guvernului Nr. 425 din 30.08.2019 cu privire la reorganizarea prin fuziune a Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” și a Întreprinderii de Stat „MoldData”. Disponibil: <https://www.legis.md/cautare/getResults?doc_id=116725&lang=ro> (vizitat: 28.11.2021) [↑](#footnote-ref-3)
4. Serviciul Tehnicologia Informației și Securitatea Cibernetică. Direcții de activitate. Disponibil: <https://stisc.gov.md/ro/directii-de-activitate> [vizitat: 28.11.2021] [↑](#footnote-ref-4)
5. Strategia Securității Informaționale a Republicii Moldova pentru anii 2018-2023. Disponibil: <https://gov.md/sites/default/files/document/attachments/intr23_86.pdf> (vizitat: 28.11.2021) [↑](#footnote-ref-5)