Universitatea de Stat din Moldova

Analiza şi prognoza obiectivă şi multilaterală a amenințărilor la adresa securității informaționale a Republicii Moldova

Elaborat: Sanduleac Adrian

Chișinău, 2023

O **analiză** obiectivă și multilaterală a amenințărilor la adresa securității informaționale a Republicii Moldova implică evaluarea diferitelor aspecte care pot afecta această securitate. Aceasta ține cont de contextul geopolitic, vulnerabilitățile tehnologice, factorii sociali și economici.

Domeniile cheie sunt:

1.CIBERNETIC:

Atacuri cibernetice - Republica Moldova se confruntă cu riscul de atacuri cibernetice asupra infrastructurii critice, instituțiilor guvernamentale și sectorului privat. Aceste atacuri pot varia de la malware și ransomware la atacuri de tip DDoS (atacuri distribuite de denegare a serviciului).

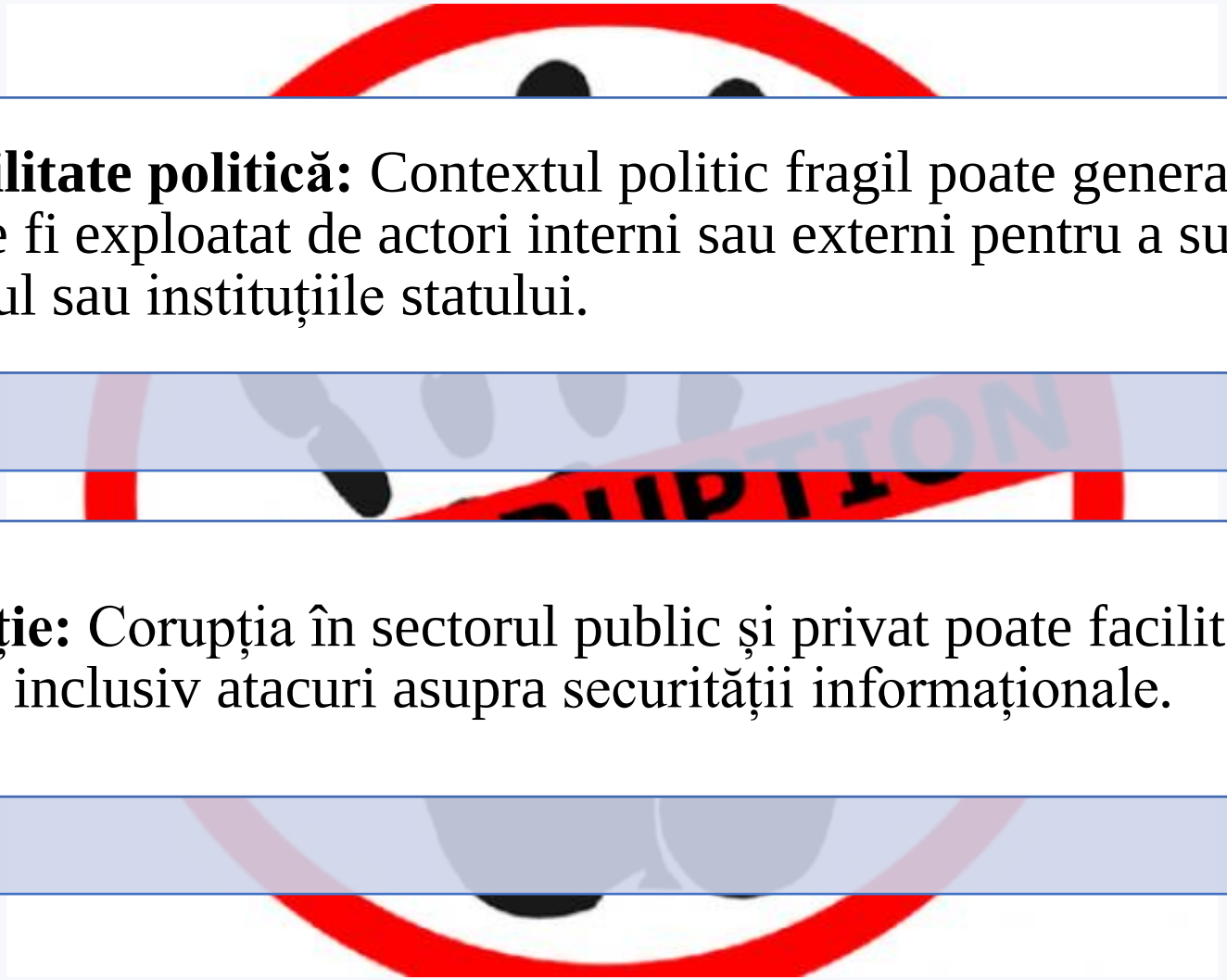
Spionaj cibernetic -Activități de colectare de informații sensibile prin intermediul atacurilor cibernetice, care pot afecta securitatea națională și economică.

2. MANIPULARE INFORMAȚIONALĂ:

Propagandă și dezinformare - Există riscul ca informații false să fie răspândite pentru a influența opinia publică și pentru a crea diviziuni în societate.

Atacuri asupra mediului online - Manipularea discuțiilor online și utilizarea rețelelor sociale pentru a disemina informații false sau pentru a spori tensiunile sociale.

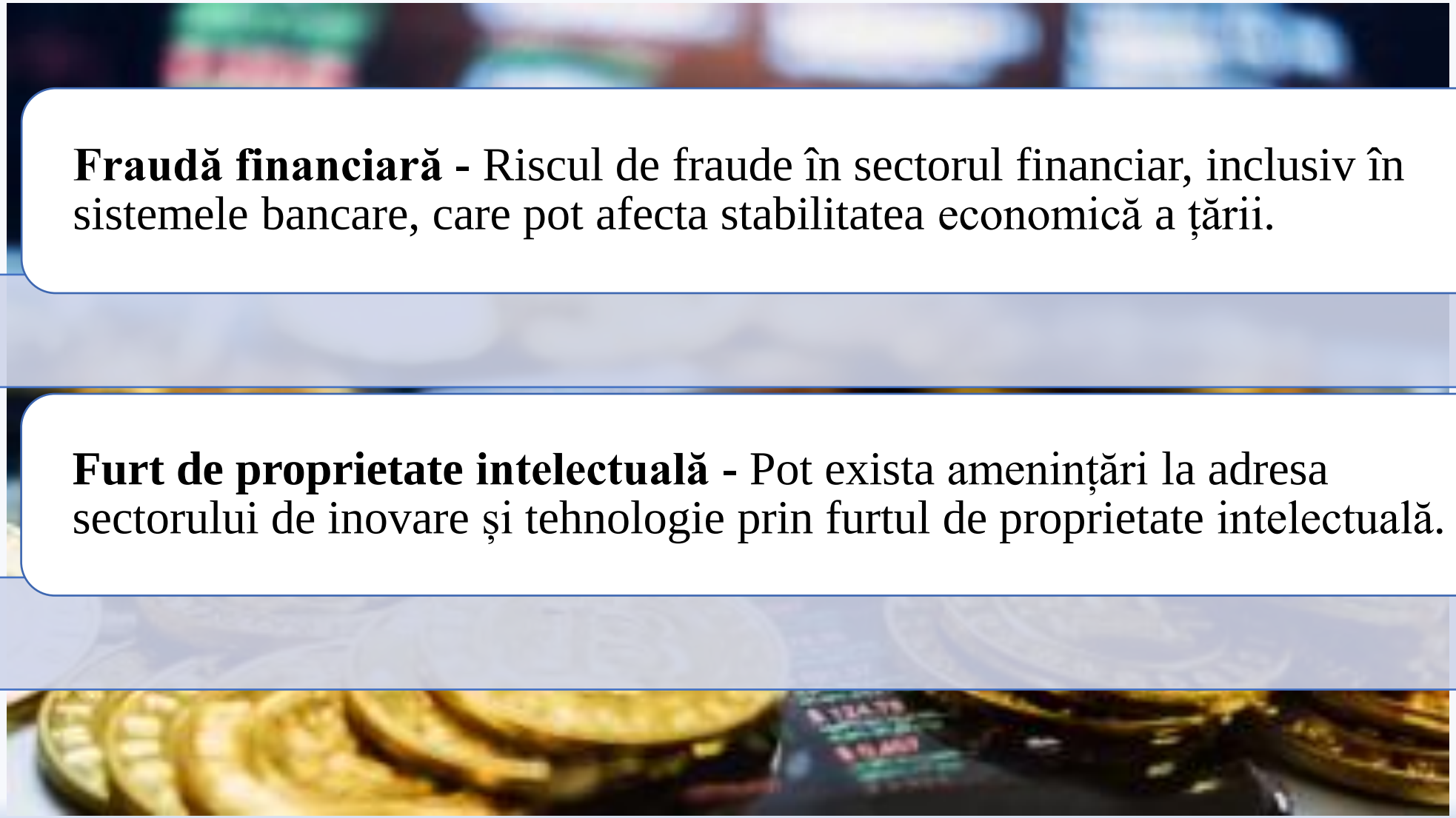
3. VULNERABILITĂȚI POLITICE ȘI SOCIALE:



Instabilitate politică: Contextul politic fragil poate genera vulnerabilități și poate fi exploatat de actori interni sau externi pentru a submina guvernul sau instituțiile statului.

Corupție: Corupția în sectorul public și privat poate facilita activități ilegale, inclusiv atacuri asupra securității informaționale.

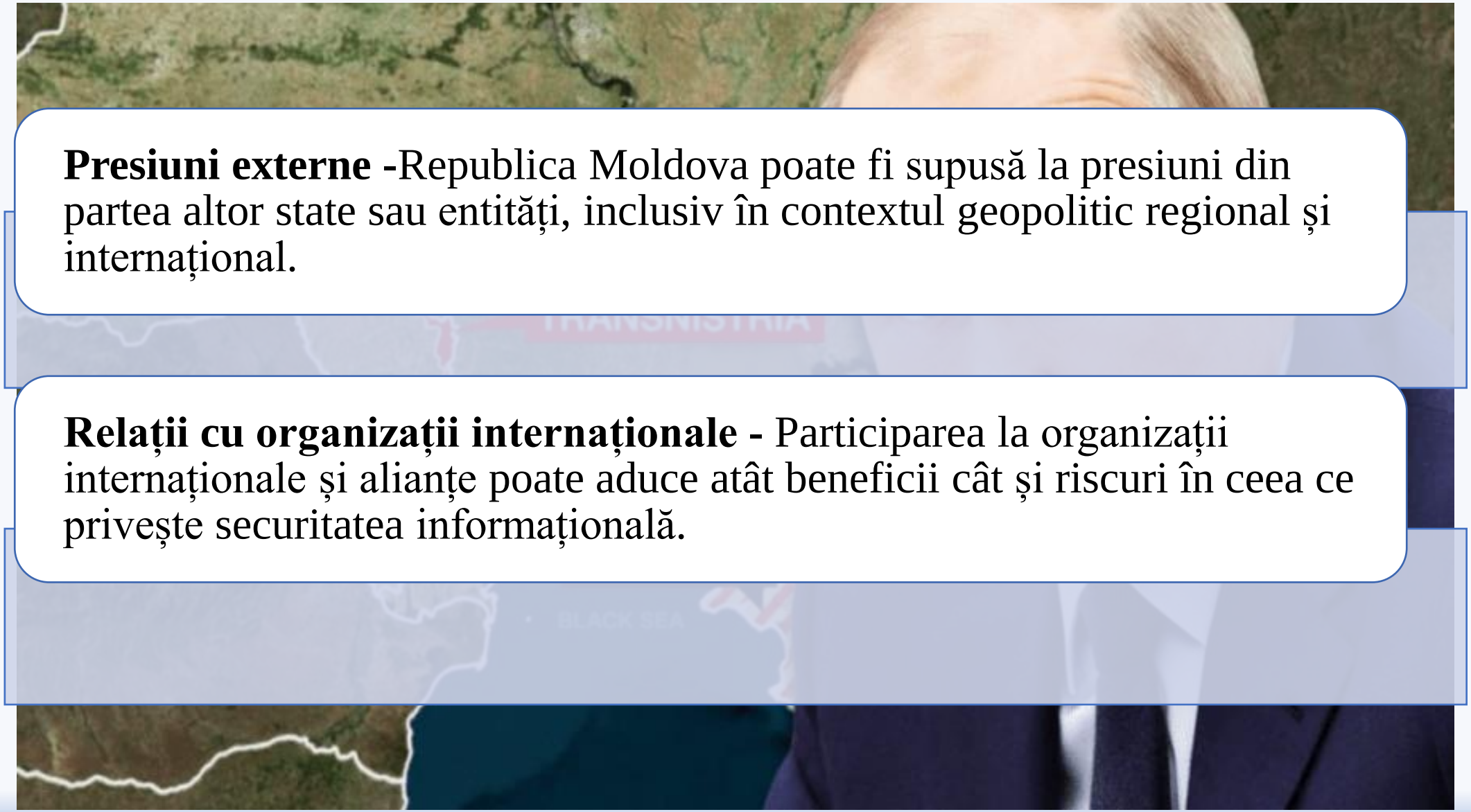
4. ECONOMIC



Fraudă financiară - Riscul de fraude în sectorul financiar, inclusiv în sistemele bancare, care pot afecta stabilitatea economică a țării.

Furt de proprietate intelectuală - Pot exista amenințări la adresa sectorului de inovare și tehnologie prin furtul de proprietate intelectuală.

5. RELAȚII GEOPOLITICE



Presiuni externe -Republica Moldova poate fi supusă la presiuni din partea altor state sau entități, inclusiv în contextul geopolitic regional și internațional.

Relații cu organizații internaționale - Participarea la organizații internaționale și alianțe poate aduce atât beneficii cât și riscuri în ceea ce privește securitatea informațională.

Conform unei analize Reuters, Republica Moldova a avut pe parcursul ultimului an (2023) peste

- **400 de alerte cu bombă,**
- **o tentativă eșuată de lovitură de stat,**
- **atacuri cibernetice,**
- **notificări false pentru recrutare, manifestații anti-guvernamentale în masă**.

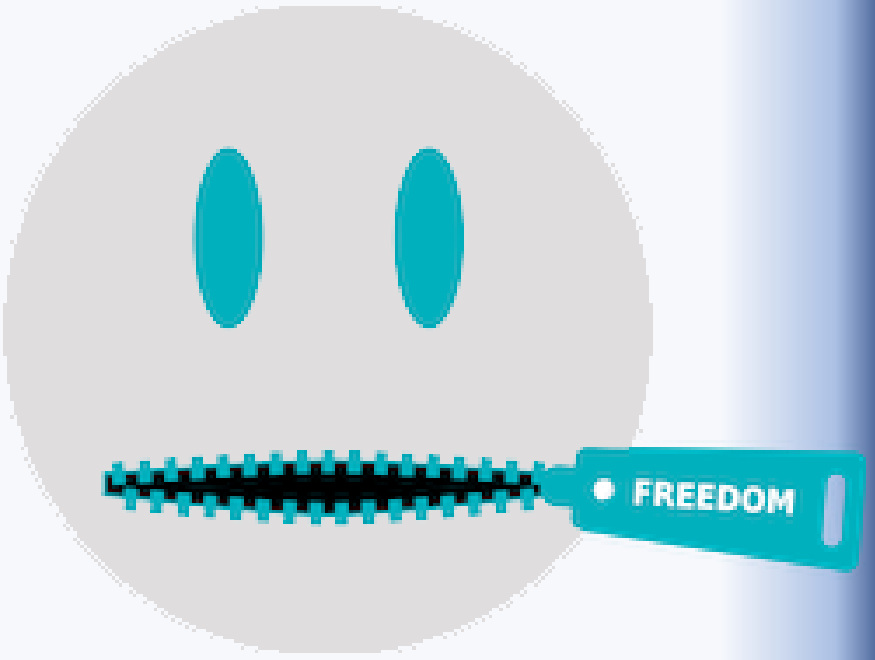
Toate desfășurare sub coordonarea directă a Moscovei.

În Republica Moldova, propaganda rusă a încercat, de asemenea, să resusciteze tema implicării guvernării pro-europene în războiul din Ucraina, mai ales în cazul în care Chișinăul ar fi oferit orice sprijin militar Ucrainei.

Aceste acțiuni fac parte dintr-un efort mai larg de destabilizare a regiunii cu scopul de a genera alte valuri de incertitudine cu privire la poziția și rolul Moldovei în securitatea regională.

În Republica Moldova **libertatea de exprimare**, în special în spațiul online, **se află într-un moment critic**. Potrivit Oficiului Avocatului Poporului, în perioada pandemiei în anul 2020 s-a înregistrat o „înrăutățire continuă” a situației în domeniul libertății de exprimare, inclusiv lipsa „progresului” în ceea ce privește dreptul de acces la informație.

Această tendință a fost evidentă în martie-iunie 2020 și martie-aprilie 2021, când Parlamentul a declarat stare de urgență din cauza pandemiei de coronavirus. Serviciul de Informații și Securitate (SIS) a blocat în mod unilateral zeci de site-uri noi invocând diseminarea de către acestea a știrilor false despre pandemia de COVID-19. Prin aceste măsuri, autoritățile Republicii Moldova au încălcat dreptul internațional la libera exprimare și dreptul de a „căuta, primi și transmite informații și idei”.



În rezultatul expertizei și analizei statistice a activității legislative din ultimii ani s-a constatat că Republica Moldova a adoptat o abordare strictă în procesul de elaborare a cadrului normativ de reglementare a spațiului online, pe alocuri fără a ține cont de experiența și recomandările internaționale în domeniu.

Proiectele de legi înaintate conțineau formulări extrem de generale și nu prevedeau criterii clare pentru interferența în drepturi și libertăți, crescând astfel riscul de interpretare greșită și abuz al legislației.

Mai mult decât atât, procesul de elaborare a cadrului normativ pe aceste subiecte nu întotdeauna a fost transparent pentru public. De exemplu, un proiect înaintat de Ministerul Justiției în iulie 2020 care are scopul de contracarare a fenomenului răspândirii informațiilor false care afectează securitatea națională până la momentul actual nu a fost supus consultărilor publice.

De asemenea, societatea este în așteptarea **proiectului Codului digital**, care promite să sistematizeze și să unifice reglementările în domeniul tehnologiei informației și să elimine un șir de probleme ce țin de securitatea informațională.

Prognoza amenințărilor la adresa securității informaționale a Republicii Moldova implică evaluarea potențialelor evoluții viitoare și identificarea tendințelor care pot afecta securitatea informațională a țării.

Prognoza potențialelor evoluții la adresa securității informaționale:

- **Cibernetică avansată**

Creșterea complexității și sofisticării atacurilor cibernetice, inclusiv utilizarea de tehnologii avansate precum inteligența artificială pentru a spori eficacitatea atacurilor.

- **Manipularea informațională**

Extinderea utilizării manipulării informaționale și a dezinformării, cu accent pe influențarea deciziilor politice, modelarea opiniilor publice și crearea de tensiuni sociale.

- **Amenințări geopolitice persistente**

Păstrarea amenințărilor din partea actorilor statali sau non-statali interesați în influențarea direcției politice și economice a Republicii Moldova.

Prognoza potențialelor evoluții la adresa securității informaționale(continuare):

- **Ransomware și extorcare digitală**

Continuarea creșterii atacurilor de tip ransomware și a cererilor de răscumpărare în schimbul datelor sau a accesului la sisteme informatice.

- **Vulnerabilități în infrastructura critică**

Expunerea la amenințări asupra infrastructurii critice, cum ar fi rețelele energetice, de transport și de comunicații, cu potențial impact asupra stabilității țării.

- **Evoluții tehnologice și Internet of Things (IoT)**

Creșterea numărului de dispozitive IoT și a altor tehnologii conectate, aducând cu sine noi vulnerabilități și riscuri de securitate.

Modalități de contracarare a amenințărilor la adresa securității informaționale a Republicii Moldova

❑ **Colaborare internațională și reglementare**

Creșterea eforturilor de colaborare internațională pentru combaterea amenințărilor cibernetice, împărtășind informații și dezvoltând norme și reglementări comune.

❑ **Educație și conștientizare**

Dezvoltarea unor programe educaționale și de conștientizare pentru a crește nivelul de cunoștințe și vigilență în rândul populației, companiilor și instituțiilor guvernamentale.

❑ **Sprijin pentru cercetare și inovație în securitatea cibernetică**

Investiții în cercetare și inovație pentru a dezvolta tehnologii și strategii avansate pentru contracararea amenințărilor cibernetice.

Mulțumesc pentru atenție!