

SECURITATEA INFORMAȚIONALĂ LA NIVEL EUROPEAN



**Autor: Tatiana Busuncian
Dr., conferențiar universitar**



Conținuturi; Obiective de referință; Termeni-cheie.

Conținuturi:

1. caracteristicile terorismului informațional în spațiul European.
2. implementarea acțiunilor UE în sporirea schimbului de informații
3. criminalitatea informațională, eforturile întreprinse pentru asigurarea securității informaționale.

Obiective de referință:

- să definească caracteristicile terorismului informațional în spațiul european;
- să determine instrumentele și metodele de luptă cu amenințările cibernetice;
- să influențeze implementarea acțiunilor UE în sporirea schimbului de informații, intensificarea verificărilor la frontierele externe, îmbunătățirea controalelor armelor de foc, digitalizarea cooperării judiciare, prevenirea radicalizării online, blocarea finanțării terorismului și altele;
- să evalueze motivele criminalității informaționale și să descrie eforturile întreprinse pentru asigurarea securității informaționale.

Termeni-cheie: *nivel european, război informațional, război hibrid, propaganșă, amenințări cibernetice, schimb de informații, frontiere.*

Terorismul informațional în spațiul european

- Actualmente, cel mai mare pericol pentru lumea contemporană îl reprezintă terorismul. Terorismul ca fenomen social-politic are rădăcini istorice profunde. De la începuturi, fenomenul terorismului a avut un caracter intern, manifestându-se doar la nivel național, în calitate de factor de influență asupra sferei social-politice și altor domenii ale vieții, ajungând să fie statuat în legislația fiecărui stat.
- Terorismul cauzează prejudicii considerabile sub aspect politic, economic, social și moral, acesta constituie o problemă serioasă, soluționarea căreia este în interesul întregii comunități mondiale, inclusiv pentru reprezentanții mediului științific. Încă la începutul secolului trecut au fost întreprinse tentative de creare a unor mecanisme internaționale eficiente de prevenire și combatere a terorismului
- Prin acțiunile întreprinse de teroriști ne dăm seama despre tipul de război. Terorismul vizează distrugerea fizică, în numele unor idealuri sau al unor „vocații” mesianice, spectaculoase, crearea unor situații-limită care să ducă la înfricoșarea populației și a conducerii politice, în cele mai multe cazuri, la bază este obiectivul politic.

La etapa actuală dezvoltarea societății se caracterizează prin aceea că informația, tehnologiile informaționale și de comunicații, precum și relațiile ce se formează în procesul de colectare, prelucrare, stocare, transmitere și diseminare a informației, au un impact direct și din ce în ce mai puternic asupra dezvoltării economice, sociale și spirituale atât în cazul anumitor state, în mod particular, cât și în privința întregii comunități mondiale, în ansamblu.

Conform datelor UNESCO, volumul tranzacțiilor de pe piața serviciilor și tehnologiilor informaționale depășește suma de două trilioane de dolari și reprezintă circa 15% din economia mondială.

Trecerea civilizației noastre în „era informațională” a coincis, practic, cu declanșarea „războiului împotriva terorismului” – o luptă ce se desfășoară sub toate aspectele, inclusiv cel informațional.

Toate acestea se referă la terorism, evoluția căruia, potrivit experților, în cea mai mare măsură se realizează în domeniul informațional.

Dezvoltarea rapidă a noilor tehnologii a extins foarte mult posibilitățile organizațiilor teroriste de a manipula cu conștiința publică. Aceste acțiuni au următoarele caracteristici ale terorismului contemporan:

orientarea spre un impact emoțional puternic asupra societății ca rezultat al acțiunilor sale, exprimat prin atingerea stării de teamă și nesiguranță în rândul populației atacate și tendința de acceptare și simpatie din partea adeptilor săi;



concentrarea pe diseminarea către un public cât mai larg a informațiilor cu privire la un act terorist comis;



realizarea atacurilor asupra unor obiecte care au o semnificație deosebită pentru societate, simbolizând anumite valori;



folosirea violenței de către teroriști este percepută în societate (în special în țările dezvoltate) ca una nenaturală, improprie, ce intră în conflict cu normele sociale și generează ca urmare o stare de anxietate, nesiguranță, neîncredere și incertitudine.



- ✓ Dezvoltarea tehnologiilor informaționale în întreaga lume contribuie la apariția și răspândirea largă a comunităților criminale transnaționale, de tip rețea organizațională.
- ✓ Scopul principal al teroriștilor este de a face actul terorist cunoscut publicului și autorităților, având o rezonanță cât mai mare.
- ✓ Un pericol real îl constituie tendința organizațiilor teroriste internaționale de a utiliza mijloacele de informare în masă în calitate de instrument pentru atingerea scopurilor lor criminale. Astfel, teroriștii contemporani au transformat în câmp de luptă inclusiv și ecranul televizorului.

Dezvoltarea mijloacelor electronice de informare în masă cu efect transfrontalier contribuie în mod semnificativ la extinderea capacităților organizațiilor teroriste internaționale în ceea ce privește manipularea cu conștiința maselor.

Nici o țară din lume, nici chiar SUA, nu-și mai poate asigura securitatea prin forțe proprii, și aceasta din cel puțin două motive:

1. mondializarea informației, dezvoltarea și proliferarea fără precedent a sistemelor de arme și mijloacelor de distrugere;
2. omniprezența și onnipotența amenințărilor asimetrice, îndeosebi a celor de natură endogenă, care își mută centrul de greutate în sfera informațională, mai târziu posibil în cea a ecosistemelor și chiar în cea genetică, afectând direct mecanismul intim al vieții umane – informația ereditară – acizii nucleici.

Terorismul mediatic incumbă două aspecte:

- cel al folosirii de către teroriști a mass-media pentru atingerea scopurilor lor criminale, violente
- și cel al terorizării populației de către instituții sau reprezentanți ai media.

- Tot mai dependenți de informații am devenit în veacul XXI.
- Digitalizarea oferă oportunități enorme și asigură soluții pentru multe dintre provocările cu care se confruntă Europa, nu în ultimul rând în timpul crizei provocate de pandemia de COVID-19 și războiului din Ucraina, dar, în același timp, expune economia și societatea la amenințări cibernetice.



În întreaga Europă atacurile cibernetice și criminalitatea informatică devin tot mai numeroase și mai sofisticate. Se preconizează că această tendință va continua să crească în viitor, date fiind previziunile conform cărora 22,3 miliarde de dispozitive la nivel mondial vor fi conectate la internetul obiectelor până în 2024 global.

Noua Agenție a UE pentru Securitate Cibernetică se bazează pe structurile predecesoarei sale, Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor, având acum un rol consolidat și un mandat permanent. În plus, agenția a adoptat același acronim, ENISA.

ATTACK ORIGINS		ATTACK TYPES		ATTACK TARGETS		LIVE ATTACKS					
#	COUNTRY	#	PORT SERVICE TYPE	#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE
57	China	6	53168 unknown	87	United States	13-11-31.265	China Unicom Heibel Province Network	120.13.138.62	Heibel, CN	Saint Louis, US	unknown
10	United States	6	80 http	8	Russia	13-11-31.555	China Unicom Heibel province network	121.18.73.19	Baoding, CN	Saint Louis, US	unknown
8	Russia	5	23 telnet	6	Saudi Arabia	13-11-31.931	S.E.A - Multimedia	199.203.59.121	Tel Aviv, IL	Saint Louis, US	ssh
6	Japan	5	1 tcpmux	2	France	13-11-32.594	N/A	43.255.188.131	JP	Clifton, US	ssh
4	Sweden	5	22 ssh	2	Cyprus	13-11-32.941	Shodan	66.240.236.119	San Diego, US	Seattle, US	unknown
2	Saudi Arabia	5	8080 http-proxy	1	Spain	13-11-32.967	Shodan	66.240.236.119	San Diego, US	Seattle, US	unknown
2	Netherlands	4	20976 unknown	1	Canada	13-11-33.255	China Unicom Heibel province network	101.28.166.2	Heibel, CN	Saint Louis, US	unknown
2	South Korea	4	19962 unknown			13-11-33.636	Computers & Tele-Comm	108.161.78.2	Independenc...	Saint Louis, US	shell
2	Jordan	3	4270 unknown			13-11-34.296	CHINANET Gansu province network	118.183.76.51	Lanzhou, CN	Saint Louis, US	unknown
2	Israel	3	17500 unknown			13-11-34.625	CHINANET Sichuan province network	182.133.136.10	Chengdu, CN	Saint Louis, US	unknown

Uniunea Europeană lucrează în mod activ la îmbunătățirea mediului digital în beneficiul tuturor europenilor. Viața digitală a europenilor trebuie să fie sigură, ușoară și să respecte libertățile fundamentale. Tehnologiile digitale schimbă viețile oamenilor – de la modul în care comunicăm până la modul în care trăim și lucrăm. Digitalizarea are potențialul de a oferi soluții pentru multe dintre provocările cu care se confruntă Europa și europenii și oferă oportunități cum ar fi:

- crearea de locuri de muncă;
- promovarea educației;
- stimularea competitivității și a inovării;
- combaterea schimbărilor climatice și facilitarea unei tranziții verzi.

ENISA Threat Landscape 2025

Raportul ENISA Threat Landscape 2025 (ETL 2025), publicat în octombrie 2025, oferă o analiză detaliată a peisajului amenințărilor cibernetice din Uniunea Europeană pentru perioada iulie 2024 – iunie 2025. Acesta subliniază intensificarea campaniilor hibride complexe, inclusiv cele orchestrate de Federația Rusă, care vizează subminarea stabilității politice și a procesului democratic în Republica Moldova.

Raportul evidențiază utilizarea de către actorii statali a unor tehnici avansate de atac cibernetic, inclusiv campanii de spionaj cibernetic și exploatarea vulnerabilităților în infrastructuri critice, precum cele din sectoarele energetic, transport și sănătate. Aceste activități au fost direcționate către instituțiile din Republica Moldova, cu scopul de a destabiliza guvernul, de a eroda încrederea publicului în procesele democratice și de a influența rezultatele alegerilor parlamentare din 2025.

ENISA Threat Landscape 2025

În ciuda complexității și sofisticării acestor campanii, instituțiile moldovenești, societatea civilă și mass-media au răspuns rapid, expunând și demontând rețelele de interferență și comunicând transparent publicului. Partenerii internaționali ai Moldovei au jucat un rol esențial în consolidarea rezilienței țării.

Pentru a contracara aceste amenințări, raportul conține câteva recomandări privind consolidarea capacităților instituționale ale Republicii Moldova:

- promovarea alfabetizării digitale;
- întărirea cooperării cu societatea civilă și mass-media independente;
- și asigurarea unui angajament internațional sustenabil și previzibil.

Aceste măsuri sunt esențiale pentru protejarea proceselor democratice și pentru menținerea stabilității politice în fața amenințărilor hibride emergente.

Misiunea de Parteneriat a UE în Republica Moldova (EUPM)

- √ Înființată în anul 2023, la solicitarea autorităților moldovene, Misiunea de Parteneriat a UE în Republica Moldova (EUPM), Moldova a fost prima misiune civilă a Uniunii Europene creată în mod specific pentru a aborda provocarea complexă a consolidării rezilienței împotriva amenințărilor hibride — inclusiv a vulnerabilităților cibernetice și a manipulării și interferenței informaționale străine (FIMI).
- La 20 mai 2025, Consiliul Afaceri Externe a extins mandatul EUPM cu încă doi ani, până la sfârșitul lunii mai 2027. Această misiune și rapoartele sale includ idei și acțiuni concrete privind consolidarea rezilienței Moldovei, inclusiv față de manipulare informațională și interferențe externe. Uniunea Europeană joacă un rol esențial în acest efort.
- Sprijinul oferit Republicii Moldova include:
 - acces la fonduri europene și investiții strategice;
 - asistență pentru întreprinderile mici și mijlocii (IMM-uri);
 - integrarea treptată în piața unică europeană;
 - tranziții structurale în domeniul energetic, digital și social, precum și dezvoltarea unei guvernante economice reziliente și predictibile.

UE și NATO, actori esențiali în creșterea capacității de reziliență instituțională și societală.

Cele mai relevante bune practici internaționale care pot fi adaptate în contextul Republicii Moldova vizează consolidarea parteneriatelor public-privat și valorificarea sprijinului strategic oferit de Uniunea Europeană și NATO, actori esențiali în creșterea capacității de reziliență instituțională și societală. Într-o lume interdependentă, aceste practici se bazează pe:

- mecanisme de cooperare intersectorială;
- schimb de informații operative;
- dezvoltarea de cadre comune de gestionare a riscurilor
- și implementarea unor standarde uniforme de securitate cibernetică și informațională

CORE-24 M

Exercițiul CORE-24 M, o inițiativă practică, un exercițiu care implică autorități naționale și parteneri NATO pentru creșterea rezilienței infrastructurilor critice, cu componente de securitate cibernetică și pregătire împotriva amenințărilor hibride, ilustrează modul în care bunele practici internaționale pot fi adaptate în Republica Moldova, prin consolidarea cooperării public-privat și valorificarea sprijinului strategic oferit de NATO și UE. Acesta contribuie direct la dezvoltarea rezilienței instituționale, prin pregătirea operatorilor energetici și a autorităților în gestionarea amenințărilor hibride și cibernetică, și la întărirea rezilienței societale, prin promovarea unui cadru colaborativ între instituții publice, sector privat și comunitatea internațională.

Exercițiul subliniază importanța integrării strategiilor internaționale în consolidarea capacității naționale de prevenire și răspuns la riscuri complexe.

UE este un domeniu care cuprinde totul, de la rețelele de informații și telecomunicații, infrastructură și datele pe care le sprijină până la sistemele informatice, operatori și persoanele împuternicite de operatori.



UE cooperează în domeniul apărării în spațiul cibernetic prin activitățile Agenției Europene de Apărare (AEA), în colaborare cu Agenția UE pentru Securitate Cibernetică și cu Europolul. AEA sprijină statele membre în construirea unei forțe de muncă militare competente în domeniul apărării cibernetice și asigură disponibilitatea unei tehnologii proactive și reactive în domeniul apărării cibernetice.



Strategia de securitate cibernetică a UE, adoptată în decembrie 2020 de Comisie și SEAE, consolidează:

- coordonarea apărării cibernetice
- cooperarea și consolidarea capacităților de apărare cibernetică.

Componente naționale și internaționale de cooperare

- Sistemele de supraveghere și de monitorizare a terorismului presupun structuri și infrastructuri cu foc continuu, distribuite în așa fel încât să acopere întreaga planetă sau, într-o primă etapă a războiului antiterorist, zonele care ating pragul de importanță ce se ia în considerație de factorii de decizie. Aceste sisteme trebuie să fie integrate, dar și suficient de flexibile pentru a face față flexibilității tactice și aleatorii a terorismului, și să asigure bazele de date și informații necesare organizării corespunzătoare a acțiunii și reacției. Tot ele trebuie să aibă componente naționale și internaționale, care să acționeze, prin cooperare în toate mediile și în toate spațiile.

Fiecare din aceste structuri trebuie să includă:

- componente de supraveghere electronică de mare sensibilitate;
- componente de cercetare directă, prin agenți și agenți de influență;
- componente de comunicații rapide și securizate;
- componente de analiză a datelor și informațiilor;
- componente de decizie rapidă;
- componente de validare și corectare oportună a acestor decizii.

Factorul cel mai important în supravegherea structurilor, infrastructurilor și acțiunilor teroriste îl reprezintă omul, agentul de informații, dotat cu toate mijloacele necesare și ajutat de un sistem tehnic-informațional permanent și eficace.

Componente naționale și internaționale de cooperare

- Republica Moldova colaborează cu Organizația Tratatului Atlanticului de Nord. Colaborarea cu NATO nu poate afecta neutralitatea Republicii Moldova. Organizația Tratatului Atlanticului de Nord este o alianță politico-militară, înființată prin Tratatul Atlanticului de Nord semnat la Washington la 4 aprilie 1949. Alianța este o asocierie de state libere unite prin hotărârea lor de a-și proteja securitatea, prin garanții reciproce și relații stabile cu alte țări.
- Scopul esențial al NATO este de a asigura libertatea și securitatea tuturor membrilor săi prin mijloace politice și militare, în conformitate cu Tratatul Nord-Atlantic și cu principiile Cartei Națiunilor Unite. Cele trei sarcini fundamentale ale Alianței sunt: apărarea colectivă, gestionarea crizelor și securitatea prin cooperare.
- Totodată, NATO cooperează cu state terțe, pentru dezvoltarea capacităților de apărare și creșterea rezilienței acestora, dar și cu organizații internaționale, în special cu Uniunea Europeană, Organizația Națiunilor Unite și Uniunea Africană în domenii de interes comun. Toate deciziile adoptate la nivelul NATO sunt luate prin consensul celor 30 de state aliate.
- Statele partenere NATO: Pe lângă statele membre, NATO are și un Parteneriat pentru Pace (PfP), care a fost introdus în ianuarie 1994. La momentul actual, din acest parteneriat fac parte 20 de țări, inclusiv Moldova.
- Scopul principal al Parteneriatului este de a întări stabilitatea și securitatea din întreaga Europă. Acest lucru este posibil datorită unui Document Cadru semnat între statele partenere și NATO.
- Documentul include sarcini specifice pe care fiecare participant trebuie să și le asume în cooperarea cu NATO.

Nivelurile securității informaționale

Politico-conceptual



Legislativ



De reglementare și tehnic



Administrativ



Nivel de software și hardware

Propaganda

- Mai puțin de jumătate dintre cetățenii Republicii Moldova, mai exact, 44%, spun că ar cunoaște ce înseamnă termenul propagandă, arată datele unui sondaj național privind percepția populației despre mass-media și aptitudinile mediatice, publicat în toamna anului trecut. Mai mult, circa jumătate dintre respondenți au fost de acord cu afirmații precum că propagandă ar fi știrile care sperie populația sau care critică guvernarea, ceea ce nu este tocmai așa.
- Toată lumea vorbește despre propagandă, dar foarte puțini încearcă să răspundă la întrebarea ce este propaganda, pentru că dacă ar răspunde, atunci propaganda dispare. Foarte stranie îmbinarea – mass-media și propaganda, când mass-media ar trebui să facă altceva decât propagandă, propagandă are cine face.
- Propaganda este o informație sau niște mesaje ale cuiva care, transmițându-le, încearcă să te afilieze, să te facă să gândești ca și dânsul. Atunci când omul se apucă de capul propagandei, atunci propaganda devine un fenomen nociv, pentru că, în general, de la începuturi și până acum, propaganda vine pe filiera religioasă. Apropo, în Roma există strada Propagandei, adică este dedicată celor care transmiteau mesajele credinței catolice și încercau să aibă tot mai mulți susținători. Ei bine, în timp, propaganda a fost luată drept armă ideologică de multă lume.
- Foarte straniu că, și în secolul 21, când avem acces la o sumedenie de canale de informare, propaganda își face treaba și, mai ales acolo unde populația săracă predomină, este un mecanism foarte subtil.

Concluzii

- Securitatea informațională este un domeniu mult prea vast și cu prea multe domenii conexe pentru a fi detaliat complet undeva. Lumea este în continuă mișcare, cerințele de securitate și confidențialitate cresc pe zi ce trece, amenințările țin pasul.
- Dependența de informație este tot mai mare, chiar periculoasă. Există state care depind totalmente de informațiile oferite de componentele spațiului cibernetic național. Blocarea acestuia timp de câteva ore poate să conducă la instaurarea haosului în țara respectivă, afectând, în bună măsură, și securitatea sistemului informațional global.
- Tehnologiile avansate oferă un șir de soluții pentru multe dintre preocupările omenirii, inclusiv pentru domeniul militar. Războiul informațional, tehnologia care a ajuns la o treaptă de dezvoltare înaltă, oferă soluții la toate provocările existente, inclusiv militare, dar nu poate înlocui aspectele referitoare la resursa umană.

Concluzii

- Republica Moldova operează într-un mediu regional complex, marcat de amenințări hibride care combină dezinformarea, atacurile cibernetice și influențele politice externe. Aceste fenomene subliniază vulnerabilitatea spațiului informațional și necesitatea unor mecanisme eficiente de reziliență.
- Cazul Republicii Moldova evidențiază faptul că reziliența democratică nu se reduce la apărarea instituțională, ci presupune un echilibru între securitatea informațională, coeziunea societală și legitimitatea guvernării.
- Rezultatele alegerilor parlamentare din septembrie 2025 confirmă că o combinație între determinarea instituțiilor naționale, implicarea civică și solidaritatea partenerilor internaționali poate contracara cu succes campaniile hibride menite să submineze suveranitatea și stabilitatea unei țări aflate la frontiera geopolitică a Europei.

Pentru contracararea cu succes a amenințărilor cibernetice este necesar a se concentra asupra următoarelor:

- Stabilirea unui cadru conceptual, instituțional (crearea sistemului național de securitate cibernetică, elaborarea legislației, dezvoltarea parteneriatului);
- Elaborarea programului național de dezvoltare a potențialului cibernetic (capacităților de prevenire, detectare și contracarare a atacurilor cibernetice, crearea unor structuri specializate, ridicarea nivelului de protecție, dezvoltarea producției produselor de profil);
- Consolidarea culturii de securitate informațională (informarea populației, instruirea adecvată a managerilor și a personalului tehnic);
- Perfecționarea cooperării internaționale (la nivel de acte normative, schimburi de experiență, de protecție colectivă împotriva atacurilor de amploare).

Bibliografie

- Aspectul informațional al luptei contemporane contra terorismului la nivel mondial. https://ibn.idsi.md/sites/default/files/imag_file/107-120.pdf
- Manualul UE privind asistență acordată victimilor terorismului. Ianuarie 2021.
- Concepția securității informaționale a Republicii Moldova
- Securitatea informațională 2013: conf. intern., 19 apr. 2013 (ed. a 10-a Jubiliară), coord. ed.: Serghei Ohrimenco. Chișinău: ASEM. 2013, 126 p.
- Chifu Iu., Nantoi O. Război informațional. Tipizarea modelului agresiunii.
- Drăgulean A. Arădăvoaice, Gheorghe; Iliescu, Dumitru; Niță, Dan Laurențiu, Terorism, antiterorism, contraterorism, Ed. Antet, București, 1997, 383 pag.
- Bădescu, Ilie; Dungaciu, Dan; Baltasiu, Radu, Istoria sociologiei. Teorii contemporane, Ed. Eminescu, București, 1996, 704 pag.
- Ce presupune parteneriat și cooperare cu NATO și de ce neutralitatea Republicii Moldovei nu ar trebui să reprezinte un impediment. <https://infocenter.md/ce-presupune-parteneriat-si-cooperare-cu-nato-si-de-ce-neutralitatea-republicii-moldovei-nu-ar-trebuie-sa-reprezinte-un-impediment-2/>
- Katzman, Kenneth, Terrorism: Near Eastern Groups and State Sponsors, Congressional Research Center Report for Congress, 2001
- Popa, N.; Mihăilescu, I.; Eremia, M., Sociologie juridică, Ed. Universității din București, București, 1997, 124 pag.
- Rădulescu, Sorin M., Homo Sociologicus. Raționalitate și iraționalitate în acțiunea umană, Casa de editură și presă "Șansa" – SRL, București, 1994, 302 pag.
- Snowden, Ben; Hayes, Laura, State-Sponsored Terrorism, 2001 XXX, Terorismul, Ed. Omega, București, 2001, 224 pag.
- Terorismul. București, 2002. https://cssas.unap.ro/ro/pdf_studii/terorismul.pdf
- Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. 372 с.