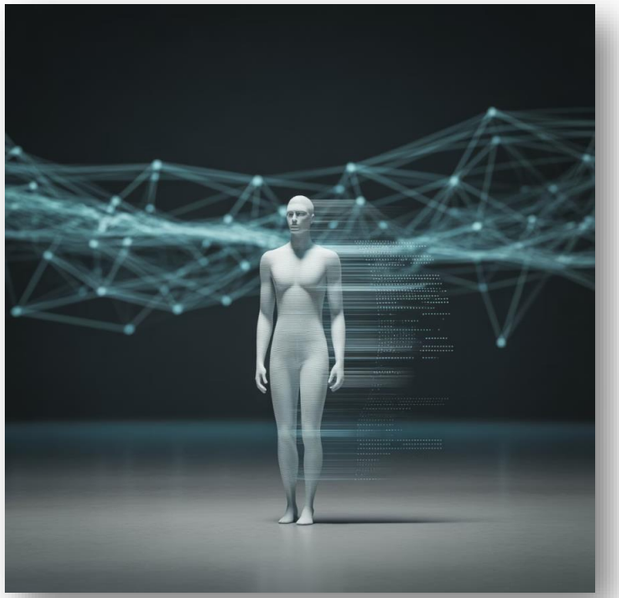
Războiul informațional: tendințe, amenințări, perspective



Autor: Tatiana Busuncian
Dr., conferențiar universitar

Conținuturi; Obiective de referință; Termeni-cheie

Conținuturi:

1. Războiul informațional - teren de confruntare
2. Războiul informațional: o componentă a războiului hybrid
3. Impactul războiului informațional asupra securității naționale a Republicii Moldova

Obiective de referință:

- Să identifice geneza și trăsăturile războiului informațional
- Să determine formele de manifestare pe arena internațională
- Să evalueze practici și strategii ale actorilor internaționali împotriva războiului informațional
- Să analizeze impactul asupra securității naționale a Republicii Moldova
- Să estimeze practici și instrumente de luptă împotriva războiului informațional

Termeni-cheie:

1. Război informațional

   Confruntare în spațiul informațional

2. Război hibrid

   Combinație de tactici convenționale și neconvenționale

3. Propagandă

   Diseminarea informațiilor pentru influență

4. Fake-news

   Informații false sau manipulate

Cine deține informația, conduce lumea

Era Informației

Informația - conceptul fundamental

Informația este conceptul care stă la baza acestei ere. Informația este obiectul principal de lucru la momentul actual și în anii ce vor urma. Odată cu dezvoltarea tehnologiei, spațiile virtuale care mai demult existau doar în imaginație au început să prindă viață.

În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informațional.

Sfera informațională

Factor de organizare a societății contemporane cu influență activă în situația politică, economică și de apărare

Societatea globală

Integritatea asigurată prin schimbul informațional continuu între state și actori internaționali

Război informațional: Definirea conceptului

Război informațional

Confruntare dintre două sau mai multe state în spaţiul informaţional cu scopul provocării daunelor la sistemele informaţionale şi reţelele de comunicaţii electronice, la procese şi resurse, la obiectivele naţionale de transport, comunicaţii, sistemul energetic, piaţa financiar-bancară, domeniul fiscal, vamal, investiţional, ramurile principale ale economiei şi relaţiile lor externe.

1. **Subminarea sistemelor**
   Atacuri asupra sistemelor politic, economic şi social ale statului țintă
2. **Manipularea psihologică**
   Influențarea masivă a populaţiei pentru destabilizarea societăţii şi statului
3. **Constrângerea decizională**
   Forțarea luării unor decizii în interesul părții adverse prin presiuni informaționale

Războiul informațional vizează obiective vitale şi de importanţă strategică pentru securitatea naţională, reprezentând o amenințare complexă și multidimensională în era digitală contemporană.

Dimensiunile războiului informațional

Realități alternative

Crearea de narațiuni prin pervertirea adevărului obiectiv, bazat pe date, fapte și argumente concrete

Răstălmăcirea informației

Utilizarea unei combinații de elemente, fapte selectate și interpretate prin raționamente alterate

Tehnici de manipulare

Folosirea de silogisme, sofisme, propagandă și interpretare forțată împănate cu minciuni

Acțiuni de negare și exploatare

Războiul informațional implică **negarea, exploatarea, distorsionarea sau distrugerea informațiilor** și a mijloacelor de comandă, control și procesare ale inamicului, protejându-le simultan pe cele proprii.

Exploatarea funcțiilor militare

Concomitent cu exploatarea funcțiilor informației militare pentru obținerea unui avantaj strategic decisiv în conflictele moderne.

Obiectivele strategice ale războiului informațional

Control și Influență

Controlul deciziei strategice

Politica externă și securitatea națională

Pervertirea instrumentelor militare

Blocarea elementelor de securitate

Mecanismul de influență

Instrumentul și mecanismul pentru atingerea acestui obiectiv este acela de a **determina publicul, cetățenii, grupurile de presiune** pregătite și condiționate, organizate și dirijate, să preseze autoritatea pentru a o îndepărta de la soluția obiectivă identificată pentru decizia într-un anumit moment pe baza lipsei de susținere, ba chiar opoziției populației.

Grupurile de presiune
Organizarea și dirijarea influenței

Cetățenii
Manipularea opiniei publice

Presiunea autorităților
Îndepărtarea de la soluții obiective

Geneza domeniului cibernetic

1

Anii 1950-1960

Situația geopolitică și surpriza tehnologică au schimbat lumea pentru totdeauna.

2

Sputnik 1 - 1957

Reușita lansării satelitului de către URSS - o mare victorie în detrimentul concurenților americani

3

Răspunsul american - 1958

Înființarea NASA ca răspuns la provocările tehnologice sovietice

Impactul tehnologic

Istoria și evoluția domeniului cibernetic este destul de veche. Unele evenimente de o importanță istorică și tehnică colosală au dat naștere domeniului cibernetic. Reușita lansării în spațiu a satelitului Sputnik 1 de către URSS a fost o mare victorie pentru URSS.

După lansarea în spațiu a satelitului Sputnik 1, **administrația Eisenhower a întreprins măsuri deliberate** de a nu rămâne în urmă în domeniul științific și tehnologic de URSS.

⚠ Aceste reușite ale sovieticilor i-au ambiționat şi mai tare pe oamenii politici și de știință americani care, în 1958, un an după trimiterea satelitului Sputnik 1 în spațiu, au înființat Administrația Naţională Aeronautică şi Spațială, cunoscută sub numele de NASA.

Sfera informațională în societatea globală

Factorul organizațional

Sfera informaţională, ca factor de organizare a societăţii contemporane, are o influenţă activă în situaţia politică, economică, de apărare şi alte componente ale securităţii statului.

Integritatea globală

În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informaţional continuu și eficient.

Globalizarea

Fenomen amplu dezbătut care influenţează aspectele legate de securitatea naţională și ameninţările privind siguranţa

Extinderea tehnologică

Utilizarea la scară globală a diferitelor mecanisme de prelucrare şi comunicare a informaţiilor

Noi provocări

Apariţia nevoii de a lua în considerare noile aspecte ce influenţează securitatea spaţiului cibernetic

Globalizarea a condus la extinderea la scară globală a utilizării diferitelor mecanisme de prelucrare şi comunicare a informaţiilor, de control al activităţilor, generând nevoia de a lua în considerare noile aspecte ce influenţează securitatea spaţiului cibernetic global.

Definirea securității informaționale

Securitate informațională - concept general

Stare de protecție a persoanei, societăţii şi a statului, care determină capacitatea de rezistență la amenințările împotriva confidențialității, integrității şi disponibilității în spaţiul informaţional.

Securitate informațională - Republica Moldova

Stare de protecție specifică a persoanei, societăţii şi a statului, a drepturilor şi intereselor acestora în spaţiul informaţional, stipulate de Constituție şi alte legi ale Republicii Moldova, precum şi a drepturilor şi intereselor ce țin de căutarea, crearea, recepționarea, expedierea, distribuirea, prelucrarea, stocarea, utilizarea şi protecția informației.

Securitatea informațională reprezintă o stare complexă de protecție care acoperă toate aspectele vieții digitale și informaționale a unei națiuni, de la drepturile individuale la interesele strategice de stat.

Caracteristicile războiului informațional

Conflictul Secolului XXI

Războiul informațional este **forma de conflict specifică acestui secol**, deoarece el răspunde la unele dintre obiecțiile aduse atât de politicieni cât și analiștii geo-strategici sau de planificatorii militari formelor clasice de desfășurare a conflictelor.

- Dificultatea precizării adversarilor
  Identificarea actorilor ostili devine extrem de complexă în mediul digital
- Absența frontierelor
  Lipsa unor frontiere de natură geografică și/sau temporale claire
- Multitudinea de ținte
  Diversitatea obiectivelor atacabile în infrastructura informațională
- Remediere dificilă
  Lipsa unor metode rapide de remediere a consecințelor generate
- Tehnologie accesibilă
  Utilizarea unei tehnologii relativ simple, ieftine și larg răspândite

Securitatea și protecția informațiilor

Securitatea informațională

Un **proces de asigurare** a confidențialității, integrității și disponibilității informațiilor în toate aspectele lor

Protecția informațiilor

Un **set de măsuri concrete** care vizează asigurarea securității informațiilor prin implementarea de politici și tehnologii

Diferența dintre securitatea informațională și protecția informațiilor constă în faptul că prima reprezintă un proces continuu și comprehensiv, în timp ce a doua se referă la măsurile concrete implementate pentru atingerea acestui obiectiv.

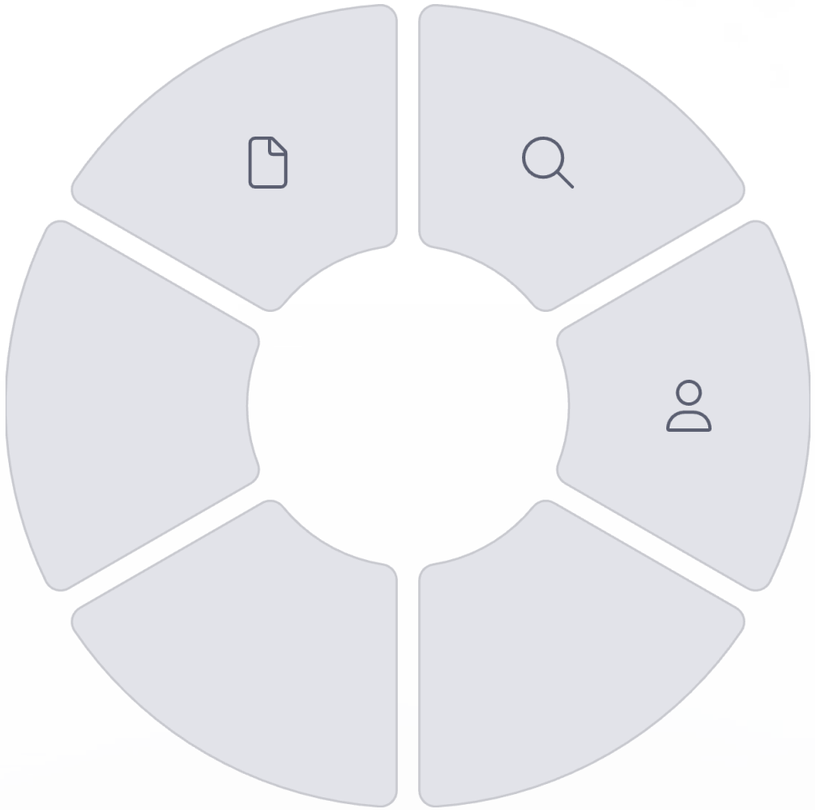
Principalele componente ale securității informaționale

Confidențialitatea

Asigurarea că informația este accesibilă doar persoanelor autorizate

Integritatea

Menținerea acurateței și completitudinii informației



Responsabilitatea

Trasabilitatea acțiunilor și deciziilor

Disponibilitatea

Garantarea accesului la informație când este necesar

Non-repudierea

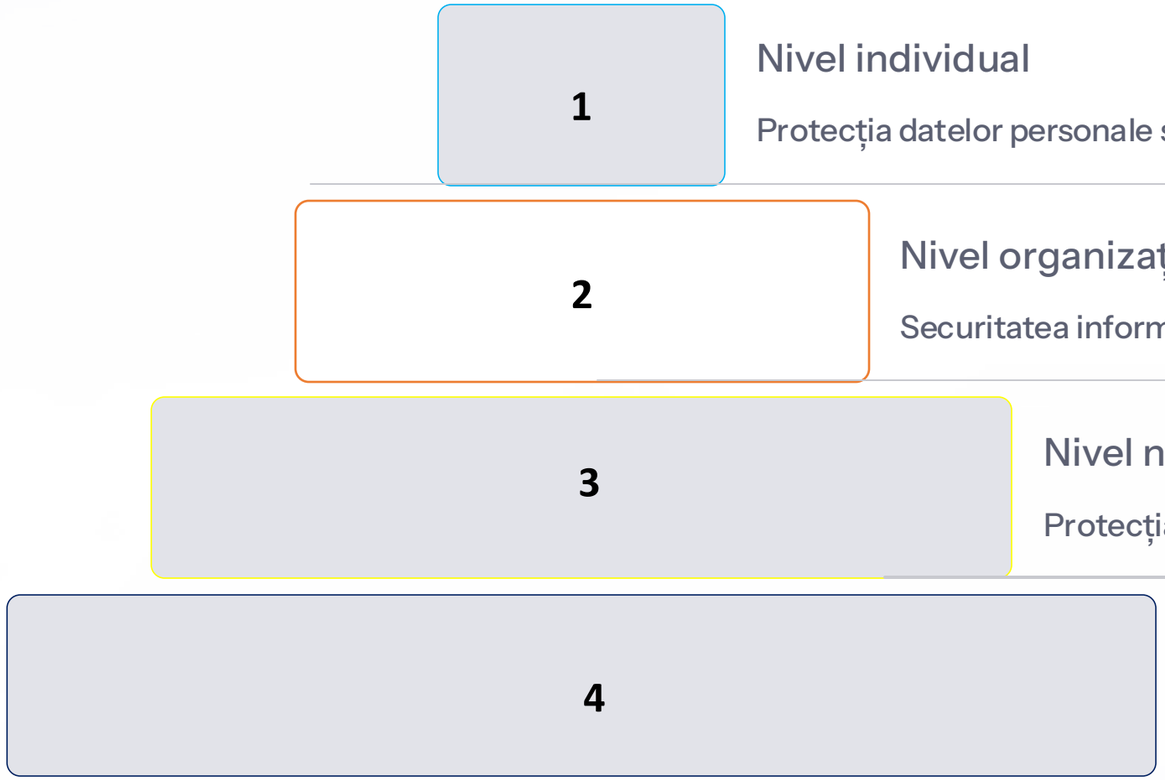
Imposibilitatea negării acțiunilor efectuate

Autentificarea

Verificarea identității utilizatorilor și surselor

Aceste componente formează baza unei strategii complete de securitate informațională, fiind interdependente și necesitând o abordare holistică pentru implementarea eficientă.

Nivelurile securității informaționale



Nivel individual

Protecția datelor personale și confidențialitatea informațiilor private

Nivel organizațional

Securitatea informațiilor în cadrul companiilor și instituțiilor

Nivel național

Protecția infrastructurii critice informaționale a statului

Nivel internațional

Cooperarea globală în domeniul securității cibernetice

Abordare multinivel

Securitatea informațională necesită o **abordare coordonată** la toate nivelurile, de la protecția individuală la cooperarea internațională.

Interdependența nivelurilor

Vulnerabilitățile la un nivel pot afecta securitatea la toate celelalte niveluri, necesitând o strategie integrată.

Sursele puterii în războiul informațional

Trei Surse de Putere

Forța fizică

Inflexibilă și limitată. Poate fi folosită doar pentru a pedepsi. Orice forță fizică poate fi limitată, prin utilizarea ei putem să distrugem ceea ce vrem de fapt să apărăm.

Bogăția

Instrument mai eficace și poate fi folosit atât pentru a pedepsi cât și pentru a recompensa, dar și ea poate fi limitată pentru că nu poate ține o veșnicie.

Cunoașterea

Puterea la cea mai înaltă calitate. Poate fi folosită pentru a pedepsi, răsplăti, convinge, transforma. Cunoașterea nu se epuizează pentru că putem genera oricâtă cunoaștere vrem.

> **În conflicte dominantă este inteligența umană.** Cunoașterea reprezintă arma supremă în războiul informațional contemporan.

Principiile asigurării securității informaționale

01

Echilibrarea intereselor

Principiul echilibrării intereselor individuale, a societății și a statului pentru o protecție optimă

02

Legalitatea și securitatea juridică

Respectarea cadrului legal și asigurarea certitudinii juridice în toate acțiunile

03

Integrarea internațională

Principiul de integrare în sistemele internaționale de securitate a informațiilor

04

Eficiența economică

Optimizarea costurilor și beneficiilor în implementarea măsurilor de securitate

05

Mobilitatea

Capacitatea de adaptare rapidă la noile amenințări și tehnologii emergente

06

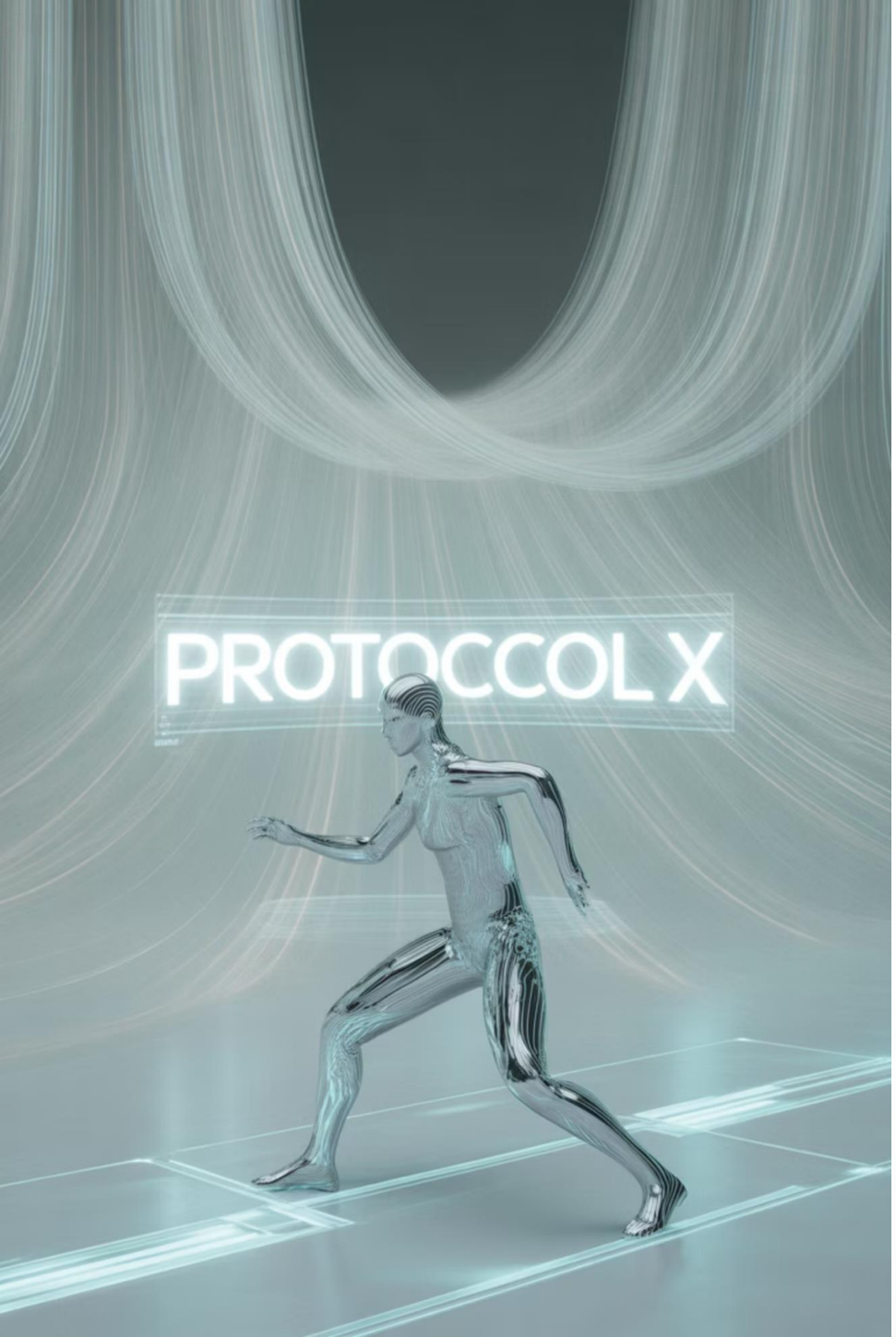
Deschiderea și secretizarea echilibrată

Principiul deschiderii egale și a secretizării egale pentru transparență optimă

07

Complexitatea

Abordarea holistică și integrată a tuturor aspectelor securității informaționale



Spațiul cibernetic - teren de confruntare

Cyber SPACE

Domeniul virtual
Spațiul cibernetic ca mediu distinct de conflict și competiție strategică

Infrastructura critică
Sistemele și rețelele care susțin funcționarea societății moderne

Actori multipli
State, organizații, hackeri și grupuri criminale în competiție constantă

Caracteristicile spațiului cibernetic

- Lipsa graniților fizice clare
- Viteză de propagare a atacurilor
- Anonimitatea și dificultatea atribuirii
- Costuri reduse de intrare
- Impact potențial devastator

Spațiul cibernetic a devenit un domeniu de conflict la fel de important ca domeniile tradiționale terestre, maritime, aeriene și spațiale.

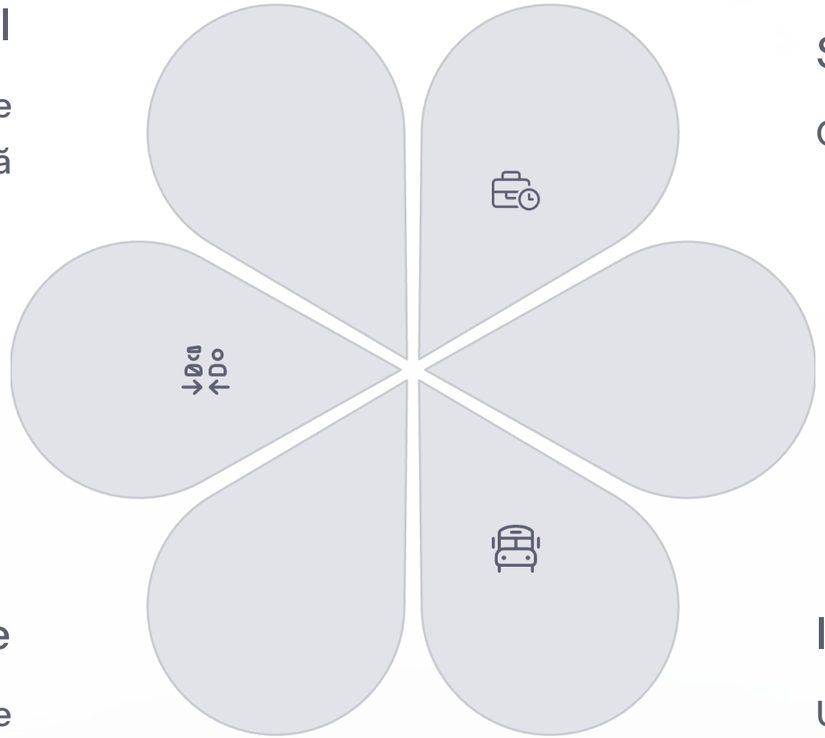
Subiecții securității informaționale

Statul

Autorități guvernamentale și instituții de securitate națională

Sectorul privat

Companii, banci și furnizori de servicii IT



Societatea civilă

ONG-uri și organizații de monitorizare

Cetățenii

Utilizatori individuali și comunitățile digitale

Organizații internaționale

NATO, UE, ONU și alte entități globale

Instituții academice

Universități și centre de cercetare

Toți acești actori joacă roluri complementare în asigurarea securității informaționale, fiind necesară **coordonarea și cooperarea** între ei pentru o protecție eficientă a spațiului informațional.

Ținte și surse ale riscurilor informaționale

Atacuri personale

- Atacuri asupra demnității personale
- Calomnie și defăimare
- Furtul informației de identificare

Manipularea opiniei

- Manipularea cu opinia publică
- Justificarea crimelor împotriva umanității
- Contradicții rasiale

Criminalitatea cibernetică

- Fraude financiare
- Crime împotriva copiilor
- Șantaj electronic

Atacuri sistemice

- Atacuri sistematice
- Atacuri de saturație
- Terorism cibernetic

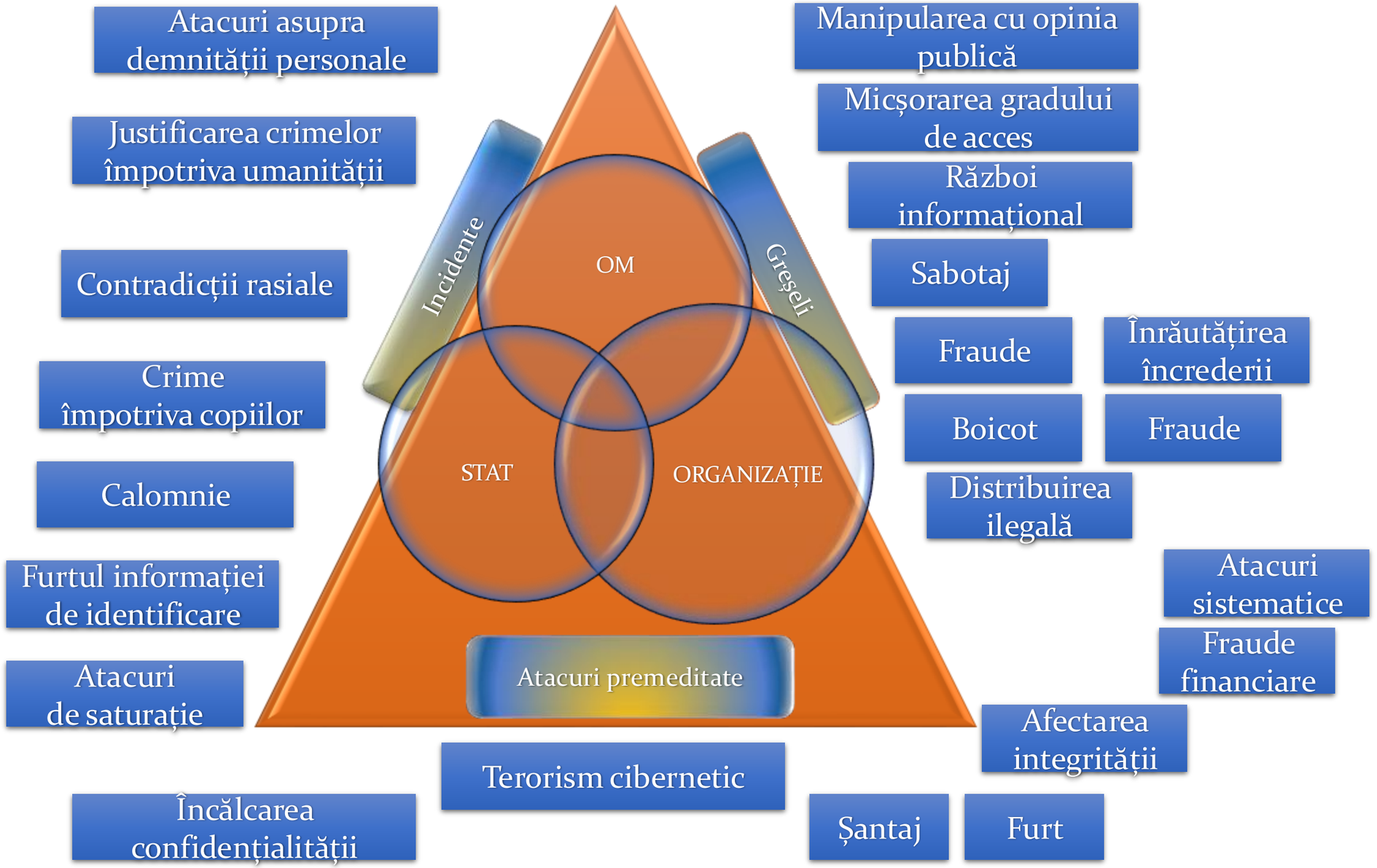
Război informațional

- Sabotaj informațional
- Distribuirea ilegală de conținut
- Micșorarea gradului de acces

Încălcarea integrității

- Afectarea integrității datelor
- Încălcarea confidențialității
- Înrăutățirea încrederii

⚠ Diversitatea și complexitatea acestor amenințări necesită o abordare comprehensivă și adaptabilă în strategiile de apărare cibernetică.


Atacuri asupra demnității personale
Justificarea crimelor împotriva umanității
Contradicții rasiale
Crime împotriva copiilor
Calomnie
Furtul informației de identificare
Atacuri de saturație
Încălcarea confidențialității
Manipularea cu opinia publică
Micșorarea gradului de acces
Război informațional
Sabotaj
Fraude
Înrăutățirea încrederii
Boicot
Fraude
Distribuirea ilegală
Atacuri sistematice
Fraude financiare
Afectarea integrității
Șantaj
Furt
Terorism cibernetic
Incidente
Greșeli
OM
STAT
ORGANIZAȚIE
Atacuri premeditate

Autorii atacurilor cibernetice

Actori statali

Guverne și servicii de intelligence care desfășoară operațiuni cibernetice sponsorizate de stat pentru obiective geopolitice

Grupuri criminale organizate

Rețele internaționale de criminalitate care vizează profit financiar prin ransomware, fraude și alte activități ilegale

Organizații teroriste

Grupuri extremiste care folosesc atacurile cibernetice pentru a semăna teroare și a-și promova agenda ideologică

Hackeri individuali

Actori solitari motivați de provocări tehnice, recunoaștere, profit personal sau activism

Amenințări din interior

Angajați nemulțumiți, contractori sau persoane cu acces privilegiat care abuzează de pozițiile lor

Hacktivști

Indivizi sau grupuri care folosesc atacurile cibernetice pentru a-și exprima convingerile politice sau sociale

Fiecare categorie de atacatori prezintă **caracteristici unice în ceea ce privește motivația, resursele disponibile și metodele preferate**, necesitând strategii de apărare diferențiate și adaptive.

Surse de amenințări cibernetice asupra securității naționale

Servicii de intelligence străine

Spionaj cibernetic și colectarea de informații clasificate

Atacuri asupra lanțului de aprovizionare

Compromiterea furnizorilor de tehnologie și servicii

Atacuri asupra infrastructurii critice

Țintirea sistemelor energetice, de transport și comunicații

Spionajul economic

Furtul de secrete comerciale și propriete intellectuale

Campaniile de dezinformare

Manipularea opiniei publice și subminarea încrederii în instituții

Impact strategic

Aceste amenințări pot afecta **securitatea națională, stabilitatea economică și coeziunea socială**, necesitând o abordare coordonată la nivel guvernamental.

Răspuns integrat

Combaterea eficientă necesită colaborarea între sectorul public și privat, precum și cooperarea internațională.

Impactul războiului informațional în Moldova

Vulnerabilitatea Moldovei

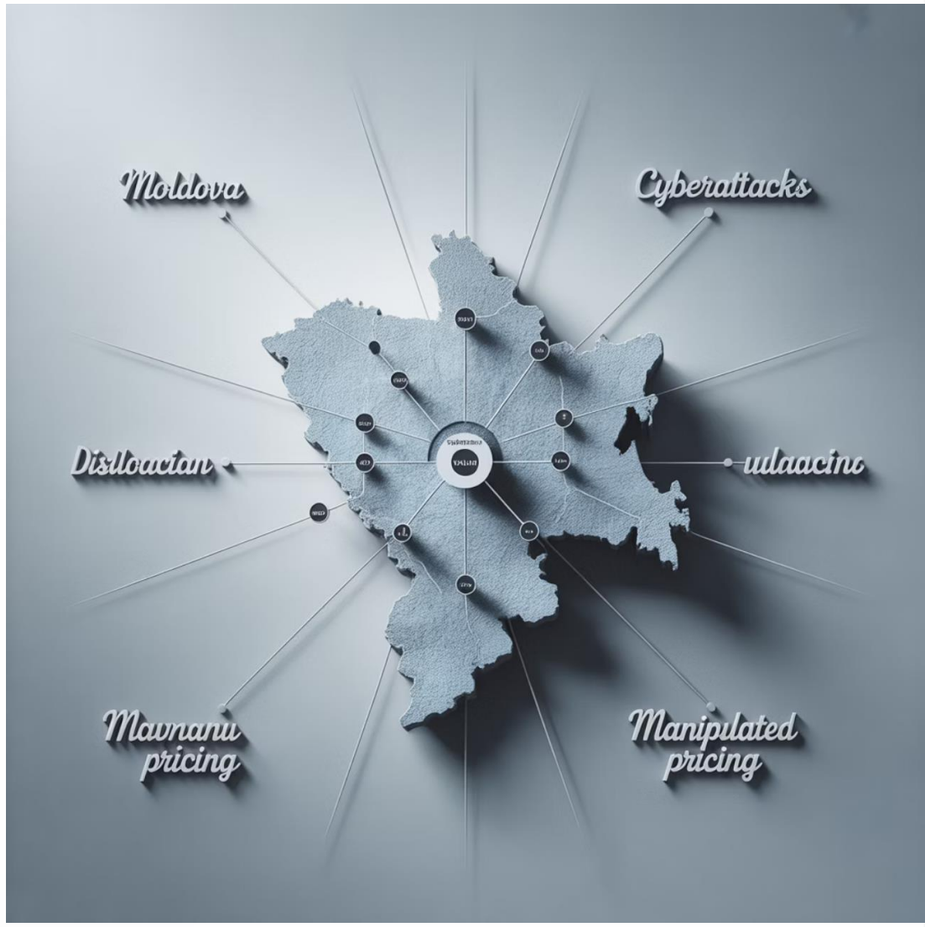
În ultimul timp, în **rapoartele internaționale ale Freedom House** și alte centre de analiză care urmăresc acest fenomen, Republica Moldova este unul dintre cele mai vulnerabile state din spațiul fost sovietic la propaganda rusă.

În opinia cetățeanului rus Pavel Durov, în Moldova **propaganda se face masiv** în media tradițională – televiziuni, ziare și site-uri web – și, mai nou, pe rețelele de socializare, cu precădere pe Telegram.

Criza energetică și manipularea

În contextul crizei energetice internaționale declanșată în toamna lui 2021, mijloacele de propagare a știrilor false și-au completat gama de narațiuni cu:

- Deconectarea în masă a consumatorilor casnici
- Sistarea furnizării electricității de către CET Moldovenească
- Diverse tactici de manipulare informațională



Comparație strategică

În războiul informațional, **Ucraina prin președintele Zelenski** a reușit să capteze empatia la nivel mondial folosind la maxim conținutul video pe rețele de socializare, în timp ce **Federația Rusă** se mișcă greoi prin clasicele metode fake-news-ul și cenzura.

Forme de exercitare a războiului informațional

Războiul informațional poate fi întreprins pe următoarele căi:

Bruiajul transmisiilor

Transmisiile de televiziune și de radio inamice pot fi supuse bruiajului electronic pentru a împiedica difuzarea informației

Atacuri asupra mass-media

Transmisiile de televiziune și de radio pot fi atacate pentru pretinse campanii de dezinformare și subminarea credibilității

Sabotajul logistic

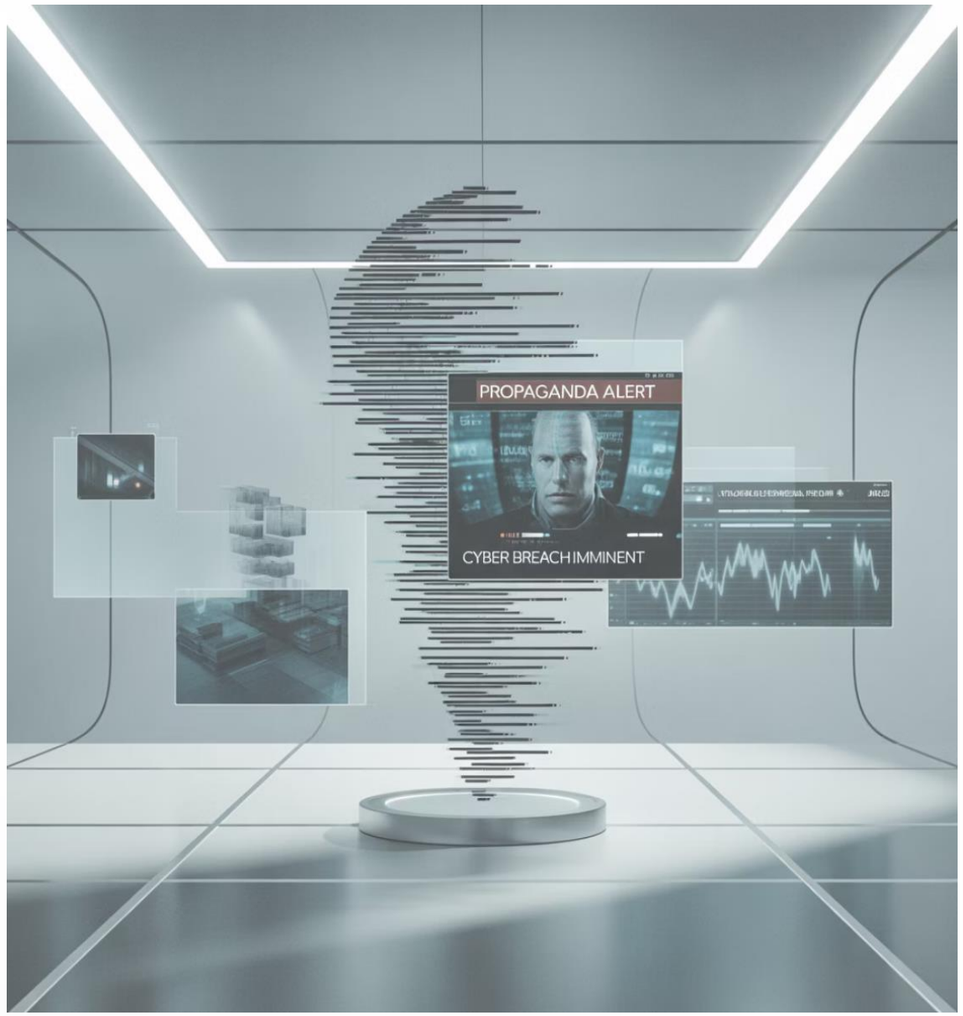
Rețele sau întregul sistem logistic advers poate fi scos din luptă, neeficientizat prin diverse forme de interferență

Atacuri asupra comunicațiilor

Rețelele de comunicație inamice pot fi scoase din luptă sau subminate prin atacuri cibernetice coordonate

Manipularea piețelor financiare

Tranzacțiile de acțiuni la burse pot să fie sabotate prin intervenții electronice sau prin știri senzaționale dezinformante



Dimensiunile războiului informațional

Șapte Forme de Conflict

Războiul informațional urmărește evitarea conflictelor convenționale, a producerii de victime și pagube, prin utilizarea acestor noi mijloace aflate la granița dintre starea convențională de război și starea convențională de pace. Războiul informațional vizează structuri ale domeniului politic, economic, social sau militar, nu doar pentru a le distruge sau paraliza, ci mai ales pentru a le influența procesele decizionale.

Războiul de comandă și control
Forma exclusiv militară care anihilează comanda și sistemele de comandă ale adversarului

Războiul bazat pe informații
Intelligence-ul clasic pentru dominarea spațiului de conflict

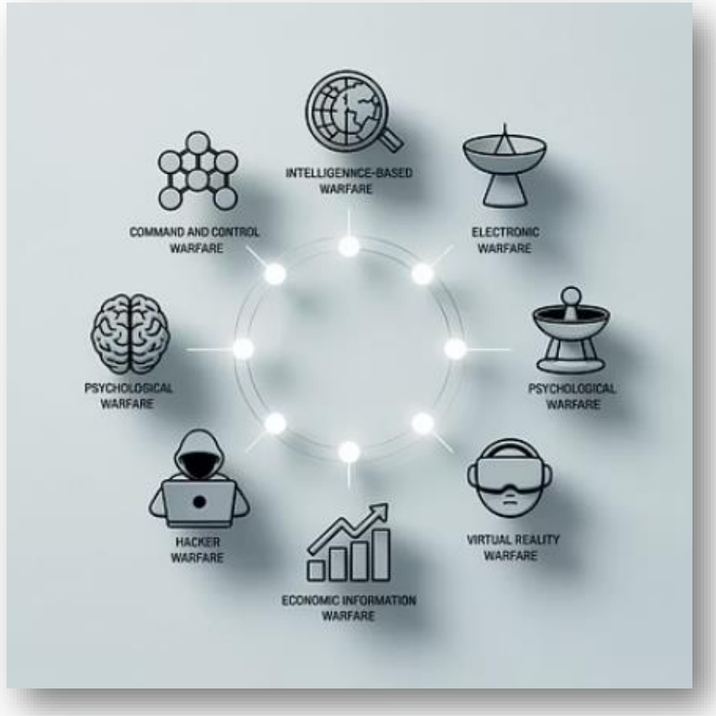
Războiul economic informațional
Blocarea informațiilor pentru supremația economică

Războiul psihologic
Modificarea atitudinilor și opțiunilor amicilor, neutrilor și adversarilor

Războiul hacker-ilor
Atacuri cu software malign asupra sistemelor informatice

Războiul în realitatea virtuală
Scenarii futuriste și cercetare tehnologică avansată

Războiul electronic
Utilizarea tehnologiei pentru dominația spațiului electromagnetic



Concluzii: Complexitatea securității informaționale

Domeniu vast și complex

Securitatea informaţională este un domeniu mult prea vast şi cu prea multe domenii conexe pentru a fi detaliat complet. Lumea este în continuă mişcare, cerinţele de securitate şi confidenţialitate cresc pe zi ce trece, ameninţările ţin pasul cu dezvoltarea tehnologică.

Dependența crescândă

Dependenţa de informaţie este tot mai mare, chiar periculoasă. Există state care depind totalmente de informaţiile oferite de componentele spaţiului cibernetic naţional. **Blocarea acestuia timp de câteva ore** poate să conducă la instaurarea haosului în ţara respectivă, afectând securitatea sistemului informaţional global.

Soluții tehnologice avansate

Tehnologiile avansate oferă un șir de soluții pentru multe dintre preocupările omenirii, inclusiv pentru domeniul militar. Războiul informațional și tehnologia oferă soluții la toate provocările existente, dar **nu poate înlocui aspectele referitoare la resursa umană**.

⚠ Tehnologia oferă instrumentele, dar factorul uman rămâne esențial în gestionarea eficientă a securității informaționale și a războiului informațional.

Concluzii: Evoluția tehnologică și resursa umană

Progresul tehnologic

Tehnologia informației şi comunicațiilor a evoluat foarte mult şi oferă acum soluții pentru multe dintre preocupările omenirii şi implicit, pentru domeniul militar. Este evident că **nu tehnologia reprezintă punctul nevralgic** al unui sistem, ci cultura organizațională şi structura operațională.

Importanța factorului uman

Din acest motiv, trebuie subliniat că, în ceea ce privește războiul informațional, **tehnologia oferă soluții la toate provocările teoretice**, dar nu poate înlocui aspectele referitoare la resursa umană.

1 Informatizarea globală

Procesul accelerat de digitalizare a societății la nivel mondial

2 Intensificarea războiului informațional

Utilizarea mai intensă a armei informaționale contemporane

3 Viitorul apropiat

Perspective și provocări în domeniul securității informaționale

Cultura organizațională şi structura operațională sunt mai importante decât tehnologia în sine.

Totodată, trebuie menționat faptul că **informatizarea globală a societății** poate duce într-un viitor apropiat la folosirea mai intensă a armei informaționale contemporane pe timpul războiului informațional.

Strategii de contracarare a amenințărilor cibernetice

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

Cadru conceptual și instituțional

Stabilirea unui cadru conceptual, instituțional prin crearea sistemului național de securitate cibernetică, elaborarea legislației și dezvoltarea parteneriatului public-privat

Program național de dezvoltare

Elaborarea programului național de dezvoltare a potențialului cibernetic: capacități de prevenire, detectare și contracarare a atacurilor, crearea unor structuri specializate

Cultura de securitate informațională

Consolidarea culturii de securitate prin informarea populației, instruirea adecvată a managerilor și a personalului tehnic specializat

04

Cooperarea internațională

Perfecționarea cooperării la nivel de acte normative, schimburi de experiență și protecție colectivă împotriva atacurilor de amploare

Aceste patru piloni formează baza unei strategii complete de apărare cibernetică, necesitând implementare coordonată și susținută în timp.

Sarcini de autoevaluare

Istoriografia cercetării

Istoriografia cercetării războiului informațional și evoluția conceptuală în timp

Geneza și trăsăturile

Geneza și trăsăturile distintive ale războiului informațional modern

Manifestări internaționale

Forme de manifestare pe arena internațională și studii de caz comparative

Practici și strategii

Practici și strategii ale actorilor internaționali împotriva războiului informațional

Impactul asupra Moldovei

Impactul războiului informațional asupra securității naționale a Republicii Moldova

Instrumente de luptă

Practici și instrumente de luptă a Republicii Moldova împotriva războiului informațional

Aceste unități de conținut oferă o abordare sistematică și comprehensivă pentru înțelegerea completă a fenomenului războiului informațional și a strategiilor de contracarare.

Teme pentru lucrul individual

Subiecte de cercetare pentru aprofundarea cunoștințelor

1. **Era digitală**
   Războiul informațional în era digitală: strategii, tactici și impact asupra societății contemporane

2. **Dezinformarea online**
   Dezinformarea și propaganda online: amenințări la adresa securității naționale și democrației

3. **Rețelele sociale**
   Rolul rețelelor sociale în războiul informațional: manipulare, influență și polarizare socială

4. **Impact asupra democrației**
   Impactul războiului informațional asupra democrației și proceselor electorale libere

5. **Infrastructura critică**
   Protecția infrastructurii critice împotriva atacurilor cibernetice și a războiului informațional

6. **Conflicte hibride**
   Securitatea informațională în contextul conflictelor hibride: provocări actuale și soluții viabile

Aceste teme oferă oportunități de cercetare interdisciplinară, combinând aspecte tehnologice, politice, sociale și de securitate pentru o înțelegere holistică a problematicii.

Bibliografie

Surse principale de documentare

Documentele oficiale

Concepția securității informaționale a Republicii Moldova - cadrul legal și strategic național

Cercetări academice

Sfetcu, Nicolae (2024), Securitatea cibernetică și războiul cibernetic, IT & C, 3:1, 57-64, DOI: 10.58679/IT37085

Studii specializate

PROTEJAREA SPAȚIULUI INFORMAȚIONAL: Analiza Strategiei Securității Informaționale (2019-2024) - pisa.md

- Chifu Iu., Nantoi O. *Război informațional. Tipizarea modelului agresiunii*
- Propaganda și războiul informațional: o amenințare la adresa securității Republicii Moldova - Diez.md
- *A History of Cyberspace*. Per Concordiam, v. 7, nr. 2, 2016, p. 64-65
- Макаренко С. И. *Информационная безопасность:учебное пособие для студентов вузов*. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. 372 с.

Aceste surse oferă o bază solidă pentru înțelegerea teoretică și practică a problematicii securității informaționale și a războiului informațional contemporan.

Vă mulțumim pentru atenție și vă încurajăm să continuați studiul acestui domeniu în continuă evoluție!