RĂZBOIUL INFORMAȚIONAL ȘI SECURITATEA CIBERNETICĂ

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 strategi ale actorilor internaționali împotriva războiului informațional și în procesul de asigurare a
securității naționale și internaționale;
- să analizeze impactul războiului informațional asupra securității naționale a Republicii Moldova;
- să estimeze practici și instrumente de luptă a Republicii Moldova împotriva războiului informațional.

Termeni-cheie: *război informațional, război hibrid, propagandă, fake-news, confruntarea informației, sfera informației.*

Cine deține informația, conduce lumea

Informația este conceptul care sta 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.

Sfera informațională, ca factor de organizare a societății contemporane, are o influență activă în situația politică, economică, de apărare și alte componente ale securității statului. În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informațional.

Război informațional - confruntare dintre două sau mai multe state în spațiul informațional cu scopul provocării daunelor la sistemele informaționale și rețelele de comunicații electronice, la procese și resurse, la obiectivele naționale de transport, comunicații, sistemul energetic, piața financiar-bancară, domeniul fiscal, vamal, investițional, ramurile principale ale economiei și relațiile lor externe, la alte obiective vitale și de importanță strategică pentru securitatea națională, subminării sistemelor politic, economic și social, manipulării psihologice masive a populației pentru destabilizarea societății și statului, precum și constrîngerii pentru luarea unor decizii în interesul părții adverse.

Războiul informațional reprezintă crearea de realități alternative prin pervertirea adevărului obiectiv – realizat pe baza datelor, faptelor și argumentelor concrete – răstălmăcirea lui prin utilizarea unei combinații de elemente, fapte și bucăți de adevăr selectate, interpretate, combinate cu raționamente alterate prin utilizarea de silogisme, sofisme, propagandă, interpretare forțată, totul împănat cu o multitudine de minciuni.
Război informațional ar putea fi definit și ca o acțiune de negare, exploatare, distorsionare sau distrugere a informațiilor și a mijloacelor de comandă, control și de procesare ale inamicului, protejându-le pe cele proprii, concomitent cu exploatarea funcțiilor informației militare.

Războiul informațional este o componentă a războiului hybrid și un instrument de sine stătător. **Obiectivul general**, principal, al războiului informațional este acela **de a determina, de a controla sau măcar de a altera decizia strategică, de politică externă, securitate și apărare, de pervertire sau îngreunare a instrumentelor destinate componentei militare a unui stat, și de îngreunarea funcționării, dacă nu chiar de blocarea unor elemente ce țin de securitatea unui stat.**

Instrumentul și mecanismul pentru a atinge acest 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 susțineri, ba chiar opoziției populației.

Istoria și evoluția domeniului cibernetic este destul de veche. Unele evenimente de o importanță istorică și tehnică colosală au dat naștere domeniul cibernetic. Situația geopolitică în anii 1950 și 1960 și surpriza parvenită odată cu apariția noilor tehnologii, a schimbat lumea. Reușita lansării în spațiu a satelitului Sputnik 1 de către URSS a fost o mare victorie pentru URSS, în detrimentul concurenților americani. 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 și mai tare pe oamenii politici și de știință americani care, în 1958, un an după trimiterea satelitului Sputnik 1 în spațiu, au înființat Administrația Națională Aeronautică și Spațială, cunoscută sub numele de NASA.

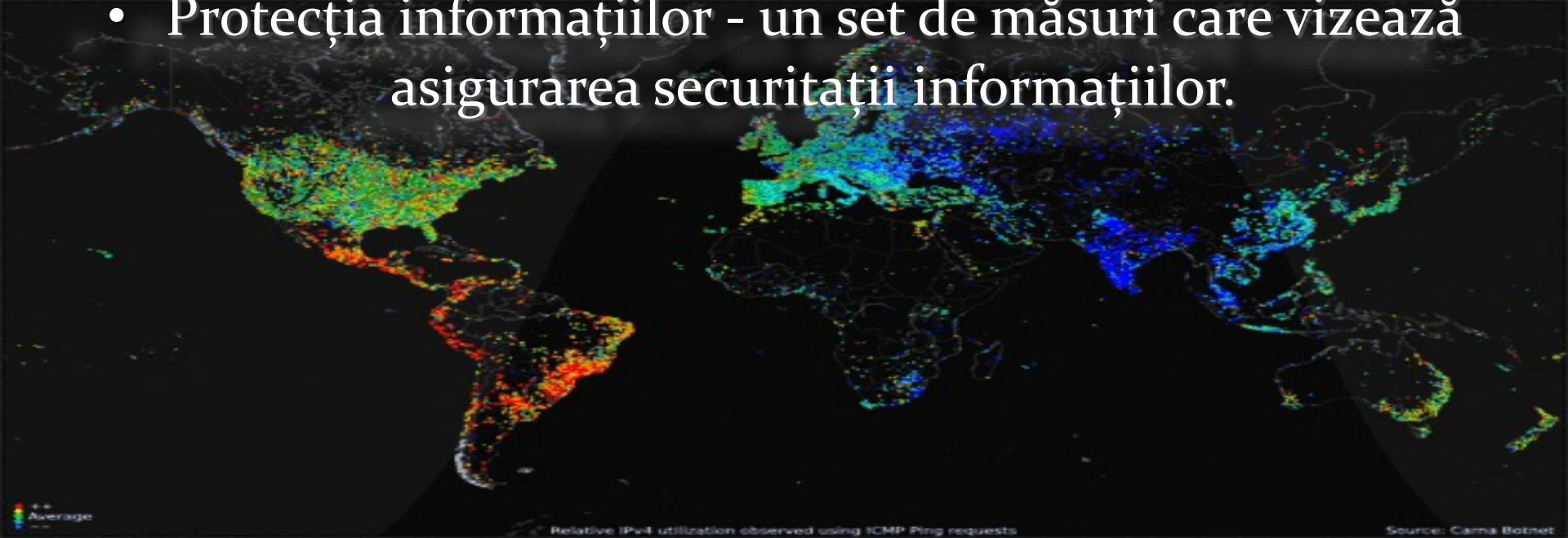
Sfera informaţională, ca factor de organizare a societăţii contemporane, are o influenţă activă în situaţia politică, economică, de apărare şi alte componente ale securităţii statului. În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informaţional.

Globalizarea, este un fenomen amplu dezbătut, nu putea să nu influenţeze aspectele legate de securitatea naţională, de ameninţările privind siguranţa oamenilor şi informaţiilor, a instituţiilor naţionale şi internaţionale. Extinderea la scară globală a utilizării diferitelor mecanisme de prelucrare şi comunicare a informaţiilor, de control al activităţilor a condus şi la apariţia nevoii de a lua în considerare noile aspecte ce influenţează securitatea spaţiului cibernetic global.

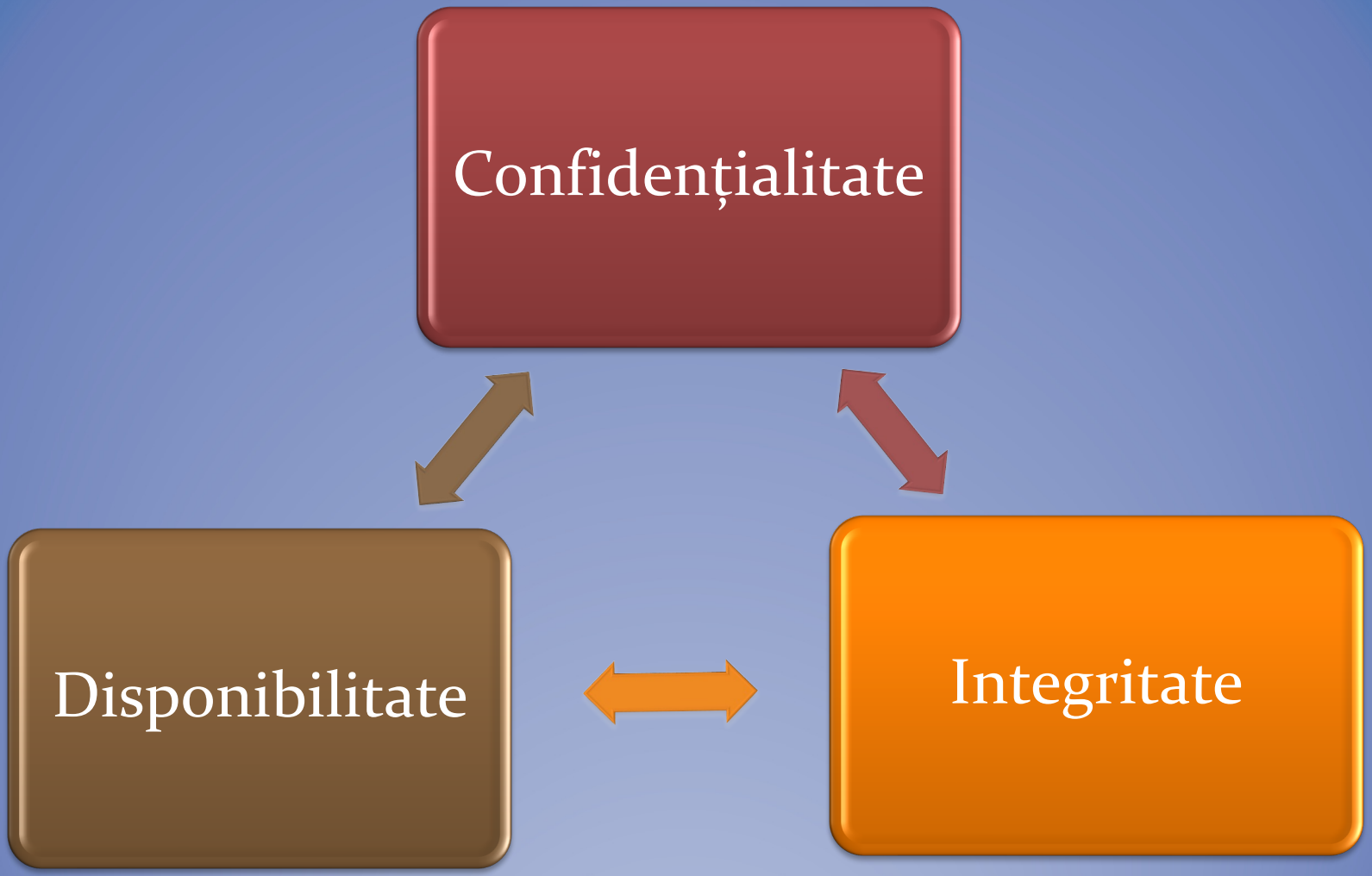
- **Securitate informațională – stare de protecție a persoanei, societății și a statului, care determină capacitatea de rezistență la amenințările împotriva confidențialității, integrității și disponibilității în spațiul informațional.**
- **Securitate informațională a Republicii Moldova – stare de protecție a persoanei, societății și a statului, a drepturilor și intereselor acestora în spațiul informațional, stipulate de Constituție și alte legi ale Republicii Moldova, precum și a drepturilor și intereselor ce țin de căutarea, crearea, recepționarea, expedierea, distribuirea, prelucrarea, stocarea, utilizarea și protecția informației în spațiul informațional.**

- Securitatea informațională - un proces de asigurare a confidențialității, integrității și disponibilității informațiilor.

- Protecția informațiilor - un set de măsuri care vizează asigurarea securității informațiilor.



Principalele componente ale securității informaționale



Nivelurile securității informaționale

Principiile asigurării securității informaționale

- principiul echilibrării intereselor individuale, a societății și a statului
- principiul legalității și securității juridice
- principiul de integrare în sistemele internaționale de securitate a informațiilor.
- principiul eficienței economice
- principiul mobilității
- principiul deschiderii egale și a secretizării egale
- principiul complexității

Spațiul cibernetic - teren de confruntare

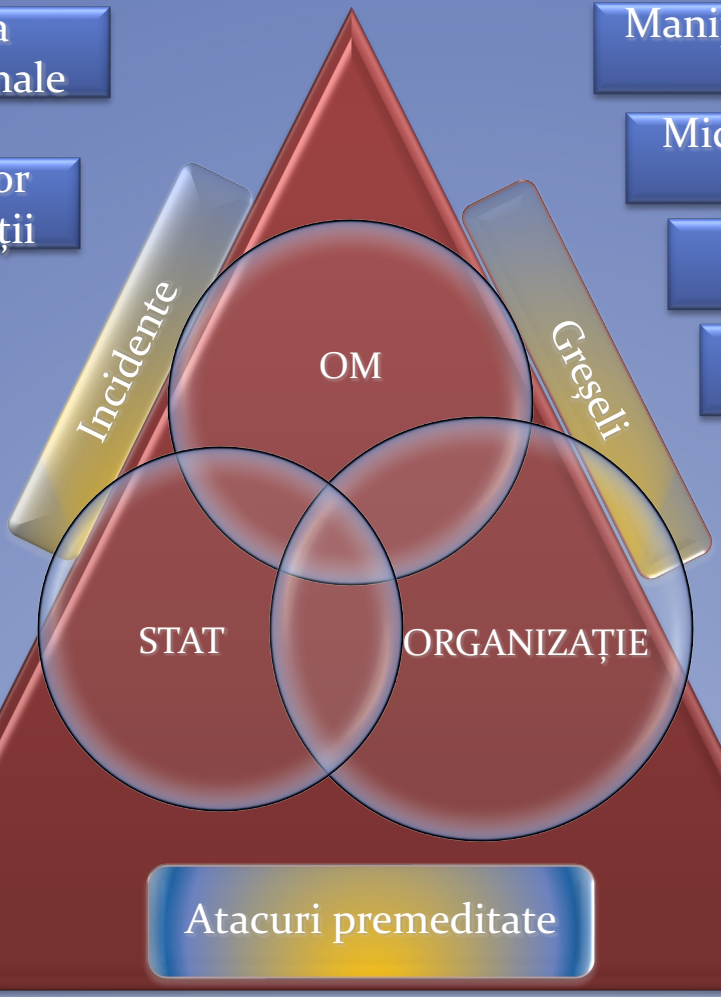
Spațiul cibernetic a devenit un nou mediu de ducere a războiului (al cincilea după uscat, mare, aer, spațiu). Este evident faptul că toate conflictele în viitor vor avea o componentă virtuală, fie în faza inițială a conflictului, fie sub formă de agresiune în sensul direct al cuvîntului, fără desfășurarea altor forme de luptă.

În absența unor acorduri internaționale și a nedorinței de a conveni asupra normelor generale de interpretare a problemei, actorii cu intenții agresive posedă agilitate și flexibilitate în dezvoltarea și punerea în aplicare a potențialilor atacuri cibernetice.

Subiecții securității informaționale

- Statul ca un întreg;
- Organizații de stat;
- Structuri comerciale;
- Persoane fizice.

Ținte și surse ale riscurilor cibernetice



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

Terorism cibernetic

Șantaj

Furt

Autorii atacurilor cibernetice

- Hackerii amatori (hobbyiști);
- Grupe mici de hackeri;
- Organizații nonguvernamentale;
- Structuri de stat.

Surse de amenințări cibernetice asupra securității naționale

Impactul războiului informațional în Moldova

- 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. 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 de la rețelele electrice și de gaze naturale; sistarea furnizării electricității de către Centrala Termoelectrică Moldovenească din Transnistria etc. Există un șir de tactici de manipulare. 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 fakenews-ul și cenzura.

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 treaptîă de dezvoltare înaltă, oferă soluții la toate provocările existente, inclusiv militare, dar nu poate înlocui aspectele referitoare la resursa umană.

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

- 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.
- 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.