



RĂZBOIUL INFORMAȚIONAL ȘI SECURITATEA INFORMAȚIONALĂ

- 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 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, propaganșă, 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 constrângerii 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.

Istoria și evoluția domeniului cibernetic este destul de veche. Unele evenimente de o importanță istorică și tehnică colosală au dat naștere domeniului 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 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.



Globalizarea, este un fenomen amplu dezbătut, nu putea să nu influențeze aspectele legate de securitatea națională, de amenințările privind siguranța oamenilor și informațiilor, a instituțiilor naționale și internaționale. Extinderea la scară globală a utilizării diferitelor mecanisme de prelucrare și comunicare a informațiilor, de control al activităților a condus și la apariția nevoii de a lua în considerare noile aspecte ce influențează securitatea spațiului cibernetic global.

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.

Principalele trăsături ale războiului informațional se desprind din natura sa deosebit de complexă:

- Dificultatea precizării adversarilor;
- Absența unor frontiere de natură geografică și/sau temporale;
- Multitudinea de ținte;
- Lipsa unor metode rapide de remediere a consecințelor pe care le generează;
- Utilizarea unei tehnologii relativ simple, ieftine și larg răspândite;
- Dificultatea stabilirii unor responsabilități clare și precise privind managementul domeniului;
- Costurile relativ scăzute ale derulării operațiilor informaționale în raport cu rezultatele ce se pot obține;
- Posibilitățile sporite de manipulare;
- Ștergerea deosebirilor dintre nivelurile de comandă.



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

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	13-41:31.265	China Unicom Heibel Province Network	120.13.138.62	Heibel, CN	Saint Louis, US	unknown
10	United States	6	80 http	8	Russia	13-41:31.555	China Unicom Heibel province network	121.18.73.19	Baoding, CN	Saint Louis, US	unknown
8	Russia	5	23 telnet	6	Saudi Arabia	13-41:31.931	S.E.A - Multimedia	199.203.59.121	Tel Aviv, IL	Saint Louis, US	ssh
6	Japan	5	1 tcpmux	2	France	13-41:32.594	N/A	43.255.188.131	JP	Clifton, US	ssh
4	Sweden	5	22 ssh	2	Cyprus	13-41:32.941	Shodan	66.240.236.119	San Diego, US	Seattle, US	unknown
2	Saudi Arabia	5	8080 http-proxy	1	Spain	13-41:32.967	Shodan	66.240.236.119	San Diego, US	Seattle, US	unknown
2	Netherlands	4	20976 unknown	1	Canada	13-41:33.255	China Unicom Heibel province network	101.28.166.2	Heibel, CN	Saint Louis, US	unknown
2	South Korea	4	19962 unknown			13-41:33.636	Computers & Tele-Comm	108.161.78.2	Independenc...	Saint Louis, US	shell
2	Jordan	3	4270 unknown			13-41:34.296	CHINANET Gansu province network	118.183.76.51	Lanzhou, CN	Saint Louis, US	unknown
2	Israel	3	17500 unknown			13-41:34.625	CHINANET Sichuan province network	182.133.136.10	Chengdu, CN	Saint Louis, US	unknown

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



Nivelurile securității informaționale

Politico-conceptual



Legislativ



De reglementare și tehnic



Administrativ



Nivel de software și hardware

Puterea războiului informațional este data de trei surse: forța fizică, bogăția și cunoașterea.

Forța fizică este inflexibilă și poate fi folosită doar pentru a pedepsi, și orice forță fizică poate fi limitată, prin utilizarea ei putem să distrugem ceea ce vrem de fapt să apărăm.



Bogăția este un 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 putea ține o veșnicie.



Cunoașterea este 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.



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

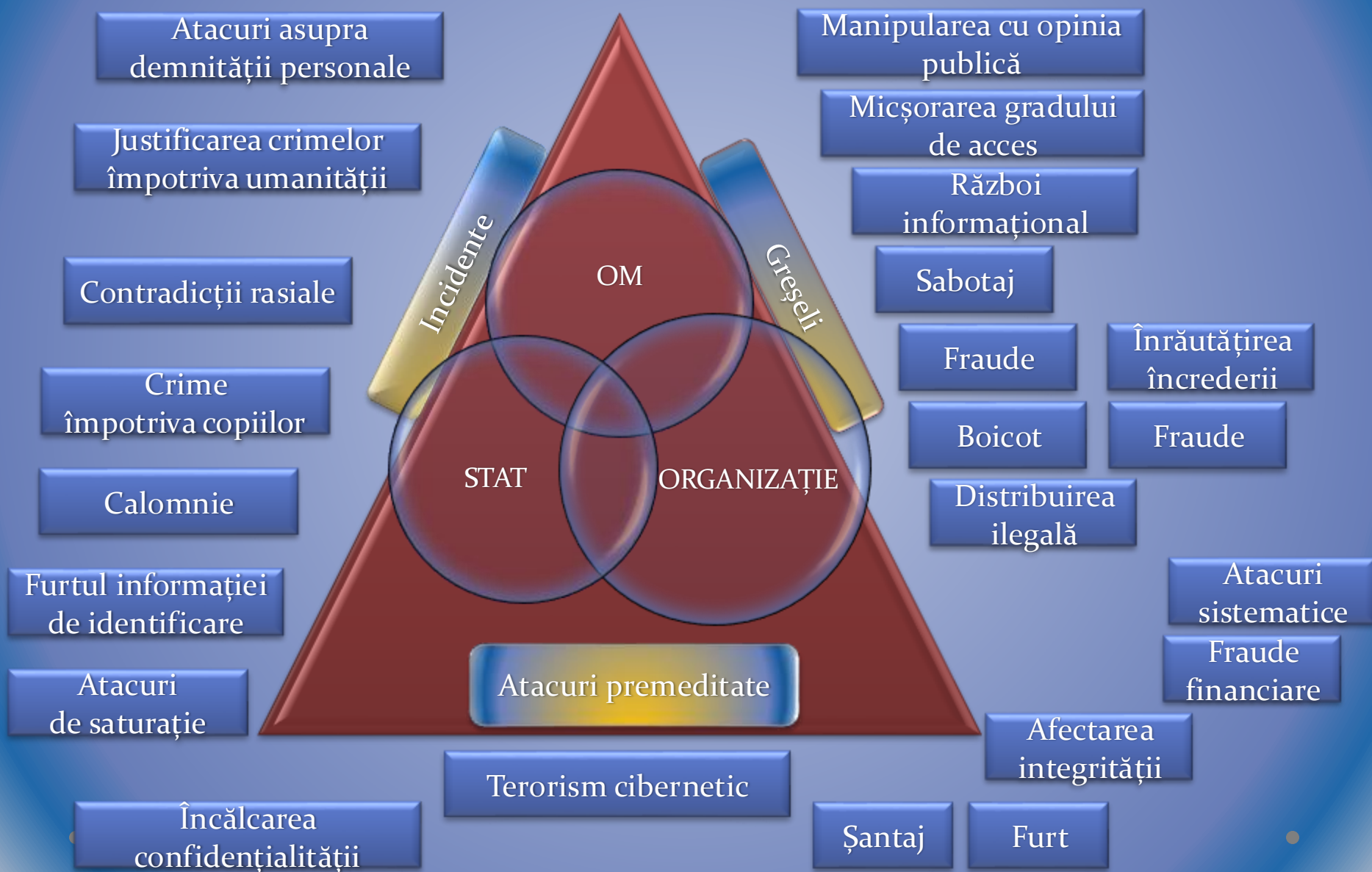
Spațiul cibernetic - teren de confruntare



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 cuvântului, 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.

Ținte și surse ale riscurilor informaționale



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.



Forme de exercitare a Războiul informațional care poate fi întreprins pe următoarele căi:

- Transmisiile de televiziune și de radio inamice pot fi supuse bruiajului.
- Transmisiile de televiziune și de radio pot fi atacate pentru pretinse campanii de dezinformare.
- Rețele sau întregul sistem logistic advers poate fi scos din luptă, neeficientizat.
- Rețelele de comunicație inamice pot fi scoase din luptă sau subminate.
- Tranzacțiile de acțiuni la burse pot să fie sabotate prin intervenții directe, electronice, sau prin derutante știri senzaționale, fie prin plasări înșelătoare dezinformante.



DE ASEMENEA, 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. ASTFEL SE FACE TRECERE DE LA STADIUL DE VIOLENȚĂ ORGANIZATĂ LA STADIUL DE INFLUENȚARE OSTILĂ. ÎN CONCLUZIE, RĂZBOIUL INFORMAȚIONAL POATE FI PRIVIT SUB ȘAPTE ASPECTE SAU, ALTFEL SPUS, ÎN FUNCȚIE DE STRATEGIILE DE ATAC-APĂRARE CONSTRUITE ȘI DE ARMELE INFORMAȚIONALE UTILIZATE COMPORTĂ ȘAPTE DIMENSIUNI DIFERITE:

RĂZBOIUL DE COMANDĂ ȘI CONTROL. ESTE FORMA EXCLUSIV MILITARĂ A RĂZBOIULUI INFORMAȚIONAL ȘI ARE MENIREA SĂ ANIHILEZE COMANDA ȘI SISTEMELE DE COMANDĂ ȘI CONTROL ALE UNUI ADVERSAR PRIN INTEGRAREA OPERAȚIILOR PSIHOLOGICE, A SECURITĂȚII OPERAȚIILOR, A INDUCERII ÎN EROARE, A RĂZBOIULUI ELECTRONIC ȘI A DISTRUGERII FIZICE;

RĂZBOIUL BAZAT PE INFORMAȚII. ESTE INTELLIGENCE-UL CLASIC ȘI CONSTĂ ÎN PROIECTAREA, PROTECȚIA ȘI ANIHILAREA SISTEMELOR CARE CONȚIN SUFICIENTE CUNOȘTINȚE PENTRU A DOMINA UN SPAȚIU DE CONFLICT;

RĂZBOIUL ELECTRONIC. UTILIZEAZĂ TEHNOLOGIE ELECTRONICĂ ȘI TEHNICI SPECIFICE PENTRU DOMINAȚIA SPAȚIULUI ELECTROMAGNETIC;

RĂZBOIUL PSIHOLOGIC. UTILIZEAZĂ INFORMAȚIA PENTRU A MODIFICA ATITUDINILE ȘI OPȚIUNILE AMICILOR, NEUTRILOR ȘI ADVERSARILOR;

RĂZBOIUL HACKER-ILOR. CONSTĂ ÎN ATACURI PASIVE ȘI ACTIVE CU SOFTWARE MALIGN ASUPRA SISTEMELOR INFORMATICE;

RĂZBOIUL ÎN SFERA INFORMAȚIILOR ECONOMICE. URMĂREȘTE BLOCAREA SAU CANALIZAREA INFORMAȚIILOR ÎN SCOPUL OBTINERII SUPREMAȚIEI ECONOMICE;

RĂZBOIUL ÎN SPAȚIUL REALITĂȚII VIRTUALE. ESTE ÎN PREZENT UN PUNCT DE ACUMULARE AL SCENARIILOR FUTURISTE, AL CERCETĂRII FUNDAMENTALE ȘI TEHNOLOGICE.



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.

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).

Sarcini de autoevaluare

- Istoriografia cercetării războiului informațional;
- Geneza și trăsăturile războiului informațional;
- Forme de manifestare pe arena internațională;
- Practici și strategii ale actorilor internaționali împotriva războiului informațional și procesul de asigurare a securității naționale și internaționale;
- Impactul războiului informațional asupra securității naționale a Republicii Moldova;
- Practici și instrumente de luptă a Republicii Moldova împotriva războiului informațional.

Teme pentru lucrul individual

- Războiului informațional în era digitală: strategii, tactici și impact asupra societății.
- Dezinformarea și propaganda online: amenințări la adresa securității naționale.
- Rolul rețelelor sociale în războiul informațional: manipulare, influență și polarizare.
- Impactul războiului informațional asupra democrației și proceselor electorale.
- Protecția infrastructurii critice împotriva atacurilor cibernetice și a războiului informațional.
- Securitatea informațională în contextul conflictelor hibride: provocări și soluții.

Bibliografie

- Concepția securității informaționale a Republicii Moldova
- Sfetcu, Nicolae (2024), Securitatea cibernetică și războiul cibernetic, IT & C, 3:1, 57-64, DOI: 10.58679/IT37085, <https://www.internetmobile.ro/securitatea-cibernetica-si-razboiul-cibernetic/>
- PROTEJAREA SPAȚIULUI INFORMAȚIONAL: Analiza Strategiei Securității Informaționale (2019-2024) și prezentarea recomandărilor pentru noua Strategie - pisa.md, https://pisa.md/wp-content/uploads/2025/01/Protejarea-spatiului-informational_STUDIU.pdf
- Chifu Iu., Nantoi O. Război informațional. Tipizarea modelului agresiunii.
- Propaganda și războiul informațional: o amenințare la adresa securității Republicii Moldova - Diez.md, <https://diez.md/2025/03/20/propaganda-si-razboiul-informational-o-amenintare-la-adresa-securitatii-republicii-moldova/>
- 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.