Universitatea de Stat din Moldova.

Facultatea de Relații Internaționale și Științe Politice și Administrative



LUCRU INDIVIDUAL

La Securitatea Informațională

Pe tema:

“Războiul informational Şi Spaţiul Cibernetic”

Realizat de: Mahu Marian,FRISPA , gr SNS01

Profesor: Busuncean T.

**Chişinău, 2023**

**Cuprins**

[INTRODUCERE *2*](file:///D:\Marian%20univer\Master\Anul%201\Sem%201\Doctrine,%20strategii%20și%20politici%20de%20securitate\Mahu%20Marian%20(%20grupa%201).docx#_Toc103857761)

***Cap 1. Războiul informaţional: definire, caracteristici şi componente....................3-5***

**Cap 2. *Forme ale războiului informational*** ................................................................... 6-8

[CONCLUZII GENERALE *9*](file:///D:\Marian%20univer\Master\Anul%201\Sem%201\Doctrine,%20strategii%20și%20politici%20de%20securitate\Mahu%20Marian%20(%20grupa%201).docx#_Toc103857774)

[BIBLIOGRAFIE *10*](file:///D:\Marian%20univer\Master\Anul%201\Sem%201\Doctrine,%20strategii%20și%20politici%20de%20securitate\Mahu%20Marian%20(%20grupa%201).docx#_Toc103857775)

**Introducere**

Războiul informaţional este o formă de conflict specifică sfârşitului secolului XX şi începutul secolului XXI, care, prin operaţiile desfăşurate, este un instrument al descurajării strategice atât în plan global cât şi în diferite teatre de operaţii.

Războiul informaţional ar putea fi definit ca o acţiune de negare, exploatare, distorsionare sau distrugere a informaţiilor şi a mijloacelor de comandă, control şi de procesare ale inamicului, protejându-le pe cele proprii, concomitent cu exploatarea funcţiilor informaţiei militare. Unele aspecte, specifice conceptului actual de război informaţional, sunt la fel de vechi ca şi societatea umană, problematica războiului informaţional nefiind nouă şi nici necunoscută.

Războiul informaţional este diferit de cel clasic. El se desfăşoară insidios şi eficace prin subversiune fiind o tehnică de slăbire a puterii şi de demoralizare a personalului; această tehnică este bazată pe cunoaşterea legilor psihologiei, pentru că vizează opinia publică, cât şi puterea şi forţele armate de care ea dispune. Ea este o acţiune asupra opiniei prin mijloace subtile şi convergente.

O abordare ştiinţifică a acestui nou tip de război, a fost făcută chiar în anii războiului rece, când nevoia de informaţii a făcut posibilă perfecţionarea acestuia pe baza dezvoltării impetuoase a tehnologiei informatice. Identificat şi cuantificat la mijlocul deceniului şapte, războiul informaţional a fost recunoscut oficial de gânditorii politico-militari ca un tip distinct de război, la fel de important ca cel terestru, maritim, aerian si spaţial. Această recunoaştere este determinată în primul rând de înţelegerea realităţii potrivit căreia omenirea a intrat în era informaţională. Revoluţia tehnologică în domeniul calculatoarelor şi comunicaţiilor a făcut ca importanţa informaţiei să crească într-un ritm mai rapid decât înainte, ceea ce a dus la colectarea, procesarea, păstrarea şi diseminarea acesteia pe distanţe mai mari şi la mai mulţi utilizatori. În aceste condiţii, este de înţeles preocuparea tot mai mare pe care statele o acordă războiului informaţional ca război politic, ca parte componentă a politicii statului, atât pentru promovarea, cât şi pentru protejarea intereselor naţionale.

În era modernă, războaiele nu se mai poartă și câștigă pe frontul clasic de luptă, în plan fizic, ci pe planul informațional. Confruntările armatelor moderne se duc tot mai mult pe planul inteligentei și al psihicului uman. Aceste noi tipuri de confruntări iau în considerare Triada puterii descrisă de Alvin Tofler in Powershift. Conform acesteia exista trei surse importane ale puterii: forța fizică, bogăția și cunoașterea. Aceste trei elemente pot fi convertite ușor dintr-una în alta. Cel mai important, mai puternic și mai flexibil dintre ele este cunoașterea: Forța brută este inflexibilă și poate fi folosită doar pentru a pedepsi.

CAPITOLUL I

**Războiul informaţional: definire, caracteristici şi componente**

Războiul informaţional a devenit mai atractiv şi din punct de vedere militar, având în vedere multiplicarea numărului de ţinte vulnerabile la atacuri informatice şi creşterea necesităţii ca acestea să fie apărate. În noile circumstanţe, se constată că nici cantitatea de informaţii şi nici timpul nu vor mai fi un factor cheie în procesele politice şi militare de luare a deciziilor. Ca atare, pe timpul situaţiilor conflictuale, adversarii vor avea acces simultan la cantităţi enorme de informaţii, dar cel care va deţine cele mai precise şi complete informaţii şi va beneficia de un sistem eficient de procesare şi protejare a acestora va fi cel avantajat.

Războiul informaţional este o acţiune „întreprinsă pentru obţinerea superiorităţii informatice prin deteriorarea sistemelor informatice inamice şi protejarea celor proprii”[[1]](#footnote-1).

Războiul informaţional mai poate fi ***definit*** ca „*acţiunile întreprinse pentru a dobândi o înţelegere relativ mare a punctelor forte, slăbiciunilor şi centrelor de greutate ale infrastructurii militare, politice, sociale şi economice ale adversarului*” sau ca „*acţiuni întreprinse pentru obţinerea superiorităţii informaţionale în sprijinul strategiei militare internaţionale, prin afectarea informaţiilor şi sistemului informaţional ale adversarului, apărându-le în acelaşi timp pe cele proprii*”[[2]](#footnote-2).

Informaţia reprezintă o lămurire, o veste, o ştire, un element nou în raport cu totalitatea cunoştinţelor anterioare/prealabile, cuprinse în semnificaţia unui simbol sau grup de simboluri (text scris, mesaj verbal, imagini plastice etc.).

Informaţia este vulnerabilă şi atacabilă. Trebuie protejate trei ***caracteristici*** ale acesteia: c*onfidenţialitatea*, *integritatea* şi *disponibilitatea*.

*Confidenţialitatea*: în domeniul civil, se vorbeşte despre secretul medical, secretul bancar etc.; în domeniul militar, se vorbeşte despre secretul de apărare.

*Integritatea informaţiilor*: în domeniul civil, putem exemplifica prin situaţia reală a unui cont bancar, iar în domeniul apărării, prin obiectivul ce trebuie atins de o rachetă. Dacă aceste informaţii sunt modificate fără ştirea autorului, riscurile sunt uriaşe.

*Disponibilitatea*: reprezintă accesibilitatea informaţiilor la momentul oportun. De exemplu, accesul la un serviciu, cum este *internetul*, sau de exemplu în domeniul militar, accesul unui stat major la situaţia tactică.

Strategia militară a României apreciază că în viitor, pe câmpul de luptă, confruntările violente se vor manifesta în câmpul informaţional şi al tehnologiei avansate, al războiului în toate mediile, iar ponderea factorilor cantitativi şi energetici se va diminua continuu în favoarea celor calitativi şi informaţionali. Succesul forţelor armate ale României într-un viitor conflict militar va depinde de: evitarea surprinderii, în special în câmpul informaţional; capacitatea de a riposta eficient; cooperarea activă cu Forţele partenere (aliate); activarea oportună a forţelor de rezerva; desfăşurarea cu profesionalism a operaţiilor întrunite; executarea apărării active; asigurarea protecţiei depline a forţelor.

Elementele metodelor de ducere a acestui tip de război nu mai au o natură exclusiv militară, fiind din ce în ce mai folosite în cadrul luptei politice pentru promovarea şi apărarea intereselor naţionale sau de alianţă (coaliţie).

Dispunând de instrumentele şi capacităţile reale din domeniul războiului informaţional se poate acţiona pentru:

- prevenirea apariţiei unor ameninţări la adresa obiectivelor siguranţei naţionale şi internaţionale;

- descurajarea prin mijloace informaţionale a entităţilor generatoare a acestor ameninţări;

- menţinerea controlului asupra gradului şi a ritmului de escaladare a conflictului.

Angajarea mijloacelor de război informaţional trebuie să se facă din fazele incipiente ale unei crize, pentru a putea fi folosit întregul spectru al acţiunilor, ca prime măsuri în opţiunile de descurajare strategică.

Războiul informaţional cuprinde două ***componente*** operaţionale: una *ofensivă* şi alta *defensivă*.

*Componenta ofensivă* se poate manifesta prin exploatarea informaţiilor părţii adverse (fie prin interferare, fie prin manipulare) desfăşurând: *acţiuni distructive directe* şi *acţiuni distructive indirecte* (inducerea confuziilor prin interferare; întârziere; saturare sau intoxicare; bruiere sau distorsionare; rutare eronată; modificare semantică); *acţiuni de manipulare prin propagandă*, *descurajare*, *ameninţare cu forţa, demonstraţii, ultimatumuri*, precum şi acţiuni *terorist­diversioniste*; *acţiuni constructive* (embargouri – economic, militar, informaţional –; apel la discernământ politic, militar, economic şi social; apel la sprijin umanitar internaţional şi declaraţii).

*Componenta defensivă* se poate manifesta prin: protejarea tehnică hardware a echipamentelor individuale şi reţelelor de comunicaţii şi calculatoare; creşterea gradului de redundanţă a informaţiilor;

Războiul informaţional are ca bază următoarele ***principii***:

- *principiul „decapitării”* – comanda şi controlul, suportul decizional, comunicaţiile, sunt ţinte primare în planificarea operaţiilor informaţionale, în intenţia de a separa conducerea de execuţie;

- *principiul întâietăţii senzorilor* – toţi senzorii adversarului trebuie să fie distruşi sau reduşi la tăcere înainte de angajarea în luptă;

- *principiul cunoştinţelor* – cât mai multe informaţii trebuie să fie disponibile la cei care au nevoie de el;

- *principiul promptitudinii* – stabileşte existenţa unei capacităţi de decizie scurtă şi a unei politici de urgenţă, ce recunoaşte natura senzitivă a informaţiei;

- *principiul interoperabilităţii* – sistemele informatice şi de comunicaţii trebuie să fie, pe cât posibil, interoperabile, astfel încât informaţiile să fie viabile;

- *principiul supravieţuirii* – strategia şi politicile de control ale războiului informaţional trebuie centralizate, iar planificarea şi execuţia descentralizate, pentru a face extrem de dificilă atacarea acestora din urmă;

- *principiul ierarhiei* – împotriva oricărui adversar trebuie utilizată toată tehnologia informaţională disponibilă;

- *principiul intensităţii* – la nivelul operaţional războiul informaţional nu se controlează de factorul politico-militar; acesta trebuie să furnizeze numai direcţiile şi treptele de escaladare[[3]](#footnote-3).

Intrarea omenirii în era informaţională a determinat recunoaşterea faptului că războiul informaţional are potenţial de a deveni un tip de război la fel de important ca şi cel terestru, naval, aerian sau spaţial. Informaţia, în era informaţională, este o armă, dar, în acelaşi timp şi o adevărată materie primă strategică, necesară deciziei şi succesului oricărei politici.

În orice stat domeniile de activitate cum sunt cel politic, economic, social, militar, cultură naţională, credinţă şi tradiţii religioase specific naţionale, precum şi cel extern pot avea de suferit în urma agresiunilor informaţionale.

Importanţa şi atenţia specială acordată războiului informaţional, preocuparea pentru perfecţionarea sa şi alocarea unor resurse financiare substanţiale în acest scop atestă valabilitatea sintagmei potrivit căreia „*cine deţine informaţia deţine puterea*”.

În această idee, unele state au trecut deja la implementarea războiului informațional drept permanent.

CAPITOLUL II

**Forme ale războiului informaţional**

***Formele de bază*** ale războiului informaţional, care implică protecţia, manipularea, degradarea şi anularea informaţiei, sunt: *războiul de comandă şi control*; *războiul „supremaţiei informaţiilor”*; *războiul electronic*; *războiul psihologic*; *războiul hacker-ilor*; *războiul informaţiilor economice*; *războiul în spaţiul de luptă al realităţii virtuale*.

*Războiul de comandă şi control* (C2W – Command & Control Warfare) – (forma exclusiv militară a războiului informaţional) are menirea să anihileze comanda şi sistemele de comandă-control ale unui adversar prin integrarea operaţiilor psihologice, a securităţii operaţiilor, a inducerii în eroare, a războiului electronic şi a distrugerii fizice, reciproc sprijinite de către activitatea informativă, în scopul interzicerii accesului la informaţii, influenţării, degradării, sau distrugerii capabilităţilor de comandă-control ale adversarilor, concomitent cu protejarea acestor capabilităţi ale aliaţilor împotriva aceloraşi tipuri de acţiuni.

Războiul de comandă-control reprezintă un subdomeniu al acţiunilor de război informaţional, fiind utilizat în toată gama de acţiuni militare desfăşurate la toate nivelurile de conflict şi are două părţi: ofensiv şi defensiv.

Partea ofensivă a războiului de comandă-control are ca scop împiedicarea funcţionării eficiente a comenzii-controlului pentru blocarea accesului la informaţii, influenţarea, degradarea sau distrugerea sistemului de comandă-control al adversarului.

Partea defensivă a războiului de comandă-control vizează utilizarea eficientă a propriilor forţe în contracararea acţiunilor adversarului pentru a împiedica accesul la informaţii, influenţarea, degradarea, sau distrugerea sistemului de comandă-control propriu.

*Războiul ,,supremaţiei informaţiilor”* – constă în proiectarea, protecţia şi anihilarea sistemelor care conţin suficiente informaţii (cunoştinţe) pentru a domina un spaţiu de conflict.

Războiul „supremaţiei informaţiilor” are consecinţe directe, mai degrabă în aplicarea atacului ţintei decât „octeţii virusaţi”. Pe măsură ce tehnologia senzorilor devine tot mai performantă (generând produse cu precizie şi fiabilitate ridicate, în tipuri şi cantităţi diversificate), misiunea dezvoltării, întreţinerii şi exploatării sistemelor ce „simt” spaţiul de conflict, îi evaluează structura şi transmit rezultatele către trăgători, atrage după sine creşterea importanţei organismelor militare de mâine.

*Războiul electronic* – utilizează tehnologia şi tehnica electronică, precum şi tehnici criptografice pentru a domina spaţiul electromagnetic. Obiectul acţiunilor acestuia îl reprezintă confruntarea în spaţiul electromagnetic, cu scopul de a distruge baza fizică de transfer a informaţiilor.

Componentele războiului electronic sunt: sprijinul electronic; atacul electronic; protecţia electronică.

*Războiul psihologic* – din perspectiva războiului informaţional, utilizează informaţia pentru a modifica atitudinile şi opţiunile forţelor proprii, a celor neutre şi adversarilor, în funcţie de interesele existente, în aşa fel încât să fie afectată îndeplinirea obiectivelor politice şi militare.

Acţiunile de război psihologic nu se limitează la slăbirea moralului populaţiei inamice, ci încearcă să întărească moralul populaţiei proprii şi să câştige adeziunea populaţiei considerate în principiu neutră.

Există patru categorii de acţiuni psihologice, astfel: acţiuni împotriva voinţei naţionale; acţiuni împotriva comandanţilor inamici; acţiuni împotriva forţelor militare; conflictul cultural.

*Războiul hacker-ilor* („Pirateria software'') – (HW – Hacker warefare) –constă în atacuri pasive şi active asupra sistemelor informatice. Sistemele modeme de comunicaţii de date şi telecomunicaţii sunt, probabil, punctul cel mai slab al infrastructurii economice şi militare din ţările industrializate, în special după răspândirea masivă a INTERNET-ului. Hackerii pot să acţioneze pe modem de la o distanţă convenabilă, fără a se teme că vor fi descoperiţi. Sunt deci necesare măsuri de protecţie considerabile pentru a împiedica căderea reţelelor de calculatoare în urma unui atac coordonat, în caz de război. Reţele şi calculatoarele insuficient protejate pot fi distruse, controlate sau infestate fără a se observa, cu „programe adormite”, care, la un moment dat, pot fi activate.

Războiul hacker-ilor, centrat pe reţelele de calculatoare şi de comunicaţii, constă în integrarea flexibilă a acţiunilor din punctele de comandă, a mijloacelor ISR, sistemelor de tragere şi sistemelor de armament şi de sprijin, pentru ca în final să permită distorsionarea informaţiilor inamicului şi vitezei lui de reacţie, astfel încât să poată declanşa o puternică operaţie informaţională.

Armatele ţărilor dezvoltate tehnologic plănuiesc pentru un război viitor să scoată din funcţiune sau să manipuleze reţelele de comunicaţii de date şi de telecomunicaţii, precum şi sistemele radar şi de armament, utilizând un spectru larg de mijloace moderne, printre care se numără şi viruşii informatici şi atentatele prin INTERNET.

*Războiul informaţiilor economice* – reprezintă ansamblul activităţilor coordonate de căutare, prelucrare şi difuzare a informaţiei despre mediul specific desfăşurării activităţilor de tip economic, asociind statul şi întreprinderile.

*Războiul în spaţiul de luptă al realităţii virtuale* (CYBW ­„cyberwarefare”) – este în prezent, un „punct de acumulare” al scenariilor futuriste, cercetării fundamentale şi tehnologice.

Procedeele luptei informaţionale sunt de trei categorii de bază: *de forţă*, *inteligente* şi *combinate*.

*Procedeele de forţă* se bazează pe distrugerea obiectivelor luptei informaţionale prin diferite categorii de armament (clasic, radioelectronic, informatic) pentru obţinerea superiorităţii informaţionale prin diferenţa cantitativă a informaţiei necesare pentru îndeplinirea misiunii de conducere a trupelor.

*Procedeele inteligente* sunt orientate spre intoxicarea cu informaţii credibile a conducerii inamicului şi se materializează prin diferenţa calitativă a informaţiilor.

*Procedeele combinate* includ cele două procedee şi asigură calitativ şi cantitativ superioritate informaţională asupra situaţiei de luptă.

În cadrul luptei informaţionale distingem două grupuri de bază: *ofensive* şi de *apărare*. Dintre acestea, de regulă, se folosesc următoarele modalităţi: *de blocare*, *de distragere a atenţiei*, *de imobilizare*, *de epuizare*, *de simulare*, *de dezintegrare (dezbinare)*, *de liniştire*, *de intimidare*, *de provocare*, *de suprasolicitare*, *de sugerare*, *de constrângere*, *de deblocare* şi *de identificare*.

O imagine realistă a urmărilor provocate de un război informaţional, în care viaţa cotidiană ar putea fi bulversată complet, ar genera cele mai diverse manifestări, cum ar fi: lipsa căldurii, a gazelor, apei şi energiei electrice în locuinţe şi centre industriale; scăderea producţiei; şomajul peste limitele prevăzute; scăderea puterii de cumpărare a populaţiei; tensionarea situaţiei sociale, greve, încercări de lovituri de stat şi nesupunerea maselor în faţa legilor; blocarea sistemelor financiar-bancare şi devalorizarea monedei naţionale; izolarea ţării respective faţă de comunitate a internaţională, limitarea accesului la resursele strategice; influenţarea deciziilor politice şi ale organelor administraţiei de stat de către cercuri străine de interesele statului. Toate aceste posibile dereglări pot fi materializate prin coroborarea cu acţiunile clasice şi cu creşterea în intensitate a atacurilor specifice acţiunilor informaţionale care ar viza:

- compromiterea prin mass-media a conducerii instituţiilor fundamentale ale statului respectiv şi a personalităţilor din conducerea acestora;

- asasinarea (tentative de asasinare) unor personalităţi străine aflate în vizite oficiale;

- acţiuni de sabotaj la obiectivele economice de importanţă vitală (hidrocentrale, centrale atomo-nucleare, accidente chimice şi industriale etc.) desfăşurate de elemente terorist-diversioniste şi apariţia de formaţiuni ilegal înarmate care sprijină politica antinaţională a unor grupări politice care au interese diferite de ale statului respectiv;

- compromiterea şi ridiculizarea valorilor naţionale;

**Concluzii**

Dezvoltarea infrastructurii informaționale, în curs de globalizare, în care se includ și structurile mediatice generează posibilități de comunicare din ce în ce mai sofisticate. Acestea transmit informațiile într-un ritm tot mai aceelerat și pe distanțe tot mai mari. Condiția esențială pentru ca aceste lucruri să se întâmple este ca conglomeratele comunicaționale să nu fie controlate de anumite centre de decizie, care pot încerca să controleze accesul oamenilor la resursele informaționale.

Agresiunile informaționale nu sunt noi. Noutatea decurge din folosirea rezultatelor cercetării științifice pentru conceperea mesajelor astfel ca ele să aibă efectul scontat precum și folosirea presei pentru transmiterea mesajelor manipulatoare. Combinarea acestor două elemente amplifică posibilitățile de agresiune informațională prin folosirea unor canale de comunicare pertinente și prin mesaje deosebit de bine elaborate. Dezvoltarea mijloacelor de comunicare și a cercetării științifice face posibilă elaborarea unor strategii de manipulare informațională atât la nivel planetar, cât și la nivel local sau chiar individual. Aceste situații nu sunt doar posibile, ci prezente în realitate.

Agresiuniile au nevoie de condiții pentru că ele să poată avea efect. Presa trebuie să fie liberă de orice control public, redacțiile trebuie să fie vaste și transnaționale, canalele de informare trebuie să fie private, accesul oamenilor la presă să fie liber, fără controlul public, discernământul oamenilor să fie redus.

Tehnologia informaţiei şi comunicaţiilor a evoluat foarte mult şi oferă acum soluţii pentru multe dintre preocupările omenirii, şi, implicit, pentru domeniul militar. Este de asemenea evident, evidenţiere mult vizibilă în business, că nu tehnologia reprezintă punctul nevralgic al unui sistem, ci cultura organizaţională şi structura operaţională. Din acest motiv, trebuie subliniat încă o dată că, în ceea ce priveşte Războiul informaţional, tehnologia oferă soluţii la toate provocările teoretice enunţate de către iniţiatorii conceptului sau de către responsabilii militari, dar nu poate înlocui aspectele referitoare la resursa umană.

Totodată, trebuie menţionat faptul că informatizarea globală a societăţii, poate duce într-un viitor apropiat la folosirea mai intensă a armei informaţionale contemporane pe timpul războiului informaţional. Numeroase indicii evoca posibilitatea unei noi revoluții științifice ce se produce în domeniul procesării informației. Strategii americani încearcă să confiște aceste descoperiri pentru a determina ca ele să fie folosite cu prioritate de Statele Unite, pentru ca ele să dețină un avantaj asupra tuturor statelor, inclusiv asupra aliaților.

Tehnicile țin de generația a doua a agresiunilor informaționale și constau în atacarea structurilor mediatice.

**Bibliografie**

1. Preşedinţia României, *Strategia de Securitate Naţională*, Bucureşti, 2007.
2. Guvernul României, *Carta albă a securităţii şi apărării naţionale*, Bucureşti, 2004.
3. Strategia Militară a Românei, ed.2007, [www.mapn.ro](http://www.mapn.ro)
4. Stan PETRESCU, *Războiul Informaţional*, Editura Militară, Bucureşti, 1999.
5. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2661368>
6. <https://www.ceeol.com/search/article-detail?id=603903>
7. <https://cji.md/blocarea-surselor-online-utilizate-in-razboiul-informational-ce-presupun-recentele-completari-din-dispozitia-cse/>
8. Gheorghe ARĂDĂVOAICEI, *Războiul de azi şi de mâine*, Editura Militară, Bucureşti, 1999.
9. Sun Tzu, *Arta Războiului*, Editura Antet, Bucureşti, 1993.
10. Alvin şi Hedi Toffler, „*Război şi antirăzboi*”, Editura ANTET XX PRESS, Bucureşti, 1995.
11. *Joint Doctrine for Jnformation Operations*, Defense Intelligence Journal, 1996.
12. Henri Pierre CATHALA, *Epoca dezinformării*, Editura Militară, Bucureşti, 1991.

1. AAP-6 (2007), Glosar NATO de termeni şi definiţii, Ed. Universităţii Naţionale de Apărare, Bucureşti, 2007. [↑](#footnote-ref-1)
2. Joint Doctrinefor lnformation Operations, Defense Intelligence Joumal, 1996. [↑](#footnote-ref-2)
3. Petrescu Stan, *Războiul Informaţional*, Editura Militară, 1999, pag. 123. [↑](#footnote-ref-3)