ABORDĂRI MODERNE PRIVIND RĂZBOIUL INFORMAȚIONAL PE TIMP DE PACE, CRIZĂ SAU RĂZBOI

Radu POPA

As a modern form of military action, information warfare is a result of a global information revolution which has fundamentally changed the society. Herein we point out the content, characteristics and components of the information warfare in the manner in which there are presented in specific literature.

Specialiştii militari care au studiat războiul contemporan afirmă, cu îndreptățit temei, că acesta s-a extins enorm[1], luând forme care altădată nu-i erau specifice şi se desfăşoară continuu, manifestându-se ca un război permanent, prin confruntări în diferite domenii (politic, economic, informațional), prin crize şi conflicte militare. În cadrul acestuia, războiul informațional ocupă un loc din ce în ce mai important, fiind deopotrivă un război fizic, care urmăreşte întârzierea utilizării de către adversar a mijloacelor de culegere, transmitere, prelucrare şi diseminare a informațiilor prin dezorganizarea rețelelor informaționale, şi un război virtual, prin care să se realizeze supremația sau cel puțin superioritatea informațională, pentru că "cine stăpâneşte informația, domină totul", aceasta devenind, astfel, şi o principală armă de luptă.

Revoluția informațională şi războiul informațional

Ampla dezvoltare a structurilor şi volumelor de informații şi posibilitățile aproape nelimitate de transmitere, memorare, afişare şi distribuire, în timp real, a acestora, datorită marilor posibilități asigurate de tehnologia informației bazată pe digitizarea aproape integrală a informațiilor, a determinat ca specialiştii occidentali (şi nu numai) să aprecieze că avem de-a face cu o adevărată revoluție informațională. Aceasta are implicații deosebite în toate domeniile de activitate: economic, politic, social, militar etc., perfecționând şi schimbând radical conținutul, funcțiile şi modul de desfăşurare a proceselor informaționale şi decizionale aferente.

[1] M. Mureşan, Gh. Văduva, *Războiul viitorului, viitorul războiului*, Editura Universității Naționale de Apărare "Carol I", Bucureşti, 2006, p. 14.

Principial, revoluția informațională a evoluat în trei faze, astfel[2]: în perioada 1837 şi 1963, aceasta s-a caracterizat prin dezvoltarea telegrafiei, radioului şi comunicațiilor cu fir, care au permis un important control asupra surselor de informații. Treptat, în cadrul acestei etape, s-a manifestat tendința de centralizare a sistemelor informaționale. Cea de-a doua fază a început în anul 1964 prin construirea familiei de calculatoare IBM-360 şi s-a încheiat în anul 1990, pe parcursul acesteia realizându-se dezvoltarea unor sisteme performante de comunicații şi informatice, destinate, în principal, marilor utilizatori de informații (organe ale administrației de stat, corporații economice, apărare şi securitate națională). A treia fază a început în anul 1991 şi poate fi definită ca era informației distribuite, a calculatoarelor şi a Internetului, bazată pe utilizarea unor mijloace tehnice de calcul şi de comunicații constituite în rețele performante de mare amploare. Noile realizări ştiințifice, miniaturizarea echipamentelor şi prețul redus al acestora au determinat ca societatea, în general, să devină preponderent informațională, iar puterea de calcul să se dubleze la fiecare 18 luni. Accesul la Internet este acum disponibil atât pentru instituții, cât şi pentru persoane fizice, devenind un instrument principal de proliferare a cunoştințelor, de informare şi comunicare.

Era calculatoarelor a creat capabilități pentru obținerea, evaluarea, utilizarea, transmiterea şi schimbul, cu mare viteză, al unor volume mari de informații adresate simultan mai multor utilizatori.

Informațiile au devenit principala resursă strategică a fiecărei națiuni. Acest lucru a fost evidențiat încă din anul 1981 de către preşedintele SUA, Ronald Reagan, care, în strategia sa de securitate națională, menționa că "informația constituie a patra dimensiune a puterii naționale"[3].

Desigur, în aceste condiții, nu puteau să nu apară şi posibilitățile de exploatare rău intenționată a vulnerabilităților sistemelor informaționale, cu precădere a rețelelor de comunicații şi calculatoare ale acestora, afectând atât structura lor tehnică, dar, mai ales, pe cea informațională, prin atacarea surselor de informații, bazelor de date, canalelor de transport al datelor, punctelor de prelucrare şi diseminare, sistemelor de operare şi gestiune şi a altor produse software realizate de firme specializate sau de către utilizatori.

Trecerea de la acțiuni distructive izolate şi de mică amploare la acțiuni de masă de ciberterorism şi de atac asupra informațiilor a determinat amplificarea preocupărilor statelor şi structurilor lor militare pentru fundamentarea războiului informațional, stabilirea principiilor şi a modului de desfăşurare a acestuia în situații de pace, criză şi la război.

---

[2] Copeland Thomas E., *The Information Revolution and National Security*, Internet (ISBN 1-58487-030-1), august 2000, p. 53.

[3] *National Strategy and Information Warfare*, SUA, 1981, p. 119.

Unele metode şi tehnici specifice războiului informaţional nu reprezintă o noutate, întrucât acţiunile de dezinformare a adversarului, prin furnizarea de informaţii false, interceptarea şi analiza comunicărilor acestuia, penetrarea sistemelor de securitate a informaţiilor, mai ales criptografice, şi sustragerea de documente, au fost utilizate şi în războaiele trecute.

Atât în trecut, cât, mai ales, în prezent, fiecare parte beligerantă va încerca să dea un anumit curs acţiunilor adversarului[4] prin manipularea convenabilă a fluxurilor de date şi informaţii, maximizarea elementelor de surpriză şi asumarea vulnerabilităţilor.

Conţinutul şi caracteristicile războiului informaţional

Războiul informaţional constituie o operaţie de luptă în mediul înalt tehnologizat. El este o componentă a războiului în general, fiind un produs al erei informaţionale, definit prin utilizarea pe scară largă a unor mijloace tehnice specifice sau nontehnice pentru afectarea informaţiilor şi a infrastructurii informaţionale a statului şi/sau a câmpului de luptă cibernetizat, structurat pe reţele. Urmăreşte distrugerea capabilităţilor de comandă şi control ale inamicului, în principal a celor bazate pe utilizarea tehnologiei informaţiei, pe baza exploatării vulnerabilităţilor adversarului în procesele informaţionale şi de luare a deciziilor.

Multe ţări consideră atacul împotriva infrastructurii informaţionale echivalent cu o lovitură strategică. Fazele proceselor de comandă şi control pe timpul cărora se pot desfăşura acţiuni de război informaţional sunt menţionate în *figura 1*.

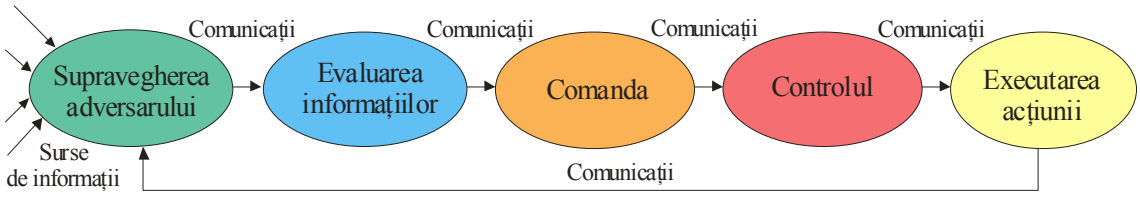

Fig. 1 *Fazele proceselor de comandă şi control supuse atacului informaţional*

Se apreciază că războiul informaţional, ca prototip al viitoarelor conflicte între state şi armatele acestora, va fi un alt fel de război, bazat pe informaţie şi tehnologia informaţiei, deosebit radical faţă de cele anterioare. Acesta necesită mijloace şi procedee de acţiune neutilizate în trecut, bazate pe principii şi măsuri de atac specifice erei informaţionale, având comunicaţiile

[4] Adversar nu este numai acela care se află într-o tabără totdeauna ostilă şi gata de luptă, ci poate fi un sistem de provocări, ameninţări şi vulnerabilităţi care se cer soluţionate, iar soluţia nu constă mereu în distrugerea celuilalt. (E. Bădălan şi alţii, *Eseu despre arta strategică*, Editura Militară, Bucureşti, 2005, p. 18).

şi reţelele de calculatoare ca domenii principale de acţiune. Utilizarea informaţiei ca armă îi conferă acesteia rolul primordial în luarea deciziilor şi asigurarea succesului, determinând schimbări esenţiale în desfăşurarea acţiunilor militare şi nonmilitare pe timp de pace, criză şi război. Experienţa dobândită a dovedit că, în toate situaţiile conflictuale, informaţia constituie un factor critic.

În condiţiile actuale, gândirea despre războiul informaţional este influenţată de ampla dezvoltare a teoriei informaţiei, informaticii şi ciberneticii, precum şi a bazelor ştiinţifice a sistemelor şi reţelelor, cu principiile lor de interconectivitate. În ansamblu, acestea au impact fundamental asupra organizării statale şi militare, precum şi asupra proceselor decizionale pentru comandă şi control, manifestându-se cu multă putere şi influenţând însăşi dinamica fenomenului de globalizare.

Războiul informaţional este legat de ampla dezvoltare a infosferei, a structurilor de informaţii şi a tehnologiei de care dispun acestea, precum şi de volumul imens al informaţiilor[5], datelor şi cunoştinţelor ştiinţifice utilizate pentru realizarea dominaţiei informaţionale asupra adversarului în întregul spaţiu de interes şi în toate sau, cel puţin, în principalele domenii de activitate.

În viziunea specialiştilor militari americani[6], domeniile războiului informaţional şi spectrul acestuia sunt cele prezentate în *figura 2*.

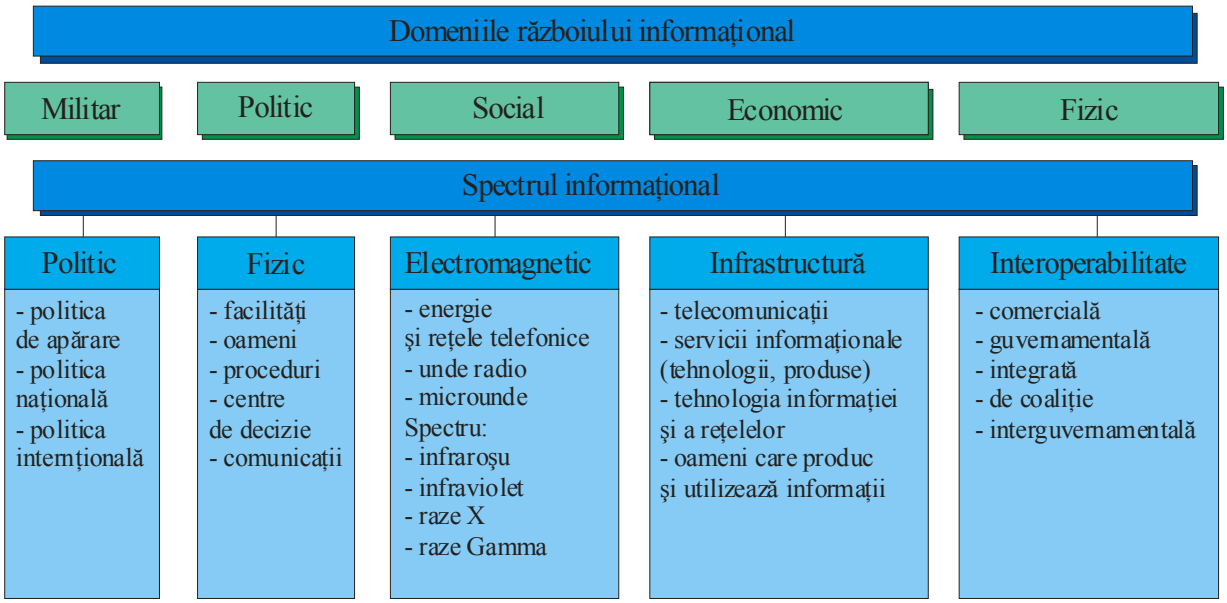

Fig. 2 *Domeniile războiului informaţional şi spectrul informaţiilor*

[5] Data reprezintă orice entitate (de informaţie) neprocesată, provenită de la surse, ce poate fi utilizată pentru producerea informaţiilor. Informaţia reprezintă produsul rezultat din procesarea datelor referitoare la state străine, forţe sau elemente ostile ori potenţial ostile, sau despre spaţiile operaţiilor în curs sau viitoare [AAP-6/2003]. În contextul acţiunilor militare, informaţia reprezintă totalitatea cunoştinţelor pe care le avem despre inamic, adică baza propriilor noastre idei şi acţiuni.

[6] I.R. Winkler, C.I. O'Shea, M.C. Stokrp, *Information Warfare*, INFOSEC and Dynamic Information Defense, iunie 1995, Command and Control Symposium, Monterey, SUA.

Se poate afirma că războiul informațional constituie o formă invizibilă, dar continuă de acțiune asupra statelor, organizațiilor economico-sociale şi structurilor militare, fără frontiere geografice, spațiale, politice etc. şi avertizare prealabilă. El cuprinde o succesiune de operații informaționale ce utilizează atât mijloace active, cât şi pasive pentru obținerea informațiilor despre adversar (potențial adversar), precum şi pentru atacul, mai ales electronic, asupra sistemelor informaționale ale acestuia, în vederea distrugerii lor şi mai puțin pentru nimicirea oamenilor. Din acest punct de vedere, războiul informațional ar putea fi considerat o "acțiune curată", cu grad de letalitate scăzut sau chiar inexistent, dar care poate fi un mare pericol chiar şi pentru existența statului.

Se poate concluziona că abordarea conceptului de război informațional cuprinde partea de cunoştințe ştiințifice specifice (informații, date, analize, metode, suport cibernetic), iar cel de operații informaționale se va referi la partea de ştiință aplicată, adică modul de organizare, planificare şi executare a unei acțiuni specifice, în funcție de obiectivul de îndeplinit.

Amenințarea războiului informațional este omniprezentă şi semnificativă atât pe timp de pace, cât şi la criză şi în situații de război, constituind un pericol permanent, care trebuie identificat şi prevenit oportun. Scopul acestuia constă în asigurarea avantajului economic, politic, diplomatic sau militar şi în separarea conducerii superioare (centrale) de instituțiile subordonate şi de mase.

Cea mai importantă caracteristică a viitorului război informațional constă în asigurarea dobândirii, prin toate mijloacele, a avantajului informațional ierarhizat pe trei niveluri: superioritate informațională, dominație informațională şi supremație informațională. Prin modul de desfăşurare şi conținutul său, războiul informațional poate fi inclus în categoria acțiunilor asimetrice, el încorporând şi elemente de terorism informațional, manifestat în diferite forme, care au scopul să contribuie la înfrângerea unui adversar superior.

În general, războiul informațional cuprinde[7] ansamblul acțiunilor ofensive şi de apărare, întreprinse prin mijloace tehnice specifice, pentru dobândirea superiorității informaționale[8], prin afectarea informațiilor adversarului, a proceselor (decizionale) bazate pe informații, a sistemelor

[7] Glossary: The Convoluted Terminology of Information Warfare (DOD-Dictionary of Military Terms).

[8] Superioritatea informațională constă în capacitatea de a derula toate procesele ciclului informațional (colectarea, procesarea şi diseminarea informațiilor în flux neîntrerupt) în timp mai scurt decât al adversarului, cu grad de securitate mare şi a împiedica inamicul să facă acelaşi lucru [US Joint Pub. 3-13]. Se bazează pe utilizarea eficientă a capabilităților C4ISR.

informaționale şi rețelelor de calculatoare, concomitent cu protecția (apărarea) informațiilor proprii, a sistemelor bazate pe informații, a sistemelor informaționale şi a rețelelor de calculatoare aferente. Altfel spus, războiul informațional constituie efortul orchestrat pentru a obține victoria prin subminarea şi neutralizarea sistemelor de comandă şi control (C2) ale inamicului, concomitent cu protecția utilizării sistemelor de comandă şi control proprii destinate pentru coordonarea acțiunilor forțelor aliate.

Războiul informațional ofensiv constă în atacul direct al sistemelor informaționale ale inamicului şi include distrugerea fizică sau suprimarea operațiilor sale informaționale prin bruiaj, precum şi executarea de acțiuni pentru slăbirea sau întreruperea proceselor de comandă şi control ale acestuia.

Apărarea constă în asigurarea creşterii rezistenței echipamentelor de calcul şi de comunicații proprii la interferențe, sporirea posibilităților de apărare împotriva atacurilor fizice ale inamicului. Se apreciază că apărarea platformelor ce utilizează tehnologia informației şi asigurarea funcționării normale a echipamentelor pentru comandă şi control are aceeaşi importanță ca şi acțiunile ofensive ale războiului informațional.

Războiul informațional ocupă un loc din ce în ce mai important, fiind, deopotrivă, un *război fizic* executat cu mijloace de luptă convenționale şi specifice, care urmăreşte distrugerea echipamentelor tehnice sau interzicerea utilizării, de către adversar, a mijloacelor proprii de culegere, transmitere, prelucrare şi diseminare a informațiilor prin dezorganizarea rețelelor informaționale, şi un *război virtual*, prin care se realizează supremația informațională asupra acestuia, pe întreaga durată a acțiunilor militare sau pe perioade determinate.

Câmpul de desfăşurare a războiului informațional este constituit din infrastructura informațională sau infosfera, cu identificarea implicațiilor rezultate din atacul informațional (activ sau pasiv) al elementelor sale asupra ciclului de comandă şi control al adversarului.

Se va avea în vedere că un sistem informațional este cu atât mai complex, cu cât cuprinde mai multe informații şi trebuie să dispună de o redundanță mai mare pentru asigurarea fiabilității.

Principalele amenințări determinate de acțiunile de război informațional ale adversarului au în vedere infrastructura informațională de stat, economică, politică, a serviciilor de informații şi de opinie publică, precum şi a apărării, serviciilor medicale şi de urgență etc., toate acestea constituind, în esență, infrastructura informațională a securității naționale, prezentată sintetic în *figura 3*.

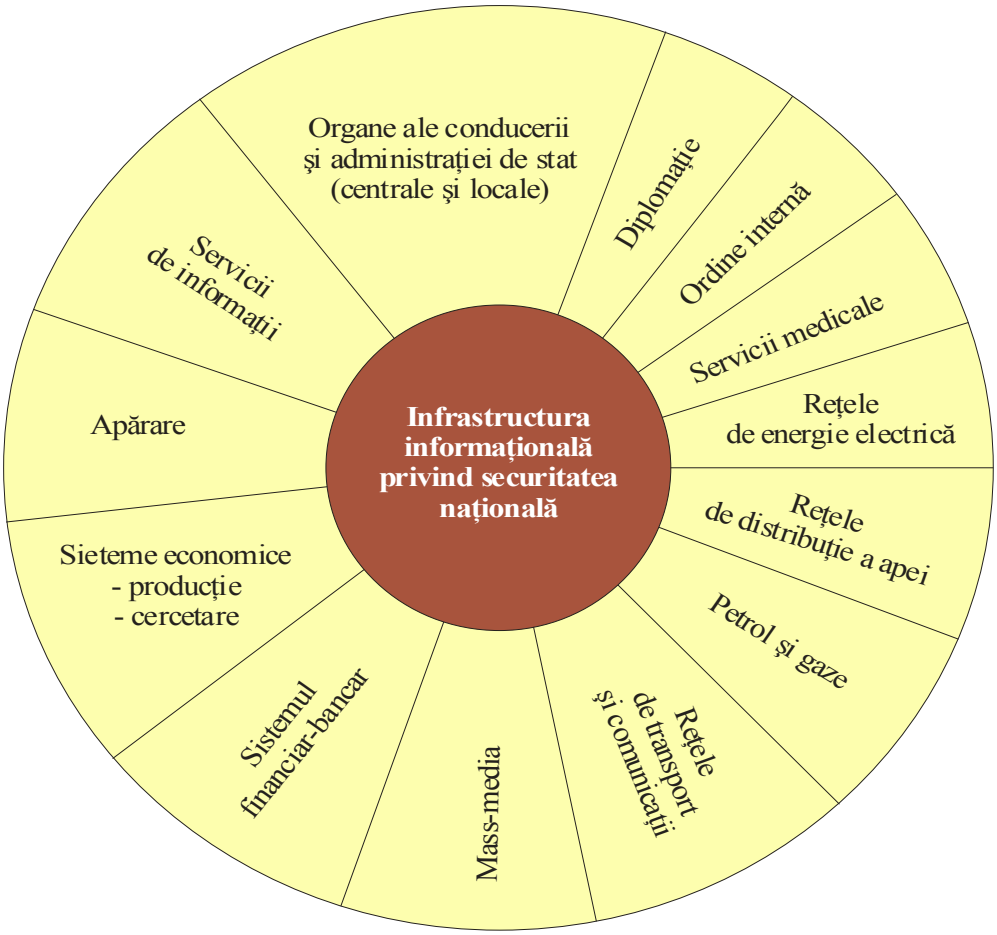

Fig. 3 *Structura infrastructurii informaționale*

Infrastructura informațională include mai mult decât facilitățile fizice utilizate pentru transmiterea, memorarea, prelucrarea şi redarea vocii, datelor şi imaginilor, precum şi pentru lucrul în rețelele de calculatoare şi accesul la Internet. Ea se bazează pe o colecție largă de echipamente informaționale, şi anume: calculatoare, comutatoare, suporți de date şi video, camere video, scannere, claviaturi, telefoane, faxuri, benzi video şi audio, cabluri, fibre optice, stații radio şi radioreleu, sateliți etc.

Informația însăşi poate cuprinde şi aplicații software pentru prelucrarea datelor şi video, baze de date ştiințifice, economice, politico-sociale şi de apărare, imagini şi înregistrări sonore, biblioteci şi tehnici de păstrare şi vehiculare a acesteia.

Arhitectura informațională a securității naționale trebuie să fie pregătită pentru a suporta şi preveni implicațiile războiului informațional, pentru că este vulnerabilă, deoarece numai principalele sisteme informaționale ale acesteia, care vehiculează informații clasificate, sunt protejate adecvat.

Telecomunicațiile constituie un sector foarte important al infrastructurii, care se află în prima linie a atacului informațional al adversarului. De aceea, trebuie adoptate măsuri pentru asigurarea legăturii în situații de criză sau război, prin mijloace cu probabilitate redusă de

interceptare (sateliți, fibre optice, linii radioreleu pe microunde, comunicații pe frecvențe greu de bruiat şi care nu produc interferențe).

Principalele trăsături ale războiului informațional[9] ar putea fi următoarele:

- multitudinea de ținte informaționale şi arme inteligente;
- dificultatea identificării adversarului;
- absența frontierelor geografice, spațiale, politice etc.;
- efecte nonletale;
- utilizarea de tehnologii moderne îndreptate împotriva caracterului cibernetic al acțiunilor militare (software reprezintă arma de bază în desfăşurarea atacului informațional);
- realizarea operațiilor informaționale cu costuri scăzute în raport cu alte forme de luptă;
- dificultatea stabilirii precise a responsabilităților pentru protecția informațiilor şi a sistemelor informaționale.

După unii autori[10], *războiul informațional* poate fi împărțit în trei clase, definite astfel:

- *războiul asupra populației* (persoanelor), care are în vedere mai ales infrastructura informațională utilizată de aceasta (rețele de comunicații, rețele de calculatoare, baze de date pe calculatorul propriu etc.); viața personală a fiecărui membru al societății ce utilizează informatica şi tehnica de calcul ar putea fi perturbată semnificativ, chiar aruncată în haos electronic, doar printr-un atac informațional al altei persoane, în general, necunoscută;
- *războiul asupra intereselor economice, financiare şi operaționale* (management) ale unor corporații, departamente guvernamentale, agenții, servicii publice, organizații civice, universități etc., incluzând şi acțiunile de spionaj economic; în această clasă de acțiuni informaționale pot fi implicate şi sistemele electronice cu utilizare generală sau restricționată, pe care organizațiile atacate îşi bazează activitatea lor zilnică;
- *războiul pentru destabilizarea unora sau mai multor economii ori societăți*, dus împotriva industriei şi sferelor economice, a domeniilor de influență politică, a forțelor globale ale unei țări (coaliții de țări) sau a economiei globale. Foloseşte, ca armă de bază, terorismul cibernetic.

Componentele războiului informațional

Războiul informațional poate fi executat de sine stătător (independent) sau în cadrul unui conflict militar declarat, de o anumită amploare, ca parte a acestuia. În funcție de situație, se pot utiliza toate sau numai o parte din componentele războiului informațional. Pe baza experienței acumulate şi a studiilor teoretice efectuate, în literatura de specialitate se defineşte suficient de clar componentele războiului informațional, ca formă principală de

[9] Constantin Stan, *Războiul informațional*, Universitatea Națională de Apărare "Carol I", Bucureşti, 2007, p. 27.
[10] Winn Schwartau, *Information Warfare – Chaos on the Electronic Superhighway*, p. 195.

manifestare a revoluției informaționale în domeniul militar, existând şi unele particularități în abordarea acestora.

Vom prezenta aceste componente aşa cum le-a definit unul dintre teoreticienii[11] războiului informațional:

- războiul pentru comandă şi control – Command and Control Warfare – C2W;
- războiul bazat pe informații – Intelligence Based Warfare – IBW;
- războiul electronic – Electronic Warfare – EW;
- războiul psihologic – Psychological Warfare – PSYWAR;
- războiul hackerilor – Hacker Warfare – HW;
- războiul informațiilor economice – Information Economic Warfare – IEW;
- războiul împotriva infrastructurii informaționale globale – Cyber Warfare – CW.

Războiul pentru comandă şi control este destinat pentru decapitarea structurii de comandă şi control, anihilarea activității comandamentelor şi neutralizarea sau distrugerea sistemelor decizionale ale adversarului, concomitent cu protecția celor proprii. Desfăşurat şi ca o apărare efectivă împotriva războiului informațional, acesta poate fi considerat analog contramăsurilor pentru asigurarea comenzii, controlului, comunicațiilor şi prelucrării informațiilor în acțiunile militare. Are în vedere concepția filozofică că "cea mai bună apărare este atacul".

Conținutul războiului pentru comandă şi control şi suportul informațional al acestuia sunt prezentate în *figura 4*.

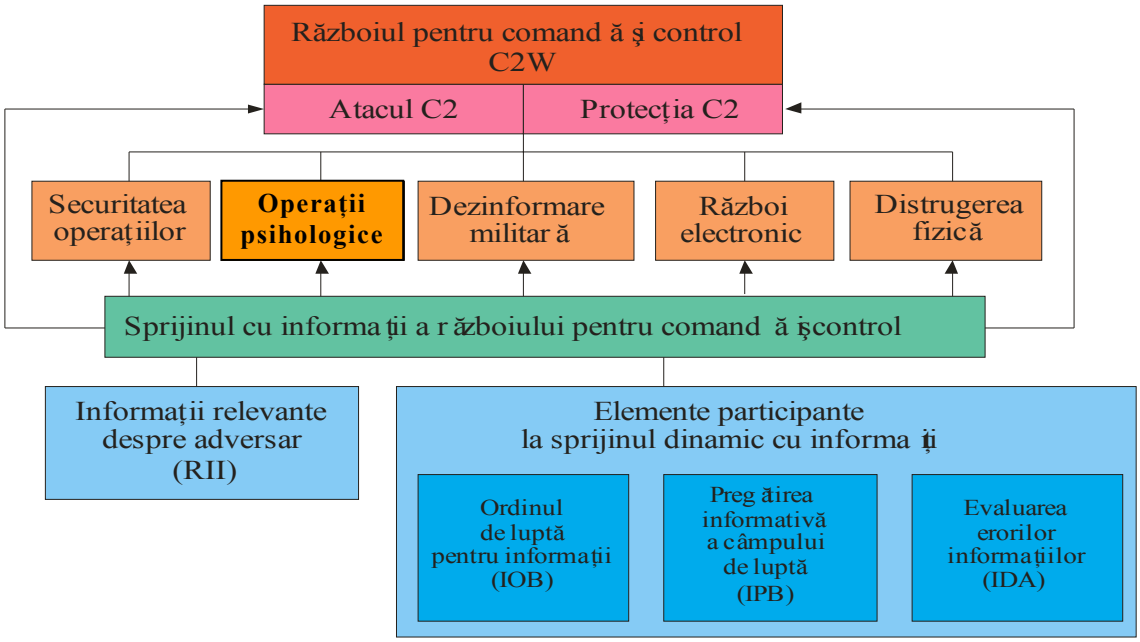

Fig. 4 *Conținutul războiului pentru comandă şi control*

[11] Martin Libicki, *What is Information Warfare*, National Defense University, Washington DC, 1995, pp. 9-41.

Evidențiem faptul că războiul pentru comandă şi control se desfăşoară în toate acțiunile militare, indiferent de nivelul conflictului, şi are două componente: ofensivă şi defensivă.

- Atacul împotriva comenzii şi controlului adversarului constă în acțiunea efectivă asupra forțelor acestuia pentru neutralizarea, distrugerea sau influențarea sistemelor de comandă şi control.
- Protecția sistemelor de comandă şi control proprii asigură funcționarea neîntreruptă a sistemelor C2 şi a comunicațiilor în condițiile atacului informațional al adversarului executat cu mijloace fizice sau radioelectronice.

Războiul bazat pe informații este utilizat împotriva intrării în timp real a informațiilor în sistemele de comandă şi control ale adversarului, inclusiv în cele ale armelor. Acesta constituie o acțiune îndreptată asupra managementului şi utilizării informațiilor în toate formele şi la toate nivelurile unui conflict, pentru obținerea de avantaje militare decisive, în special în mediul integrat, concomitent cu adoptarea de măsuri pentru asigurarea integrității, disponibilității şi interoperabilității informaționale a forțelor proprii şi aliate. Războiul bazat pe informații este aplicat şi în domeniile politic, economic şi social pentru asigurarea informațiilor pentru securitate națională pe timp de pace, criză sau război. De asemenea, el este îndreptat şi asupra centrelor de comandă care folosesc tehnologia informației pentru dominarea spațiului de luptă. Este caracterizat prin două forme de luptă: una *ofensivă*, îndreptată asupra mijloacelor tehnice de culegere a informațiilor de către adversar şi cealaltă, *de apărare*, destinată să prezerve invizibilitatea acestei componente a războiului informațional dus de către forțele proprii.

Războiul electronic cuprinde ansamblul mijloacelor pentru cercetarea şi atacul echipamentelor electronice ale adversarului (radare, comunicații, radionavigație etc.), a căror funcționare se bazează pe propagarea undelor electromagnetice şi acustice, precum şi pe utilizarea mijloacelor automate de criptare a informațiilor, concomitent cu asigurarea protecției acestora la forțele proprii şi aliate. El constituie o acțiune militară care utilizează energia electromagnetică şi pe cea directă pentru controlul spectrului electromagnetic şi atacul inamicului. Are trei componente principale: *atacul electronic, sprijinul electronic* şi *protecția electronică.*

- *Atacul electronic* reprezintă forma ofensivă de luptă care utilizează energia electromagnetică şi directă sau a armelor antiradiație pentru atacul personalului, facilităților şi echipamentelor, în vederea neutralizării sau distrugerii capabilităților de luptă ale adversarului. Include acțiuni pentru prevenirea sau reducerea utilizării efective de către inamic a spectrului electromagnetic prin bruiaj şi dezinformare, şi utilizarea de arme (laser, cu frecvență radio, cu particule) pentru distrugerea tehnicii acestuia.
- *Sprijinul electronic* are în vedere acțiunile de cercetare, identificare şi localizare a surselor de radiație electromagnetică în vederea neutralizării lor.

• *Protecţia electronică* urmăreşte asigurarea apărării personalului, facilităţilor şi echipamentelor proprii împotriva acţiunilor inamicului în spectrul electromagnetic.

Războiul psihologic asigură utilizarea informaţiilor împotriva minţii oamenilor prin acţiuni de informare, dezinformare, manipulare, propagandă şi tehnici de influenţare subliminală, în scopul modificării concepţiei, atitudinilor, opţiunilor şi comportamentului forţelor adversarului sau neutrilor. El se desfăşoară sub forma unor operaţiuni care vizează: voinţa naţională, conducerea de stat, structurile politice, comandanţii şi trupa adversarului, moştenirea culturală etc.

Acţiunile psihologice sunt un subiect dificil de studiat, întrucât acestea se pot identifica cu greutate din cauza naturii lor clandestine. Ele nu produc distrugeri materiale, sunt omniprezente pe timp de pace, criză şi, mai ales, la război, au o rază de acţiune mare şi pot produce efecte deosebite.

Războiul psihologic se poate duce atât prin mijloace de informare specializată, cât şi prin utilizarea unora folosite temporar în acest scop.

Războiul hackerilor constă în acţiunea persoanelor neautorizate (hackeri) asupra echipamentelor sistemelor informaţionale şi a reţelelor de calculatoare ale acestora pentru modificarea conţinutului informaţiei iniţiale, distrugerea informaţiilor şi a sistemelor informatice, folosirea datelor în folosul adversarului şi efectuarea pirateriei software. Hackerii exploatează imperfecţiunile sistemelor de securitate a reţelelor de calculatoare pentru penetrarea acestora şi atacul componentelor software şi chiar hardware, în vederea realizării neutralizării sau funcţionării lor eronate la nivel fizic, sintactic sau semantic, urmărind producerea haosului în infrastructura informaţională atacată.

Războiul informaţiilor economice constituie un rezultat al integrării războiului informaţional şi a celui economic, ceea ce permite utilizarea blocării informaţionale cu acelaşi efect ca şi blocarea economică efectuată asupra unor naţiuni ţintă, în scopul obţinerii supremaţiei economice. Acţiunile desfăşurate au drept scop blocarea sau canalizarea convenabilă a informaţiilor economice, care să determine neacordarea de facilităţi sau împrumuturi, invadarea pieţei adversarului cu mărfuri în scopul falimentării economiei naţionale a acestuia, devalorizarea monedei naţionale şi producerea de masă monetară fără acoperire, afectarea operaţiilor comerciale şi bancare etc.

Războiul împotriva infrastructurii globale, denumit şi lupta în spaţiul virtual (Libicky – 1995) sau în ciberspaţiu (ansamblu integrat de sisteme şi reţele de calculatoare şi comunicaţii), constituie cea mai complexă formă de manifestare a războiului informaţional. El cuprinde acţiunile îndreptate asupra tehnologiei informaţiei, reţelelor de calculatoare şi de comunicaţii, precum şi asupra altor ţinte critice ale infrastructurii informaţionale, pentru neutralizarea sau distrugerea acestora prin terorism informaţional, atac semantic, operaţii de simulare şi alte acţiuni asupra structurii informaţionale sau echipamentelor tehnice (hardware).

Se are în vedere faptul că societatea şi economia postindustriale sunt dependente strict de informaţiile din reţelele de calculatoare sau cele vehiculate prin sistemele de comunicaţii, acestea manifestând multe vulnerabilităţi ce pot fi exploatate de războiul informaţional. Pe timp de pace, atacul cibernetic asupra adversarului urmăreşte şi scăderea însemnată a nivelului de trai şi degradarea economiei şi a vieţii sociale.

Revoluţia informaţională, cu componenta sa principală privind adoptarea structurilor electronice digitizate, a adus mari avantaje societăţii umane, determinând apariţia şi dezvoltarea epocii informaţionale, care a produs schimbări importante în toate domeniile de activitate. Informatica, sistemele informaţionale şi reţelele lor de comunicaţii şi calculatoare, integrate în conceptul de tehnologia informaţiei, au dobândit un rol primordial în dezvoltarea societăţii umane, influenţând şi transformând corespunzător şi domeniul militar, mai ales în ceea ce priveşte mijloacele pentru comandă şi control, dar şi sistemele de arme bazate pe informatică şi cibernetică.

Desigur, noul impact al ştiinţei şi tehnologiei a determinat şi apariţia a numeroase vulnerabilităţi care pot fi exploatate de adversar în situaţii de pace, criză sau conflict militar, prin acţiuni de război informaţional. Studiul temeinic al acestuia şi adoptarea măsurilor ofensive şi de apărare specifice constituie o obligaţie pentru toate domeniile care sunt implicate în asigurarea bunei funcţionări a infrastructurii informaţionale a ţării şi nu numai a celor care privesc apărarea naţională.

Bibliografie

• Bădălan E., Arsenie V., Văduva Gh., *Eseu despre arta strategică*, Editura Militară, Bucureşti, 2005.

• Mc. Lendon J.W., Battlefield on the Future: Information War Impact and Concerns (http://www.totse.com/en/badideas/gunandweapons/botiz08.html

• Szafranski R., *A Theory of Information Warfare*, Air University, 1995 (http://www.airpower.maxwel.af.mil/airchronicles/apj/szfran.html

• Toffler Alvin şi Heidi, *Război şi antirăzboi. Supravieţuirea în zorii secolului XXI*, Editura Antet, 1995.

• Topor Sorin, *Războiul informaţional*, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 2006.

• Waltz Eduard, Information Warfare: Principles and Operations, Artech House, Boston, 1998.

• AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2006.

• FM 34-10-2, *Intelligence and Electronic Warfare Equipment Handbook,* Headquarters Department of the Army, Washington D.C.

• FM 34-1, *Intelligence and Electronic Warfare Operations,* Headquarters Department of the Army, Washington D.C.

• J.Pub. 3-13, *Joint Doctrine for Command and Control Warfare.*

• xxx Sisteme informaţionale – sesiunea anuală de comunicări ştiinţifice cu participare internaţională, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti, 12-13 aprilie 2007.