RĂZBOAIELE EREI INFORMAȚIONALE

THE WARS OF INFORMATIONAL ERA

Colonel (r) prof. univ. dr. ing. Eugen SITEANU*

Acest articol prezintă pe scurt războaiele erei informaționale. Confruntările teroriste şi neconvenționale (în special cele asimetrice) nu au linii de demarcație şi tind să se amplifice. Apărarea armată e componenta de bază a securității statelor, dar nu e cea mai importantă parte a componentelor sale.

***Cuvinte cheie**: războaiele erei informaționale; confruntările teroriste; confruntări neconvenționale; confruntări asimetrice; apărarea armată.*

This paper presents briefly the wars of informational era. Terrorist and unconventional (especially asymmetric) confrontations have not demarcation lines and tend to amplify. Armed defence is the basic component of state's security, but is not the most important part of its components.

***Keywords**: wars of informational era; terrorist; unconventional; confrontations; armed defence.*

Impactul tehnologiei informației şi comunicațiilor (IT&C) asupra războaielor erei informaționale poate fi ilustrat de evoluția operațiilor militare ale statelor dezvoltate, operații în care informarea se face în timp real, ceea ce influențează opinia publică națională şi internațională şi afectează deciziile politicienilor.

IT&C[1] determină interferența dintre cele trei componente ale artei militare: strategie, artă operativă şi tactică, astfel încât orice eveniment este cunoscut, în timp real, la toate cele trei niveluri (tactic, operativ şi strategic).

* Profesor univ. dr. ing., Academia Comercială, Satu Mare şi Universitatea Națională de Apărare „Carol I"; membru asociat al AOŞR; vicepreşedintele Asociației Absolvenților UNAp „Carol I"; e-mail: esiteanu@yahoo.com; tel.:0720566911.

[1] Tehnologia Informației şi Comunicațiilor

În războaiele erei informaționale toți comandanții, indiferent de nivel, primesc date şi informații precise şi relevante, ceea ce îi ajută să cunoască situația trupelor proprii şi inamicului în timp real.

Datele şi informațiile sunt culese, prelucrate/analizate, sintetizate şi apoi transmise/difuzate prin intermediul sistemelor informaționale integrate (SII).

Printre aceste sisteme se remarcă cele de comandă, control, comunicații, calculatoare, informații, supraveghere şi recunoaştere (C4ISR), care permit statelor majore şi comandanților să vadă, să perceapă, să analizeze/interpreteze şi să ia hotărâri/decizii în cel mai scurt timp, uneori în timp aproape real, pentru a conduce acțiuni de luptă (operative şi sau strategice) în orice mediu (terestru, aerian, naval, cosmic).

În era informațională se utilizează din plin informatica, comunicațiile şi mijloacele de luptă computerizate, astfel încât informația a devenit un mijloc al domeniului informațional de acțiune.

Dimensiunea informațională a războaielor erei informaționale este reală (nu e una fabricată) şi de mare actualitate; informația a devenit o armă, un factor de risc, un instrument operațional, dar şi tehnologic.[2]

Revoluția informațională modernă a început după anul 1850 şi a cunoscut mai multe etape. Prima etapă a durat până la mijlocul secolului XX, fiind cunoscută sub denumirea de Prima Revoluție Informațională (apariția telegrafului, telefonului şi radioului).

A doua Revoluție Informațională a durat până în anul 1985 şi se caracterizează prin apariția televiziunii, calculatoarelor electronice, dar şi a sateliților şi comunicațiilor prin satelit. A urmat cea de a Treia Revoluție (Revoluția Cunoaşterii), care a adus cu ea tehnologia informației şi comunicațiilor, a cărei dezvoltare spectaculoasă poate fi pusă în evidență prin câteva exemple semnificative[3]: 4 miliarde de telefoane celulare; 1,3 miliarde telefoane fixe; cca 2 miliarde de oameni au acces la Internet, iar 60% dintre ei au conexiuni pe bandă largă etc.

Implicațiile tehnologiei erei informaționale asupra războaielor erei informaționale, dar şi asupra securității naționale sunt multiple; printre acestea evidențiem impactul lor asupra doctrinelor de apărare a statelor. Acestea au suferit modificări corespunzătoare apariției noilor capacități militare furnizate de tehnologiile

[2] Gruia Timofte, *Tendințele de evoluție ale ştiinței militare în era informațională,* Revista de Ştiințe Militare, nr. 3 (20), Anul X, 2010, p. 162.
[3] Ibidem, p. 154.

erei informaţionale (TEI). Totodată au crescut vulnerabilităţile infrastructurilor de apărare şi securitate, au crescut ameninţările la adresa informaţiei şi mijloacelor de informaţii.

Efectele TEI asupra Războaielor Erei Informaţionale (REI) sunt multiple şi complexe şi nu ne vom opri decât la câteva: numărul şi importanţa riscurilor şi ameninţărilor cresc; creşte probabilitatea declanşării unor războaie asimetrice; se modifică substanţial atât strategia cât şi tactica şi arta operativă; revoluţia în afacerile militare (în domeniul militar) se dezvoltă prin combinarea IT&C cu tehnologii din alte domenii, dar care au aplicaţii în prima. IT&C oferă oportunităţi pentru Războaiele Erei Informaţionale prin asigurarea de noi condiţii privind organizarea, dotarea, înzestrarea şi modul de ducere a acestui război (acestor războaie) şi anume: o diversitate de senzori, radare şi alte aparate pentru colectarea informaţiilor, prelucrarea şi diseminarea informaţiilor.

Astăzi, fluxul de informaţii e prea mare pentru a mai putea fi gestionat de comandanţi. Deoarece volumul de informaţii este prea mare este necesară utilizarea IT&C pentru a putea culege, prelucra şi disemina informaţiile în organizaţiile militare. Pentru transmiterea fluxului de date şi informaţii din domeniul militar se impune existenţa unei infrastructuri de securitate care să contracareze/interzică orice încercare de alterare sau sustragere a conţinutului informaţiilor de la orice eşalon.

Noile riscuri şi ameninţări ale actualului mediu internaţional de securitate sunt numeroase şi multe dintre ele reprezintă efectele negative ale globalizării: atacurile teroriste de genul şi amploarea celor din 11.09.2001, sărăcia extremă, bolile, încălzirea globală, reducerea grosimii stratului de ozon, competiţia acerbă pentru controlul resurselor planetare, criza economico-financiară fără precedent, proliferarea ADM[4] (MDW), fenomenul criminalităţii organizate, insecuritatea cibernetică şi energetică, schimbările climatice etc.

În Raportul privind punerea în aplicare a Strategiei Europene de Securitate, apărută în urmă cu doi ani, sunt analizate principalele ameninţări la adresa UE: terorismul, fenomenul criminalităţii organizate, criminalitatea informatică, riscurile la adresa controlului frontierelor statelor UE, riscurile apărute la adresa protecţiei civile, infracţionalitatea transfrontalieră, corupţia şi violenţa.[5]

[4] Arme de Distrugere în Masă

[5] Anghel Andreescu, *Ameninţări şi riscuri la adresa UE în contextul ameninţărilor globale*, Revista de Ştiinţe Militare, Nr. 3 (20), Anul X, 2010, p. 42.

Fenomenul terorismului este considerat acum ca o privatizare a războiului. Ideea nu e nouă şi aparţine lui Robert Cooper,[6] care mai adăuga: „este non-statul care atacă statul". Pentru UE şi NATO, terorismul islamic este o ameninţare. Organizaţia Al-Qaeda are o ideologie fundamentalist-integristă şi suficiente resurse financiare şi de altă natură şi reprezintă cea mai mare ameninţare nu numai la adresa UE şi NATO, ci la adresa întregii lumi civilizate.[7] Există şi în unele state ale UE (Spania, Franţa, Irlanda de Nord) acţiuni teroriste separatiste. De asemenea, Turcia se confruntă cu acţiunile teroriste ale PKK, care au desfăşurat acţiuni de acest gen şi în Europa Occidentală. Al-Qaeda recrutează adepţi nu numai din Africa de Nord, Orientul Mijlociu, ci şi din alte state, inclusiv din cele membre ale UE (Marea Britanie, Elveţia, Austria, Franţa, Olanda, Norvegia, Spania, Halia, Danemarca şi altele) în care există imigranţi islamici, chiar şi din a doua sau a treia generaţie.[8] Acest proces de recrutare a teroriştilor s-a extins în lumea întreagă cu ajutorul internetului.

Terorismul a evoluat rapid şi astăzi are posibilitatea de a trece la utilizarea unor mijloace neconvenţionale chimice, biologice, radiologice sau chiar nucleare.

În scopul prevenirii sau combaterii fenomenului terorist (terorismului) se face intervenţia contrateroristă sau cea antiteroristă. Prima dintre acestea (intervenţii) reprezintă un ansamblu de măsuri şi acţiuni ofensive pentru capturarea ori anihilarea teroriştilor, eliberarea ostaticilor şi restabilirea ordinii publice (legale).

Intervenţia antiteroristă este un ansamblu de măsuri şi acţiuni defensive executate înaintea producerii atacurilor teroriste. Intervenţia contrateroristă se poate face nu numai din interiorul unui stat, ci şi din afara acestuia în cadrul unor forţe militare internaţionale în diverse teatre de operaţii.

O asemenea intervenţie a fost cea din Afganistan, ca răspuns la atacurile teroriste din 11.09.2001 asupra SUA. Războiul antiterorist din Afganistan a fost declanşat la data de 07.10.2001 deşi ONU nu autorizase încă invazia din această ţară. În prima fază a războiului, SUA au lansat Enduring Freedom în vederea ocupării teritoriului afgan şi desfiinţării acestei baze de operaţiuni teroriste. În cea de a doua fază Consiliul de Securitate al ONU, în ultima săptămână a lunii decembrie 2001, a înfiinţat forţa internaţională pentru Asistenţă şi Securitate (ISAF) pentru a securiza capitala afgană, Kabul. Apoi NATO a preluat conducerea/comanda Operaţiunii ISAF, în anul 2003. până la mijlocul anului 2009 ISAF a primit trupe din

[6] Robert Cooper, *Destrămarea naţiunilor. Ordine şi haos în secolul XXI,* Editura Univers, 2007, p. 13.
[7] Anghel Andreescu, *op. cit.*, p. 43.
[8] Ibidem.

19 ţări, iar efectivele forţei de intervenţie contrateroristă au ajuns la aproximativ 64500 militari.

Terorismul de sistem îşi are sorgintea în „incompatibilităţile şi disfuncţionalităţile existente între sisteme şi nu se va ameliora decât în măsura în care se vor ameliora relaţiile între aceste sisteme. (...). Un asemenea terorism a existat şi există şi în România. El s-a manifestat şi se manifestă, sub diferite forme, îndeosebi în zonele Covasna şi Harghita, împotriva populaţiei de etnie română.

În anumite etape a cunoscut forme violente. Este posibil ca terorismul de sistem, îndeosebi în Europa, să se diminueze simţitor odată cu integrarea deplină a continentului, deşi s-ar putea ca, dimpotrivă, să asistăm la o recrudescenţă a acestui fenomen."[9]

Astăzi, UE are o Forţă de Reacţie Rapidă, care are una dintre misiuni, am putea spune o misiune principală de participare la combaterea acţiunilor teroriste.[10]

Celebrul autor Alvin Toffler, în cartea sa „Război şi antirăzboi", prezintă corelaţia dintre economie şi război şi apreciază, pe bună dreptate, că în viitor omenirea va fi ameninţată „esenţialmente de război economic, nu de cel militar".[11] Umanitatea secolului XXI se îndreaptă implacabil „spre un nou eveniment întunecat de ură tribală, pustiire planetară şi războaie multiplicate prin alte războaie".[12] Acelaşi autor afirmă că „războiul geoeconomic nu este un substitut al conflictului militar (...), ci un simplu preludiu, dacă nu chiar o provocare la războiul propriu-zis, cum s-a întâmplat cu rivalitatea economică americano-japoneză anterioară atacului japonez de la Pearl Harbor din 1941. Cel puţin în acest caz, concurenţa a apăsat pe trăgaci".[13]

Concluzia scriitorului de succes Alvin Toffler este previzibilă: „cursa concurenţei globale va fi câştigată de ţările care-şi încheie transformarea spre Al Treilea Val cu minimum de dislocări şi nelinişti interne"[14], dar în finalul cărţii sale ne surprinde cu altă concluzie: cele mai puternice conflicte şi războaie vor avea loc între ţările celui de Al Treilea Val şi ţările care aparţin civilizaţiilor primelor două

[9] Eugen Ungureanu, *Coerenţă şi consistenţă în combaterea terorismului*, în Revista Univers Strategic, Nr. 2, iunie 2010, p. 211.
[10] Eugen Ungureanu, *Strategii de prevenire şi combaterea terorismului*, în Revista Univers Strategic, Nr. 3, septembrie 2010, p. 212.
[11] Alvin şi Heidi Toffler, *Război şi antirăzboi. Supravieţuirea în zorii secolului XXI*, Editura Antet, 1995, p. 28.
[12] Ibidem, p. 15.
[13] Ibidem, p. 29.
[14] Ibidem, p. 39.

valuri. Acestea ar trebui să dea de gândit factorilor de decizie politico-militară de pe Planeta Albastră.

Conflictele erei informaționale şi în special războaiele (REI) se pot clasifica în trei categorii principale: simetrice (proporționale); disimetrice sau non-simetrice (disproporționale); asimetrice, care sunt caracterizate de o disproporționalitate dinamică, „adică o ieşire din incompatibilitate, prin folosirea la maximum a vulnerabilităților celuilalt şi chiar prin crearea acestor vulnerabilități la adversar (este o întoarcere la arta stratagemelor, dar pe un alt palier şi la o altă scară a confruntării)”.[15]

În această eră, ca urmare a noilor tehnologii, armele şi sistemele de arme sunt foarte performante, iar vulnerabilitățile societății informaționale sunt mari, ceea ce a deplasat războaiele din spațiul simetriei înspre disimetrie şi asimetrie (inclusiv terorism).

În consecință, nici o țară din lume, nici măcar SUA ori Rusia, nu-şi mai permite şi nici nu-şi poate asigura singură securitatea, ci cu ajutorul sau prin intermediul organizațiilor internaționale, alianțelor sau coaliților. Cu ajutorul acestora, statele pot gestiona mediul de securitate, pot elabora politici şi strategii viabile şi executa misiunile necesare combaterii terorismului şi ducerii operațiilor sau războaielor asimetrice.

Pentru a răspunde cât mai eficace şi eficient noilor amenințări, conflictelor asimetrice, terorismului etc. organizațiile internaționale şi în primul rând NATO sunt nevoite să adopte şi să pună în aplicare un permanent proces de transformare, să-şi modifice strategiile şi tacticile, precum şi misiunile armatelor şi forțelor de securitate. Astfel NATO şi UE, confruntate cu unele conflicte asimetrice, adoptă noi tactici şi strategii, diferite de cele folosite în secolul XX. Aşa, de pildă, „obiectivul militar nu mai poate fi atacarea sistematică şi eficientă a liniilor inamicului, ci, în cele mai multe situații erodarea susținerii populare a războiului în țara adversarului.”[16]

La Conferință de Securitate de la München, care a avut loc în anul 2011, Secretarul General al NATO a lansat conceptul „smart security”, ceea ce în limba română înseamnă „securitate inteligentă”, dar mai înainte , la summit-ul de la Lisabona, fusese lansat conceptul „smart defense”, adică de „apărare inteligentă”.[17]

---

[15] Viorel Buța, *Simetrie şi asimetrie în acțiunile militare*, în Revista de Ştiințe Militare, nr. 3(20), Anul X, 2010, p. 52.

[16] Ibidem, p. 53.

[17] Visarion Neagoe, *„Smart defence” şi securitatea națională a României,* Revista de ştiințe Militare, nr. 4 (25), Anul XI, 2011, p. 70.

De fapt, la Lisabona s-a pus problema cheltuielilor NATO de apărare care erau prea mari şi s-a propus să se cheltuiască mai bine, adică mai inteligent, datorită crimei economico-financiare. Criza a lovit şi statele membre NATO, inclusiv SUA, care nu mai puteau susține financiar planurile de înzestrare şi nici operațiile şi activitățile Alianței. SUA asigura circa 75% din bugetul Alianței, dar în noile condiții de austeritate, atât ele cât şi celelalte state membre întâmpină mari dificultăți privind deficitele bugetare care au impact negativ asupra bugetelor de apărare. Ca urmare, a fost necesară o nouă abordare a realizării obiectivelor apărării colective şi anume = „SMART DEFENCE”[18]

Aceasta („apărarea inteligentă”) va asigura o securitate şi apărare mai bune, cu fonduri financiare mai mici. În acest scop, însă, va fi nevoie ca statele membre să lucreze împreună cu mai multă flexibilitate. Deoarece nici un aliat european nu mai are posibilitatea să pună în aplicare singur toate acțiunile necesare pentru a contracara toate pericolele şi amenințările, chiar şi statele puternice sunt nevoite să-şi dea mâna pentru a coopera mai bine, mai inteligent în realizarea obiectivelor de apărare comune. În acest sens putem da exemplul Franței şi Regatului Unit care derulează deja proiecte comune de realizare a unor capacități militare comune.[19]

În cadrul conceptului NATO de „apărare inteligentă” se realizează în comun proiecte de înzestrare, instrucție, educație logistică etc.

Totuşi, războiul asimetric nu este nou, ci este foarte greu pentru că mereu cei slabi s-au confruntat cu cei puternici. Acest tip de război a încălcat întotdeauna şi continuă să încalce nu numai legile războiului, ci şi ale păcii. Astăzi, războiul asimetric încalcă legile şi principiile ONU. Explicația ar fi aceea că în secolul XXI nu mai există o delimitare precisă între guvernul unei țări şi cetățenii acesteia, nici între armată şi civili sau între domeniul public şi cel privat, ceea ce determină presiuni mari exercitate asupra guvernului în ceea ce priveşte maniera de ducere a războiului. Se ştie că societatea civilă nu acceptă războiul ca pe o soluție şi se opune acestuia, cu excepția unui război de apărare a țării împotriva unei invazii militare. Guvernele vor ține seama de opinia publică deoarece în caz contrar vor fi sancționate în votul popular.

[18] Ibidem, p. 71.
[19] Ibidem.

Răspunsul SUA la atacurile teroriste din 11.09.2001 prin bombardarea Afganistanului şi acţiunile pentru nimicirea bazelor teroriste reprezintă o etapă superioară în desfăşurarea războiului asimetric.

Esența războiului asimetric este confruntarea dintre forțele înzestrate cu sisteme de armamente produse de o tehnologie de vârf şi luptători care nedispunând de asemenea arme sofisticate folosesc orice mijloace pe care le transformă în arme: pietre, bâte, sticle incendiare, arme de foc, avioane civile şi fanatismul şi spiritul de sacrificiu suprem împotriva tehnologiei erei informaționale. Ba uneori utilizează şi tehnologia informației în măsura în care le este disponibilă.

Războiul terorist, cel de gherilă sau insurgență reprezintă forme de război asimetric, însă mai există şi alte forme ale acțiunilor asimetrice pe care însă nu ne-am propus să le abordăm aici.

Conflictele armate din Afganistan, Irak, Cecenia şi Orientul Apropiat, la care am asistat şi noi, sunt războaie asimetrice întrucât sunt războaie disproporționate.

Atât sistemele informaționale, cât şi cele informatice sunt vulnerabile deoarece reprezintă o cale de amenințare, de risc şi chiar de agresiune datorită scurgerilor de informații sau deformării acestora, indiferent de caracterul lor (economic, militar, social, personal etc.), dar şi marilor pierderi financiare sau de imagine (războiul sau agresiune imagologică). Aşadar, SII (militare) sunt vulnerabile la penetrarea lor de către adversar (inamic), la deteriorări ale hardware-ului şi software-ului, precum şi la schimbarea/modificarea de date, informații şi programe. „Tendința actuală privind amplificarea conectivității, în special la Internet şi în rețele Intranet, măreşte riscul de vulnerabilitate, fiind tot mai greu să se localizeze un punct de acces ilegal în rețea sau un utilizator cu un comportament agresiv”.[20]

Principala resursă a Războaielor Erei Informaționale este cea informațională indiferent de domeniu (militar, politic, economic sau social).

Resursa informațională este necesară conducerii/comenzii la toate nivelurile, cunoaşterii capacității militare (capabilităților) adversarului, elaborării doctrinelor de apărare, organizării şi pregătirii militare a echipamentelor militare, populației economiei naționale şi a teritoriului pentru apărare şi securitate, activității de cercetare ştiințifice în scopul apărării şi securității etc.

În categoria operațiilor şi Războaielor Erei Informaționale putem considera: războiul antiterorist (războaie împotriva terorismului); războiul asimetric; războiul bazat pe rețea; războiul paralel; războiul informațional; conflictele înghețate; operații

[20] Gruia Timofte, *op. cit.,* p. 159.

bazate pe efecte; operaţii decisive rapide; operaţii bazate pe reţea, operaţii în spectru complet etc.

În cadrul războiului bazat pe reţea se utilizează realizările IT&C , noile tactici, strategii, tehnici şi proceduri, structuri de forţe şi se interconectează în reţea în vederea câştigării şi menţinerii iniţiativei şi menţinerii succesului la toate nivelurile războiului (tactic, operativ şi strategic); prin interconectarea în reţea a tuturor forţelor (aeriene, terestre, navale şi cosmice) se comunică extrem de rapid se îmbunătăţeşte substanţial nu numai coerenţa, ci şi eficacitatea şi eficienţa operaţiilor şi bătăliilor, ceea ce înseamnă subunităţi şi unităţi de dimensiuni mici, care luptă independent şi, cunoscând situaţia în timp real, pot să execute cu succes diverse misiuni de o gamă diferită faţă de cele care nu sunt conectate în reţea. În acest tip de REI forţele de la toate categoriile, armele şi eşaloanele acţionează curent prin autosincronizarea acţiunilor şi misiunilor, perceperea exactă şi oportună a intenţiei comandanţilor eşaloanelor superioare, creşterea vitezei de comunicare/accesare a cunoştinţelor comune ale diverselor eşaloane (aparţinând nu numai forţelor proprii, ci şi coaliţiei în ansamblu) în scopul micşorării incertitudinii şi riscurilor, precum şi a dificultăţilor de a acţiona în ideea/concepţia (intenţia) comandanţilor.

Războiul bazat pe reţea şi operaţiile bazate pe reţea au la baza lor principii, doctrină, un anumit tip de organizare, o instruire şi o înzestrare corespunzătoare erei informaţionale. De asemenea, au un leadership de nivel înalt, personal cu o cultură organizaţională nouă, educat în spiritul principiilor acestui război şi care utilizează facilităţi performante în condiţii de interoperabilitate perfectă.

Principiile războiului bazat pe reţea nu sunt noi, dar sunt îmbunătăţite, adaptate la cele mai noi descoperiri şi realizări nu numai în domeniul IT&C, ci şi în al celorlalte tehnologii de vârf. Astfel, operaţiile se duc în scopul asigurării superiorităţii informaţionale şi inducerii în eroare a inamicului (adver), accesului continuu la informaţii prin partajarea cunoaşterii situaţiei.[21] Printre aceste principii se remarcă şi mărirea vitezei de elaborare a hotărârii comandantului şi de transmitere a deciziilor, realizarea unei dispersări raţionale a forţelor şi executarea operaţiilor discontinue pentru inducerea în eroare a adversarului, precum şi mărirea ariei de cercetare cu ajutorul senzorilor astfel încât să se poată reduce diferenţele dintre nivelurile războiului bazat pe reţea prin executarea simultană a operaţiilor în toate mediile.

[21] Gruia Timofte, *op. cit.,* p. 163.

Conceptul de război paralel a fost elaborat atunci când s-a considerat inamicul/adversarul ca fiind un „organism” sau un „sistem” conform teoriei generale a sistemelor.

Pe baza acestei teorii, organizarea (structura) adversarului (inamicului), considerat un sistem, a fost împărțită în câteva subsisteme: 1) subsistemul forțelor armate; 2) mulțimea cetățenilor care nu sunt combatanți; 3) subsistemul de transport (infrastructura de transport); 4) subsistemul produselor şi serviciilor esențiale necesare desfăşurării războiului şi operațiilor în toate mediile; 5) subsistemul de comandă şi control (figura nr. 1).

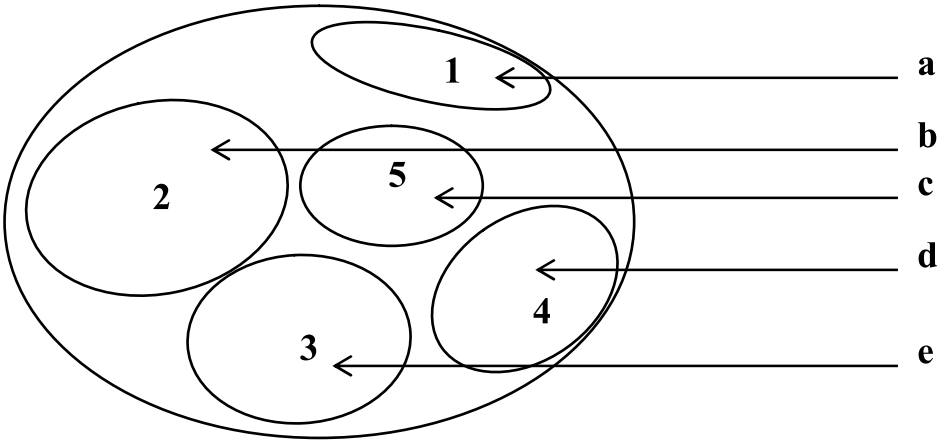

Figura nr. 1. *Prezentarea schematică a esenței conceptului de război paralel*

În această figură se prezintă schematic esența conceptului de război paralel: principalele lovituri (reprezentate sub forma săgeților a, b, c, d şi e) se îndreaptă simultan asupra celor cinci subsisteme (1, 2, 3, 4 şi 5).

Aşadar obiectivul principal al acestui război constă în planificarea, organizarea, executarea şi coordonarea simultană a acțiunilor asupra tuturor subsistemelor inamicului/adversarului.

Războiul informațional utilizează tehnologii de vârf, respectiv IT&C, în bătălia informatică având drept țintă fluxul de informații al inamicului/adversarului din rețelele de comunicații şi de calculatoare electronice, dar şi protejarea împotriva spionajului şi pirateriei cibernetice a rețelelor proprii de comunicații.

IT&C aduce mari avantaje în organizarea, eficacitatea şi eficienţa operaţiilor forţelor NATO, dar, totodată, şi numeroase riscuri şi vulnerabilităţi. Datorită noilor sisteme tehnice de comandă şi control al forţelor armate, sistemele de senzori optoelectronici sunt utilizate în timp aproape real pentru creşterea eficacităţii (şi eficienţei) sistemelor de arme terestre, aeriene, navale şi cosmice. Noile echipamente de comunicaţii şi informatice, cu benzi radio lărgite, cu noi tipuri de modulaţie şi de codare, au efecte benefice asupra creşterii vitezei fluxurilor informaţionale şi asupra protecţiei împotriva acţiunilor de război, electronic. Noile sisteme de calcul (calculatoare), cele de senzori, de arme inteligente şi alte entităţi sofisticate au un rol esenţial în multitudinea de activităţi ale războiului informaţional.[22] De asemenea, în acest tip de război se utilizează subsisteme şi sisteme puternic integrate de tipul C41, prin unirea conceptuală, tehnologică şi operaţională a echipamentelor şi reţelelor de comunicaţii digitale cu cele de calcul electronic şi aplicaţii software, care sunt destinate tuturor eşaloanelor, forţelor, armelor şi categoriilor de forţe, dar şi sistemelor de armamente supersofisticate.

Conceptul de „război informaţional conţine ideea luării măsurilor de protecţie pentru infrastructura informaţională proprie, de distrugere a infrastructurii inamicului/adversarului, concomitent cu efectele directe şi perverse asupra planificării şi ducerii acţiunilor militare în orice mediu fizic"[23]. Dacă nu se iau în consideraţie cu cea mai mare seriozitate şi responsabilitate aceste aspecte ale războiului informaţional. Statul respectiv este înfrânt, iar impactul asupra vieţii sociale şi militare va fi devastator.[24]

Războiul informaţional are ca armă sau muniţie informaţia şi de aceea urmăreşte drept ţintă reţelele de comunicare şi calculatoarele electronice. Armatele angajează hakeri (experţi în hardware şi software) pe post de crackeri şi le dau misiunea de a sparge codurile şi parolele astfel încât computerele şi reţelele de comunicare ale inamicului nu mai sunt protejate şi sunt furate informaţiile respective; în plus sunt împrăştiaţi viruşi în computerele adversarului, viruşi foarte greu de depistat şi eliminat.

În conflictele de generaţia a IV-a (armata noastră este pregătită pentru conflictele generaţiei a III) armatele au (unele) şi vor avea (altele) departamente de

[22] Constantin Mincu, *Evoluţii ştiinţifice şi tehnologice în domeniul comunicaţiilor şi informaticii militare şi influenţa acestora asupra planificării şi ducerii acţiunilor militare*, în Revista de Ştiinţe Militare, nr. 2 (27), Anul XII, 2012, pp. 8-9.
[23] Ibidem, p. 10.
[24] Ibidem.

bruiaj – interceptare înzestrate (dotate) cu tehnologii de vârf, ţinute în strict secret, care pot bloca instantaneu comunicaţiile radio şi TV. Astfel se va practica o dezinformare continuă şi nestingherită.[25]

Armata americană deţine computere şi comunicaţii într-o proporţie mult mai mare decât orice altă armată de pe mapamond. De aceea aceasta reprezintă o adevărată armă foarte puternică şi în acelaşi timp foarte vulnerabilă deoarece se poate întoarce împotriva ei oricând. Totodată, experienţele (lecţiile învăţate) din Irak şi Afganistan au arătat cu claritate că războiul informaţional nu este nici eficace, nici eficient împotriva unor adversari/inamici care nu dispun de o asemenea tehnologie sau care nu o utilizează.

În scopul descurajării eventualilor inamici/adversari şi promovării intereselor economice, politice, militare şi culturale ale statului se poate utiliza cu succes războiul informaţional prin aplicarea lecţiilor învăţate din războaiele purtate de armata SUA în ultimele decenii.

O caracteristică nouă a Războaielor Erei Informaţionale este aceea că dacă în urmă cu unu-două decenii organizaţiile internaţionale de securitate, inclusiv NATO, nu planificau încă de la început şi ultima fază a războiului/conflictului pe care îl declanşau, acum se prevede şi modul de acţiune în această fază finală. Aşa, de pildă, pentru ISAF, NATO a decis trecerea acestei misiuni în faţa transferului responsabilităţilor de securitate către forţele afgane, gradual, începând cu anul 2011 şi terminând cu 2014, când forţele de securitate afgane îşi vor exercita autoritatea suverană la nivel naţional (pe întreg teritoriul Afganistanului).

În această fază, pe lângă transferul (predarea) autorităţii administrative şi de securitate către guvernul Afganistanului se începe şi se desfăşoară procesul complex al retragerii forţelor NATO. Modalitatea retragerii este complicată, costisitoare şi dificilă având în vedere faptul că sistemul logistic integrat al NATO este dispersat în Asia Centrală pe teritoriile Kazahstanului, Kîrgîzstanului, Tadjikistanului, Turkmenistanului şi Uzbekistanului în scopul asigurării optime a fluxurilor de aprovizionare a forţelor internaţionale din Afganistan.

La summit-ul NATO de la Chicago, din 20-21 mai 2012, liderii statelor participante la războiul din Afganistan au declarat că, după retragerea forţelor internaţionale, „ţara nu va fi lăsată singură”.

SUA au decis să contribuie cu 2,3 miliarde USD la susţinerea forţelor afgane (aproximativ 350.000 soldaţi şi poliţişti afgani), iar restul până la 4,1 miliarde

[25] Ibidem, p. 19.

dolari (bugetul pentru susținerea acestor forțe) să fie asigurat de cele 49 țări ale ISAF, precum şi de Afganistan, care până în anul 2024 trebuie să fie în măsură să îl susțină în totalitate (singur).[26]

Parlamentul României, imediat după aprobarea misiunii ISAF de către Consiliul de Securitate ONU, a hotărât ca România să participe cu forțe la operația ISAF. Inițial trupele române au acționat în Afganistan sub egida ONU, iar apoi (din anul 2003) sub comanda NATO. Acum țara noastră are în teatrul de operații din Afganistan 1800 de militari (aparținând MApN, dar şi MAI) în provincia Zabol, dar şi în alte localități.

Sintagma de conflicte înghețate se referă la luptele pentru suveranitate națională sau mai degrabă suveranitate teritorială înghețate la un moment dat, însă nesoluționate şi oricând gata să reizbucnească.

Noi apreciem că acestea reprezintă mişcări separatiste violente pentru dobândirea statutului de stat autonom şi suveran prin luptă armată. În urma acestor conflicte s-au înființat pseudostate pe teritoriile Republicii Moldoveneşti (Transnistria) şi ale altor state (osetia de sud, Abhazia, Nagorno-Karabah, Cecenia etc.); ele nu au fost recunoscute internațional, dar au toate instituțiile şi prerogativele unui stat suveran.

Concluzii

Pentru elaborarea unui plan de retragere a militarilor din Afganistan, autoritățile române trebuie să coopereze strâns cu ISAF şi NATO, în primul rând cu SUA care asigură sprijinul logistic al forțelor române, dar şi unele capabilități (capacități) de luptă. Totodată, după stabilirea momentului şi modului de retragere, trebuie stabilită strategia operației de retragere a forțelor în care o parte importantă o reprezintă operația logistică care trebuie planificată pe faze. Toate aceste probleme se pot rezolva pe baza experienței repatrierii forțelor româneşti din teatrul de operații din Irak. În vederea aplicării conceptului apărării inteligente, specialiştii români trebuie să stabilească soluții inteligente pentru modificarea sistemului militar vechi şi realizarea unuia nou care să facă față conflictelor de generația a IV-a specifice erei informaționale. În acest scop este necesar sprijinul politic necondiționat al Parlamentului României, inclusiv de acordare Armatei Române a

[26] Visarion Neagoe, *Considerații privind retragerea NATO din Afganistan*, în Revista de Ştiințe Militare, nr. 2 (27), Anul XII, 2012, p. 84.

resurselor financiare necesare achiziționării unui sistem C4ISR cu toate echipamentele şi aparatele aferente.

BIBLIOGRAFIE

ANDREESCU Anghel, *Amenințări şi riscuri la adresa UE în contextul amenințărilor globale*, Revista de Ştiințe Militare, Nr. 3 (20), Anul X, 2010.

BUȚA Viorel, *Simetrie şi asimetrie în acțiunile militare*, în Revista de Ştiințe Militare, nr. 3(20), Anul X, 2010.

COOPER Robert, *Destrămarea națiunilor. Ordine şi haos în secolul XXI,* Editura Univers, 2007.

Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm

MINCU Constantin, *Evoluții ştiințifice şi tehnologice în domeniul comunicațiilor şi informaticii militare şi influența acestora asupra planificării şi ducerii acțiunilor militare*, în Revista de Ştiințe Militare, nr. 2 (27), Anul XII, 2012.

NEAGOE Visarion, *„Smart defence" şi securitatea națională a României,* Revista de ştiințe Militare, nr. 4 (25), Anul XI, 2011, p. 70.

NEAGOE Visarion, *Considerații privind retragerea NATO din Afganistan*, în Revista de Ştiințe Militare, nr. 2 (27), Anul XII, 2012.

TIMOFTE Gruia, *Tendințele de evoluție ale ştiinței militare în era informațională,* Revista de Ştiințe Militare, nr. 3 (20), Anul X, 2010.

TOFFLER Alvin şi Heidi, *Război şi antirăzboi. Supraviețuirea în zorii secolului XXI*, Editura Antet, 1995.

UNGUREANU Eugen, *Coerență şi consistență în combaterea terorismului*, în Revista Univers Strategic, Nr. 2, iunie 2010.

UNGUREANU Eugen, *Strategii de prevenire şi combaterea terorismului*, în Revista Univers Strategic, Nr. 3, septembrie 2010.