APĂRAREA CIBERNETICĂ – COMPONENTĂ A CONFRUNTĂRILOR MILITARE

CYBER DEFENSE – A COMPONENT OF MILITARY CONFRONTATIONS

Lt.col.drd. Valentin MANEA*

Dezvoltarea Societăţii Informaţionale a permis creşterea fluxului de informaţii şi a vitezei de trafic al acestora, influenţând decisiv rezultatele individuale şi de grup, precum şi eficienţa prestaţiei în cadrul tuturor domeniilor de activitate.

Utilizându-se suportul tehnic al tehnologiei informaţiilor şi al comunicaţilor, se poate vorbi despre o schimbare pragmatică în configurarea relaţiilor de putere dintre indivizi, instituţii sociale şi state, despre generarea unui război tacit, purtat în spaţiul virtual, numit război cibernetic şi în acest context despre apărarea cibernetică pe timpul operaţiilor militare.

Principalul obiectiv al războiului cibernetic este distrugerea capacităţii decizionale, prin neutralizarea capacităţii de acţiune a liderilor sau a comandanţilor, concomitent cu desfăşurarea activităţilor de protecţie proprii.

The Development of Information Society has enabled increased information flow and speed of traffic influencing in a decisive way the individual and group results and performance efficiency in all areas of activity.

Using the technical support of information and communication technology, we can speak about a pragmatic shift in the configuration of power relations between individuals, social institutions, and countries about generating a silent war fought in cyberspace called cyber warfare and, in this context, about cyber defense during military operations.

The main objective of cyber war is the destruction of decisional capacity by neutralizing the capacity of the leaders and commanders while conducting their protective activities.

Cuvinte-cheie: acţiuni militare; război cibernetic; apărare cibernetică; supremaţie cibernetică.
Keywords: *military actions; cyber war;cyber defence; cyber supremacy.*

În concordanţă cu analizele realizate în ultima perioadă, în domeniul securităţii, se poate vorbi astăzi despre schimbări ale fizionomiei conflictelor provocate de dezvoltarea tehnologică şi de dezvoltarea cunoaşterii în domeniu. Pe acest fundal, asistăm la apariţia unor noi actori, a unor noi centre de putere, precum şi la diversificarea ameninţărilor şi a vulnerabilităţilor sistemelor de securitate. Privit ca o formă de escaladare a conflictului, războiul capătă valenţe din ce în ce mai complexe, principiile de ducere a acţiunilor fiind din ce în ce mai greu de definit, de anticipat şi, în anumite cazuri, chiar de contracarat.

Pornind de la specificul acţiunilor întreprinse şi de la natura şi identitatea adversarului, se pot menţiona mai multe forme de manifestare şi de ducere a războiului care tind să se îndepărteze din ce în mai mult de cele purtate prin acţiuni militare convenţionale. Dacă istoria prezintă ca modalitate de desfăşurare a războiului confruntarea directă a forţelor militare, războaiele recente au scos în evidenţă faptul că termeni precum „lupta de apărare” sau „lupta ofensivă” şi conceptele care stăteau la baza desfăşurării acestora se transformă în principii generale de ducere a acţiunilor militare, menţinându-se în terminologia de specialitate pentru a surprinde sensul propagării forţei, respectiv a promovării puterii. Astfel, termeni precum „război hibrid” sau „război asimetric” reflectă mult mai fidel tipologia, paradigma strategică, concepţia, doctrina războiului, fiind repede preluaţi în limbajul de specialitate şi în cel al liderilor politico-militari contemporani.

Datorită transformărilor înregistrate în natura războiului însuşi, precum şi datorită tranziţiilor de la economiile bazate pe producerea de bunuri de larg consum, la economiile de tip speculativ, bazate pe exploatarea maximizată a potenţialului intelectual, războiul, atât de devastator în trecut,

**** Universitatea Naţională de Apărare „Carol I”***
e-mail: *vmanea60@yahoo.com*

a devenit în prezent un război bazat pe inteligența umană sau cea artificială, în care strategia este direct influențată de tehnologia avută la dispoziție. Pe acest fond, creşterea rolului armelor de înaltă precizie apare mai mult ca o consecință decât ca o necesitate. În aceste condiții, liderii militari şi politici conştientizează necesitatea direcționării conflictelor către spații cu caracteristici speciale, greu de controlat, dar în care pot fi obținute efecte majore la adresa securității adversarului.

Noile tipuri de amenințări şi de vulnerabilități au impus războiului o dezvoltare semnificativă în domeniile nonmilitare. Acest lucru este de cele mai multe ori favorizat de decalajele imense existente în lume între state şi se amplifică pe zi ce trece prin manifestarea profundă a diverselor forme de criză (economică, politică, socială şi morală), care la rândul lor se desfăşoară asimetric şi haotic.

În acest context, se simte nevoia ca statele să-şi concentreze eforturile în vederea atingerii obiectivelor, apărând astfel coalițiile şi alianțele, destinate echilibrării balanței de putere, sau de cele mai multe ori, sporirii decalajului în favoarea membrilor acestor grupări. Dacă până acum puțin timp puteam considera că acțiunile clasice ale unui stat contra altui stat s-au restrâns foarte mult, recentele evenimente din Ucraina au reînviat, cel puțin în rândul strategilor militari, necesitatea existenței unor politici şi strategii clare, viabile indiferent de tipul, natura şi caracteristicile amenințărilor.

Necesitând o abordare concretă, multilaterală, războiul bazat pe ştiință a devenit principalul vector de putere politică, economică, socială şi militară. Astfel, pe câmpul de luptă modern, se pot întâlni atât arme letale, cât şi nonletale, ponderea deținând-o cele din urmă. Conform acestei realități, acțiunea militară îşi va schimba permanent fizionomia, fiind adaptată specificului actorilor implicați în conflict şi gradului de dezvoltare intelectuală şi tehnologică al acestora.

Asistăm astăzi la diferite forme de manifestare a forței, iar războiul nu mai reprezintă o simplă problemă de strategie, aspect identificat şi demonstrat pe timpul tuturor conflictelor militare recente, indiferent de actorii implicați şi de nivelul de dezvoltare al acestora. Lupta pentru informație, modul de manifestare a acțiunilor şi a reacțiunilor în domeniul informațional au condus la apariția unui nou tip de conflict, în plan informațional, şi anume „războiul informațional”, care după unii specialişti posedă caracteristicile războiului clasic.

În cadrul acestui nou tip de conflict, informația a căpătat treptat o importanță deosebită, pe măsură ce era conştientizată necesitatea exploatării ei.

În acest context, ținând cont că „cine deține informația deține puterea”, este justificată tendința statelor, guvernelor, armatelor, diverselor instituții guvernamentale şi neguvernamentale şi chiar a unor persoane publice sau private de a dezvolta capabilități favorizante culegerii, exploatării şi transmiterii informațiilor, în vederea realizării scopurilor propuse. În acelaşi timp, toate statele şi organizațiile, indiferent de tipul acestora, au conştientizat faptul că la rândul lor pot constitui o țintă, respectiv o sursă de scurgere a informațiilor, în situațiile în care nu adoptă un sistem de protecție a informațiilor, bazat pe reguli stricte, proceduri şi personal cu expertiză pentru protecția acestora.

Deşi în aparență respectă principiile unui război clasic, războiul informațional diferă foarte mult de acesta, presupunând folosirea unei arme mai puțin convențională, informația, care, prin folosirea sau nefolosirea ei, poate reprezenta un pericol la adresa securității părții adverse. Acest tip de război vizează în special afectarea opiniei publice, a personalului armatei adverse, reprezentând mai mult o tehnică de slăbire a puterii acestora prin folosirea unor mijloace de influențare psihologică. Specificul acestei noi forme de dezvoltare a conflictului îl reprezintă faptul că se desfăşoară subtil, vizând un număr relativ mic de ținte, dar care prin folosirea mijloacelor subversive poate conduce la îndeplinirea obiectivelor şi obținerea succesului cu pierderi umane şi materiale minime.

Datorită complexității sale şi a existenței unui număr foarte mare de variabile în cadrul acțiunii şi reacțiunii informaționale, au existat numeroase încercări de a defini acest concept, fără a exista, în acest moment, o variantă unanim acceptată.

Apariția Internetului şi dezvoltarea rapidă de care a avut parte a contribuit la apariția unui nou spațiu, cel virtual, intitulat şi „spațiul cibernetic”, care oferă multiple variante de comunicare, de gestionare a datelor şi de culegere de informații. Toate aceste posibilități sunt practic puse la dispoziția oricărei persoane care are la dispoziție un calculator conectat la rețea. Spațiul cibernetic se întinde de la simplul calculator personal, până la uriaşele calculatoare ale sistemelor naționale:

de apărare, bancar, energetic, transport auto, naval sau aerian etc. Astfel, beneficiind de posibilitatea accesării acestor surse de informație de la orice calculator personal interconectat în sistem, orice persoană poate avea acces rapid la cele mai variate informații, fiind foarte greu de estimat sau de evaluat modul practic în care acestea vor fi exploatate, prelucrate şi în unele cazuri retransmise în rețea.

În aceste condiții protejarea informației devine un proces deosebit de complex a căror caracteristici fundamentale ar fi continuitatea şi adaptabilitatea permanentă la progresele înregistrate în dezvoltarea tehnologică proprie sau a celorlalți utilizatori, în scopul prevenirii, limitării sau contracarării unei eventuale agresiuni informatice sau a unui eventual atac la care sistemul sau sistemele conectate la rețea sunt supuse. În absența unor astfel de măsuri, propriul sistem sau rețeaua în care este conectat devin ele însele principalele vulnerabilități în asigurarea protecției informațiilor gestionate.

În acest caz se poate vorbi despre o securitate a informației gestionată sau vehiculată în spațiul cibernetic care creşte proporțional cu investițiile realizate în dotarea cu tehnologie soft şi hard, iar la nivel macro cu investițiile realizate în cercetarea în domeniu, precum şi în pregătirea utilizatorilor şi a personalului destinat asigurării securității informaționale. Acesta este şi motivul pentru care majoritatea actorilor prezenți în spațiul cibernetic, indiferent de natura lor, investesc numeroase resurse pentru echilibrarea balanței între amenințările care se manifestă în spațiul cibernetic (terorism, spionaj, sabotaj, subversiune şi crimă organizată).

Fără a avea dorința de a minimiza importanța celorlalte componente ale războiului informațional, în continuare mă voi referi la *Războiul cibernetic*, deoarece acest concept este cel mai recent şi alături de cel de *apărarea cibernetică* se află din ce în ce mai des pe agenda întâlnirilor liderilor militari şi politici, până la cel mai înalt nivel.

În esență, războiul cibernetic reprezintă o formă complexă de confruntare, prin manifestarea capacității de folosire a tehnicilor şi a tehnologiilor de management al informațiilor, specifice rețelelor informatice, capabilă să conducă la atingerea obiectivelor. Războiul purtat în spațiul cibernetic reprezintă „un război tăcut”, dar care poate produce pagube imense ca şi orice altă intervenție militară. În esență, el reprezintă o succesiune de atacuri cibernetice asupra terminalelor care asigură buna funcționare a infrastructurilor critice vizate, însoțite de măsuri de limitare sau de contracarare, în situația în care sunt identificate la timp.

În cadrul acestuia, țintele pot îmbrăca forme diverse, după cum urmează[1]:

- rețelele de telefonie – ținte uşor de lovit, alături de ele fiind transcodoarele cu microunde sau chiar sateliții, care pot fi distruşi doar prin reprogramarea motoarelor de poziționare şi care sunt controlate de la sol; se pot întrerupe centralele de telefonie de urgență, serviciile medicale, ambulanțele, pompierii, serviciile poliției, alarmele de orice fel conectate la sisteme centralizate de supraveghere;
- centralele energetice – sistemul de distribuție al energiei electrice şi sistemele de supraveghere constituie ținte relativ uşor de atins;
- sistemul financiar – țintele cele mai evidente sunt rețelele de transfer financiar apoi băncile locale şi noile metode de acces la fonduri. Alte ținte ar putea fi sistemele de credit, inclusiv cărțile de credit sau birourile de credit; cu puțin ajutor din partea sistemelor deja aflate în funcțiune, poate fi posibilă distrugerea pieței de valori şi financiare a lumii în câteva minute;
- transport-logistică – sistemul de transport aerian este uşor de paralizat, dat fiind faptul că sistemele de control al traficului aerian sunt esențiale şi complet dependente de computere; la fel stau lucrurile şi în cazul transportului fluvial, terestru sau feroviar, care pot fi anihilate prin intermediul bazei lor de date de coordonare şi programare;
- serviciile sociale – pot fi introduse în haos prin distrugerea sau virusarea bazelor de date privind plata salariilor, pensiilor, alocațiilor de toate felurile;
- comunicațiile – se va adăuga mult mai multă panică şi teroare prin incapacitarea mijloacelor convenționale de comunicare, a televiziunilor şi a radiourilor; sistemele IT sunt complet dependente în livrarea mesajului de conexiune la satelit, securitatea acestor sisteme fiind foarte slabă, cea mai mare atenție fiind acordată până acum prevenirii furtului de semnal;
- comunicațiile guvernamentale – acestea pot fi țintele preferate, mai ales la nivelul infiltrărilor în bazele de date şi al unei eventuale campanii de comenzi contradictorii care să provoace autoblocarea sistemelor informaționale, ceea ce se poate obține fie prin introducerea unor comenzi de

operare precise, fie prin plasarea unui virus care să acționeze în trepte, spre exemplu, după integrarea unui mesaj parvenit prin e-mail în baza operațională de date.

Așa cum este de așteptat, printre primele ținte atacate vor fi serverele care deservesc legăturile operative între puterea politică, de decizie, și statul major sau conducerea forțelor armate, apoi între statul major și structurile/unitățile subordonate, precum și cele care asigură legăturile între diverse comandamente. Pe același plan, se situează serverele guvernului și cele ale diverselor agenții de securitate și spionaj, organisme și instituții guvernamentale. Motivul îl constituie, desigur, îngreunarea, pe cât posibil, a traficului prin asemenea servere și, în cel mai fericit caz pentru atacatori, blocarea ori chiar scoaterea completă din uz.

De asemenea, pot fi atacate și site-uri întregi sau doar pagini web ale organizațiilor amintite anterior, cărora li se adaugă de această dată și ținte din sectorul politic și civil: parlament, partide politice, organizații civice, organizații neguvernamentale, instituții financiare, organisme mass-media.

Prin conectarea la Internet, Intranet sau alt tip de rețea, organizațiile din sistemul securității naționale devin vulnerabile la pătrunderi neautorizate, cu rea intenție sau provocate din neatenție. Din cauza caracterului ascuns al atacurilor cibernetice, există pericolul real ca acestea să rămână nedetectate sau să fie detectate mult prea târziu.

Printre inițiatorii acestor tipuri de atac, John D. Howard, specialist în domeniu, propune următoarele șase categorii de autori[2]:

- hackeri – persoane, mai ales tineri, care pătrund în sistemele informatice din motivații legate mai ales de provocare intelectuală, sau de obținerea și menținerea unui anumit statut în comunitatea prietenilor;
- spioni – persoane ce pătrund în sistemele informatice pentru a obține informații care să le permită câștiguri de natură politică;
- teroriști – persoane ce pătrund în sistemele informatice cu scopul de a produce teamă, în scopuri politice;
- atacatori cu scop economic – pătrund în sistemele informatice ale concurenței, cu scopul obținerii de câștiguri financiare;
- criminali de profesie – pătrund în sistemele informatice ale întreprinderilor pentru a obține câștig financiar, în interes personal;
- vandali – persoane ce pătrund în sistemele informatice cu scopul de a produce pagube.

Indiferent de nivelul la care se află (strategic, operativ sau tactic), pentru îndeplinirea misiunilor primite, structurile militare folosesc echipamente de comunicații și sistemele informatice, iar în lipsa unor măsuri de protecție specifice, informațiile gestionate devin inevitabil vulnerabile, ceea ce poate conduce la eșecul total sau parțial al acțiunilor planificate.

Pentru asigurarea securității sistemelor militare sunt prevăzute în statele de organizare structuri cu sarcini specifice și au fost create proceduri specifice de administrare și utilizare a rețelelor de calculatoare folosite.

Sistemul informațional de conducere de la nivelul ministerelor apărării naționale, în special al celor aparținând statelor membre NATO, se bazează pe sistemul de comandă și control (C2), care asigură legătura cu toate structurile de la eșaloanele din subordine și se interfațează cu sistemele similare ale aliaților.

Din punct de vedere al capabilităților cibernetice în domeniul militar se poate afirma că a fost atins obiectivul privind obținerea avantajului cibernetic dacă prin acțiunile întreprinse este atins unul dintre cele trei niveluri de așteptare, fiecare nivel reprezentând atât o atitudine, cât și o percepție, iar aceste niveluri sunt: superioritatea cibernetică, dominația cibernetică și supremația cibernetică.

În cadrul războiului cibernetic, cucerirea superiorității informaționale, de către una sau mai multe dintre părțile beligerante, are loc prin dominarea confruntării pentru informație. Informația este utilizată ca armă împotriva adversarului sau ca mijloc de convingere și influențare a opiniei publice proprii ori internaționale atât de către adversari, cât și de alți actori interesați de situația geopolitică din zonă.

Prima dovadă certă a *supremației cibernetice* a fost dovedită în Războiul din Osetia de Sud (2008), în urma coordonării unui atac militar cu un atac cibernetic. Pagina electronică a președinției georgiene (www.president.gov.ge) a fost atacată în noaptea zilei de 20 iulie 2008[3]. Metoda aleasă: negarea serviciului DDoS-Distributed Denial of Service[4], altfel spus serverul care găzduia pagina președinției georgiene a început să primească pachete mari de fișiere în mod continuu, ceea ce a dus la blocarea sa. Pe lângă pagina președinției, au

mai fost blocate şi paginile Serviciului de Asistență Socială din Georgia. Atacul a continuat câteva zile după care s-a oprit. La acea dată, pagina electronică *www.shadowserver.org* anunța că acest atac este foarte asemănător cu cel din luna mai 2007 executat împotriva Estoniei, în perioada în care autoritățile estoniene se aflau în conflict cu Moscova din cauza mutării unui monument al ostaşului sovietic. Atacurile proveneau de la un server cu date de identificare false, apărut de foarte puțină vreme şi care nu a avut altă activitate până la atacul din 20 iulie. Cel mai probabil, la această dată a avut loc un atac „de probă”, iar după ce pagina preşedinției georgiene a fost blocată timp de două zile, serverul care a pornit atacul a dispărut brusc.

În momentul în care s-au declanşat luptele convenționale în regiunea separatistă Osetia de Sud, serverele georgiene au dispărut de pe Internet. Paginile electronice ale Preşedinției, Parlamentului, Ministerului Afacerilor Externe, Ministerului Educației şi Băncii Naționale din Georgia au fost bombardate continuu cu solicitări false care le-au blocat total activitatea. Pe lângă sursele oficiale de informare, au fost scoase din circulație şi toate paginile electronice ale presei georgiene, ceea ce presupune o blocadă informațională privind accesul la Internet.

În termeni de transfer de date, atacurile împotriva paginilor electronice georgiene au ajuns la o medie de 211,66 Mbps – cu un maxim de 814,33 Mbps. Atacurile au durat în medie două ore şi 15 minute, cel mai susținut atac cibernetic durând peste şase ore[5].

Având în vedere acțiunile cibernetice desfăşurate în Georgia se poate aprecia că aceste acțiuni „pot fi o parte integrantă a războiului armat, substituindu-se artileriei sau acțiunilor aeriene. În acest sens, NATO trebuie să colecteze informații relevante, să elaboreze măsuri de contracarare şi de apărare, să dezvolte planuri, programe de acțiune şi trebuie să existe o finanțare, o participare şi un sprijin mai mare pentru CCDCOE[6], inclusiv participarea statelor partenere, care pot contribui în mod pozitiv la eforturile Alianței de apărare cibernetică”[7].

În încercarea de a contracara astfel de atacuri se impune o cooperare permanentă între toate autoritățile şi organizațiile competente care dispun de capabilități în domeniul apărării cibernetice.

Un bun exemplu în acest sens îl reprezintă colaborarea inițiată de către SUA şi Marea Britanie, care pe lângă desfăşurarea unor exerciții desfăşurate în comun şi-au propus chiar înființarea unei „celule cibernetice” cu rol în identificarea vulnerabilităților componentelor aparținând fiecărui sistem de securitate cibernetică al acestora şi în adoptarea procedurilor menite să remedieze şi să anihileze nişele de securitate[8].

De asemenea, un exemplu de cooperare în asigurarea normalității în spațiul cibernetic l-a oferit chiar FBI, care a preluat de la gruparea Anonymous o listă cu 11 IP-uri participante la atacul contului oficial de Twitter al Comandamentului Central SUA (US CENTCOM). Acest atac a fost realizat de către hackerii grupului Cyber Caliphate care pretind a sprijini grupul terorist ISIS şi se dorea a reprezenta un răspuns la campania dusă împotriva site-urilor jihadiste, organizată de către Gruparea Anonymous, pentru a răzbuna atacul împotriva redacției Charlie Hebdo[9].

Analizând cele afirmate anterior, se poate trage concluzia că este esențial ca instituțiile guvernamentale să dispună de capabilități permanente de avertizare, evaluare, analiză şi reacție, precum şi să întrețină o stare continuă de modelare structurală şi doctrinară, care să permită realizarea intereselor naționale în acest mediu cibernetic. Indiferent de formele sub care sunt efectuate sau se manifestă atacurile cibernetice şi de specificul țintelor vizate, asigurarea protecției cibernetice reprezintă o prioritate imediată a tuturor entităților structurale. În acest context, la nivel guvernamental, însuşirea conceptului de apărare cibernetică reprezintă mai mult decât o necesitate, iar înființarea structurilor de răspuns la incidente de securitate, de tip CERT (Computer Emergency Response Team), reprezintă o prioritate.

NATO, fiind o organizație specializată în domeniul apărării colective a membrilor săi, are propria Politică de apărare cibernetică (Cyber Defence). Unul dintre obiectivele politicii NATO în domeniul apărării cibernetice îl constituie asigurarea interoperabilității şi a cadrului legal pentru cooperarea cu națiunile membre în cazul în care acestea sunt ținta unor atacuri cibernetice.

Stadiul privind implementarea măsurilor de apărare cibernetică la nivelul NATO, precum şi Strategia NATO privind apărarea cibernetică, au reprezentat puncte importante de pe ordinea de zi, în cadrul Summitului de la Chicago (2012) şi în cadrul celui din Țara Galilor (anul 2014), fiind

în acelaşi timp preocupări permanente la nivelul Alianței.

În acest domeniu, al apărării cibernetice, este folosită şi expertiza asigurată de Centrul de Excelență pentru Apărare Cibernetică, situat la Tallin, Estonia. Centrul a fost acreditat NATO la data de 28 octombrie 2008, având ca misiune principală sporirea capacității de cooperare şi informare între NATO, incluzând şi națiunile membre, şi alți parteneri din domeniul apărării cibernetice. De asemenea, centrul desfăşoară activități de cercetare, elaborează *lecții învățate* şi asigură consultanță de specialitate națiunilor membre şi partenerilor alianței[10].

În acest scop, în perioada 26-28 noiembrie 2013, s-a desfăşurat exercițiul de apărare cibernetică „Cyber Coaliția 2013”, care a avut ca obiectiv, printre altele, testarea capacității Alianței de a-şi apăra rețelele împotriva atacurilor cibernetice, care au crescut în ultima vreme atât ca număr, cât şi din punct de vedere al complexității. Cu acest prilej, Jamie Shea, adjunctul Secretarului General pentru provocări de securitate de la NATO, a afirmat că „NATO trebuie să țină pasul cu această evoluție a acestui tip de amenințare, iar exercițiul Cyber Coaliția 2013 permite testarea pe deplin a procedurilor şi sistemelor noastre, pentru a-şi apăra în mod eficient rețelele – astăzi şi în viitor”[11].

Apărarea cibernetică în sensul acceptat de către specialiştii în domeniu şi preluat în Strategia de securitate cibernetică a Uniunii Europene, precum şi în cea națională, aprobată prin Hotărârea Guvernului României nr. 271/2013, reprezintă acțiuni desfăşurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice[12].

De asemenea, Strategia Națională în domeniul Securității Cibernetice (anul 2013) delimitează direcțiile de acțiune ale României, în vederea asigurării unei stări de normalitate, în spațiul cibernetic, pentru reducerea riscurilor şi valorificarea oportunităților, precum şi pentru îmbunătățirea cunoştințelor, a capabilităților şi a mecanismelor de decizie. Crearea unei culturi de securitate cibernetică, întreținerea şi dezvoltarea cooperării între sectorul public şi cel privat, inclusiv prin stimularea schimbului reciproc de informații alături de dezvoltarea capacităților naționale reprezintă priorități ale managementului riscurilor cibernetice.

Prin crearea condițiilor operaționale şi tehnice de luare şi implementare a deciziilor, cu o rapiditate mai mare decât capacitatea de reacție a adversarului, comandantul viitoarei structuri de forțe întrunite va avea posibilitatea să modeleze mediul pentru a-l utiliza cât mai eficient în raport cu nevoile şi obiectivele sale[13]. Superioritatea în luarea deciziei va depinde în mare măsură de capacitatea de colectare a informațiilor, de partajarea cunoştințelor referitoare la situația din timpul tuturor fazelor operației militare, cât şi de capacitatea de diseminare a acestor informații.

Deşi elementul central ale acestui nou tip de război îl reprezintă tot luptătorul, în cazul războiului cibernetic acesta a fost treptat înlocuit cu unul impersonal, capabil să conducă la obținerea de performanțe superioare în condițiile folosirii de resurse limitate şi cu pierderi materiale şi umane minime. În aceeaşi măsură trebuie avut în vedere că şi inamicul are aceleaşi însuşiri, diferența fiind reprezentată doar de nivelul tehnologiei folosite sau gradul de pregătire a utilizatorului.

Existența acestor ipoteze şi a celor care decurg din ele constituie instrumente raționale prin care se pot formula concluzii referitoare la mutațiile privind lupta armată şi tendințele privitoare la combinarea cât mai frecventă a acțiunilor militare „clasice“ cu cele „asimetrice“, precum şi mutații în structura şi fizionomia luptei armate datorate armamentelor şi tehnologiilor folosite.

Conform teoreticienilor militari, războiul are şi va avea un puternic caracter multidimensional şi se va desfăşura în toate mediile: terestru, aerian, maritim, cosmic, informațional, obținerea superiorității fiind vizată în toate aceste medii, dar în mod special în controlul mediului informațional.

Se poate afirma că războiul viitorului va fi bazat pe tehnologii performante. Astfel, în societatea contemporană, nimeni nu mai poate percepe războiul decât ca pe un proces continuu de transformări atât în dimensionarea şi dotarea armatelor, cât şi în arta militară, transformări condiționate de dezvoltarea economică şi socială a fiecărei părți implicate în conflict.

Lucrarea a beneficiat de suport financiar prin proiectul cu titlul „Studii doctorale şi postdoctorale Orizont 2020: promovarea interesului național prin excelență, competitivitate şi responsabilitate în cercetarea științifică fundamentală şi aplicată românească”, număr de identificare contract POSDRU/159/1.5/S/140106. Proiectul este cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. Investeşte în Oameni!

NOTE:

1 Gh. Arădăvoaice, V. Stancu, *Războaiele de azi şi de mâine agresiuni nonconvenționale*, Editura Militară, Bucureşti, 1999, pp. 43-44.

2 Ilie C., *Războiul informatic componentă a războiului asimetric, vulnerabilități şi riscuri, soluții de contracarare*, Editura UNAp „Carol I”, Bucureşti, 2014, p. 29.

3 http://www.cîrr.iftîH com/posts/20081016 graphs russiageorgias cyberattacks, accesat la 15.08.2013.

4 Un atac de tipul *Denial of Service* (DoS) este un incident de securitate a informației în care o organizație sau un utilizator independent este privat de serviciile unei resurse pe care în mod normal o folosea fără probleme.

5 http://www.ziare.com/international/stiri-externe/ accesat la 22.08.2013.

6 *Cooperative Cyber Defence Centre of Excellence* – Centrul de Excelență NATO pentru Cooperarea în Protecția Cibernetică.

7 Khatuna Mshvidobadze, *New threats: Energy Security, Cyber Defense, Critical Infrastructure Protection*, la conferința „NATO and the New Strategic Concept”: http://georgiandaily.com/index.php?option=com_content&task=view&id=15501&Itemid=129, accesat la 22.08.2013.

8 http://www.cyberdefensemagazine.com/usa-and-uk-announce-joint-cyber-war-games-to-improve-cyber-defenses/ , accesat la 20.01.2015.

9 http://www.cyberdefensemagazine.com/anonymous-supports-fbi-in-the-investigation-of-the-us-centcom-hack/ , accesat la 19.01.2015.

10 http://www.ccdcoe.org/38.html, accesat la 18.07.2012.

11 http://www.nato.int/cps/en/natolive/news_105205.htm?selectedLocale=en, accesat la 28.06.2014.

12 Strategia de securitate cibernetică a României, http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesat la 30.07.2014.

13 T. Frunzeti, M. Mureşan, Gh. Văduva, *Război şi haos,* Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009, p. 112.

BIBLIOGRAFIE

Alexandrescu C., Alexandrescu G., Boaru Gh., *Sisteme informaționale – servicii şi tehnologie*, Editura UNAp „Carol I”, Bucureşti, 2010.

Arădăvoaice Gh., Stancu V., *Războaiele de azi şi de mâine agresiuni nonconventionale*, Editura Militară, Bucureşti, 1999.

Frunzeti T., Mureşan M., Văduva Gh., *Război şi haos*, Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009.

Ilie C., *Războiul informatic componentă a războiului asimetric, vulnerabilități şi riscuri, soluții de contracarare*, Editura UNAp „Carol I”, Bucureşti, 2014.

Strategia de securitate cibernetică a României.

http://www.nato.int/cps/en/natolive/news_105205.htm?selectedLocale=en

http://www.ccdcoe.org/38.html

http://www.ziare.com/international/stiri-externe/

http://georgiandaily.com/index.php?option=com_content&task=view&id=15501&Itemid=129