ROLUL APĂRĂRII CIBERNETICE ÎN CADRUL SISTEMELOR DE COMANDĂ ȘI CONTROL

THE ROLE OF CYBER DEFENSE WITHIN COMMAND AND CONTROL SYSTEMS

Lt.col.instr.avs.drd. Ștefan-Antonio DAN-ȘUTEU*

Succesul utilizării instrumentului de putere militar, la toate nivelele artei operative, este influențat de existența unui sistem de comandă și control rezilient. Acest articol analizează rolul apărării cibernetice în asigurarea reziliență componentei tehnologice a sistemului C2 din perspectiva strategică a accelerării și flexibilității procesului de luare a deciziei, în condițiile existenței riscurilor și amenințărilor cibernetice. Necesitatea asigurării cerințelor de interoperabilitate și conectivitate a sistemelor de comunicații și informatice militare determină abordarea apărării cibernetice într-o manieră unitară și integrată la toate nivelurile artei operative. Implementarea apărării cibernetice necesită o strategie unitară la nivelul instituției militare, strategie care trebuie să includă comunicarea și cooperarea interagenții, precum și consultarea, și direcționarea industriilor specifice. În caz de conflict armat, acest proces contribuie la translatarea rapidă a obiectivelor politico-militare la nivel operativ și tactic.

The successful use of the military instrument of power, across all levels of the operational art, is influenced by the existence of a rezilient command and control system. From the perspective of an accelerated and flexible decision-making process, this article analyzes the role of cyber defense in providing the requested resilience of the technological component of the C2 system, in an operational environment characterized by the proliferation of cyber risks and threats. The interoperability and connectivity standards required by the military communication and information systems determine a comprehensive and integrated approach to cyber defense, at every level of operational art. Cyber defense implementation requires a unitary military strategy, that should include an extensive interagency communication and cooperation, as well as consultation with specific industries. During armed conflict, this process enables a quick translation of politico-military objectives at operational and tactical level.

Cuvinte-cheie: apărare cibernetică; strategie; operații militare; sisteme de comandă și control; sisteme de comunicații și informatice; vulnerabilități cibernetice.

***Keywords**: cyber defense; strategy; military operations; command and control systems; communication and information systems; cyber vulnerabilities.*

În concordanță cu dovezile furnizate de istorie și știință, războiul, conflictul extrem între adversari organizați în grupuri socio-militare, este probabil cel mai fidel companion al speciei umane. Studiul acestui fenomen social complex relevă caracteristicile sale fundamentale. Astfel, se poate afirma că războiul are o natură persistentă, este direcționat politic și este caracterizat printr-o extremă violență. Totuși, chiar dacă este caracterizat de aceste trăsături comune, fiecare război este unic ca desfășurare, datorită contextului istoric specific, a actorilor implicați, dar și a strategiilor utilizate de părțile aflate în conflict. Dacă agresiunea este o constantă în toate confruntările armate, căile și mijloacele utilizate pentru implementarea acesteia au evoluat constant, datorită, în special, implementării unor tehnologii revoluționare. Astfel, dacă natura intimă a războiului nu este dependentă de factorul timp, în sensul că agresiunea și comportamentul antagonic sunt caracteristici perene ale conflictului armat, în schimb caracterul războiului este supus transformărilor, fiind determinat de contextul istoric în care confruntarea militară are loc.

Modelul propus de către viitorologii Alvin și Heidi Toffler se dovedește util pentru o mai bună înțelegere a corelației dintre natura și caracterul războiului. Modelul se bazează pe conceptul de „avuție revoluționară”, definit drept modalitatea

Universitatea Națională de Apărare „Carol I”
e-mail*: dan.antonio@gmail.com*

fundamentală prin care o societate creează avuția necesară supraviețuirii, progresului și dominanței sale în raport cu alte societăți[1]. Analiza modelului subliniază ideea că uneltele războiului sunt o reflexie a gradului de dezvoltare tehnologică a unei societăți, societățile avansate tehnologic beneficiind de un avantaj strategic față de societățile mai puțin avansate. Astfel, se poate infera că elementul de bază care determină schimbarea caracterului războiului este gradul de implementare, în cadrul societății, în general, și în cadrul forțelor armate, în particular, a tehnologiilor noi, revoluționare. Praful de pușcă, avionul, bomba nucleară, comunicațiile digitale și computerul sunt exemple de tehnologii care au schimbat radical caracterul războiului. În esență, după cum și numele o indică, o tehnologie revoluționară modifică fundamental abordarea, planificarea și evaluarea activităților, necesitând revizuirea, adaptarea sau crearea unor noi politici și doctrine de asigurare, integrare, instruire și întrebuințare în luptă a capabilităților bazate pe respectiva tehnologie. Acceptând importanța implementării tehnologiilor noi în modelarea caracterului războiului, se poate estima potențiale dezvoltări ale spectrului conflictului. Subsecvent, pe această bază putem elabora strategii inovative care să ofere cadrul de lucru necesar pentru implementarea unor soluții eficiente de utilizare a instrumentului militar al puterii de stat.

Se poate observa cu ușurință modul în care implementarea tehnologiei informației a produs intensificarea informațională a majorității aspectelor, elementelor și instituțiilor fundamentale ale societății. Accentuarea dependenței de informație a determinat extinderea la nivel global a rețelelor și a serviciilor bazate pe tehnologia informațiilor. Noua tehnologie digitală cu care societatea realizează avuție a fost extinsă și adaptată domeniului militar, fiind transformată într-o nouă unealtă a războiului și determinând apariția unui nou mediu operațional – spațiul cibernetic, asemuit unui înveliș virtual care acoperă întreaga planetă. Chiar dacă conceptul de putere bazată pe informație nu este nou, analiza evenimentelor recente relevă faptul că spațiul cibernetic a deschis o nouă formă de manifestare a puterii în relațiile internaționale. Spre deosebire de celelalte tipuri de putere statală, această „putere cibernetică” depinde de infrastructura digitală, de resursele hardware și software, precum și de informațiile canalizate prin mediul cibernetic. Unii experți definesc „puterea cibernetică” drept „abilitatea de a utiliza spațiul cibernetic pentru crearea avantajelor și influențarea evenimentelor în celelalte medii operaționale și de-a lungul tuturor instrumentelor de putere”[2]. Din analiza definiției rezultă că aplicarea puterii cibernetice are o dublă dimensiune, având potențialul de a genera atât efecte interne, în cadrul mediului cibernetic, cât și externe, în cadrul celorlalte medii operaționale. De asemenea, caracteristici, precum acces relativ facil și ieftin, asimetrie a vulnerabilităților, anonimitate, întindere globală, viteză sporită de acțiune și flux temporal specific, asigură condiții pentru aplicarea puterii cibernetice și de către actori nonstatali, pentru promovarea unor interese proprii, de natură politică, economică sau socială.

La nivelul actorilor statali se constată existența unor percepții diferite a mediului cibernetic, a Internetului și a modului de interacțiune a acestuia cu mediul informațional, fapt ce influențează modul de abordare a proiecției puterii cibernetice. Spre exemplificare, statele democratice consideră Internetul drept un bun comun, destinat să fie utilizat de către toate statele pentru beneficii reciproce. Conform modelului Westphalian, atunci când este necesar, puterea actorului statal poate fi aplicată în mediul cibernetic într-o manieră similară cu proiecția acesteia în mediile operaționale naturale. Decizia de aplicare a instrumentului de putere în mediul cibernetic ar trebui să constituie o responsabilitate a statelor, aplicarea urmând a fi făcută într-un cadru legal proiectat în conformitate cu principii consacrate ale dreptului internațional, precum principiul proporționalității și principiul discriminării. În schimb, statele conduse de regimuri autoritare consideră Internetul un mediu-extensie al suveranității naționale. Comportamentul acestor actori-statali în mediul cibernetic este caracterizat de un control strict, reflectat pe plan intern în cenzură și restricționarea accesului la resursele informaționale globale, iar pe plan extern prin utilizarea indirectă sau în ascuns a capabilităților cibernetice proprii împotriva altor state. De regulă, aceste intruziuni sau operații cibernetice ofensive sunt executate sub masca anonimității și sub pragul de declanșare a unui răspuns militar conform legislației internaționale.

Într-un articol publicat în 2015[3] am analizat modul în care apariția mediului operațional cibernetic este reflectată în strategiile de securitate

și apărare a unor state moderne, concluzionând că acțiunile cibernetice cu caracter militar se vor intensifica, concomitent cu dezvoltarea unor capabilități cibernetice care să asigure avantaje strategice și tactice în spațiul de confruntare. Într-adevăr, utilizarea spațiului cibernetic pentru desfășurarea unor operații cibernetice cu caracter ofensiv este tot mai des semnalată și analizată în presa și în literatura de specialitate, relevând încă o dată aspectul dual al tehnologiilor și rolul acestora în modelarea caracterului războiului. Comunicațiile globale și accesul rapid la informație face posibil ca războiul să nu mai fie apanajul exclusiv al statelor și accentuează slaba demarcație între starea de pace și cea de război. Caracteristica dual a tehnologiei informației este exploatată cu succes de către actori nonstatali, precum și de grupuri teroriste sau grupări de crimă organizată transnațională, pentru avansarea obiectivelor politice sau economice proprii. Capacitatea Internetului este exploatată de actori nonstatali, precum Hezbollah, al-Qaeda sau ISIS pentru asigurarea comenzii, controlului și sincronizării unor operații proprii, precum și pentru strângerea de fonduri, răspândirea ideologiei extremiste, recrutarea de noi adepți și instruire în metode teroriste. De asemenea, grupările de crimă organizată, de multe ori în cooperare cu grupările teroriste, utilizează mediul cibernetic pentru comercializarea de droguri, trafic de materiale și substanțe controlate, furt și spălare de bani. De partea cealaltă a baricadei, forțele armate moderne dezvoltă capabilități militare avansate bazate pe tehnologia informațiilor, inclusiv „arme cibernetice”. Aceste noi capabilități pot fi utilizate într-o manieră nondistructivă asigurând supravegherea și culegerea de informații din cadrul rețelelor adversarului, sau într-o manieră distructivă, făcând posibilă alterarea sau distrugerea informațiilor rezidente în sistemele cibernetice, precum și distrugerea fizică a sistemelor de comandă și control sau a unor părți ale acestora care sunt controlate prin intermediul mediului cibernetic[4]. Concomitent, sub umbrela unei anonimități plauzibile, unele state utilizează capacitățile cibernetice proprii pentru spionaj militar și industrial, pentru supravegherea și interceptarea comunicațiilor, precum și pentru manipularea informațiilor și a comunicațiilor adresate unor actori țintă.

Care este, totuși, relevanța mediului cibernetic pentru modelarea și utilizarea instrumentului militar de putere? Este doar un subiect de noutate sau un element care va produce sau a produs deja o schimbare de paradigmă? Majoritatea actorilor statali mențin utilizarea instrumentului militar al puterii de stat ca ultimă instanță de apărare și/sau impunere a intereselor naționale, de asigurare a securității și de protecție a instituțiilor statului și a populației acestuia. Totuși, mediul operațional contemporan este caracterizat prin schimbări și evoluții permanente la nivel geopolitic. Astfel, evoluția unor noi centre de putere regională, noile tipuri de amenințări asimetrice la adresa securității, vulnerabilitățile infrastructurilor fizice, corelate cu lecțiile învățate din conflictele militare desfășurate în ultimele două decenii, relevă faptul că noțiunea clasică a războiului trebuie revizuită. Acest fapt trebuie să determine schimbări sesizabile în gândirea militară și în abordarea conflictului armat, la nivel strategic, operativ și tactic.

Probabil conceptul de strategie a câmpului de luptă nu mai este de actualitate, din cauza faptului că majoritatea conflictelor curente și previzibile din viitorul apropiat, au caracter asimetric sau hibrid, cu variații ale intensității în perioade lungi de timp și cu utilizarea intensă a mediului cibernetic. În schimb, conceptul de sincronizare a mediului operațional trebuie să fie implementat cu precădere, datorită faptului că forțele armate acționează într-un mediu mutidimensional, caracterizat drept volatil, incert, complex și ambiguu. Riscurile asociate acestui tip de mediu operațional pot fi reduse prin alinierea obiectivelor pe toate palierele artei operative, prin creșterea rezilienței structurilor militare, adaptabilitate, claritate a intenției și o mai bună comunicare în interiorul organizației militare, precum și între aceasta și celelalte instituții sau organizații cu care cooperează în domeniul securității, apărării, cercetării și dezvoltării capabilităților militare[5]. Aceste elemente presupun implementarea unui sistem de comandă și control robust, capabil să reziste agresiunilor cibernetice severe.

Majoritatea activităților de coordonare și de sincronizare a mediului operațional se realizează prin intermediul sistemului de comandă și control, descris drept un „ansamblu format din personal, activități de management al informațiilor, proceduri, echipamente și mijloace auxiliare utilizate de comandant pentru conducerea operațiilor militare”[6]. Componenta tehnologică a

sistemului de comandă și control este materializată de către sistemul de comunicații și informatic, sistem care asigură conectivitatea structurii militare la mediul cibernetic. Pentru menținerea activă a componentelor și a serviciilor C2 asociate cu culegerea, procesarea, stocarea, analiza și diseminarea informațiilor, asigurarea continuității proceselor de planificare, luare a deciziei și de conducere a operațiilor militare, precum și crearea și actualizarea imaginii operaționale comune, sistemul de comunicații și informatic trebuie să fie protejat atât împotriva atacurilor cinetice, cât și împotriva atacurilor cibernetice. Sistemele de comunicații și informatice integrate prezintă o serie de vulnerabilități care constituie suprafețe de atac pentru adversar. Aceste vulnerabilități cibernetice se datorează unor multitudini de cauze, incluzând erori de proiectare, configurare sau operare a elementelor sistemului de comunicații și informatic, complexitate tehnică și logică crescută, pregătire deficitară a personalului în domeniul apărării cibernetice, interfațarea domeniilor de securitate a rețelelor și utilizarea neadecvată a instrumentelor de secretizare. Vulnerabilitățile sunt, de regulă, vizate în cadrul atacurilor cibernetice pasive sau active, de către amenințări la vedere, acoperite sau accidentale, având surse din interior, din exterior sau din mediu[7]. În cadrul măsurilor specifice de apărare cibernetică aceste vulnerabilități trebuie reduse la maxim prin măsuri tehnice, organizatorice și procedurale, care să conducă la creșterea rezilienței sistemului de comunicații și informatic și implicit a sistemului de comandă și control.

Prin extensie, utilizarea eficientă a instrumentului militar este influențată de existența unui sistem de comandă și control rezilient. Astfel, în condițiile existenței riscurilor și amenințărilor cibernetice, implementarea conceptului de apărare cibernetică activă în cadrul sistemelor de comandă și control contribuie la asigurarea rezilienței componentei tehnologice a acestuia, determinând accelerarea și flexibilitatea procesului de luare a deciziei. Necesitatea asigurării cerințelor de interoperabilitate și conectivitate a sistemelor de comunicații și informatice militare determină abordarea apărării cibernetice într-o manieră unitară și integrată la toate nivelele artei militare. Implementarea acestui deziderat necesită o strategie unitară la nivelul instituției militare, strategie care trebuie să includă comunicarea și cooperarea interagenții, precum și consultarea și direcționarea industriilor asociate. Atât în starea de pace, cât și pe timp de război, acest proces contribuie la translatarea obiectivelor politico-militare în obiective militare de nivel operativ și tactic.

Mediul operațional cibernetic, cu provocările sale asociate, este luat în considerare și abordat diferențiat în legislația națională în vigoare. Astfel, *Strategia de securitate cibernetică a României*[8] stabilește obiective generale și responsabilități pentru diversele ministere și agenții implicate în securitatea și apărarea cibernetică a României, indicând măsuri și direcţii de acţiune pentru punerea în aplicare a *Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*. Subsecvent, *Strategia Națională de Apărare a Țării pentru perioada 2015-2017* include consolidarea și securitatea infrastructurilor critice cibernetice în lista obiectivelor naționale de securitate. Din perspectivă externă, strategia ia în considerare amenințările cibernetice asupra infrastructurilor informaționale strategice și menționează riscurile asociate atacurilor cibernetice lansate de grupuri ostile, posibil în cadrul unor conflicte militare de joase intensitate. În final, din perspectivă acțională, strategia vizează asigurarea mecanismelor de prevenire și contracarare a atacurilor cibernetice, în special în cadrul unor acțiuni asimetrice de tip hibrid[9]. Preluând prevederile *Strategiei de securitate cibernetică* și ale *Strategiei Naționale de Apărare*, Ministerul Afacerilor Interne abordează și operaționalizează obiective specifice domeniului său de responsabilitate, precum criminalitatea cibernetică sau camuflajului informatic, în cadrul *Strategiei naționale de ordine și siguranță publică 2015-2020*[10]. Documentul stabilește ca obiectiv strategic „creșterea nivelului de securitate a persoanelor fizice/juridice și entităților statului în spațiul cibernetic”[11], indicând și direcțiile specifice de acțiune pentru îndeplinirea acestuia. O direcție importantă o constituie „dezvoltarea planurilor de punere în aplicare a *Strategiei de Securitate Cibernetică a României*. În contextul operațional actual, modelat de amenințări cibernetice, este recomandabil ca și forțele armate să abordeze problematica mediului cibernetic în cadrul unei strategii specifice. Pe lângă asigurarea unei alinieri strategice între abordarea amenințărilor cibernetice ce se manifestă sub nivelul sau deasupra pragului de

declanșare a unui conflict, această strategie trebuie să asigure cadrul legal și resursele necesare pentru implementarea conceptului de apărare cibernetică. De asemenea, pornind de la alinierea doctrinară la conceptul NATO de apărare cibernetică, principalul efect al strategiei va fi creșterea rezilienței sistemelor de comandă și control și asigurarea unor capabilități cibernetice interoperabile atât cu parteneri interni, cât și cu cei din cadrul Alianței.

Formularea unei strategii naționale de securitate și apărare trebuie să asigure cadrul legal și resursele necesare pentru implementarea subsecventă a căilor și a mijloacelor moderne necesare forțelor armate pentru îndeplinirea obiectivelor stabilite la nivel politico-militar, prin succes le nivel operativ și tactic. Considerând caracterul schimbător al războiului și influența pe care mediul operațional cibernetic o are asupra modificării acestuia, este preferabil ca actualul cadru de referință să fie adaptat noilor cerințe operaționale ale mediului de tip VUCA[12]. Strategia militară și doctrinele categoriilor de forțe ale armatei trebuie să fie integrate și să asigure modalități de asigurare a sincronizării mediului operațional, cu integrarea apărării cibernetice în procesul de planificare operațională. De asemenea, dotarea, echiparea și instruirea forțelor armate trebuie să fie reproiectate în ariile responsabile pentru asigurarea comenzii și controlului operațiilor militare, indiferent de natura acestora, ținându-se cont de existența riscurilor și a amenințărilor cibernetice. Aceste măsuri pot determina transformarea actualelor forțe armate, majoritatea proiectate pentru operații militare simetrice, în forțe moderne, agile, interoperabile, sincronizate și capabile să exploateze și să controleze dimensiunile geofizice, spațiale, temporale, informaționale, cibernetice, tehnologice și cognitive ale spectrului confruntării asociat mediului operațional contemporan.

NOTE:

1 Alvin and Heidi Toffler, *War and Anti-War – Making sense of today global chaos*, Grand Central Publishing, New York, 1995, pp. 79-83.

2 Joseph S. Nye, *Cyber Power*, Harvard Kennedy School: Belfer Center for Science and International Affairs, Cambridge, 2010, pp. 4-12.

3 Ștefan-Antonio Dan-Șuteu, *Apărarea cibernetică în concepția unor armate moderne*, Buletinul UNAp, nr. 3/2015, Editura UNAp „Carol I”, București, 2015.

4 James Turitto, *Understanding Warfare in the 21st Century*, International Affairs Review, Vol. XXIV, No. 1/2016, http://www.iar-gwu.org/node/145, accesat la 01.07.2016.

5 Amanda MacArthur, *Beating VUCA's Whiplash Factor*, 2016, https://www.td.org/Publications/Magazines/TD/TD-Archive/2016/06/Beating-Vucas-Whiplash-Factor, accesat la 01.06.2016.

6 *** *F.T./T-2, Manualul pentru luptă al Batalionului de Comunicații și Informatică*, Sibiu, 2006.

7 *Ibidem*.

8 Guvernul României, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*, publicată în Monitorul Oficial, Partea I, nr. 256/23.05.2013, București, 2013.

9 Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – o Românie puternică în Europa și în lume*, București, 2015, pp. 9-20.

10 Guvernul României/Ministerul de Interne, *Strategia națională de ordine și siguranță publică 2015-2020*, publicată în Monitorul Oficial, Partea I, nr. 763/13.10.2015, București, 2015, pp. 3-18.

11 *Ibidem*.

12 „VUCA” este un acronim introdus de *Colegiul de Război al Armatei Statelor Unite*.

BIBLIOGRAFIE

Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – o Românie puternică în Europa și în lume*, București, 2015.

Guvernul României, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*, publicată în Monitorul Oficial, Partea I, nr. 256/23.05.2013, București, 2013.

Guvernul României, *Hotărârea nr. 779/2015 pentru aprobarea Strategiei naționale de ordine și siguranță publică 2015-2020*, publicată în Monitorul Oficial, Partea I, nr. 763/13.10.2015, București, 2015.

*** *F.T./T-2, Manualul pentru luptă al Batalionului de Comunicații și Informatică*, Sibiu, 2006.

Dan-Șuteu Ștefan-Antonio, *Apărarea cibernetică în concepția unor armate moderne*, Buletinul UNAp „Carol I”, nr. 3/2015, Editura UNAp „Carol I”, București, 2015.

MacArthur Amanda, *Beating VUCA's Whiplash Factor*, 2016, https://www.td.org/Publications/Magazines/TD/TD-Archive/2016/06/Beating-Vucas-Whiplash-Factor, accesat la 01.06.2016.

Nye S. Joseph, *Cyber Power*, Harvard Kennedy School: Belfer Center for Science and International Affairs, Cambridge, 2010.

Toffler Alvin and Heidi, *War and Anti-War - Making sense of today global chaos*, Grand Central Publishing, New York, 1995.

Turitto James, *Understanding Warfare in the 21st Century*, International Affairs Review, Vol. XXIV, No. 1/2016, http://www.iar-gwu.org/node/145, accesat la 01.07.2016.