PREGĂTIREA STRUCTURILOR DE APĂRARE CIBERNETICĂ PENTRU SPRIJINUL OPERAȚIEI MILITARE

TRAINING OF CYBER DEFENSE STRUCTURES IN SUPPORT OF MILTARY OPERATION

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

Analiza conflictelor curente relevă tendința ascendentă a amenințărilor cibernetice exercitate asupra infrastructurilor critice și a mediului politic, economic și militar, cu accent pe atacul sistemelor de comandă și control și a rețelelor de comunicații și informatice ce deservesc entitățile componente ale sistemelor naționale de apărare. Evoluția accelerată și virulența amenințărilor cibernetice sunt luate în considerare de către actorii statali, alianțe și organizații internaționale, care prin politicile proprii promovează dezvoltarea capacităților de securitate și apărare cibernetică. Pentru a contracara operațiile cibernetice sofisticate lansate de unii actori statali sau nonstatali, se impune abordarea prioritară a deficitelor de „luptători cibernetici”, ținând cont de faptul că în actualele condiții de reduceri bugetare, majoritatea forțelor armate moderne întâmpină dificultăți în recrutarea, instruirea, perfecționarea și retenția personalului de specialitate din domeniul securității și apărării cibernetice.

The analysis of current conflicts reveals the ascendant trend of cyber threats against critical infrastructure and political, economic and military environments, with emphasis on cyber-attacks targeting the national defense entities command and control systems, communication and information networks. The accelerated evolution and the virulence of cyber-attacks are considered by state-actors, alliances and international organizations through specific policies that promotes cyber security and cyber defense capacity building. To counter the sophisticated cyber operations perpetrated by some state and non-actors, it is necessary to approach and prioritize the "cyber warriors" shortcomings, taking into account that, within the current budgetary restraints, the majority of armed forces face difficulties with recruiting, training, development, and retaining of a performant cyber work force.

Cuvinte-cheie: apărare cibernetică; strategie; operații militare; atac cibernetic; instruire.
Keywords*: Scyber defense; strategy; military operations, cyber attack, training.*

Pe baza observațiilor efectuate asupra modului de desfășurare a conflictelor din ultimul deceniu se poate afirma că operațiile din mediul cibernetic sunt un ingredient de bază în rețeta succesului politico-militar. Cercetările științifice din domeniu laolaltă cu analizele din presa tradițională relevă tendința ascendentă a amenințărilor cibernetice atât asupra mediului de afaceri, a economiei, a infrastructurilor critice, cât și asupra rețelelor informatice ale entităților componente ale sistemelor naționale de apărare.

Pentru a răspunde acestui nou tip de amenințare la adresa securității și apărării, majoritatea guvernelor statelor dezvoltate au crescut investițiile în domeniul apărării cibernetice în pofida presiunii publice de a reduce cheltuielile asociate în general dezvoltării de noi capabilități militare. Acest aparent paradox accentuează încă o dată importanța pe care operațiile din mediul cibernetic o au în actualul context geostrategic, caracterizat de volatilitate, ambiguitate, incertitudine și complexitate. Aceste caracteristici alimentează apetența unor actori pentru evitarea conflictelor militare tradiționale și favorizează abordări neconvenționale, indirecte, pentru obținerea succesului la nivel tactic, operativ și strategic, prin utilizarea operațiilor cibernetice. Datorită structurii și dinamicii sale specifice, mediul cibernetic are potențialul de a intensifica schimbul de informații, cooperarea, coordonarea

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

și sincronizarea acțiunilor militare, dar și de a produce perturbații extreme în procesul de luare a deciziei și de implementare a acesteia. În special „intensificarea informațională”[1] asociată mediului cibernetic și dificultatea atribuirii atacurilor cibernetice oferă posibilitatea obținerii unor efecte importante la un preț relativ scăzut. Această afirmație este susținută de abordarea rusească a utilizării operațiilor cibernetice pentru a obține avantaje pe toate palierele artei operative, utilizând capabilități și forță de lucru specializată din organică sau apelând la „externalizarea” anumitor tipuri de servicii.

Astfel, conform rezultatelor unor investigații de criminalitate informatică, atacurile cibernetice majore de tipul *distributed denial-of-service* (DDOS), care au paralizat infrastructura informatică a Estoniei în anul 2007, au fost executate de către „hackeri patrioți” de naționalitate rusă. O operație similară, aparent executată tot de către „hackeri patrioți”, s-a petrecut concomitent cu invazia militară a Georgiei de către trupele ruse în anul 2008. Ambele evenimente au afectat grav capacitatea de comunicare internă și externă a celor două națiuni, izolând guvernele de populația proprie și de comunitatea internațională. Originea acestor atacuri cibernetice este greu de probat cu exactitate, deoarece atacatorii cibernetici și-au mascat locația reală prin rutarea traficului asociat intruziunii în servere situate în zone geografice diferite. Chiar dacă probe circumstanțiale indică faptul că aceste atacuri au fost sponsorizate de către executivul rus, acesta a reușit să utilizeze spre propriul beneficiu problema atribuirii în spațiul cibernetic, menținându-și o poziție de negare plauzibilă a acuzațiilor ce i-au fost aduse.

O dezvoltare a aceleiași abordări indirecte s-a observat în cadrul conflictului din Ucraina din anul 2014, abordare concretizată în ceea ce unii specialiști militari numesc „război hibrid”. Acest concept cuprinde combinarea și utilizarea instrumentelor militare și nonmilitare în cadrul unei campanii proiectate să determine surpriza strategică, să asigure preluarea și menținerea inițiativei, simultan cu câștigarea avantajelor de ordin fizic și psihologic asupra adversarului, inițial prin intermediul mijloacelor diplomatice și presiunii economice. Războiul hibrid presupune, de asemenea, utilizarea unor sofisticate operații informaționale, electronice și cibernetice, sprijinite de acțiuni militare cinetice și de culegere de informații executate, de regulă, sub acoperire și ocazional la vedere[2]. Analizând conceptul descris mai sus putem infera că amenințarea cibernetică este parte integrantă a unui cadrul operațional de tip hibrid. Astfel, în toate cele trei cazuri amintite anterior, operațiile cibernetice „externalizate” au fost utilizate în mod agresiv, probabil sub direcționarea serviciilor de informații și de securitate ruse. Acestea au asigurat coordonarea și sincronizarea acțiunilor forțelor regulate cu cele ale miliților separatiste, grupurilor de „hackeri patrioți” și de criminalitate informatică organizată atât în domeniile operaționale naturale, cât și în mediul cibernetic, combinând instrumente diplomatice, informaționale, militare, economice și cibernetice pentru a exercita influență psihologică și presiune atât asupra populației, forțelor armate și de securitate adverse, cât și asupra opiniei publice din statul țintă.

În cadrul conflictului din Ucraina, forțele ruse și partenerii acestora au executat în teatrul de operații o gama largă de tehnici, tactici și proceduri de război cibernetic. Acestea includ culegere de informații, din și despre mediul cibernetic, spionaj cibernetic sofisticat, atacuri DDOS masive, alterarea site-urilor web și, cel mai notabil, atacuri cibernetice încununate de succes asupra rețelelor de alimentare cu energie electrică ucrainiene. Investigațiile companiilor de securitate cibernetică sugerează faptul că atacul respectivelor rețele electrice a fost inițializat prin intermediul calului troian numit BlackEnergy, care a fost utilizat pentru implantarea pe stațiile de control ale rețelei electrice din vestul Ucrainei a malware-ului KillDisk[3]. Analiza efectuată de către compania de securitate cibernetică iSight face legătura atacurilor cibernetice asupra rețelelor electrice ucrainiene cu grupul de criminalitate cibernetică numit Sandworm, care aparent are legături cu guvernul rus. Analiza precizează că în urma monitorizării de peste un an a grupului Sandworm s-a descoperit că acesta colecta informații atât din cadrul computerelor oficialităților din administrația ucraineană, cât și din cadrul rețelelor informatice NATO și UE, cu un accent deosebit pe datele referitoare la sistemele de control industrial[4]. De asemenea, în conformitate cu analiza efectuată de compania de securitate cibernetică FireEye, pe măsură ce conflictul fizic sporea în intensitate și activitatea luptătorilor cibernetici urma o curbă ascendentă. Atacurile

executate de luptătorii cibernetici afiliați părții ruse se concretizau sub forma propagandei online, culegerii de informații din mediul cibernetic și acțiunilor de corupere a datelor și de distrugere a sistemelor informaționale. Ținând cont de cele sus-menționate se poate concluziona că dimensiunea cibernetică a confruntărilor militare moderne a depășit faza speculativ-teoretică, operațiile cibernetice ruse asigurând avantaje tactice în toate domeniile de confruntare, care ulterior au fost transformate în efecte de ordin strategic[5].

Din studiul doctrinei pentru securitatea informației reiese importanța strategică pe care guvernul rus o acordă securității informației, acesta etichetând „armele informaționale” drept instrumente adecvate pentru atingerea unor obiective politice și militare, caracterizând amenințările informaționale ca și amenințări de natură preponderent psihologică. Spațiul informațional este definit de doctrina rusă drept „sfera de activitate destinată modelării, construirii, transmiterii, utilizării și stocării informațiilor ce influențează individul și conștiința socială[6] atât din perspectiva infrastructurii informaționale, cât și a informației propriu-zise”. Doctrina stabilește pe larg principalele linii de acțiune pentru asigurarea protecției împotriva amenințărilor informaționale prin intermediul unei abordări duale, care combină elemente de natură tehnologică cu elemente de natură psihologică. În pofida terminologiei ambigue și a elementelor de propagandă inserate în doctrinele și în politicile ruse de securitate a informației, analiza documentelor disponibile sugerează faptul că forțele armate ruse beneficiază de personal specializat și autorizat să planifice și să execute operații ofensive și defensive în cadrul mediului informațional/cibernetic.

În cadrul acțiunilor sale asimetrice, pe lângă personalul specializat în operații cibernetice, forțele ruse utilizează personal specializat în diseminarea informațiilor în scopul influențării populațiilor-țintă utilizând canale de comunicare ce converg în mediul cibernetic și care includ social media, radio, TV, telefonia mobile și Internetul. Aceste capabilități, tehnici, tactici și proceduri asimetrice sunt combinate într-o manieră cuprinzătoare, fiind proiectate să asigure efecte care altădată nu puteau fi obținute decât prin mijloace pur militare. Într-un cadru operațional de tip hibrid, majoritatea vectorilor de atac, chiar dacă sunt lansați și controlați din medii operaționale diferite, au o componentă cibernetică, deoarece mediul cibernetic alături de cel electromagnetic asigură cerințele de comunicații și de transmiterea a informațiilor necesare comenzii și controlului vectorilor respectivi. Această convergență a vectorilor de atac în mediul cibernetic implică abordarea cuprinzătoare a amenințării cibernetice, nu numai dintr-un punct de vedere îngust, tehnologic, cât mai degrabă dintr-o perspectivă multidisciplinară.

Evoluția accelerată și virulența amenințărilor cibernetice sunt luate în considerare de către actorii statali, alianțe și organizații internaționale, care prin politicile proprii promovează dezvoltarea capacităților de securitate și apărare cibernetică, cu accent pe acoperirea deficitelor de specialiști în domeniu. Astfel, pe măsură ce importanța operațiilor cibernetice a crescut în economia strategiilor de promovare sau de protecție a intereselor naționale a actorilor statali cu armate puternice, investițiile în capabilități cibernetice a crescut proporțional. De exemplu, bugetul apărării din 2014 aprobat de administrația Obama prevedea suma de 4,7 miliarde dolari americani la capitolul cheltuieli în domeniul apărării cibernetice, ceea ce reprezenta în fapt o creștere cu 800 de milioane de dolari americani față de bugetul precedent[7].

În concluzie, dacă elementele hardware și software necesare construirii unor capabilități cibernetice robuste sunt relativ ușor accesibile la un preț rezonabil pe piața liberă, nu același lucru se poate afirma despre forța de muncă necesară pentru exploatarea eficientă a unor astfel de capabilități. În particular, majoritatea forțelor armate moderne întâmpină dificultăți în recrutarea, instruirea, perfecționarea și retenția personalului de specialitate din domeniul securității și apărării cibernetice. Este necesară o nouă abordare a modului de satisfacere a cerinței tot mai crescute pentru luptători în mediul cibernetic, în sensul creării unei categorii de personal motivat, înalt specializat și instruit. Acesta trebuie să fie capabil să planifice, să execute și să evalueze operații cibernetice cu caracter atât defensiv, cât și ofensiv, executate în sincronicitate cu operațiile din mediile naturale, contribuind astfel la crearea efectelor sinergice și, în final, la obținerea succesului operațiilor militare.

NOTE:

1 Bob Johansen, James Euchner, *Navigating the VUCA World*, Research Technology Management no. 1 (January), New York, 2013, pp. 10-15.

2 Mark Galeotti, *Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?*, Small Wars & Insurgencies, 27:2, 2016, pp. 282-301.

3 Gabi Siboni, Zvi Magen, *The Cyber Attack on the Ukrainian Electrical Infrastructure: Another Warning*, INSS Insight Nr. 798, 2016.

4 *Ibidem*.

5 Kenneth Geers, Martin Libicki, Jeffrey Mankoff, Alina Polyakova, *Watch live: Cyberwar in Ukraine?*, Christian Science Monitor, 14 Apr. 2016, pp. 1-2.

6 Jolanta Darczewska, *Russia's armed forces on the information war front. Strategic documents*, Centre for Eastern Studies, Ośrodek Studiów Wschodnich im. Marka Karpia, 2016, pp. 3.

7 Jennifer J. Li, Lindsay Daugherty, *Training Cyber Warriors – What Can Be Learned From Defense Language Training*, RAND Corporation, Santa Monica, California, 2015, pp. 9-12.

BIBLIOGRAFIE

Darczewska Jolanta, *Russia's armed forces on the information war front. Strategic documents*, Centre for Eastern Studies, Ośrodek Studiów Wschodnich im. Marka Karpia, 2016, https://www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents, accesat la 12.06.2017.

Galeotti Mark, *Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?*, Small Wars & Insurgencies, nr. 27:2, 2016.

Geers Kenneth, Libicki Martin, Mankoff Jeffrey, Polyakova Alina, *Watch live: Cyberwar in Ukraine?*, Christian Science Monitor, 2016.

Li Jennifer J., Daugherty Lindsay, *Training Cyber Warriors – What Can Be Learned From Defense Language Training*, RAND Corporation, Santa Monica, California, 2015.

Johansen Bob, Euchner James, *Navigating the VUCA World*, Research Technology Management no. 1 (January), New York, 2013.