DIMENSIUNEA CIBERNETICĂ A CONFLICTELOR MILITARE CONTEMPORANE

CYBER DIMENSION OF CURRENT MILITARY CONFLICTS

Drd. Benedictos IORGA*

Dezvoltarea tehnologică a societății civile, în ultimii douăzeci de ani, şi globalizarea infrastructurilor de comunicaţii au condus la schimbări profunde în toate sistemele de securitate. Extinderea reţelei de Internet, dezvoltarea reţelelor mobile de comunicaţii şi creşterea dependenţei de informaţii a întreagii societăți umane, a generat, alături de explozia economică, apariţia unor noi riscuri şi ameninţări în mediile de reţele, generic cunoscute ca „cyber ameninţări”.

Naţiunile cu un grad ridicat de digitalizare sunt, în prezent, sub ameninţări de atacuri cibernetice care au ca scop perturbarea activităţilor statelor din sfera de informaţii, prin distrugerea sau alterararea resurselor de informaţii şi a infrastructurii critice, sau prin afectarea imaginii publice şi inducerea unui sentiment de insecuritate şi de neîncredere în capacitatea lor de apărare.

Technological development of civil society în the last 20 years and the globalization of communications infrastructures have led to profound changes în all nations security systems. Expansion of the Internet network, the large development of mobile communication networks and the increasing dependence of information for the entire human society generated în addition to economic boom, the emergence of new risks and threats to networks environments generically known as “cyber threats”.

Nations with a high degree of digitization are currently under threats of cyber attacks, aiming to the disruption of states activities în information sphere, by destruction or alteration of information resources and critical infrastructure, or by affecting the public image and engendering a sense of insecurity and distrust în their defense capabilities.

Cuvinte-cheie: cyber război; cyber operaţien; cyber atac; cyber security; cyber arme; cyberspace; cyber-terorism; cyber spionaj; cyber capabilităţi.

Keywords: *cyber war; cyber operation; cyber attack; cyber security; cyber weapons; cyberspace; cyber-terrorism; cyber espionage; cyber capabilities.*

Dezvoltarea tehnologiei informaţiei, la scară globală, creşterea dependenţei societăţii de instrumentele informatice, de mediile de reţea şi de informaţie, ca principalul element al cunoaşterii, a generat, pe lângă o evoluţia socială accelerată, şi premisele apariţiei şi dezvoltării riscurilor cibernetice ca efect al exploatării slăbiciunilor umane şi tehnologice din mediul informaţional. Reţelele de comunicaţii, privite ca elementul principal al infrastructurii mediului informaţional, au devenit, astfel, mediul de interacţiune şi convieţuire asemenea infrastructurii clasice din viaţa de zi cu zi. Dacă, iniţial, o reţea informatică sau de comunicaţii nu reprezenta altceva decât un instrument de natură administrativă şi un mijloc facil de realizare a comunicării, la momentul actual, odată cu dezvoltarea WEB-ului pe scară largă şi cu informatizarea accelerată pe toate palierele sociale (industrie, medicină, economie, educaţie, apărare, securitate etc.), mediul de reţea a devenit subiect de discuţie pe problematici care ţin de securitatea mondială.

Din punct de vedere militar, apariţia şi dezvoltarea societăţii informaţionale dependentă de mediul de reţea a generat posibilitatea dezvoltării acţiunilor în noul spaţiu creat, asemenea unor acţiuni clasice, treptat, pornind de la instrumente şi acţiuni simple, de pionierat, până la executarea de campanii cibernetice desfăşurate după reguli şi legi hibride. Dacă iniţial o ameninţare cibernetică, precum

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

existenţa unui virus sau a unui cod maliţios, a fost considerată o problemă care ţine de funcţionalitatea unor servicii informatice la nivelul entităţilor, fără implicaţii asupra securităţii unui stat, în momentul de faţă asemenea elemente au devenit provocări majore de securitate şi instrumente aproape perfecte pentru acţiunile militare care pot fi comparate cu armele clasice, dar cu efect letal asupra informaţiei. Apariţia acestor noi oportunităţi, reprezentate de acţiunile cibernetice, au deschis cale unor noi tipuri de operaţii militare, diferite de cele clasice prin modul de manifestare şi prin regulile de angajare şi executare, dar cu acelaşi scop, de eliminare a adversarului sau de zădărnicire a acţiunilor acestuia în mediul operaţional cibernetic.

Deşi realitatea conflictelor militare din ultimii 10 ani pare a ne da dreptate, există analişti care ridică semne de întrebare cu privire la „definirea spaţiului cibernetic ca un nou mediu de desfăşurare a conflictelor militare”. De asemenea, ca urmare de diversităţii de opinie şi a lipsei unor dovezi palpabile, bazate pe dreptul internaţional al conflictelor armate” apare firesc întrebarea dacă „conflictele ultimilor 10 ani au avut sau nu o dimensiune cibernetică”.

al celor patru spaţii de acţiune militară clasice (cosmic, aerian, terestru şi maritim) şi aceasta, în principal, datorită faptului că la baza tuturor acţiunilor militare se află nevoia de comunicare în sensul existenţei mediului de reţea şi, nu în ultimul rând, a utilizării tehnologiei ca mijloc de luptă (figura 1).

În ciuda dovezilor din ce în ce mai evidente (conflictul din fost Iugoslavie, atacurile din Estonia, conflictul din Georgia şi conflictul actual din Ucraina) ca suport al argumentaţiei anterioare, scepticismul privind punerea în practică a noilor concepte referitore la spaţiul cibernetic, privit ca un mediu nou „individualizat” de ducere a luptei armate, poate fi acceptabil, aşa cum şi posibilitatea existenţei unui război nuclear a fost negată, în etapa de pionierat. În plus, pot fi parţial adevărate afirmaţiile numeroşilor analişti şi experţi în problematica securităţii statelor, potrivit cărora spaţiul cibernetic reprezintă doar elementul de diversitate modern al conflictelor armate contemporane, fiind practic o nouă oportunitate exploatată, ca rezultat a evoluţiei tehnologice din sfera socialului.

Referitor la cel de-al doilea aspect, privind dimensiunea cibernetică a conflictelor militare

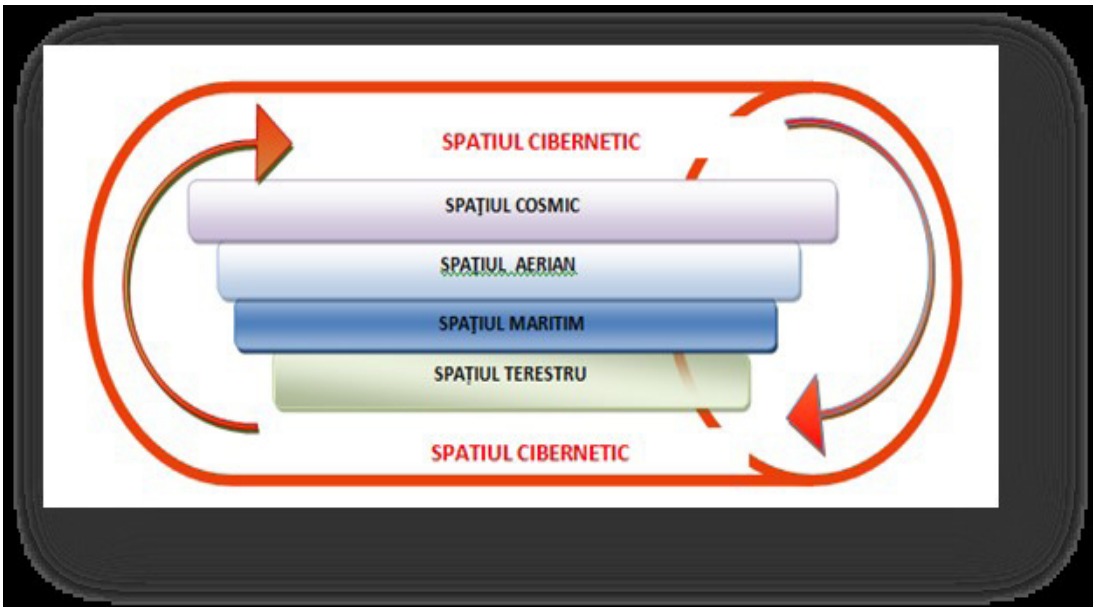

Fig. 1 *Reprezentarea mediilor de confruntare militară*[1]

În ceea ce priveşte primul aspect, am încercat, în una dintre preocupările ştiinţifice anterioare intitulată „Atacul cibernetic – o ameninţare hibridă într-un război hibrid” să argumentez, sintetic, faptul că „spaţiul cibernetic reprezintă un spaţiu integrator

contemporane, consider că o concluzie pertinentă poate fi exprimată în urma unei analize succinte a acţiunilor cibernetice din ultimii 10 ani desfăşurate la nivel mondial, fie pentru pregătirea sau în sprijinul unor acţiuni militare clasice, fie ca acţiuni

independente menită să elimine sau să creeze prejudicii infrastructurilor informatice naţionale, afectând astfel securitatea şi afacerile militare la nivel statal.

Primul exemplu, care a făcut obiectul unor intense dezbateri publice şi a constituit elementul o filozofie simplă (figura 2) şi puţin costisitoare. Pentru pregătirea unui atac de tip DDoS, un atacator acţionează în două faze, infectând, în prealabil, un număr mare de calculatoare răspândite pe o suprafaţă geografică extinsă, din întreaga lume, cu un cod sau produs software maliţios, în scopul

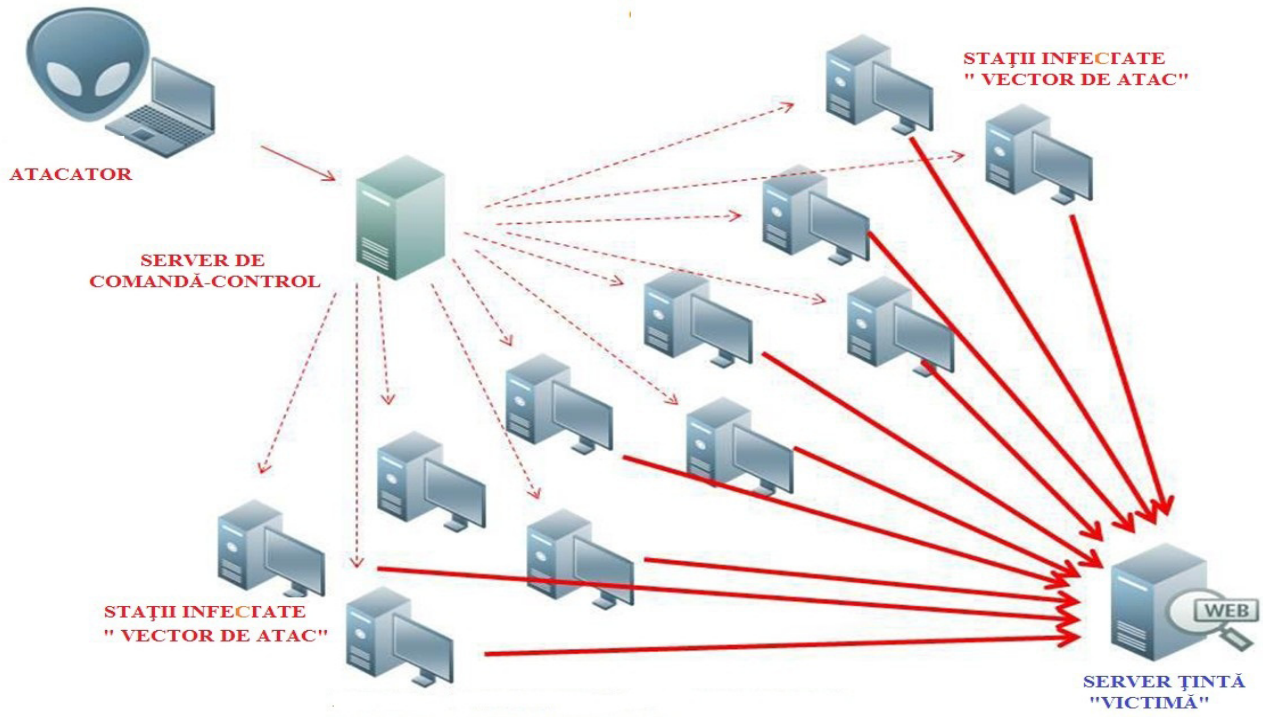

Fig. 2 *Reprezentarea atac de tip DDos*

de cotitură în ceea ce priveşte regândirea strategiilor militare şi a concepţiilor de evoluţie a luptei armate, a fost „cazul Estonia”. În acest sens, importanţa eforturilor de contracarare a ameninţării de tip cibernetic a atras atenţia opiniei publice a statelor atunci când Estonia s-a confruntat cu primele atacuri cibernetice de tip DoS „Denial-of-Service” şi DDoS „Distributed Denial-of-Service” în perioada aprilie-mai 2007. Atacul cibernetic, primul de acest gen îndreptat împotriva unei infrastructuri critice a unui stat, a fost declanşat de către entităţi şi structuri informatice de pe teritoriul a 178 de state, ca urmare a reprimării manifestaţiilor stradale proruse din capitala Tallin. Deşi nu a putut fi dovedit clar şi nici nu a putut fi determinat tehnic elementul declanşator al atacului ori factorul agresor, prim-ministrul estonian din acea perioadă, Andrus Ansip, a atribuit atacul Federaţiei RUSE şi organizaţiilor ruseşti care activau în regiune.

Cu toate acestea, tehnologia de realizare a unui asemenea atac este relativ simplă şi primitivă pentru perioada actuală, bazându-se în principal pe preluării ulterioare a controlului staţiilor spre a fi utilizate împotriva unei „ţinte” viitoare, prestabilite. În cea de-a doua fază a atacului, atacatorul, ca urmare a infectării unui număr suficient de mare de staţii de tip „vector”, va solicita la acestea transmiterea către computerele „victimă” a unor cereri de comunicaţii, comandându-le, astfel, să inunde „ţinta” cu zeci de mii de cereri de acces, blocând şi dezafectând serverele care gestionează serviciile de web şi traficul către acestea.

O soluţie dezvoltată a unui astfel de atac, presupune introducerea, la nivelul staţiilor de lucru de tip „vector” compromise, a unui cod maliţios de tip trigger cu ceas (timer) care poate declanşa automat un atac coordonat asupra ţintelor prestabilite.

Existenţa, la nivelul societăţii, a unei infrastructuri informatice dezvoltate, şi dependenţa întregului sistem bancar şi de comunicaţii al statului de mediul de reţea, a făcut ca Estonia să fie extrem de vulnerabilă la acest tip de atac, iar concretizarea vulnerabilităţii s-a tradus prin scoaterea din folosinţă

a site-urilor guvernamentale, a autorităţilor publice, a infrastructurii informatice bancare şi a sistemului public de urgenţă.

Atacurile cibernetice din Estonia au constituit primul pas de transformare a conceptului de apărare cibernetică la nivelul NATO, sintetizat prin declaraţia fostului Secretar General al Alianţei, Jaap de Hoop Scheffer, care a subliniat că *„cyber defence reprezintă o responsabilitate naţională, dar NATO poate oferi consultanţă şi poate sprijinii cu echipe mobile naţiunile, în caz de nevoie”*[2].

La un an după evenimentele din Estonia, cu ocazia Summitului NATO de la Bucureşti (aprilie 2008), prin declaraţia semnată de către şefii de state şi de guverne a fost adoptată o politică primară a alianţei care vizează, în premieră, domeniul cibernetic (Policy on Cyber Defence, paragraful 47)[3]. Prin acest fapt, NATO a devenit prima structură militară care a anunţat şi elaborat un pachet de politici în domeniul apărării cibernetice ca răspuns la atacurile cibernetice posibile, plecând de la exemplul estonian, şi care a subliniat necesitatea de întărire a sistemelor informatice ale Alianţei împotriva agresiunilor din mediul de reţea. Politica primară prezentată în cadrul paragrafului 47 al declaraţiei de la Bucureşti a subliniat necesitatea ca statele membre să-şi protejeze sistemele informatice cheie, să-şi împărtăşească cele mai bune practici în domeniu şi să asigure capabilităţi pentru a oferi asistenţă naţiunilor membre, la nevoie, pentru a contracara un atac cibernetic. Ulterior, în luna mai 2008, şapte state membre NATO şi Comandamentul Aliat pentru Transformare au semnat documentele care au stat la baza înfiinţării *Cooperative Cyber Defence (CCD)* Centre of Excellence (CoE) din Tallinn, Estonia.

Evoluţia ulterioară a acţiunilor militare din Europa a făcut posibilă apariţia unui nou caz similar cu atacurile cibernetice din Estonia, de această dată în Georgia, în luna august 2008, pe baza tensiunilor ruso-georgiene referitoare la regiunea Osetia de sud.

Pe fondul acestor tensiuni, a fost declanşată operaţiunea ofensivă de invadare a Georgiei începând cu data de 9 august 2008, prin pătrunderea trupelor în Defileul Kodori, în partea de nord-vestul a acesteia. Anterior acestei operaţii ofensive, au avut loc o serie de atacuri cibernetice concertate asupra mediului de reţea naţional georgian, care au avut rolul de a destabiliza spaţiul cibernetic şi a de a întrerupe sistemul naţional de comunicaţii, diminuând astfel capacitatea operaţională a forţelor georgiene şi resursele de administrare şi răspuns la criză ale statului. Din punct de vedere tehnic, infrastructura informatică naţională a Georgiei se baza, în proporţie de 40%, pe serviciile asigurate de reţeaua Internet, prin intermediul a cinci companii externe, dintre care trei ofereau conexiunii şi servicii de reţea din Rusia. Atacurile cibernetice au fost realizate pe modelul aplicat cu succes în Estonia, numai că, de această dată, au fost alese routerele de graniță şi serverele aparţinând sistemului bancar georgian, precum şi site-ul președinției, guvernului, Ministerului Afacerilor Externe şi Ministerului Apărării. Atacurile au culminat, în data de 9 august, cu blocarea portalului de ştiri „Georgia Online” (apsny.ge), şi a sistemului informatic a celei mai mari bănci georgiene –TBC Bank.

Scott Borg, director în cadrul U.S. Cyber Consequences Unit, preciza: „Consider că în spatele atacurilor cibernetice din Gerogia s-au aflat grupuri civile de hackeri ruși ajutați de organizații criminale, dar guvernul rus este cel care controlează serverele de pe care aceștia operează”[4]. De asemenea, el a subliniat faptul că atacurile au început în faza premergătoare invaziei ruse şi s-au încheiat odată cu finalizarea acesteia.

Atacurile cibernetice s-au bazat pe două tehnologii asemănătoare, respectiv pe utilizarea pe scară largă a atacurilor de tip DDoS concentrate asupra ţintelor cheie din sistemul informatic georgian şi pe utilizarea serverelor de „bootnet (figura 3)[5]”, precum şi a sistemelor de comandă-control folosite pentru controlul şi eficientizarea atacurilor.

Tehnic, atacul a fost executat în două faze, iniţial au fost atacate un număr limitat de site-uri web şi de servere prin tehnologii DDoS şi prin utilizarea unor aplicaţii software dedicate pentru atacuri la nivel HTTP. În faza a doua a atacului au fost puse la dispoziţia a mii de utilizatori din spaţiul virtual din regiune instrumente de atac cibernetic (comenzii de interogare site-uri web, instrumente de executare a atacurilor de tip boot-net), precum şi adresele site-urilor şi serverelor care se doreau a fi atacate, împreună cu instrucţiunile minime de executare a atacurilor. De asemenea, în scopul diminuării capacităţii de comunicaţii a reţelelor georgiene şi pentru testarea diferitelor tehnici de atac, au fost utilizate, la nivelul anumitor site-uri web, atacuri de tip „SQL injection”. Practic,

această metodă combinată şi susţinută reprezintă factorul declanşator a primei campanii de atacuri cibernetice împotriva infrastructurii cibernetice critice a unui stat executată, controlată şi comandată de la distanţă de către o entitate organizată.

La cinci ani distanţă de conflictul georgian şi de prima campanie de atacuri cibernetice susţinută şi comandată din mediul de reţea, în anul 2013 odată cu escaladarea divergenţelor şi tensiunilor politice concomitent cu atacarea site-urilor guvernamentale prin atacuri masive care au combinat tehnica DDoS cu soluţii de malware şi produse software de tip virus modificate.

Cea mai elocventă analiză publică destinată acestei campanii cibernetice concertate a fost realizată de către compania de securitate BAE Systems care a monitorizat din punct de vedere al securităţii IT, infrastructura de reţea din Ucraina. În

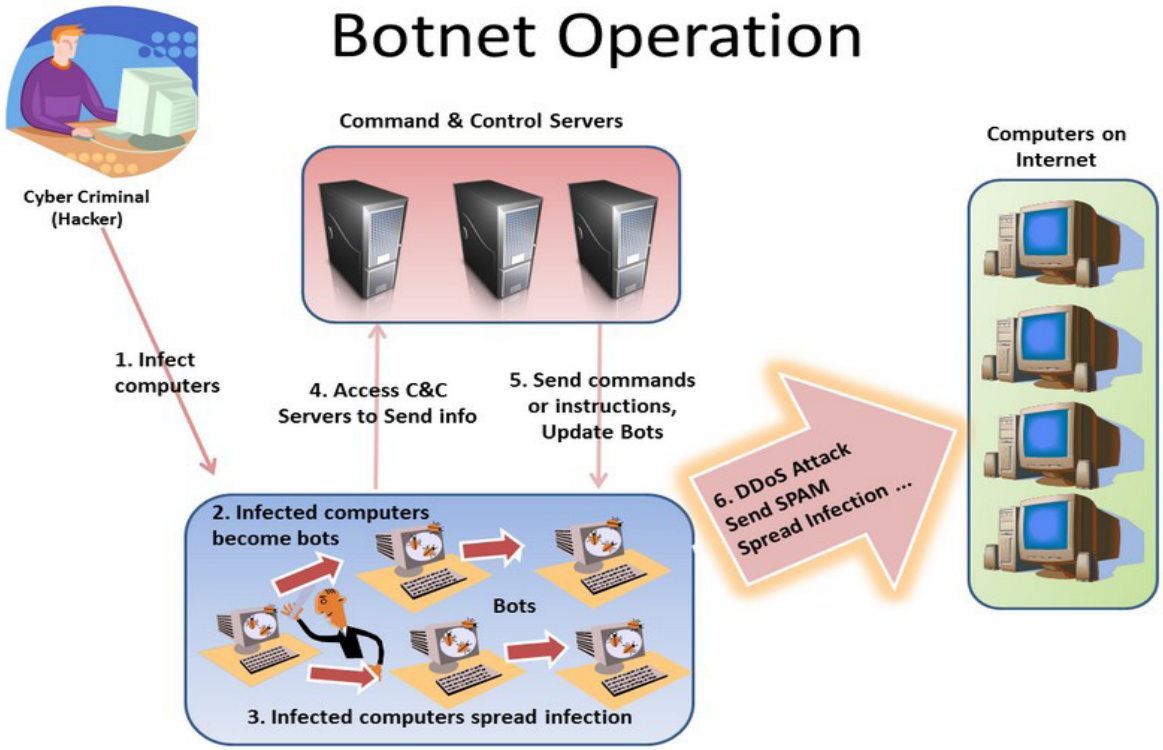

Fig. 3 *Atacul de tip Bootnet*

din Ucraina, acţiunile cibernetice şi-au făcut simţită prezenţa în mediul de reţea. În luna februarie 2014, odată cu plecarea de la putere a fostului preşedinte ucrainean Viktor Yanukovych, concomitent cu invazia aeroporturilor Sevastopol şi Simferopol din Peninsula CRIMEA de către grupurile paramilitare proruse, a fost declanşată o amplă operaţiune de atacuri cibernetice combinate asupra serverelor companiei de telefonie Telco Ukrtelecom care oferea servicii telefonice şi de date la nivel naţional cu o arie ridicată de acoperire şi care au avut drept rezultat blocarea activităţii acestei şi scoaterea din funcţiune.

În perioada imediat următoare, legăturile guvernamentale şi cele necesare de funcţionare a sistemului social, asigurate între Peninsula Crimea şi restul teritoriului Ucrainean au fost blocate analiza elaborată, experţii companiei nu au indicat, în mod direct, RUSIA ca fiind principalul agresor cibernetic, dar au documentat faptul că atacurile au fost produse din zona geografică GMT+4 şi că, în componenţa codurilor maliţioase au fost integrate caractere ruseşti. Unul dintre cele mai importante şi particulare aspecte ale acestor acţiuni cibernetice îndreptate împotriva Ucrainei, este reprezentat de utilizarea, pentru a doua oară, a unui produs de tip malware modificat – denumit generic SNAKE, asemenea unei reconstituiri după modelul virusului STUXNET[6], aplicat cu succes împotriva reţelelor informatice iraniene care au controlat facilităţile nucleare din Natanz şi Fordo, în anul 2008.

Produsul software Snake este un cod maliţios de tip malware care exploatează o breşă de securitate a sistemului de operare Windows 64-bit (în special)

şi care are capacitatea să rămână inactiv pe staţiile infectate pentru o bună perioadă de timp, până la o activare ulterioară executată prin comandă de la distanţă. Deşi malware-ul Snake a fost cunoscut de mai mult timp, modul în care a fost modificat şi exploatat pentru atacarea sistemelor informatice din spaţiul ucrainean, este esenţial. În conformitate cu analizele de securitate publice realizate de către experţii BAE Systems, varianta modificată a codului maliţios a permis lansarea masivă a peste 22 de atacuri şi a avut drept rezultat obţinerea accesului distant, sustragerea de date şi penetrarea infrastructurii cibernetice critice a statului ucrainean şi a organizaţiilor nonguvernamentale îndreptate împotriva operaţiunilor în Peninsula Crimeea.

Analizând din punct de vedere militar atacurile cibernetice exemplificate anterior, se poate susţine faptul că nu avem de-a face cu acţiuni militare clasice care au loc pe baza unor planuri militare liniare, ci sunt executate folosind tehnologia şi mijlocele hibride de ducere a luptei, precum şi forţe militare antrenate şi specializate în operaţii în mediul de reţea.

Asemenea oricăror tipuri de acţiuni militare, acţiunile cibernetice deţin, la momentul actual, toate atuurile şi mijlocele necesare individualizării acestora în sfera luptei armare, ca operaţii militare separate şi nu complementare unei acţiuni clasice. Deşi nu putem vorbi încă despre existenţa unui război cibernetic, din cauza constrângerilor din sfera juridică şi a limitărilor conceptuale militare, care nu pot fundamenta o strategie integratoare de luptă cibernetică, devine din ce în ce mai evident că majoritatea conflictelor contemporane se dezvoltă prin agresiuni masive în spaţiul de reţea şi prin acţiuni punctuale destabilizatoare pentru infrastructurile critice ale statelor.

Din punctul de vedere al modului de documentare al dimensiunii cibernetice a conflictelor curente şi de stabilire a factorilor agresori, modul de utilizare a tehnologiei face imposibilă determinarea, cu certitudine, a generatorilor de ameninţări, dar şi încadrarea agresiunilor cibernetice în tipare clasice.

Plecând de la aceste aspecte, viitorul conflictelor militare va deveni imprevizibil, în principal din cauza apariţiei unei noi dimensiuni incontrolabile la momentul actual şi a lipsei legilor de angajare a operaţiunilor cibernetice. Cu atât mai mult, efectele unor astfel de acţiuni în mediul de reţea nu pot fi evaluate, iar posibilitatea de a contracara aceste efecte sau de a elimina acţiunile factorilor agresori este aproape imposibilă, având în vedere că în spatele unui atacator se află o maşină de calcul, care poate fi virtuală.

Infrastructurile digitale au devenit, astfel, bunuri naţionale strategice, fiind locul de desfăşurare a unor noi tipuri de acţiuni militare, iar concluzia generală exprimă faptul că dezvoltarea tehnologică, deşi aduce beneficii incontestabile la nivel militar, poate fi exploatată asemenea unei vulnerabilităţi, cu efect de bumerang la nivelul securităţii statelor. Nu putem afirma cu certitudine dacă vom avea un război cibernetic, în adevăratul sens al cuvântului, pe baza legilor luptei armate şi modelelor militare actuale, deşi, ţinând cont de evoluţia rapidă a tehnologiei şi de dependenţa societăţii de informaţie, acest lucru poate fi posibil, dar, cu siguranţă, conflictele contemporane au o dimensiune cibernetică importantă, care tinde a se manifesta pregnant în ceea ce priveşte câştigarea supremaţiei militare, indiferent de tipul sau zona de conflict.

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului **POSDRU/159/1.5/S/138822**, cu titlul **„Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile „Ştiinţe Militare”, „Securitate şi Informaţii” şi „Ordine Publică şi Siguranţă Naţională” – Program de Formare Continuă a Cercetătorilor de Elită – „SmartSPODAS”.”**

NOTE:

1 Gheorghe Boaru, Benedictos Iorga, *Atacul cibernetic – o ameninţare hibridă într-un război hibrid*, Bucureşti, 2015, The 11th International Scientific Conference „Strategii XXI”, Volumul 3, Universitatea Naţională de Apărare „Carol I”, Bucureşti, 2015, p. 232.

2http://www.nato.int/docu/speech/2008/s080208c.html, Press Conference, VILNIUS Estonia, 2008, accesat la 11 iunie 2015.

3http://www.ingepo.ro/download-materiale/110/SuplimentBuletin27Ro.pdf, accesat la 08 iunie 2015.

4http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf, accesat la 14 mai 2015.

5http://www.vice.com/en_au/read/internet-terrorism-is-really-confusing, accesat la 16 iunie, 2015.

6 În octombrie 2012, virusul Stuxnet a atacat facilităţile nucleare iraniene de la Natanz şi Fordo, reuşind să „paralizeze” echipamentele de comandă şi control bazate pe sistemul Scada realizat de Siemens.

BIBLIOGRAFIE

The next wave, Building a national program for cyber security science, Central security agency, vol.19, nr. 4, 2012.

Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines, 2009.

Dreo Rodosek Gabi, *Challenges of cyber defence în future internet*, Universitatea din Munchen, 2011.

Boaru Gheorghe, Iorga Benedictos, *Atacul cibernetic – o ameninţare hibridă într-un război hibrid*, The 11th International Scientific Conference „Strategii XXI”, Volumul 3, Universitatea Naţională de Apărare „Carol I”, Bucureşti, 2015.

http://rt.com/news/iran-us-israel-cyberwar-virus-weapon-770/

http://news.yahoo.com/report-secret-u-cyberwar-against-iranian-nukes-began-65204641.html

http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

http://www.vice.com/en_au/read/internet-terrorism-is-really-confusing.

http://www.nato.int/docu/speech/2008/s080208c.html, Press Conference, VILNIUS Estonia, 2008.

http://www.ingepo.ro/download-materiale/110/SuplimentBuletin27Ro.pdf