RĂZBOIUL CIBERNETIC – O REALITATE GREU DE CONTESTAT ÎN LUMEA DE ASTĂZI

CYBER WAR – A HARDLY CONTESTABLE REALITY OF OUR DAYS

Gl. mr. (r) prof. asoc. dr. Constantin MINCU*

Rezumat: *Articolul este o continuare a materialului publicat în revista noastră nr. 2 (43)/2016, cu titlul „**ATACURILE CIBERNETICE ÎN TOPUL AMENINŢĂRILOR ŞI VULNERABILITĂŢILOR LA ADRESA STATELOR, ORGANIZAŢIILOR ŞI CETĂŢENILOR, ÎN PREZENT ŞI ÎN VIITOR**”.*

Am considerat necesară această continuare datorită evenimentelor din ultimul timp şi, în primul rând, a situaţiilor create în Marea Britanie şi Statele Unite ale Americii prin atacurile cibernetice masive şi diversificate, cu intenţia de a influenţa procesele politice din aceste ţări. Consider că nu sunt lipsite de interes nici atacurile produse asupra unor instituţii şi companii din unele ţări ale Uniunii Europene şi/sau NATO şi necesitatea luării unor măsuri ferme şi diversificate de apărare.

Cuvinte-cheie*: război cibernetic; atacuri cibernetice; Marea Britanie; Statele Unite ale Americii; Federaţia Rusă; România.*

Abstract: *This article is a prolongation of the material published in our journal no. 2 (42)/2016, entitled „**CYBER ATTACKS, MAJOR THREATS AND VULNERABILITIES AGAINST STATES, ORGANIZATIONS AND CITIZENS AT PRESENT AND IN THE FUTURE**”.*

We considered necessary this prolongation owed to the lately events and, mainly, because of the situations created in the United Kingdom of Great Britain and United States of America by massive and diversified cyber attacks intending to influence the political process in these countries.

I also consider there are also interesting the attacks produced on some institutions and companies in some EU and/or NATO countries and the need to take some firm and diversified measures of defence.

Keywords: *cyber war; cyber attacks; UK; US; Russian Federation; Romania.*

* Membru titular al Academiei Oamenilor de Ştiinţă din România, membru al Consiliului Onorific al Academiei Oamenilor de Ştiinţă din România, secretar ştiinţific al Secţiei de Ştiinţe Militare, Telefon: 0722.303.015, email: mincu_constantin@yahoo.com.

Problematica atacurilor cibernetice tot mai agresive, precum şi conturarea tot mai clară a transformării acestora în adevărate *războaie cibernetice* a devenit un subiect public de maximă importanţă şi a determinat o abordare mai activă şi responsabilă din partea statelor, organizaţiilor, utilizatorilor individuali şi, desigur, a specialiştilor din domeniul IT.

Un scurt istoric al acestor atacuri arată că acestea s-au intensificat după anul 2007 (lansarea de către un actor statal a virusului *Octombrie Roşu*) urmate apoi de alte acţiuni ostile de amploare care au produs pagube politice, economice, financiare şi de imagine ţintelor (state şi organizaţii).

Episoadele recente, cu implicarea unor actori statali şi a unor grupuri organizate şi susţinute financiar şi logistic de actori statali, cum a fost cazul în procesul politic al ieşirii Marii Britanii din Uniunea Europeană – BREXIT şi mai nou, cu efecte politice, potenţial grave, implicarea prin atacuri directe, furt de informaţii şi diseminarea de informaţii false în rândul publicului ţintă (celebrii deja troli) în încercarea disperată de a influenţa alegerile prezidenţiale din statele Unite – ridică la un alt nivel confruntarea, putându-se vorbi clar, cu argumente, de *război cibernetic*.

Evoluţii ale atacurilor cibernetice în anii 2014-2016

Conflictul ruso-ucrainean din 2014, urmat de reacţii mai mult sau mai puţin ferme din partea statelor membre UE şi/sau NATO, a condus la înrăutăţirea relaţiilor politice, diplomatice, economice şi culturale între Federaţia Rusă şi statele democratice menţionate. Anexarea Crimeei şi implicarea în conflictul din estul Ucrainei a arătat, fără echivoc, faţa agresivă a Rusiei, îngrijorând, în primul rând, statele din vecinătatea sa.

Această nouă situaţie cu implicaţii geopolitice importante în viitorul apropiat nu putea să rămână fără efect şi în domeniul confruntării cibernetice.

Aşa se face că aproape toate ţările europene membre ale UE, precum şi statele membre NATO s-au trezit cu atacuri puternice şi zilnice asupra instituţiilor politice, guvernamentale, financiare, industriale şi media, având ca efecte grave prejudicii de securitate, economice, financiare, urmate inclusiv de afectarea moralului cetăţenilor prin introducerea ştirilor false şi prin montarea unor diversiuni fabricate de profesioniştii cu state vechi în materie.

Să încercăm un scurt inventar:

a) Cazul conflictului ruso-ucrainean devoalează modul agresiv şi fără scrupule morale al demonizării de către partea rusă a ţării vecine, şi până nu demult, parte a Imperiului Sovietic. Prin vectori media controlaţi de Kremlin (din Rusia şi din străinătate) s-au răspândit ştiri false, cu scopul de a nega implicarea forţelor militare ruse în Crimeea şi în estul Ucrainei.

Au fost declanşate atacuri cibernetice asupra tuturor instituţiilor importante ale statului ucrainean (Parlament, Guvern, armată, serviciile de securitate şi infrastructura economică) concomitent cu dezvoltarea unor acţiuni complexe şi sofisticate pentru influenţarea opiniei publice din ţările occidentale, utilizând, în primul rând, reţelele de socializare şi publicaţiile media online. În multe cazuri aceste acţiuni au dat rezultatele scontate.

b) Cazul BREXIT

Este deja notoriu faptul că Moscova urmăreşte slăbirea coeziunii europene, acţionează pentru ruperea unor state membre din UE şi doreşte o slăbire a relaţiilor UE-SUA şi subminarea, pe această bază, a NATO.

Declanşarea referendumului în Marea Britanie pentru ieşirea sau rămânerea în Uniunea Europeană a reprezentat pentru forţele, controlate de Kremlin, din toată lumea şi din ţara ţintă în acest scenariu, un adevărat caz şcoală, prin utilizarea, fără economie de forţe şi mijloace a influenţării cetăţenilor britanici prin vectori media şi prin atacuri cibernetice asupra instituţiilor principale ale statului.

Teme de atac:

- UE este o instituţie profund birocratică, asemănătoare fostei Uniuni Sovietice;
- Marea Britanie a pierdut din suveranitatea sa politică şi economică;
- Marea Britanie contribuie cu sume prea mari la bugetul comunitar, în favoarea ţărilor membre mai sărace din centrul şi estul Europei;
- cetăţenii unor ţări membre UE sosesc în număr mare în Regatul Unit, sufocând serviciile sociale şi „furând" locurile de muncă ale băştinaşilor;
- denunţarea politicii „dezastruoase" ale unor lideri europeni în problema admiterii imigranţilor din zonele de conflict (Siria, Iraq, nordul Africii etc.).

Aşa cum se ştie deja referendumul a fost pe muchie de cuţit, iar aportul acţiunilor prezentate mai sus nu a fost unul neglijabil.

c) Cazul alegerilor prezidenţiale din Statele Unite ale Americii

O fostă superputere numită Uniunea Sovietică şi moştenitoarea sa principală numită Federaţia Rusă (care aspiră la locul deţinut pe timpul Războiului Rece) nu putea rata implicarea în cel mai important eveniment politic al anului 2016 – alegerea unui nou preşedinte american. După o analiză îndelungată şi amănunţită, utilizând diverse surse de informaţii, inclusiv furtul masiv din sistemele electronice ale competitorilor şi apropiaţilor acestora, Moscova a decis să meargă pe mâna candidatului Donald Trump, considerat de ruşi mai pragmatic şi mai realist şi, potrivit declaraţiilor acestuia, dispus să lase baltă NATO, cu tot cu articolul 5.

Teme de atac asupra candidatei democrate Hillary Clinton:

- candidata democrată este imprevizibilă şi coruptă, primind prin fundaţia Clinton bani din unele ţări arabe;
- furtul şi publicarea a mii de e-mailuri ale acesteia şi ale unor membri ai Staffului de campanie, cu scopul clar al denigrării şi al incitării organelor de anchetă americane;
- dacă va fi aleasă confruntarea între Rusia şi Statele Unite se va apropia de nivelul de pericol (teză susţinută şi de contracandidatul Donald Trump)[1];
- Hillary Clinton s-ar afla sub influenţa unor cercuri de putere oculte care ar urmări dominaţia mondială şi dezmembrarea federaţiei Ruse;
- alianţa politico-militară NATO ar fi inutilă în condiţiile actuale (coincide cu atacuri asupra NATO ale candidatului republican Donald Trump);
- Rusia trebuie să-şi „lipească" la loc bucăţile desprinde din Uniunea Sovietică, iar SUA nu au nici un drept să intervină;
- Rusia trebuie să-şi apere, fără nici o ezitare, pe ruşii aflaţi în statele desprinse din URSS (aproximativ 25 de milioane) fără a se sinchisi de criticile venite din partea SUA şi a aliaţilor europeni;
- Rusia şi-a revenit din punct de vedere politic, economic şi militar şi poate fi oricând o ameninţare mortală pentru SUA şi NATO (agită tot mai des ameninţarea nucleară);

În acest context tensionat al relaţiilor Rusia - SUA şi Rusia - UE este necesar să prezentăm reacţiile occidentale la ultimele atacuri şi intruziuni cibernetice în timpul procesului electorat din Statele Unite[2]:

- Guvernul Statelor Unite a acuzat oficial Rusia, vineri 11.10.2016, de o campanie recentă de atacuri cibernetice împotriva unor organizaţii ale Partidului Democrat din SUA, transmite Reuters;
- În ultimele luni, mai multe oficialităţi americane afirmaseră că atacurile cibernetice respective au aparţinut unor hackeri sprijiniţi de Moscova, posibil pentru a perturba alegerile prezidenţiale, în care se confruntă democrata Hillary Clinton cu republicanul Donald Trump. Rusia a respins aceste acuzaţii (n.a. – în nota obişnuită faţă de acţiunile sale agresive);
- **Departamentul pentru Securitate Internă (DHS) şi Biroul Directorului pentru Informaţii Naţionale** au transmis în octombrie (11.10.2016) presei o declaraţie comună, citată integral de Reuters:
- „Comunitatea de informaţii a SUA (USIC) este convinsă că Guvernul Rusiei a dirijat recentele compromiteri ale e-mailurilor unor persoane şi instituţii

[1] Articolul a fost scris înainte de alegerile prezidenţiale din SUA (06.11.2016)
[2] Site-ul: antena3.ro/externe/sua-acuză-rusia-de-atacuri-cibernetice-380293.html

din SUA, inclusiv a unor organizaţii politice americane. Recentele dezvăluiri ale unor presupuse e-mailuri piratate pe site-uri cum ar fi DCLeacs.com şi WikiLeacs şi de către personajul online Guccifer 2.0 sunt în concordanţă cu metodele şi motivaţiile dirijate de Rusia. Aceste furtuni şi dezvăluiri sunt făcute cu intenţia de imixtiune în procesul electoral din SUA. Astfel de activităţi nu sunt noi pentru Moscova – ruşii au folosit astfel de tactici şi tehnici peste tot în Europa şi Eurasia, de exemplu, pentru influenţarea opiniei publice. Credem, ţinând cont de amploarea şi sensibilitatea acestor eforturi, că numai cei mai înalţi responsabili din Rusia ar fi putut autoriza aceste activităţi";

- „Unele state au observat recent, de asemenea, scanarea şi testarea sistemelor lor legate de alegeri care în cele mai multe cazuri şi-au avut originea în servere administrate de o firmă rusească. Cu toate acestea, nu suntem acum în situaţia de a atribui aceste activităţi Guvernului Rusiei. USIC şi Departamentul pentru Securitate Internă (DHS) apreciază că ar fi extrem de dificil pentru cineva, inclusiv pentru un actor nestatal, să modifice numărătoarea reală a voturilor sau rezultatele alegerilor prin atacuri sau intruziuni cibernetice. Această evaluarea se bazează pe natura descentralizată a sistemului nostru electoral în această ţară şi pe numărul de protecţii implementate de autorităţile electorale de stat şi locale. Statele asigură că echipamentele de vot nu sunt conectate la internet şi există multiple mecanisme de reglare, precum şi o supraveghere extensivă pe multiple niveluri inerente procesului nostru electoral";
- După ultimele atacuri din 11 noiembrie a venit şi o reacţie din partea casei Albe[3]:
- Răspunsul va fi „proporţional", a declarat secretarul de presă de la Casa Albă Josh Eamest, fără să detalieze. A mai declarat că un „registru" de posibile răspunsuri este pe masă. Prin anunţul de vineri, a fost prima dată când guvernul american a dat vina în mod public pe o altă ţară pentru atacuri cibernetice cu scopul de a influenţa alegerile din SUA. Declaraţia comună a Departamentului de Securitate Internă şi Biroului Directorului Agenţiei Naţionale de Informaţii a menţionat nu numai că oficialii sunt siguri că atacurile asupra grupurilor politice democrate şi oficialilor campaniei proveneau de la niveluri înalte din guvernul rus, dar şi că publicarea online a acestor e-mailuri a fost parte a efortului;
- Consilierul naţional de securitate Lisa Monaco a menţionat pentru Washington post, luna trecută (12.10.2016) ce ar putea face guvernul în general ca răspuns la aceste atacuri. *„Vom răspunde într-un timp, loc şi mod ales de noi, iar când vom face acest lucru vom lua în considerare o gamă completă de*

[3] http://adevărul.ro/continut/ştiri/casa-albă.

instrumente: economice, diplomatice, de drept penal, militare, iar unele dintre aceste reacţii pot fi publice, însă unele dintre ele nu pot fi."

d) Cazul atacurilor cibernetice masive asupra unor servicii IT:

- La 21.10.2016 s-au produs unele atacuri împotriva reţelelor Twitter, Spotify şi eBay;
- Scopul acestora a fost descurajarea şi bulversarea utilizatorilor americani şi nu numai în preajma alegerilor prezidenţiale din 08 noiembrie;
- În acelaşi timp, autorii atacurilor au vrut să demonstreze că nu prea le pasă de poziţiile exprimate de unii oficiali americani în 11 şi 12 octombrie a.c.

Atacurile cibernetice asupra ţărilor Uniunii Europene

Nicio ţară membră UE nu a scăpat în ultimii ani de atacurile cibernetice orchestrate de actori statali sau grupuri organizate sprijinite de aceştia.

Dintre ţările europene se detaşează ca ţintă Germania, asupra căreia s-au declanşat atacuri vizând organizaţiile politice, ministerele, infrastructura industrială, organizaţiile financiare şi media. Unii oficiali germani au acuzat Rusia de aceste atacuri. Sunt însă indicii că au fost orchestrate atacuri şi din alte centre de putere.

În mod surprinzător unele state europene sunt menajate şi nu suferă decât atacuri marginale. Din motive lesne de înţeles nu cred că este bine să le nominalizez, mai ales că în unele sunt în plină desfăşurare procese electorale.

Atacurile cibernetice asupra organizaţiilor din România

Oficiali ai SRI, dar şi din alte instituţii recunosc recrudescenţa atacurilor cibernetice venite din diferite surse, având ca obiectiv instituţiile politice, apărarea şi securitatea naţională, organizaţiile financiare, companiile multinaţionale care operează în România, dar şi micile firme autohtone.

Totodată, s-au intensificat atacurile venite din partea unor grupări teroriste asupra unor instituţii de învăţământ superior şi de administraţie publică, precum şi asupra unui site web al Patriarhiei Române.

Oficialii români apreciază, pe bună dreptate, că *„acest context complex evidenţiază necesitatea implementării unor standarde minime de securitate cibernetică la nivelul sistemelor informatice deţinute de entităţi publice şi private, precum şi a verificării regulate a respectării normelor şi politicilor din acest domeniu."*[4]

În cazul României, un subiect de analiză ar putea fi şi activismul neobişnuit de intens, în ultimul timp, a aşa numitelor **troli**, care postează la subiectele lansate pe site-urile de ştiri şi pe reţelele de socializare.

[4] www.sri.ro/romania-a-fost-ţinta-unor-atacuri-cibernetice.html

Am urmărit în mod deosebit postările la subiectele privind armata şi apărarea şi am putut constata că la subiecte banale, obişnuite se lansează atacuri incorecte şi nemeritate la adresa instituţiei şi a militarilor activi, în rezervă şi în retragere. Promit că voi încerca să revin cu o analiză mai cuprinzătoare asupra acestui subiect.

În ceea ce priveşte România consider că o întărire a cadrului legislativ şi normativ urmată de acţiuni practice de implementare este deopotrivă presantă şi necesară.

Notă (09.11.2016).

Din păcate atacurile cibernetice şi de altă natură asupra procesului politic al alegerilor din Statele Unite au avut efectul scontat de către iniţiatori.

BIBLIOGRAFIE

*** Strategia Naţională de Apărare, Bucureşti, 2010;

*** Strategia de Securitate Cibernetică a României, aprobată de CSAT, în luna februarie 2013;

*** Proiect de Lege privind Securitatea Cibernetică a României, lansat în dezbatere publică de către MCTI, în luna Ianuarie 2016;

*** Ghidul Strategiei Naţionale de Apărare a ţării pentru perioada 2015-2019, aprobat prin Hotărârea CSAT nr. 128, din 10 decembrie 2015;

Durmigan F. James, *Noua ameninţare mondială - Cyber-Terorismul,* Editura Curtea Veche, Bucureşti, 2010;

Raiu Costin, *Laboratoarele Kaspersky*, Interviu acordat Ziarului Adevărul, 19 februarie 2013;

www.internetworldstats.com/stats.html

http://www.nato.int/dom/review/2011111-september/Cyber-ThreadsIRO/index.htm

http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/

Alte site-uri de profil utilizând căutarea cu „atacuri cibernetice”.