SECURITATEA EUROPEANĂ ŞI RĂZBOIUL CIBERNETIC

EUROPEAN SECURITY AND CYBER WAR

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

Rezumat: *Autorul încearcă, în limita spaţiului acordat, să readucă în atenţia celor interesaţi problema complexă, cu dezvoltare rapidă la nivel global, privind riscurile, ameninţările şi vulnerabilităţile cibernetice, mergând până la nivelul de „război cibernetic" cu implicarea directă a unor actori statali şi a unor grupuri sponsorizate şi protejate de actori statali. Informaţii de ultimă oră demonstrează că pericolele sunt mult mai grave decât se considera în urmă cu şase luni.*

Sunt prezentate unele mijloace şi vectori de atac, precum şi unele măsuri legislative, administrative, tehnice şi în domeniul resursei umane pentru a spori capabilităţile pentru protecţia utilizatorilor individuali, companiilor, structurilor guvernamentale şi a celor militare.

Cuvinte-cheie *atacuri cibernetice, război cibernetic, vulnerabilităţi, ameninţări cibernetice, John McAfec.*

Abstract: *In the limits granted for the material, the author tries to bring to the attention of those interested in the complex problem, fast growing globally, of cyber risks, threats and vulnerabilities, up to the level of "cyber war" with direct involvement of the state actors and some groups sponsored and protected by state actors. Up to date information shows that the dangers are much more serious than is often believed six months ago.*

Here are also presented some tools and attack vectors, and measures in the legislative, administrative, and technical and human resources fields created to increase capabilities to protect individual users, companies, government agencies and the military structures.

Keywords: *cyber attacks, cyber war, vulnerabilities, cyber threats, John McAfee.*

Introducere

Numeroşi autori români şi străini au abordat şi abordează, îndeosebi după anul 2005, problematica complexă a atacurilor cibernetice efectuate de actori individuali şi, în ultimii ani, de actori statali interesaţi, din raţiuni diferite, să dezorganizeze sistemele informaţionale ale adversarilor, să fure informaţii

* 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.

sensibile, să obţină beneficii materiale importante, să afecteze grav funcţionarea unor sisteme publice vitale cum sunt: sistemele medicale, sistemele financiar-bancare, comunicaţiile civile şi militare, sistemele militare de comandă şi control, precum şi cele de arme complexe, utilităţile (energie electrică, gazele naturale, reţelele de apă, reţelele de transport) precum şi vectorii mass-media şi instituţiile culturale.

Mai nou, un nou tip de război îşi face simţită prezenţa, din ce în ce mai mult în ultimul timp, unul purtat în faţa calculatorului, iar câmpul de luptă este internetul. Studierea, cu atenţie sporită, a tuturor aspectelor războiului informaţional şi cibernetic, precum şi a efectelor sale asupra civilizaţiei umane cade în sarcina tuturor serviciilor şi instituţiilor specializate, dar şi în sarcina fiecărui utilizator de bună credinţă, conectat la internet.

În acest articol nu putem epuiza această temă complexă, dar vom încerca să punctăm câteva aspecte, care, să arate importanţa dezvoltării unor sisteme solide de protecţie prin acţiuni ale factorului politic (legislaţie adecvată), instituţiilor statului cu atribuţii în domeniu, corporaţiilor şi societăţilor comerciale şi nu în ultimul rând a fiecărui cetăţean conectat la internet şi reţelele sociale.

Vulnerabilităţi şi ameninţări cibernetice

Între autorii care au analizat, utilizând un limbaj accesibil marelui public, problematica complexă a sistemelor informaţionale actuale şi ale atacurilor cibernetice venite din surse diferite, se află şi specialistul american James F. Dunnigan[1], care pe lângă descrierea evoluţiei sistemelor de comunicaţii şi informatice, prezintă, în oglindă, partea neplăcută a proceselor, prin dezvoltarea atacurilor şi înmulţirea atacatorilor fie ei indivizi, grupuri sau unele state.

Specialistul afirmă că cyber-războiului este lupta pentru supremaţia asupra internetului şi a marelui segment din economie care acum depinde de această reţea de computere. Vulnerabile sunt şi structurile guvernamentale şi cele militare, atât în faţa atacatorilor individuali cât şi a atacatorilor state.

Hackerii civili, fie ei individuali sau grupuri, atacă pentru a da lovituri financiare şi de imagine, pe când războinicii militari o fac pentru a ajuta la câştigarea războiului, pentru a produce pagube maxime economiei şi forţelor armate ale adversarului.

Pentru a înţelege mai bine ce distrugeri pot face atacatorii cibernetici este necesar să reamintim câteva elemente ale vocabularului specific acestui gen de acţiuni:

[1] James F. Dunnigan, *Noua ameninţare mondială – Cyber-Terorismul*, Editura Curtea Veche, Bucureşti, 2010.

• Caii troieni sunt programe deghizate în programe legale. La început, caii troieni au fost folosiţi în scop de farse şi realizau doar nişte glume inofensive. Dar pe parcursul anilor ’80 aceştia au devenit periculoşi, unii dintre ei fiind capabili să distrugă date şi programe. Alţii, odată rulaţi, se răspândeau prin modificarea altui software cu ajutorul propriilor rutine.

• Viruşii sunt ceea ce au devenit caii troieni. Virusul se ataşează de un program sau document autentic. În anii ’90 când caii troieni au început să se răspândească rapid pe internet, au fost numiţi viruşi informatici.

• Viermii sunt viruşi care se ataşează de alte programe. De exemplu *„Logic Bomb”*. Acesta este un program ascuns din sistemul Computerului care devine activ numai când sunt îndeplinite anumite condiţii.

• Zombie (uneori numiţi boţi, de la roboţi) sunt o variantă a calului troian. Spre deosebire de adevăratele programe cal troian, zombie sunt mai degrabă controlaţi (pe internet) de către persoana care i-a inserat, decât să fie lăsaţi să acţioneze automat.

• Vampirii sunt viermi sau viruşi al căror unic scop este să pătrundă atât de adânc în sistem, încât calculatorul infestat să nu mai poată face nimic altceva.

• Adulmecătorii sunt instrumente de hacking care colectează informaţiile ce intră sau ies dintr-un computer (de obicei în server). Informaţia este apoi trimisă către cel care a implantat adulmecătorul. Adulmecătorii sunt utili pentru colectarea parolelor sau ID-urilor utilizatorilor.

• Buffer Overflow Exploitation este o tehnică prin care se trimite un anumit tip de date către un server web şi se declanşează manifestarea unei deficienţe a software-lui (comună multor produse Microsoft), lucru care permite strecurarea un virus sau un program zombie şi astfel se pătrunde în server, în ciuda apărării.

• Există şi alte instrumente de hacking şi arme sofisticate, în permanentă dezvoltare cantitativă şi perfecţionare calitativă care pot aduce multe necazuri utilizatorilor individuali şi celor din corporaţii şi structuri guvernamentale.

Să rememorăm câteva elemente ale evoluţiei ameninţărilor cibernetice resimţite de NATO, Uniunea Europeană şi majoritatea ţărilor membre ale acestor organizaţii, precum şi de către alte state aflate în vizorul unor atacatori[2]:

• Atacurile executate cu implicarea unui grup numeros de calculatoare care generează refuzul de a presta serviciile solicitate (distributed denial of service - DDOS), privite până acum ca, de fapt nimic mai mult decât nişte *„blocaje de protest”*, au devenit un instrument în războiul informaţional.

• În anul 2007 a fost lansat de către un actor statal virusul *„Octombrie Roşu.”* Cele mai multe victime au fost instituţii diplomatice, guvernamentale,

[2] http://www.nato.int/dom/review/2011/11-september/Cyber-Threads

companii de energie, inclusiv energie nucleară, instituţii de cercetare ştiinţifică, contractori militari şi firme care se ocupă de industria petrolieră şi de gaze. Atacurile au fost axate pe extragerea de informaţii de la victime, informaţii care puteau oferi avantaje geostrategice. Instituţii importante din România au fost, la rândul lor, afectate de acest virus.

- În anul 2008, unul din cele mai serioase atacuri de până în prezent a fost lansat împotriva sistemelor americane de computere. Prin intermediul unui singur memory-stick conectat la un laptop al armatei, la o bază militară din Orientul Mijlociu, un program spion s-a răspândit nedetectat, atât în sisteme clasificate, cât şi în cele neclasificate. Acest eveniment a realizat ceea ce a echivalat cu un *„cap de pod digital”*, prin care mii de dosare cu date au fost transferate în servere aflate sub control străin. Începând de atunci, spionajul cibernetic a devenit o ameninţare constantă. Incidente similare s-au produs în toate ţările membre NATO.
- În iunie 2010, softul maliţios *„Stuxnet”* a devenit public, ceva ca o *„bombă de penetrare a ţintelor blindate digitale”* care a atacat programul nuclear iranian. Prin aceasta, avertizările timpurii transmise de experţi începând din 2001, au devenit realitate, sugerând că dimensiunea cibernetică ar putea fi folosită mai devreme sau mai târziu pentru executarea unor atacuri serioase care vor avea consecinţe letale în lumea reală.
- În timpul conflictului Georgia - Rusia s-au produs atacuri masive împotriva website-urilor şi serverelor guvernamentale din Georgia, oferind termenului de război cibernetic o formă mai concretă.
- În vara lui 2010 s-a răspândit vestea că aproximativ 45 000 de sisteme de control industrial Siemens din întreaga lume au fost infectate cu un virus troian special conceput, care putea manipula procesele tehnice de o importanţă crucială pentru controalele nucleare din Iran. Deşi evaluarea avariilor este în continuare neclară, acest lucru a evidenţiat riscul softului maliţios care afectează sisteme de computere de o importanţă crucială în managementul aprovizionării cu energie sau al reţelelor de trafic. Pentru prima dată, aici a existat dovada existenţei atacurilor cibernetice care pot cauza avarii fizice reale şi generează riscul pierderii de vieţi umane.
- În februarie 2013[3] se înregistrează un atac puternic prin programul *„Adobe Reader”*. Acesta nu este un atac obişnuit, e un atac extraordinar de sofisticat care apare cam o dată pe an. O vulnerabilitate le permite hackerilor să copieze nişte fişiere pe sistem şi o a doua le permite să scape din sandbox. Cine a făcut atacul este extraordinar (funcţionează pe sisteme Adobe Reader în limba arabă, ebraică, engleză şi greacă).

[3] Costin Raiu, *Laboratoarele Kaspersky*, Interviu acordat Ziarului Adevărul, 19 februarie 2013.

Concluzia specialiştilor este că avem de a face cu un atac sponsorizat de un stat, de cel mai înalt nivel, atac care a necesitat resurse enorme.

- După debutul crizei, dintre Ucraina şi Rusia (2014), s-au amplificat atacurile cibernetice împotriva Ucrainei, dar şi împotriva statelor membre NATO şi UE.
- Este de remarcat că în 1996 apărea câte un virus nou pe săptămână sau pe lună, acum apar peste 250 000 de viruşi noi pe zi.
- România, fiind la ora actuală, puternic conectată la Internet este afectată, mai ales după 2010 de atacurile cibernetice asupra utilizatorilor individuali şi mai nou, ţinte au devenit instituţiile guvernamentale, cele militare şi companiile.

O evaluare echilibrată a ameninţărilor demonstrează clar două lucruri:

- Până în prezent, cei mai periculoşi actori în domeniul cibernetic sunt tot statele-naţiuni. În pofida unor capabilităţi ofensive aflate din ce în ce mai mult la dispoziţia reţelelor de criminalitate, care ar putea fi folosite de actori non-statali precum teroriştii, spionajul şi sabotajul de înaltă sofisticare în domeniul cibernetic, aceste grupări au nevoie, în continuare, de capabilităţile, hotărârea şi raţiunea cost-beneficii ale unui stat-naţiune.
- Pagubele fizice şi terorismul cibernetic în lumea reală nu s-au produs încă, dar este foarte aproape acest moment. Este clar că tehnologia atacurilor evoluează de la câteva probleme agasante, la o ameninţare serioasă la adresa securităţii informaţiilor şi chiar la adresa infrastructurilor naţionale de o importanţă majoră.

Nu există nici o îndoială că unele ţări investesc deja masiv în capabilităţi cibernetice care pot fi folosite în scopuri militare. La prima vedere, cursa digitală a momentului se bazează pe o logică clară şi implacabilă, deoarece domeniul războiului cibernetic oferă numeroase avantaje: este asimetric, atrăgător prin costurile scăzute, iar atacatorul deţine în faza iniţială toate avantajele.

Mai mult decât atât, nu există practic nicio formă reală de descurajare în cadrul războiului cibernetic, deoarece până şi identificarea atacatorului este extrem de dificilă şi, respectând dreptul internaţional, probabil, aproape imposibil.

Este însă de remarcat că cele mai multe state membre NATO şi UE dezvoltă, în ritm accelerat, capabilităţi de apărare în domeniul cibernetic, mergând de la crearea unui cadru legal şi până la constituirea unor puternice capabilităţi tehnice şi asigurarea cu specialişti de cea mai înaltă clasă în domeniu.

Aflat în faţa provocărilor, în domeniul securităţii cibernetice, NATO încearcă să se adapteze la acest tip de ameninţări şi vulnerabilităţi:

- În 2002 a adresat statelor membre o solicitare vizând îmbunătăţirea *„capabilităţilor acestora de a se apăra împotriva atacurilor cibernetice”*, ca parte a angajamentelor de la Praga privind capabilităţile (noiembrie 2002).

• Totuşi, în anii de după 2002, Alianţa s-a concentrat, în primul rând, asupra reglementării unor măsuri pasive de protecţie, care fuseseră solicitate de partea militară.

• Evenimentele din Estonia din primăvara lui 2007 au impulsionat Alianţa să-şi regândească în mod radical nevoia de o politică în domeniul apărării cibernetice şi să-şi ridice contra-măsurile la un nou nivel. De aceea, organizaţia a elaborat pentru prima dată o *„Politica NATO privind Apărarea Cibernetică”*, adoptată în ianuarie 2008, document în care au fost stabiliţi trei piloni centrali ai politicii în spaţiul cibernetic:

- subsidiaritatea – asistenţa este furnizată numai la cerere, altfel se aplică principiul responsabilităţii proprii purtate de statele suverane.

- Neduplicarea, de exemplu, prin evitarea unei duplicări inutile la nivelul structurilor sau au capabilităţilor – la nivel internaţional, regional şi naţional.

- Securitatea – cooperarea bazată pe încredere, luând în considerare sensibilitatea informaţiilor legate de sisteme care trebuie puse la dispoziţie şi posibilele vulnerabilităţi.

• La Summitul de la Lisabona (noiembrie 2010) Alianţa a pus, cu succes, bazele unei examinări factuale autogestionate a problematicii, din ce în ce mai complexe, a războiului cibernetic.

• În conformitate cu Noul Concept Strategic al NATO**,** politica Alianţei privind Apărarea Cibernetică revăzută defineşte ameninţările cibernetice drept o sursă potenţială care face obiectul apărării colective în concordanţă cu Articolul 5 al NATO. Mai mult decât atât, noua politică şi *„Planul de Acţiune”* pentru implementarea sa – oferă NATO linii directoare clare şi o listă de priorităţi agreată în privinţa modului în care să avanseze apărarea cibernetică a Alianţei.

Evoluţii îngrijorătoare pentru ţările lumii. Acţiuni de „război cibernetic” declanşate de actori statali în perioada 2016-2017

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 profesionişti 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)[4];
- Hillary Clinton s-ar afla sub influenţa unor cercuri de putere oculte care ar urmări dominaţia mondială şi dezmembrarea federaţiei Ruse;

[4] Articolul a fost scris înainte de alegerile prezidenţiale din SUA (06.11.2016)

- 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);

d) Cazul atacurilor cibernetice masive asupra unor servicii IT:

- Vineri, 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.

e) 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 indici 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.

f) 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."[5]

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.

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.

Securitatea cibernetică – o dimensiune importantă a securităţii naţionale a României

Toate statele lumii resimt efectele pozitive ale evoluţiilor din domeniul tehnologiei informaţiilor şi comunicaţiilor, dar aşa cum am arătat anterior, acestea vin la pachet cu riscuri, ameninţări şi vulnerabilităţi în domeniul atacurilor cibernetice şi chiar a războiului cibernetic. *„Aceste fenomene implică crearea şi finanţarea unor instituţii care să se ocupe doar de securitatea cibernetică, realizând planuri pentru prevenirea atacurilor cibernetice, pentru posibilitatea de a avea un răspuns rapid în cazul în care asemenea evenimente au loc, pentru abilitatea de a descoperi persoanele sau organizaţiile responsabile pentru acestea astfel încât să fie aduse în faţa justiţiei, şi nu în ultimul rând, pentru abilitatea de a înlocui sau repara în cel mai scurt timp componentele afectate ale reţelei digitale."*[6]

Securitatea cibernetică reprezintă o provocare ce trebuie abordată prin cooperare între diverşi actori naţionali, precum instituţii, companii private sau organizaţii nonguvernamentale, dar şi la nivel internaţional prin cooperarea între state, organizaţii regionale şi globale, având în vedere faptul că securitatea cibernetică este o problemă globală. Şi România a recunoscut securitatea cibernetică drept o dimensiune importantă pentru securitatea sa naţională în anul 2010, atunci când a fost inclusă în *„Strategia Naţională de Apărare"*. Acest document politico-militar include, în ceea ce priveşte securitatea cibernetică, obiective pe termen scurt şi pe termen lung, deoarece menţionează că ţara depinde

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

[6] http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/ (Autor: Andra Alexandru)

de buna funcţionare a multiplelor reţele de care depind vieţile cetăţenilor români şi economia naţională. În Strategie se recunoaşte de asemenea, faptul că România are vulnerabilităţi în a asigura securitatea spaţiului cibernetic naţional, deoarece prezintă deficienţe în ceea ce priveşte protecţia şi funcţionarea infrastructurii digitale şi a celei critice.

Totodată, Strategia evidenţiază că un nivel mai ridicat de securitate a infrastructurii digitale este necesară, deoarece la nivel mondial atacurile cibernetice sunt din ce în ce mai frecvente şi mai complexe. De aceea, România a avut în vedere anumite obiective care între timp au fost îndeplinite, precum înfiinţarea unei comunităţi de experţi în domeniul informaticii şi a securităţii reţelelor digitale, CERT-RO (Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică).

CERT-RO este acum un centru funcţional responsabil pentru *„Prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice”* şi pentru dezvoltarea de politici publice în domeniu.

Există, de asemenea, instituţii naţionale implicate în activităţi specifice securităţii cibernetice, precum Ministerul Comunicaţiilor şi Societăţii Informaţionale, Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism (DIICOT), Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal şi alte câteva având capabilităţi limitate.

Cu toate acestea, nu există încă o instituţie centrală care să se ocupe în mod direct şi cuprinzător de riscuri cibernetice la nivel naţional, având ca fundament o strategie de securitate cibernetică.

De menţionat că Ministerul Comunicaţiilor şi Societăţii Informaţionale a lansat în iunie 2011 un document de lucru numit *„Strategia de Securitate Cibernetică a României”*, care, întro formă mai complexă a fost aprobat de către CSAT, în februarie 2013.

A fost lansat în dezbatere publică, la începutul acestui an proiectul *„Legea privind Securitatea Cibernetică a României”*. Acesta nu a ajuns în dezbaterea Parlamentului din cauza numeroaselor critici şi rezerve privind viaţa privată a cetăţenilor şi confidenţialitatea necesară pentru mediul de afaceri. Este însă, un document mult aşteptat şi necesar în această fază a atacurilor cibernetice. Să sperăm că până la 31 decembrie 2016 se va găsi o soluţie de compromis şi legea va fi votată şi promulgată.

Trebuie să arătăm că problema securităţii cibernetice este tratată în mod corespunzător şi în *„Ghidul Strategiei Naţionale de Apărare pentru perioada 2015-2019”*, document aprobat prin Hotărârea CSAT nr. 128, din 10 decembrie 2015.

După câte se observă documente sunt şi vor mai fi, dar noi credem că se impun măsuri practice mai hotărâte pentru a răspunde eficient riscurilor, ameninţărilor şi vulnerabilităţilor cibernetice.

Sunt numeroşi specialişti, români şi străini, în domeniul ITC, care propun soluţii de securitate pentru utilizatorii individuali, companii şi structuri guvernamentale, între care menţionăm:

- Să fie folosită o soluţie de securitate actualizată constant;
- Să se remedieze şi să se actualizeze toate programele software care rulează pe terminale şi servere web;
- Să fie instalate soluţii de backup;
- Să se administreze fişierele care rulează în calea de director, *„AppData/Local AppData”* şi să se asigure politici care împiedică utilizatorii să execute aplicaţii sau fişiere;
- Să fie limitată utilizarea de către unele persoane a accesării unor destinaţii din reţea;
- Să se aplice soluţii performante de protecţie a serverelor de e-mail, prin filtrarea conţinutului;
- Să se asigure că angajaţii pot identifica e-mailuri care răspândesc viruşi şi să evite accesarea acestora provenite de la expeditori necunoscuţi;
- Mai sunt şi alte măsuri care privesc alegerea şi protejarea parolei, protecţia împotriva programelor spyware, protecţia atunci când utilizăm reţelele publice folosind şi conexiunile Wi-Fi (cu laptop, telefoane sau tablete).

Revoluţiile tulburătoare aduse la cunoştinţa publicului român de către John McAfee, specialist de vârf în industria soluţiilor antivirus din SUA[7]

Studiind mai multe cărţi , studii şi articole pe tema atacurilor cibernetice şi a războiului cibernetic observăm o accelerare, fără precedent, în unele ţări, în ultimii doi ani, pentru a asigura distrugerea facilităţilor informaţionale ale adversarului şi în primul rând a reţelelor de utilităţi. O atenţie deosebită este acordată reţelelor de energie electrică.

Să redăm principalele informaţii relevate de John McAfee:

- Cel puţin patru ţări au arme cibernetice capabile să distrugă reţeaua de energie electrică a unui alt stat: China, SUA, Rusia şi Israel;
- China este fără îndoială ţara cu cele mai puternice arme cibernetice. Chinezii au înţeles încă de acum patru decenii că electronica şi computerele sunt esenţiale pentru viitorul armelor;

[7] HotNews.ro, Interviu Vlad Barza luat specialistului din industria antivirus americană John McAfee, 23 februarie 2017.

- Dacă o ţară ar începe un război cibernetic pentru a distruge alt stat, urmările ar fi catastrofale pentru că riscăm distrugerea generală.
- Să încerci să realizezi ceva în guvern este cel mai greu lucru din lume, fiindcă toată lumea te dă la o parte pentru că fiecare are propriul interes (justifică refuzul de a fi numit şeful strategiei de securitate cibernetică în Administraţia Trump).
- Ce s-ar întâmpla dacă America ar rămâne fără energie electrică? Am muri cu toţii, nu am mai avea mâncare, comunicaţii sau servicii de urgenţă, ne-am întoarce în Epoca de Piatră. Un studiu recent prezentat în Congres estima că în doi ani 90% dintre americani ar muri dacă am rămâne fără curent.
- Va fi un atac distrugător asupra altui stat? Este prea periculos şi cred că lumea nu ar supravieţui nici dacă atacul ar fi asupra unei singure ţări, fiindcă ar fi represalii. Diferenţa între armele clasice şi cele cibernetice este că te costă enorm să construieşti o bombă nucleară, dar când o ţară a construit o armă cibernetică, poate face după ea un milion de copii cu costuri minime, fiindcă este vorba de date digitale.
- Împotriva ştirilor false nu putem lupta cu un soft de inteligenţă artificială. Dacă noi oamenii nu suntem în stare să judecăm ce e fals şi ce nu, cum putem construi un soft care să facă asta?
- Diversele aparate ce formează *„Internet of things”* sunt scoase pe piaţă fără pic de grijă pentru securitatea informativă şi fără să se ţină seama de cum gândesc hackerii.

Interviul foarte instructiv şi plin de învăţăminte este mult mai amplu, iar cei interesaţi ar putea să îl studieze în întregime.

De la început am menţionat că problematica complexă, de mare actualitate, a atacurilor cibernetice şi a războiului cibernetic nu poate fi clarificată întrun simplu articol dintr-o revistă. Scopul este doar ridicarea, în faţa celor interesaţi, a acestor probleme şi descoperirea celor mai bune soluţii de protecţie.

Pentru un studiu mai complet este necesară parcurgerea a zeci de cărţi, studii şi articole activitate care intră în fişa postului administratorilor de reţea şi responsabililor din instituţiile statului cu atribuţii directe în securitatea cibernetică a României. Să nu se uite însă că noi surprize apar zilnic şi trebuie analizate şi luate în seamă în vederea contraacarării lor.

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;
DUNNIGAN F.J., *Noua ameninţare mondială – Cyber-Terorismul*, Editura Curtea Veche, Bucureşti, 2010;
RAIU C., *Laboratoarele Kaspersky*, Interviu acordat Ziarului Adevărul, 19 februarie 2013;
www.internetworldstats.com/stats.html
http://www.nato.int/dom/review/2011/11-september/Cyber-Threads/RO/index.htm
http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/
Alte site-uri de profil utilizând căutarea cu „atacuri cibernetice”;
HotNews.ro, Interviu Vlad Barza luat specialistului din industria antivirus americană John McAfee, Bucureşti, 23 februarie 2017.