AMENINȚĂRI CIBERNETICE GLOBALE ŞI NAȚIONALE

Adrian-Victor Vevera

Administrația Prezidențială

Rezumat: Această lucrare îşi propune să sintetizeze principalele riscuri, vulnerabilități şi amenințări la adresa securității naționale şi internaționale pe care le prezintă armele cibernetice. În prezent, analiştii militari şi de intelligence consideră spațiul cibernetic drept al cincilea domeniu ca importanță în care se poate desfăşura un război. Dacă cea de-a doua jumătate a secolului XX aducea în prim-plan amenințarea cu utilizarea armelor nucleare, prima jumătate a secolului XXI este dominată de preocuparea pentru prevenirea şi combaterea amenințărilor cibernetice. Spre deosebire de amenințarea nucleară, atacul cibernetic nu poate fi descurajat întotdeauna printr-un contra-atac deoarece pur si simplu este dificil să se identifice actorul statal sau non-statal care l-a provocat. Amenințările cibernetice la adresa securității naționale şi internaționale au atras atenția opiniei publice relativ recent. Atacurile cibernetice executate, cel mai probabil, de Federația Rusă asupra Estoniei în 2007 şi Georgiei în 2008 au determinat au reevaluare a doctrinelor militare ale statelor membre NATO, securitatea cibernetică ocupând o atenție sporită. Stat membru NATO şi UE, România nu a fost ocolită de atacuri cibernetice. Dimpotrivă, cel mai mare atac cibernetic asupra țării noastre – Octombrie Roşu – a fost înregistrat în 2013. Prin adoptarea Strategiei de Securitate Cibernetică a României şi constituirea unor centre operative pentru prevenirea şi contracararea incidentelor din cadrul infrastructurilor cibernetice, țara noastră este apreciată de partenerii strategici ca fiind un actor important în lupta împotriva războiului cibernetic.

Cuvinte cheie: securitate națională, securitate globală, spațiu cibernetic, amenințări cibernetice.

Abstract: This paper aims to summarize the main risks, vulnerabilities and threats to national and international security posed by cyber weapons. Currently, military and intelligence analysts consider cyberspace as the fifth most important area in which a war can be generated and developed. If the second half of the twentieth century brought to the fore the threat of use of nuclear weapons, the first half of the XXI century is dominated by the concern to prevent and combat cyber threats. Unlike nuclear threat, cyber attacks can not always be discouraged by a counter-attack simply because it is difficult to identify the state or non-state actor provoked. Cyber threats to national and international security have drawn public attention recently. Cyber attacks executed, most likely, the Russian Federation on Estonia in 2007 and Georgia in 2008 have caused reassessment of military doctrines of NATO member states, bringing cybersecurity into attention of policymakers. As NATO and EU member state, Romania has not been spared by cyber attacks. On the contrary, the largest cyber attack on our country - Red October - was recorded in 2013. By adopting The Cyber Security Strategy and the establishment of some operational centers, Romania will play an important rol in preventing and combating incidents of cyber infrastructures. Therefore, our country is valued by our strategic partners as one of the major player in the fight against cyber warfare.

Keywords: national security, global security, cyber space, cyber threats.

1. Introducere

Nu demult, James Comey şi alți directori ai comunității de informații americane li s-au alăturat lui James Clapper pentru a prezenta în fața Congresului American evaluarea anuală a amenințărilor actuale la adresa securității naționale a SUA.

Lista amenințărilor mondiale prezentată de către Directorul Comunității de Informații a SUA include următoarele: cyber, contra-spionajul, terorismul, armele de distrugere în masă şi proliferarea acestora, crima organizată transnațională, tendințele economice, resursele naturale, hrana, apa, energia, evenimentele meteo extreme, zona Arcticii, riscuri la adresa sănătății şi atrocitățile în masă.

2. Amenințări cibernetice la nivel internațional

Pe măsură ce economiile țărilor dezvoltate exploatează avantajele oferite de spațiul virtual, infrastructura acestora devine tot mai vulnerabilă atacurilor cibernetice. Fenomenul agresiunilor a cunoscut o diversificare permanentă, direct proporțională cu dezvoltarea tehnologiilor informației şi a societății informaționale. Metodele de atac sunt permanent adaptate evoluției din domeniul tehnologic şi vulnerabilităților identificate.

Teoreticienii consideră spațiul cibernetic drept al cincilea domeniu în care se poate desfăşura un război, după sol, mare, aer şi spațiu, caracterizat prin dinamism extrem, asimetrie,

predictibilitate redusă şi dificultatea atribuirii agresiunilor.

În cazul armei-cheie a secolului al XX-lea, bomba nucleară, ţările ce o puteau folosi în luptă au ales să nu o facă, fiind descurajate de faptul că un contraatac ar fi fost la fel de devastator. În schimb, atacul cibernetic ar putea evita acest impediment dacă victima atacului nu ştie împotriva cărei ţări să lanseze contraatacul[1].

Primul atac cibernetic a fost semnalat în 1982, când spionii sovietici au furat un sistem de control computerizat de la o companie canadiană, fără să ştie că specialiştii CIA reuşiseră să introducă în software-ul acestuia o linie de cod care a generat o explozie masivă la o conductă de gaz din Siberia. Deflagraţia a fost atât de mare încât a fost detectată din spaţiu de sateliţii americani, iar Thomas Reed, fost comandant al aviaţiei SUA, a descris-o în autobiografia sa ca fiind „cea mai mare explozie non-nucleară detectată vreodată din spaţiu".

Cu toate acestea, atacurile cibernetice au intrat în atenţia opiniei publice abia după 25 de ani de la acest eveniment, respectiv în 2007, când o ţară întreagă - Estonia - a fost afectată, ministerele, băncile şi numeroase companii fiind nevoite să îşi oprească activitatea. Primul atac cibernetic asupra unei întregi ţări a venit pe fondul unei dispute politice pe tema mutării unui monument dedicat eroilor sovietici, propunere îndelung contestată de minoritatea rusă din Estonia şi de Kremlin. Majoritatea informaţiilor au indicat ca sursă a atacului adrese de internet originare din Rusia.

Un an mai târziu, în 2008, Georgia a suferit atacuri similare, într-o perioadă ce a coincis cu conflictul georgiano-rus din Osetia de Sud. Din cauza atacurilor venite dinspre Rusia, routerele din Turcia şi Rusia ce făceau legătura cu Georgia au fost supraîncărcate cu date despre ţara gruzină, astfel că traficul în exterior a fost complet sufocat, cetăţenii Georgiei fiind în imposibilitatea de a accesa vreun site. De asemenea, Georgia a pierdut controlul asupra domeniului *.ge*, fiind nevoită să transfere site-urile guvernamentale pe servere din afara ţării.

Cel mai devastator impact a fost cel creat asupra sistemului bancar. Întrucât băncile şi-au sistat orice activitate online şi nu puteau, astfel, să fie atacate, agresorii au direcţionat atacuri către sistemul bancar internaţional, camuflând sursa acestora pentru a părea că sunt originare din Georgia. În aceste condiţii, sistemele de securitate ale băncilor internaţionale au reacţionat, blocând toate conexiunile cu sistemul bancar georgian, context care a dus la blocarea imediată a operaţiunilor bancare din Georgia şi la paralizarea sistemului de cărţi de credit.

Atacurile cibernetice asupra celor două ţări au determinat o reevaluare a doctrinelor militare ale statelor membre NATO, securitatea cibernetică căpătând astfel mai multă importanţă.

Totuşi adevăratul început al războiului cibernetic poate fi datat în anul 2010, odată cu apariţia primei arme cibernetice (virusul Stuxnet), primul virus proiectat să preia sub control şi să saboteze subtil infrastructurile critice ale unui stat. În 2011, a fost descoperit Duqu, un troian cu caracteristici similare Stuxnet, dar proiectat să acţioneze ca un „backdoor" în sistemul infectat şi să fure informaţii confidenţiale.

Anii următori s-au remarcat prin descoperirea unui număr tot mai mare de agresiuni cibernetice persistente (de tip Advanced Persistent Threat), cu impact semnificativ asupra securităţii naţionale. Amintim întregul arsenal de arme cibernetice descoperit: Flame (apreciat de specialiştii în domeniu drept cel mai sofisticat malware cunoscut până în prezent), Wiper, Mahdi, Shamoon, Gauss - malware produse de actori statali antagonici, folosite împotriva unor infrastructuri critice (transport resurse energetice, bănci, agenţii guvernamentale, universităţi).

Aceste descoperiri subliniază faptul că securitatea naţională nu este aşa de sigură pe cât se credea. Războiul cibernetic a adăugat o nouă dimensiune, prezentând lumii, în mod clar, modul în care ţările avansate din punct de vedere tehnologic îşi pot utiliza cunoştinţele superioare pentru a ataca alte ţări.

De altfel, în ultimii trei ani au fost realizate zeci de atacuri majore, care au afectat state şi organizaţii suprastatale, atacatorii fiind interesaţi prioritar de domeniile guvernamental, politică

[1] vezi, pe larg, http://www.descopera.ro/capcanele-internetului/9627768-traim-in-epoca-ciber-razboaielor

externă, militar, industrial şi financiar-bancar.

Numărul complexitatea şi modul de derulare a acestor atacuri evidenţiază nivelul ridicat şi în creştere exponenţială al ameninţării cibernetice, respectiv că:

- până în prezent, cei mai periculoşi actori în domeniul cibernetic sunt entităţile statele; în pofida unor capabilităţi ofensive aflate din ce în ce mai mult la dispoziţia reţelelor de criminalitate informatică şi care ar putea fi folosite în viitor şi de către entităţi non-statale, spionajul şi sabotajul au în continuare nevoie de capabilităţile, determinarea şi raţiunea cost-beneficiu a unui stat-naţiune[2];
- chiar dacă pagubele fizice şi terorismul cibernetic cinetic real nu s-a produs încă, securitatea cibernetică nu trebuie neglijată, având în vedere că tehnologia atacurilor evoluează de la mici probleme agasante la o ameninţare serioasă la adresa securităţii informaţiilor şi chiar la adresa infrastructurii naţionale de o importanţă crucială.

Nu există nicio îndoială că unele ţări investesc masiv în capabilităţi cibernetice care pot fi folosite în scopuri militare, cu atât mai mult cu cât, pe lângă avantajele evidente oferite de spaţiul cibernetic agresorilor (asimetrie, costuri scăzute etc.), nu există nicio formă reală de descurajare în cadrul războiului cibernetic, întrucât până şi identificarea atacatorului este extrem de dificilă şi, respectând principiile dreptului internaţional, aproape imposibilă.

Riscuri suplimentare derivă şi din probabilitatea ca entităţi non-statale ce nu au fost protejate împotriva ingineriei reversibile să fi intrat în posesia unor părţi ale acestor viruşi, care pot deveni disponibile pe piaţa neagră, fie ca servicii oferite unor entităţi private, fie ca malware dezvoltat la comandă.

Pe de altă parte, capabilităţile apărării cibernetice evoluează în mod egal şi cele mai multe ţări occidentale şi-au sporit considerabil apărarea în ultimii ani. O bună apărare în domeniul cibernetic face ca aceste ameninţări să fie gestionabile, în măsura în care riscurile reziduale par în mare parte acceptabile, în mod similar ameninţărilor clasice.

3. Ameninţarea cibernetică la nivel naţional

Deşi se află încă la un nivel redus de utilizare a serviciilor informatice şi de comunicaţii comparativ cu alte state ale lumii, România a cunoscut în ultima decadă o dezvoltare semnificativă a acestora, tot mai multe activităţi guvernamentale şi comerciale derulându-se prin intermediul Internetului.

Pe acest fond, România nu este exclusă de pe harta statelor susceptibile la atacuri cibernetice, risc potenţat şi de statutul de ţară membră a unor organizaţii internaţionale, însă riscurile asociate agresorilor cibernetici se situează încă la un nivel mediu.

De altfel, securitatea cibernetică a devenit în ultimii doi ani o problemă de securitate naţională deoarece s-a constatat că spaţiul cibernetic românesc este în vizorul agresorilor cibernetici. La începutul anului 2013, România s-a confruntat cu două atacuri cibernetice de mare amploare care au vizat, în special, accesul la informaţii confidenţiale prin accesarea site-urilor guvernamentale şi a anumitor entităţi private cu influenţă în economia naţională.

Cel mai mare atac cibernetic, *Octombrie Roşu*, a vizat o serie de reţele guvernamentale pentru obţinerea de informaţii cu caracter clasificat.

Studiile efectuate de Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) reliefează faptul că, la jumătatea anului 2013[3]:

- ameninţările cibernetice s-au diversificat, fiind relevate tendinţe evolutive, atât din perspectivă cantitativă, cât şi din punct de vedere al complexităţii tehnice;

[2] vezi, pe larg, Revista NATO - Noi ameninţări dimensiunea cibernetică
[3] vezi, pe larg, Raport cu privire la alertele de securitate cibernetică primite de CERT-RO în primele 6 luni ale anului 2013

- majoritatea incidentelor analizate se referă la entități din România, victime ale unor atacatori care vizează infectarea unor sisteme informatice cu diverse tipuri de aplicații malware, în scopul constituirii unor rețele de tip botnet;
- peste 12,5% din plaja de IP-uri alocată României este infectată cu diverse variante de malware, majoritatea alertelor de tip botnet vizând utilizatori de tip rezidențial (home user);
- *prin intermediul calculatoarelor unor victime din România, folosite ca proxy, sunt desfăşurate atacuri asupra unor ţinte din afara ţării, identitatea reală a atacatorului rămânând ascunsă;*
- *România nu mai poate fi considerată doar o ţară generatoare de incidente de securitate cibernetică, analiza datelor prezentate demonstrând caracterul intermediar/ de tranzit al unor resurse informatice semnificative conectate la reţeaua Internet în România;*
- amenințările de tip Advanced Persistent Threat sunt deja o realitate şi în România;
- 5.678 domenii *.ro* au fost compromise, reprezentând mai puțin de 1% din totalul domeniilor existente; dintre acestea peste 51% au suferit atacuri de tip defacement, iar 43% au fost infectate cu diverse variante de malware.

Rezultate similare au fost produse şi de studiile efectuate de Kasperski Lab, care subliniază că România se situează pe locul 36 la nivel mondial în ceea ce priveşte pericolele asociate navigării pe Internet.

În pofida nivelului încă mediu, amenințarea cibernetică se situează pe un trend ascendent, favorizat în condițiile în care:

- cetățenii vor utiliza tot mai mult serviciile societății informaționale şi spațiul cibernetic în activitățile zilnice.

Dependența de Internet este probabil cel mai bine ilustrată de creşterea exponențială a gradului de penetrare a acestuia în România, statisticile în domeniu relevând faptul că Internetul devine tot mai relevant în activitățile cotidiene.

De exemplu, la mijlocul anului 2012[4], rata de penetrare a Internetului în România era de aproximativ 44,1%, comparativ cu 3,6% în anul 2002. Potrivit unui studiu realizat de GFK-Omnibus, la începutul anului 2013 această rata era de 61% în rândul orăşenilor şi de 33% în mediul rural, crescând semnificativ gradul de utilizare în rândul persoanelor mature.

- societatea civilă, instituțiile guvernamentale şi mediul de afaceri rămân vulnerabile la atacuri cibernetice.

Dezvoltarea web-ului a creat premisa apariției vulnerabilităților specifice oricărui produs tehnologic. Deşi, per total, numărul acestora este în scădere, ca urmare a măsurilor de securizare avute în vedere în momentul proiectării şi dezvoltării aplicațiilor, gradul de diversificare a lor creşte continuu.

În fiecare zi sunt descoperite noi vulnerabilități, a căror exploatare ar putea avea un impact tot mai mare asupra țintelor vizate de agresorii cibernetici.

Gradul de complexitate a atacurilor creşte continuu chiar dacă media nivelului cunoştințelor tehnice de care beneficiază marea masă a agresorilor cibernetice scade. Această situație este explicabilă prin faptul că agresorii cibernetici cu abilități tehnice excepționale dezvoltă instrumente pe care un novice le utilizează ulterior cu un singur click, fără a fi un bun tehnician, iar efectele produse pot fi dezastruoase.

Mai mult, atât instituțiile guvernamentale, cât şi mediul de afaceri şi utilizatorii casnici înregistrează un flux masiv de date confidențiale care nu sunt întotdeauna protejate adecvat. În cele mai multe situații, factorul uman este veriga cea mai slabă în procesul de securitate, din cauza lipsei culturii de securitate cibernetică ori a insuficientei informări cu privire la necesitatea şi modurile de

[4] www.internetworldstats.com

protejare a propriilor sisteme informatice.

- efectele crizei economice se repercutează tot mai mult asupra bunăstării sociale.

Situaţia precară cu care se confruntă un segment tot mai ridicat din populaţia României are ca efect implicarea indivizilor în săvârşirea de infracţiuni informatice, care le facilitează obţinerea rapidă de câştiguri financiare substanţiale şi favorizează racolarea unui număr din ce în ce mai mare de specialişti IT în activitîţi infracţionale.

Coroborând toate aceste elemente şi analizând incidentele şi atacurile cibernetice produse pe teritoriul naţional, se pot desprinde următoarele concluzii:

- România este vizată de entităţi cibernetice ostile, interesate să obţină acces la sisteme informatice de interes naţional şi să culeagă informaţii, respectiv să obţină beneficii patrimoniale ilicite;
- dintre formele de manifestare a ameninţărilor cibernetice, cele mai agresive şi cu cel mai mare impact asupra securităţii naţionale au fost criminalitatea cibernetică şi spionajul cibernetic, urmate de activităţile hacktiviste;
- până în prezent nu s-au înregistrat consecinţe distructive asupra infrastructurilor critice vizate de atacuri;
- atacurile realizate până în prezent ar fi putut avea, totuşi, o finalitate distructivă din perspectiva complexităţii tehnice, în condiţiile în care nivelul de securitate cibernetică a ţării noastre este insuficient pentru a face faţă unor agresiuni cibernetice de nivel mediu-ridicat.

Similar altor ţări, România a conştientizat necesitatea întreprinderii de acţiuni concrete pe componenta securităţii cibernetice, fiind - în prezent - ţara cu una dintre cele mai actualizate legislaţii privind securitatea spaţiului cibernetic, în sensul în care, în anul 2001, a ratificat Convenţia de la Budapesta, iar în perioada 2001-2004 a elaborat actele normative şi a aderat la organismele internaţionale şi europene privind combaterea criminalităţii informatice, protecţia datelor personale sau securizarea informaţiilor din spaţiul cibernetic.

În acest context, la nivel naţional, iniţiativele privind reglementarea securităţii cibernetice şi operaţionalizarea unor instituţii implicate s-au concretizat în:

- aprobarea Strategiei de Securitate Cibernetică a României, care stabileşte obligativitatea reevaluării suportului legislativ şi a instrumentelor legale pe care instituţiile abilitate le deţin în vederea îndeplinirii sarcinilor ce decurg prin punerea în aplicare a acesteia;
- constituirea Consiliului Operativ de Securitate Cibernetică ce include instituţiile cu responsabilităţi în securitatea sistemelor informatice de interes naţional şi care are rolul de a asigura o abordare coerentă a domeniului şi a cerinţelor necesar pentru funcţionarea Sistemului Naţional de Securitate Cibernetică;
- demararea acţiunilor privind instituirea Sistemului Naţional de Securitate Cibernetică, format din autorităţi şi instituţii publice cu responsabilităţi în domeniu, a cărui misiune este de a asigura elementele de cunoaştere, prevenire şi contracarare a ameninţărilor, vulnerabilităţilor şi riscurilor specifice spaţiului cibernetic;
- constituirea a patru organisme de tip CERT, respectiv CERT-RO, CORIS-STS, CERTMIL şi CERT-INT, care asigură elaborarea şi diseminarea politicilor publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competenţă.

4. În concluzie

Aceasta penetrare fără precedent a tehnologiei are, de asemenea, partea sa de provocări. Există o luptă continuă pentru a atenua provocările legate de ameninţările la adresa securităţii datelor

cibernetice. Nu există soluții simple sau clare la aceste provocări. Persoanele fizice, întreprinderile, societatea şi guvernul trebuie să lucreze împreună pentru a avea o viziune comună asupra adevăratului potențial al revoluției digitale.

Pentru a încheia, aş spune că infrastructura de software este aici pentru a rămâne. Aceasta ne aduce noi oportunități de creştere şi inovare. Pentru a beneficia de întregul potențial al acestor tendințe, trebuie să depăşim unele dintre provocările inerente.

BIBLIOGRAFIE SELECTIVĂ

1. Amenințări cibernetice la adresa utilizatorilor din România. Raport realizat de Bitdefender în cadrul campaniei de conştientizare a riscurilor de securitate cibernetică derulată în România de către CERT-RO.
2. Centrul Național de Răspuns la Incidente de Securitate Cibernetică. Raport cu privire la alertele de securitate cibernetică primite de CERT-RO în primele 6 luni ale anului 2013.
3. ENISA Threat Landscape 2013, ediție online.
4. Revista NATO - Noi amenințări dimensiunea cibernetică, ediție online.
5. Strategia de securitate cibernetică a României, 2013.
6. www.internetworldstats.com
7. www.descopera.ro/capcanele-internetului/9627768-traim-in-epoca-ciber-razboaielor