O NOUĂ EPOCĂ DIGITALĂ

Adrian Victor Vevera

Administrația Prezidențială

Rezumat: Prăbuşirea Turnurilor Gemene în fatidica zi de 11 septembrie 2001 reprezintă momentul de cotitură care a schimbat percepția oarecum tradițională privind riscurile, vulnerabilitățile şi amenințările la adresa securității naționale, regionale şi internaționale. Dezvoltarea tehnologiei informațiilor şi comunicaților a însemnat intrarea omenirii într-o nouă eră – era digitală, care a eliminat complet barierele tradiționale impuse de spațiu şi timp. În contextul emergenței epocii digitale, incidentele de securitate cibernetice generate de actori statali sau non-statali, intenționat sau accidental, s-au multiplicat şi riscă să afecteze grav funcționarea infrastructurilor critice, strategice ale unui stat sau ale comunității internaționale. În prezent, securitatea energetică constituie o preocupare majoră mai ales pentru decidenții politici şi militari care au început să-şi concentreze eforturile pe elaborarea şi implementarea de politici coerente în domeniu, atât pentru protejarea intereselor publice, cât şi a celor din sectorul privat. Lucrarea de față descrie principalele provocări cu care se confruntă societatea informațională, precum şi tipurile de amenințări cibernetice: războiul cibernetic, terorismul cibernetic, agresiunile informatice la adresa persoanelor fizice. În finalul lucrării, formulez câteva recomandări în materie de protecție şi combatere a amenințărilor cibernetice care interesează securitatea națională: elaborarea unui sistem unitar de standarde de securitate cibernetică la nivel național, eficientizarea managementului rețelelor intranet ale statului, reorganizarea instituțiilor cu atribuții în domeniu pentru o mai bună coordonare, coerență şi eficiență în lupta împotriva amenințărilor cibernetice şi, nu în ultimul rând, dezvoltarea, în componente de cybersecurity în interiorul culturii de securitate.

Cuvinte cheie: era digitală, amenințări cibernetice, război cibernetic, cultură de securitate.

Summary: The collapse of the Twins Tournament in the fateful day of September 11, 2001 is the turning point that changed traditional perception of risks, vulnerabilities and threats to the national, regional and international security. The development of information and communication technology meant the entry of the humanity into a new era - the digital age that has completely eliminated the traditional barriers imposed by time and space. In the framework of the emergence of the digital age, cyber security incidents generated by state or non-state actors, intentional or accidental, have multiplied and could seriously affect the functioning of critical and strategic infrastructure of the state or the international community. Currently, cyber security is a major concern especially for policy makers who began to focus their efforts on the development and implementation of coherent policies in the field, both to protect the public interests and those of the private sector. This paper describes the main challenges facing the information society and the types of cyber threats: cyber war, cyber terrorism, cyber scum – attacks against individuals. At the end of the paper, I proposed several recommendations concerning protection and combating the cyber threats to national security: development of a unified cyber security standards, nationally efficient intranet management of state institutions, reorganization of the main institutions in the filed of cyber security for a coordination and coherence and efficiency in the fight against cyber threats and, last but not least, the development of the component of cybersecurity within security culture.

Keywords: digital age, cyber threats, cyber warfare, security culture.

1. Introducere

La nivel internațional este recunoscut faptul că data de 11 septembrie 2001 reprezintă data care a schimbat percepția tradițională asupra amenințărilor, scenariul Războiului Rece - care dominase timp de peste 50 ani - fiind schimbat în mod radical şi irevocabil.

Prăbuşirea Turnurilor Gemene a trasat noi repere în economia securității mondiale: amenințarea nu mai avea o adresă clară a unui expeditor (apărând deja conceptul de *anonimizare*), iar granițele deveneau fără sens, sfidând regulile militare clasice de spațiu şi timp.

Aceste două trenduri urmau să fie tot mai accentuate în următorii ani pe fondul dezvoltării tehnologiei informației şi comunicațiilor - componentă esențială în procesul de globalizare, dar care a eliminat definitiv barierele tradiționale impuse de spațiu şi timp şi a generat efecte pe termen lung încă dificil de perceput.

De la un instrument administrativ utilizat în urmă cu 20 de ani pentru optimizarea proceselor de birou, tehnologia informației reprezintă în acest moment un instrument strategic al industriei, administrației şi armatei.

Tehnologia informației şi comunicațiilor a devenit coloana vertebrală a creşterii noastre economice şi reprezintă o resursă de importanță majoră pe care se bazează toate sectoarele

economiei, stând la baza sistemelor complexe care asigură funcţionarea economiilor noastre, în sectoare-cheie cum ar fi finanţele, sănătatea, energia şi transporturile.

Deşi a generat schimbări economice şi sociale fără precedent, aducând beneficii incontestabile, creşterea gradului de utilizare a tehnologiei informaţiei şi comunicaţiilor este asociată şi cu creşterea activităţilor ilicite în spaţiul virtual, societatea informaţională devenind o opţiune tot mai atractivă pentru agresorii cibernetici de a-şi materializa intenţiile ilicite, întrucât nu implică resurse foarte mari iar beneficiile pot fi imense.

Numărul incidentelor de securitate cibernetică, fie ele intenţionate sau accidentale, creşte într-un ritm alarmant şi ar putea perturba furnizarea unor servicii. Ameninţările pot veni din surse diverse – cum ar fi atacurile criminale, teroriste, motivate politic sau sponsorizate de stat, precum şi catastrofele naturale sau greşelile neintenţionate.

Pe acest fond, ultimii trei ani au fost marcaţi de schimbări majore ale mediului de securitate cibernetică, semnificativ influenţat de creşterea produselor IT, factori externi variaţi (precum contextul economico-financiar actual, „lupta pentru supremaţie" a marilor puteri), apariţia continuă de vulnerabilităţi, gradul tot mai crescut de complexitate a instrumentelor şi tipurilor de atac etc.

Ameninţările cibernetice au ajuns să fie un impediment tot mai prezent în vieţile noastre, fiind în continuă creştere.

Din nefericire, aşa cum se precizează în *„ENISA Threat Landscape 2013"*, în acest moment infractorii cibernetici sunt cu un pas înainte, ajungând să folosească metode din ce în ce mai avansate pentru a implementa vectori de atac care sunt nedetectabili şi dificil de neutralizat.

În aceste condiţii, asigurarea securităţii cibernetice trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, atât la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu, cât şi la nivelul entităţilor private, interesate de protejarea propriului patrimoniu şi a proprietăţii intelectuale.

2. O mică trecere în revistă

Şapte luni după ce Snowden a dat publicităţii documentele clasificate ale NSA, prejudiciul evaluat relevă efectul profund pe care l-au cauzat şi continuă să-l cauzeze dezvăluirile sale, care „au făcut din SUA o naţiune mai puţin sigură". „Ca rezultat, ne-am pierdut surse importante de colectare de informaţii externe, inclusiv parteneri de valoare", arăta Clapper.

Benjamin Franklin a spus odată, „În această lume nimic nu este sigur, cu excepţia morţii şi a impozitelor". Aş adăuga !atacurile cibernetice", la această listă.

Ce s-ar întâmpla dacă România ar pierde brusc accesul la e-mail, mass-media on-line, la site-urile guvernamentale şi de Home Banking? Aceasta nu a fost o intrigă într-un film Hollywoodian, ci realitate pentru populaţia din Estonia, atunci când a fost lovită de un val de atacuri cibernetice, în 2007.

Fără îndoială, cyber-securitatea este problema momentului. De la atacurile cibernetice asupra Estoniei, descoperirea Stuxnet, super viermele folosit în sabotajul industrial în 2010, mai multe cazuri de cyber spionaj, culminând cu revelaţiile Snowden anul trecut, şi sofisticarea tot mai mare a infracţiunilor cibernetice, toate alăturate lasă impresia că atacurile informatice sunt din ce în ce mai frecvente, mai organizate, mai costisitoare, şi mult mai periculoase. Suntem acum la un punct în istorie în care orice putere politică cu aspiraţii la nivel mondial trebuie să ia parte la acest „joc" cibernetic. Ca urmare, orice strategie de securitate trebuie să ia în considerare aceste aspecte.

La sfârşitul anului 2013 s-a estimat că sunt mai multe dispozitive mobile decât oameni în lume. Există aproape 2,7 miliarde de utilizatori de internet şi 1,5 miliarde de utilizatori de smartphone-uri. Această penetrare fără precedent a tehnologiei, combinată cu agilitatea şi accesibilitatea puterii de calcul mare prin cloud, schimbă modul în care producem şi consumăm date. Telefoanele mobile sunt astăzi mult mai mult decât dispozitive de comunicare. Ele stochează şi informaţii personale. Tranziţia la societatea informaţională şi creşterea gradului de democratizare împreună cu

deschiderea societăților contemporane au crescut considerabil importanța surselor deschise (OSINT) în Intelligence. Folosirea de surse deschise de informații s-a impus ca o bază pentru sprijinul multor decizii strategice. Succesele obținute prin exploatarea la adevărata valoare a caracteristicilor specifice ale OSINT au condus la interesul crescut față de acestea, în special în rândul instituțiilor care sunt implicate în apărarea şi securitatea națională, la nivel regional şi internațional. Răspunsurile la noile provocări au condus la creşterea diversității surselor de informare.

O evoluție complementară a cloud este aceea că prin telefonia mobilă şi internet infrastructura software devine accesibilă pentru mase. Se schimbă mentalitățile şi modelele de consum. La nivel global, vânzările prin e-commerce au ajuns la 1200 miliarde USD până la sfârşitul lui 2013. Companiile se folosesc de aceste tehnologii disruptive pentru a crea noi modele de afaceri la costuri semnificativ mai mici. Ecuația s-a schimbat de la a construi, la a cumpăra sisteme informatice, iar conversia de la investiții CAPEX la cerințele OPEX a redus barierele de intrare pentru noii-veniți.

Guvernele pe de altă parte, au posibilitatea de a oferi servicii centralizate cetățenilor prin folosirea Apps and Services (aplicații şi servicii). Fie că este vorba de numere de identificare unice sau de opțiuni de depunere a impozitului pe venit, statul se poate folosi de infrastructura software în beneficiul maselor sale. Infrastructura de software permite guvernelor recuperarea unor decalaje de dezvoltare în domenii precum sănătatea, bancar şi educație. Aceste evoluții sunt pe scurt o revoluție. Astăzi, afaceri cum ar fi Transaction-as-a-service sau Information-as-a-service conferă putere cetățenilor prin accesul la informații. Cel mai important, la o scară ce nu s-a cunoscut înainte, oameni din diferite medii de viață, culturi şi zone geografice se reunesc pentru a împărtăşi cele mai bune practici, de a colabora şi de a-şi modela destinul.

La nivel european există o varietate de organisme care activează în domeniul securității cibernetice, cum ar fi Agenția Europeană pentru Securitatea Rețelelor Informatice Europene şi a Datelor (ENISA), Parteneriatul public-privat european pentru reziliență (EP3R), Computer Emergency Response Team (CERT) şi Centrul de combatere a criminalității informatice ale UE, din cadrul Europol. Au fost luate şi măsuri pentru a se garanta "securitatea rețelelor şi a informației" (NIS) pentru a sprijini protecția infrastructurilor critice (CIP sau CIIP), măsuri destinate combaterii atacurilor cibernetice de toate tipurile, inclusiv cele de mare amploare, care au un accent pe activități de prevenire a cyber–criminalității, dar şi cu un potențial accent pe aspectele militare ale securității cibernetice.

Dar sunt aceste abordări suficiente pentru a se asigura nivelul necesar de cyber-reziliență în Europa?

3. Propuneri şi recomandări

Există un vechi proverb irlandez care spune că „nu există nicio putere fără unitate”. Amenințările cibernetice sofisticate de astăzi se bazează pe rețele internaționale de persoane care lucrează împreună pentru a-şi executa atacurile şi fraudele. Poate ar trebui să ne bazăm pe conceptul conform căruia este nevoie de o rețea pentru a învinge o rețea.

Ce ar putea face România?

România ar putea să îşi propună să devină un lider recunoscut în domeniul securității cibernetice. Relațiile sale pe cyber, bilaterale sau în cadrul NATO şi UE trebuie să includă eforturi de colaborare în materie de protecție a rețelelor, cooperare pentru dezvoltare, combatere a criminalității cibernetice, aliniere politică globală strategică, libertate a internetului, şi îmbunătățire a educației cibernetice. CERT-RO şi CERT-urile partenere trebuie să fie în contact permanent în scopul de a coopera în mod eficient şi a răspunde la incidente cibernetice.

CERT-RO ar putea să îşi dezvolte o bibliotecă de expertiză pe probleme de securitate cibernetică, la nivel cel puțin regional. Scopul acesteia să fie de a spori capacitatea de partajare, cooperare şi informare între aliați şi parteneri în apărare cibernetică în virtutea educației, cercetării şi dezvoltării, a lecțiilor învățate şi de consultare.

Nu în ultimul rând, România ar putea să devină un partener puternic pe probleme de politică cibernetică internațională, inclusiv pentru guvernarea Internetului şi libertatea acestuia. Misiunea ar fi de a ne conecta cu profesionişti în securitate din țările partenere pentru a ne permite să fim mai productivi şi de succes în eforturile noastre comune împotriva amenințărilor cibernetice, cum ar fi:

1) Criminalitatea cibernetică, prin infracțiuni pe bază de computer sau pe Internet, inclusiv:

- infracțiuni împotriva confidențialității, integrității şi disponibilității datelor şi sistemelor informatice (acces ilegal, interceptarea ilegală, ingerință a datelor, interferența în sistem, abuzul de dispozitive, spionaj);
- infracțiuni legate de calculator (fals, fraudă informatică, criminalitate financiară etc.);
- infracțiunile legate de conținut (infracțiuni legate de pornografia infantilă, exploatarea copiilor şi îngrijire a copilului);
- infracțiuni legate de încălcarea drepturilor de autor şi conexe;
- hărțuirea (hărțuirea online, urmărire cibernetică, infracțiunile motivate de ură, prădători on-line), alias „Cyber Scum".

2) Cyber Warfare: acțiuni ale unui stat-națiune de a pătrunde în calculatoarele sau rețele altei națiuni, în scopul de a provoca daune şi avarii.

3) Cyber Terorismul: terorismul cibernetic este o expresie folosită pentru a descrie utilizarea de atacuri bazate pe Internet, în activități teroriste, inclusiv a actelor deliberate, pe scară largă, întrerupere de rețele de calculatoare, în special de computere personale conectate la Internet, prin mijloace cum ar fi viruşii de computer.

4) Cyber Scum: „Cyber Scum" nu este un termen universal acceptat, dar se referă la agresori şi persoane fizice care folosesc anonimatul de pe Internet în scopul de a teroriza.

Pentru ca acestea să se realizeze, găsesc utilă implementarea a patru proiecte:

A. Elaborarea şi implementarea de standarde de securitate cibernetică la nivel național. Definirea normelor şi a comportamentului responsabil a statului în Cyber Space. Dezvoltarea de strategii şi instrumente informatice, fără teamă pentru costurile ridicate pe care le implică acest lucru, chiar dacă, există însă o serie de măsuri de igienă „cyber" low-cost - cum ar fi a luarea unui inventar de dispozitive şi software autorizate, asigurarea pentru configurații hardware şi software-ul de pe dispozitive mobile şi servere, precum şi efectuarea unor analize de vulnerabilitate continue şi de remediere - care pot reduce în mod semnificativ riscurile. Este imperativ a se stabili ce constituie un „atac" şi ce capacități ar putea fi mobilizate în situația confruntării cu un atac?

B. Generarea, extinderea şi managementul intranetului statului. In acest sens existența rețelei de intranet a statului, construită pe facilitățile existente alături de o bibliotecă de programe şi aplicații şi un spațiu de stocare comun de tip cloud ar fi o soluție ieftină şi mult mai sigură pentru comunicare inter şi intra instituțională. Nu este o necesitate sau o obligație ca fiecare angajat din aparatul de stat să aibă acces la internet de pe echipamentele puse la dispoziție pentru îndeplinirea sarcinilor de serviciu.

C. Reorganizarea instituțiilor statului cu atribuții în domeniu, astfel: a) reorganizarea MSI şi înființarea în locul său a unei Agenții Naționale în subordinea Parlamentului, care să acopere pe zona de IT aceleaşi atribuții cu cele ale ANCOM în zona comunicațiilor şi b) trecerea CERT-RO în subordinea Primului Ministru, cu rang de Agenție Națională şi cu atribuții inclusiv în domeniul controlului şi avizării pe zona de securitate cibernetică (excepție făcând zona instituțiilor de securitate națională).

Atacurile cibernetice sunt incidente stresante şi emoționale. O mare provocare este de a înțelege domeniul de aplicare al atacului. Pe de altă parte, nimeni nu poate spera să poată remedia un atac, dacă nu înțelege domeniul de aplicare. În acest sens, un model eficient este în continuare acela care presupune utilizarea de echipe mici de elită de experți care să se ocupe de incidente, mai degrabă decât implementarea de către o armată de "consultanți" a unor proceduri. Acesta, desigur,

are avantajul de a reduce factorul de perturbare şi îmbunătăţeşte ciclurile de comunicare.

D. Dezvoltarea unei culturi de securitate, dublată de susţinerea mai puternică a inovaţiei.

Cultura de securitate, pe componenta de cyber ar asigura implementarea unor deprinderi de bază la toţi utilizatorii (prin programe în parteneriat cu zona educaţională, ar avea un impact pozitiv de la copiii din zona gimnazială până la adulţii angrenaţi în sisteme de învăţare continuă), asigurând în acelaşi timp şi identificarea celor cu potenţial ridicat de hacking şi implicarea lor în activităţi legale.

Pentru a beneficia de adevăratul potenţial al acestui moment trebuie să recurgem la inovare şi la noi obiective de angajament. Este nevoie ca mai multe părţi interesate să dorească a lucra pentru un scop comun, mai degrabă decât să reinventezi roata de fiecare dată.

4. Evoluţii şi perspective ale ameninţării cibernetice la nivel naţional

Nivelul ameninţării cibernetice în România va depinde de gradul de securitate cibernetică a infrastructurilor critice, cu o dinamică influenţată de:

- *evoluţia tehnologică în domeniu IT&C:* riscurile generate de dezvoltarea fără precedent pe această dimensiune vor deriva din rezultanta a două evoluţii divergente: pe de o parte, preocupaţi de creşterea competitivităţii, producătorii de resurse informaţionale se vor grăbi să scoată pe piaţă produse noi, de multe ori insuficient testate, cu consecinţa diversificării considerabile a vulnerabilităţilor software; pe de altă parte, din aceleaşi raţiuni se vor accentua preocupările lor pentru amplificarea măsurilor de securizare avute în vedere în momentul proiectării şi dezvoltării aplicaţiilor;
- *factorul uman:* diversitatea de utilizatori ai sistemelor informatice ale unei instituţii (angajaţi, clienţi, competitori, public larg) şi nivelele lor diferite de cunoaştere, instruire şi interes vor reprezenta, în continuare, factori care influenţează utilizarea sistemelor informatice, în condiţiile în care operatorul uman este cea mai mare sursă de erori din orice sistem complex. Utilizatorul va rămâne în continuare vulnerabilitatea internă majoră, atât timp cât nu va fi suficient informat cu privire la necesitatea şi modurile de protejare a sistemelor informatice, iar cultura de securitate cibernetică va fi insuficientă la nivelul conducătorilor instituţiilor/entităţilor respective;
- *dezvoltarea societăţii informaţionale:* Agenda Digitală pentru Europa 2020 prezintă o viziune asupra viitorului Europei în care va exista o piaţă unică digitală, caracterizată de interoperabilitate crescută, siguranţă şi încredere în Internet, acces mult mai rapid, investiţii în cercetare şi dezvoltare, alfabetizare digitală, aplicarea tehnologiilor informaţiei pentru a soluţiona problemele cu care se confruntă societatea.

În aceste condiţii, lipsa unor strategii şi programe de securitate sau neadaptarea acestora la noile riscuri din domeniu vor permite apariţia de noi breşe de securitate la nivelul reţelelor/ sistemelor IT&C sau diversificarea acestora.

Cum va continua era războaielor cibernetice?

Tehnologia mobilă va deveni tot mai exploatată de către infractorii cibernetici, sens în care ameninţări deja cunoscute în spaţiul tradiţional IT vor prevala şi pe terminalele mobile.

De altfel, conform unui studiu al Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii, la 30 iunie 2013 în România erau active 8,2 milioane de conexiuni mobile de acces la internet de bandă largă, în creştere cu 11% faţă de finalul anului 2012. Astfel, rata de penetrare a accesului la internet la puncte mobile (numărul total de conexiuni raportat la 100 de locuitori) a înregistrat în prima jumătate a anului 2013 o creştere cu peste 5 puncte procentuale, atingând la 30 iunie 2013 un nivel de 56% din populaţie, în timp ce rata de penetrare a conexiunilor la puncte mobile în bandă largă a ajuns la valoarea de 41%.

Activitatea infracţională care se desfăşoară în mediul online are acum noi perspective: consumerizarea malware-ului, instrumete şi servicii de hacking, apariţia valutei digitale şi servicii

de plată anonime.

Cu toate că viruşi semnaţi cu certificate digitale nu sunt o noutate, compania Bitdefender avertizează cu privire la faptul că, în 2014, aceştia vor reprezenta principala tendinţă în industrie. Reprezentanţii sursei menţionate se aşteaptă ca volumul software-ului periculos semnat cu certificate digitale achiziţionate în scop ilegitim să crească foarte mult.

Spam-ul prin email este în scădere, însă reclamele adaptate pe reţelele sociale sunt în creştere. Agresorii cibernetici se vor concentra în 2014 mai mult asupra reţelelor sociale, unde îşi vor ţinti mai bine victimele.

Botneţii vor rămâne coloana vertebrală a oricărei operaţiuni criminale, de la atacuri de tipul Denial of Service, până la trimiterea de spam sau acumularea de Bitcoins în defavoarea victimei. Escrocii se vor concentra pe exploatarea software-ului neactualizat pentru a transforma calculatoarele victimei în componente ale unei reţele de atac. Cei mai mulţi dintre botneţii mari vor utiliza modele de comunicaţii peer-to-peer pentru a nu fi blocate, în timp ce restul vor folosi reţelele sociale pe post de mecanism de comunicare de back-up cu serverele de comandă şi control.

BIBLIOGRAFIE SELECTIVĂ

1. Ameninţări 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 Naţional 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, ediţie online.
4. Revista NATO - Noi ameninţări dimensiunea cibernetică, ediţie 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