RISCURI ŞI AMENINŢĂRI CIBERNETICE LA ADRESA SECURITĂŢII INTERNAŢIONALE. TERORISMUL CIBERNETIC - UN FLAGEL CARE AMENINŢĂ SECURITATEA GLOBALĂ

CYBER RISKS AND THREATS TO INTERNATIONAL SECURITY. CYBER TERRORISM – A SCOURGE THREATENING GLOBAL SECURITY

Gl. mr. (r) prof. univ. dr. Visarion NEAGOE*
Drd. Mr. Silviu-Stelian BORŞA**

Rezumat: *În zilele noastre, totul este controlat de tehnologie şi mai ales de computere. Ameninţările cibernetice la adresa unui sistem controlat se referă la persoanele care încearcă să obţină acces neautorizat la un dispozitiv şi/sau o reţea, folosind o cale de comunicaţie a datelor. Acest acces poate fi direcţionat din interiorul unei organizaţii, de către utilizatori din cadrul organizaţiei respective, sau din locaţii externe, de persoane necunoscute care folosesc internetul. Ameninţări la adresa sistemelor de control pot veni din numeroase surse, printre care guverne ostile, grupări teroriste, angajaţi nemulţumiţi, şi intruşi răuvoitori. Ameninţarea potenţială pe care o reprezintă terorismul cibernetic a declanşat un semnal de alarmă deosebit de serios. Numeroşi specialişti în securitate, politicieni şi alţii au vorbit despre pericolele asociate teroriştilor cibernetici care ar pătrunde în sistemele de computere guvernamentale şi private, producând daune considerabile în domeniile militar, financiar, de servicii ale statelor cu economie avansată. Fără îndoială, terorismul cibernetic este o opţiune foarte avantajoasă pentru teroriştii zilelor noastre, care pun mare preţ pe posibilitatea oferită de acesta de a rămâne în anonimat şi de a provoca pagube considerabile, ca şi pe impactul său psihologic şi atractivitatea pentru media. Pentru a contracara aceste ameninţări este necesară crearea unei bariere cibernetice sigure care să protejeze sistemul; astfel, statele se confruntă cu provocarea de a crea o societate „invulnerabilă" din punct de vedere cibernetic, dar în care să funcţioneze în continuare drepturile şi libertăţile democratice actuale. De asemenea, trebuie găsite soluţii pentru această problemă complicată, fără a întrerupe conexiunile curente şi sistemele aflate în funcţiune în momentul de faţă, astfel încât efectul resimţit de societate să fie menţinut la un nivel acceptabil.*

* Membru corespondent al Academiei Oamenilor de Ştiinţă din Romania, E-mail: visarionneagoe@yahoo.com
** Doctorand la Universitatea Naţională de Apărare „Carol I", E-mail: borsaliviu1979@gmail.com
[1] *Strategia cibernetică de securitate a României*, 2013, p.4.

Cuvinte-cheie: *terrorism cibernetic; extorcare cibernetică; mediu virtual; spaţiu cibernetic; hacker; strategie cibernetică; ameninţare cibernetică; imposibilitate de accesare; reţea; organizaţie teroristă.*

Abstract:. *Nowadays technology and particularly computers are controlling everything. Cyber threats against a controlled system refer to persons who attempt unauthorized access to a device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. The potential threat posed by cyber terrorism has raised considerable alarm. Numerous security experts, politicians, and others have publicized the danger associated with cyber terrorists hacking into government and private computer systems and crippling the military, financial, and service sectors of advanced economies. Cyber terrorism is, to be sure, an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. To protect against these threats, it is necessary to create a secure cyber-barrier around; the states are facing the challenge of creating a "cyber proof" society while maintaining the actual democratic liberties. Also, they have to seek solutions to this complicated issue, without interrupting the current connections and systems in place, so the effect on society is kept to an acceptable level.*

Keywords: *cyber terrorism; cyber extortion; virtual environment; cyber space; hacker; cyber strategy; cyber threat; denial-of-service; network; terrorist organization.*

Introducere

În ultima perioadă, internetul a transformat total linia frontului şi a lăsat strategiile guvernamentale cu mult în urmă. Conflictul modern este purtat on-line între grupuri non-statale, activişti şi corporaţii private, iar peisajul digital se dovedeşte a fi un teren fertil pentru recrutarea şi radicalizarea teroriştilor. Asfel, *„spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând, deopotrivă, oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, dar şi riscuri la adresa funcţionării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră)"*[2].

Alături de beneficiile incontestabile pe care informatizarea le induce la nivelul societăţii moderne, aceasta introduce şi vulnerabilităţi, astfel că asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor

[2] Idem.

actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu[3].

Aşadar, spaţiul cibernetic se află în centrul societăţii moderne. Acest lucru are un impact deosebit asupra vieţii noastre personale, afacerilor şi serviciilor noastre esenţiale. Securitatea cibernetică cuprinde atât sectorul public, cât şi sectorul privat şi se întinde pe o gamă largă de aspecte legate de securitatea naţională, prin terorism, crimă sau spionaj industrial. E-crima sau criminalitatea cibernetică, fie legată de furt, hacking sau refuzul de serviciu la sistemele vitale, a devenit un fapt de viaţă. Riscul de spionaj cibernetic industrial, în care o societate execută atacuri active pe o alta, prin intermediul spaţiului virtual, pentru a obţine informaţii de mare valoare este, de asemenea, foarte real.

Terorismul cibernetic prezintă provocări pentru viitor. Trebuie să fim pregătiţi pentru terorişti care doresc să profite de dependenţa de internet, care este în continuă creştere, pentru a ataca sau a dezactiva sisteme cheie.

Principalele riscuri şi ameninţări cibernetice

Metodele, procedeele şi tehnicile folosite pentru a executa atacuri în mediul cibernetic sunt foarte multe şi în continuă dezvoltare, de aceea riscurile şi ameninţările cibernetice sunt departe de a fi identificate în totalitate. Probabil, chiar în acest moment sunt dezvoltate noi şi noi metode de atac cibernetic, hackerii fiind în permanenţă cu un pas înaintea instituţiilor şi autorităţilor care încearcă să ţină pasul cu dezvoltarea tehnologică. În continuare vom prezenta riscurile şi amenin-ţările identificate până în prezent, această listă putând fi actualizată periodic cu noi metode de atac. Astfel, putem vorbi de următoarele metode de atac cibernetic:

Drive-by exploits

Ameninţările de tip Drive-by pot exploata în mod automat vulnerabilităţi existente în software-ul instalat pe un PC, fără a interacţiona cu utilizatorul de drept. Atunci când un utilizator vizitează un site ce conţine exploit-uri drive-by, se pot exploata vulnerabilităţi în browser, în plugin-urile acestuia sau în sistemul de operare pentru a instala malware pe PC fără ştirea utilizatorului.

Mai există posibilitatea ca atacatorii să conceapă anumite site-uri speciale (false website-uri sau chiar phishing) pentru a infecta pe cei ce îl accesează. Astfel, pentru a determina utilizatorii obişnuiţi să îl viziteze, se apelează la o strategie bazată pe e-mail-uri de tip spam ce conţin link-uri către astfel de site-uri ilegale. Exploit-urile de tip drive-by şi-au extins aria de acţiune din 2012 şi la terminalele mobile, astfel, începînd cu luna mai 2012 apar primele rapoarte cu privire la folosirea acestui instrument de către atacatori pentru exploatarea vulnerabilităţilor sistemului de operare Android.

[3] Idem.

Viermi/Troieni

Viermi: programe care se pot auto-replica. Acestea folosesc reţeaua de calculatoare pentru a-şi trimite propriile copii în alte noduri (calculatoare din reţea), reuşind să facă acest lucru fără intervenţia utilizatorilor. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie ataşat la un program existent.

Troieni: aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidenţiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat. Astfel, troienii constituie marea majoritate a infecţiilor (80%).

Injecţie de cod

Acest tip de ameninţare include tehnici de atac binecunoscute împotriva aplicaţiilor web, cum ar fi SQL Injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. Astfel, atacatorii care generează un astfel de atac încearcă să extragă date, să fure credenţiale, să preia controlul serverului web ţintit sau să îşi promoveze activităţile maliţioase prin intermediul exploatării vulnerabilităţilor de aplicaţii web.

În ultimii ani, cel mai frecvent vector de atac împotriva aplicaţiilor web este SQL Injection. Mai mult de cât atât, atacurile de acest tip sunt populare în rândul grupurilor hacktivist (cum este Anonymus), grupurilor de hackeri (cum este LulzSec) şi în rândurile infractorilor cibernetici (cum este LizaMoon25).

Kit-uri de exploatare

Această categorie se referă la acele software-uri automatizate care ajută atacatorii, mai puţin experimentaţi, în compromiterea sistemelor prin exploatarea vulnerabilităţilor de tip client-side, în special a celor din browsere web sau aplicaţii ce pot fi accesate de site-uri web (de exemplu Adobe Reader, Flash, JRE etc.). Practic, aceste pachete "gata de utilizare" automatizează procesul criminalităţii informatice. De regulă acestea se bazează pe atacuri de tip drive-by download, în urma căruia codul maliţios este injectat în site-urile web compromise.

Botnet

Un botnet reprezintă un set de computere care se află sub controlul unui atacator. Aceste sisteme compromise poartă denumirea de "bots" sau "zombies". Aceasta este o reţea de sisteme informatice infectate care sunt controlate de alte persoane/organizaţii decât deţinătorii acestora. O reţea de tip botnet poate fi utilizată cu scopuri multiple: atacuri de tip „Distributed Denial of Service - DDoS", spamming, furt de identitate, distribuire de malware, infectarea sistemelor informatice etc.

Denial of Service

Un atac de tip Denial of Service este o încercare de a afecta disponibilitatea unor sisteme/servicii informatice sau comunicaţii electronice. Sistemul ţintă este

atacat prin transmiterea unui număr foarte mare de solicitări nelegitime, ce consumă resursele hardware sau software ale acestuia, făcându-l indisponibil pentru utilizatorii legitimi. Astfel, principalele motivări ale atacurilor de tip DDoS sunt hacktivismul, vandalismul şi înşelăciunea.

Phishing

Phishing-ul este o formă de înşelăciune în mediul online care constă în folosirea unor tehnici de manipulare a identităţii unor persoane/organizaţii pentru obţinerea unor avantaje materiale sau informaţii confidenţiale. Atacatorii folosesc diverse tehnici de inginerie socială pentru a-şi determina victimele să-şi dezvăluie datele de autentificare. Ţintele cele mai întâlnite sunt site-urile instituţiilor financiare, precum băncile. Alte ţinte sunt reprezentate de serviciile de plată online, reţelele de socializare, furnizorii de servicii de internet, organizaţiile non-profit, servicii de coletărie sau site-urile unor sectoare guvernamentale.

Compromiterea informaţiilor confidenţiale

Compromiterea informaţiilor confidenţiale se referă la încălcări ale securităţii datelor care au apărut prin dezvăluirea (fie intenţionată, fie neintenţionată) de informaţii confidenţiale de către agenţi interni sau externi. Această ameninţate are ca ţintă informaţii confidenţiale din diferite sectoare, cum ar fi sectorul public de sănătate, organizaţii guvernamentale, întreprinderi mici şi mijlocii etc. Scurgerea de informaţii se realizează de regulă prin hacking, distribuire de malware, atacuri de tip social engineering, atacuri fizice sau prin abuz de privilegii. Un astfel de exemplu este dezvăluirea dosarelor Panama din anul 2016, în urma cărora s-au dat publicităţii nume extrem de importante care fac parte dintr-un sistem offshore prin care încearcă să-şi păstreze veniturile fără a plăti taxe şi impozite în ţările de proveniență.

Rogueware/scareware

Mesaje electronice nesolicitate, de cele mai multe ori cu caracter comercial, care fac publicitate pentru produse şi servicii, fiind folosite de către industria e-marketingului şi de către proprietarii de site-uri cu conţinut indecent. De obicei mesajele spam sunt trimise de către calculatoare infectate cu troieni, care fac parte dintr-un botnet (o reţea de calculatoare compromise şi utilizate pentru trimiterea de spam, sau atacuri asupra unor site-uri de internet, fără ştirea posesorilor calculatoarelor respective).

Atacuri direcţionate

Tip de ameninţare ce vizează o anumită persoană sau organizaţie. Are ca scop fie colectarea de date cu caracter personal/confidenţial sau compromiterea sistemelor informatice ţintă. Acest tip de atac are în general o fază prin care atacatorul se informează prin diverse tehnici (ex. inginerie sociala) asupra

sistemului informatic vizat şi apoi declanşează atacul. De multe ori acţiunile lui par legitime deoarece par a fi venite din partea unei persoane de încredere.

Furt/Pierderi/Distrugere fizică

Furtul fizic, pierderea sau distrugerea efectivă pot fi considerate o ameninţare la adresa securităţii cibernetice. Datorită mobilităţii crescute pe care o oferă laptopurile, telefoanele inteligente sau tabletele, acest tip de ameninţare este pe cale să devină una majoră. În acest sens backup-ul consistent al datelor şi criptarea conţinutului pot fi o soluţie de limitare a pierderilor efective de date sau de divulgare către persoane străine a datelor confidenţiale.

Furt de identitate

Furtul de identitate este o ameninţare reală într-un mediu ce devine pe zi ce trece cu preponderenţă online. Credenţialele de acces sau datele cu caracter personal sunt astăzi ţinta atacatorilor. Odată intrat în posesia acestora, atacatorul poate efectua tranzacţii frauduloase (în special financiare) sau obţine date cu caracter confidenţial.

Scurgere de informaţii

Scurgerea de informaţii se referă la dezvăluirea în mod voit sau nu de informaţii către o persoană neautorizată. Odată ajunse în mâna unei persoane neautorizate aceste informaţii pot fi folosite fie pentru a porni un atac (targeted attacks), fie pentru a avea acces la surse suplimentare de informaţii.

Se cuvine a fi menţionată aici şi scurgerea de informaţii în mod voit prin instalarea de aplicaţii pe telefoanele mobile fără ca utilizatorul să se informeze suficient asupra datelor la care aplicaţia are acces.

Manipularea motoarelor de căutare (SEP)

Acest tip de atac manipulează motoarele de căutare pentru a afişa rezultate de căutare care conţin referinţe către site-uri maliţioase. Există o multitudine de metode pentru a efectua SEP, unul din ele fiind preluarea controlului unor site-uri populare şi includerea de link-uri sponsorizate către site-urile maliţioase.

O altă metodă este SEP via Cross-Site Scripting, în acest caz un motor de căutare este forţat să returneze referinţe către site-uri infestate cu Cross Site Scripting (XSS).

Certificate digitale false

Certificatele digitale false sunt folosite de către atacatori pentru semnarea digitală a resurselor (site-uri web, aplicaţii, coduri sursă etc.) folosite în diverse atacuri cibernetice, cu scopul de a trece nedetectabile de utilizatorul final. Acestea sunt des folosite pentru semnarea aplicaţiilor web maliţioase de tip e-banking sau e-commerce, ce folosesc protocolul HTTPS. Un astfel de certificat poate fi creat sau furat prin exploatarea unor vulnerabilităţi ale asistemelor de tip PKI (Public

Key Infrastructure) ale autorităţilor de certificare, care emit certificate digitale pentru site-uri web securizate.

Metodele de atac cibernetic mai sus prezentate sunt folosite într-un fel sau altul, simple sau combinate între ele, de către hackeri, activişti, hoţi sau terorişti cibernetici.

Terorismul cibernetic – ca ameninţare la adresa securităţii globale

Imaginaţi-vă o armată de infractori informatici care se folosesc de internet pentru a utiliza reţelele de calculatoare asupra cărora au preluat controlul. Folosindu-se de aceste reţele, numite botneturi (de la englezescul „robot networks“, adică „reţele robot“), îşi bombardează ţinta, o ţară anume, cu o mulţime de coduri maliţioase. În câteva minute, site-urile instituţiilor militare, financiare şi comerciale din ţară cad. Bancomatele şi reţelele de telefonie nu mai funcţionează. Avioanele sunt consemnate la sol, iar sistemele computerizate şi cele de siguranţă ale unei centrale nucleare sunt blocate. Cum ar reacţiona populaţia? Cum ar reacţiona instituţiile?

Probabil că scenariul de mai sus pare rupt de realitate. Însă o asemenea situaţie poate apărea şi în viaţa reală. De fapt, atacuri cibernetice au avut loc deja. Este greu de crezut că o organizaţie teroristă are capabilităţile necesare să execute un astfel de atac la ora actuală, însă pe viitor este o posibilitate pe care trebuie să o luăm în calcul. Scenariul mai sus menţionat poate fi însă, pus în practică de către unii actori statali care au dezvoltate aceste capabilităţi cibernetice şi se pot folosi de ele pentru a crea dificultăţi mari altor state unde interesul strategic ”justifică” acţiunile.

În războiul modern, în care sunt implicate două sau mai multe state dar şi organizaţii de diverse tipuri, această armă este tot mai des folosită ca parte a ”războiului hibrid” în combinaţie cu alte arme şi capabilităţi pentru a produce daune şi a afecta mai mulţi piloni sau dimensiuni strategice ale statului agresat.

Strategia cibernetică de securitate a României defineşte terorismul cibernetic ca fiind activităţile premeditate desfăşurate în spaţiul cibernetic de către persoane, grupări sau organizaţii motivate politic, ideologic ori religios ce pot determina distrugeri materiale sau victime, de natură să determine panică ori teroare.[4]

O altă definiţie a terorismului cibernetic este dată de Biroul Federal de Investigaţii al Statelor Unite (FBI). Astfel, în acord cu FBI *terorismul cibernetic* reprezintă orice atac premeditat, motivat politic, împotriva informaţiilor, sistemelor informatice, programelor de calculatoare, precum şi datelor care au ca rezultat violenţa împotriva unor ţinte necombatante, de către grupuri sub-naţionale sau agenţi clandestini. [5]

Spre deosebire de un virus nedorit sau de un atac cibernetic de tip DoS (Denial of Service), un atac terorist cibernetic este proiectat pentru a provoca violenţă sau

[4] Idem, p. 6.
[5] http://searchsecurity.techtarget.com/definition/cyberterrorism

daune financiare extreme. Astfel, posibile ţinte ale terorismului cibernetic pot include industria bancară, instalaţii militare, centrale electrice, centrele de control al traficului aerian, precum şi sistemele de distribuţie a apei. Uneori terorismul cibernetic mai este denumit şi terorism electronic sau război informaţional.

Pentru obţinerea de beneficii financiare este folosită ca metodă *cyberextortion* (şantajul cibernetic). În acest caz este lansat un atac cibernetic greu de controlat împotriva unei companii sau organizaţii, iar în schimbul opririi atacului sunt cerute livrarea anumitor sume de bani în conturi străine şi greu de identificat. În ultimii ani infractorii cibernetici au dezvoltat *ransomware* (ransom din engleză = a răscumpăra) care criptează datele victimei. Aceasta primeşte de obicei un e-mail care oferă cheia de decriptare privată, în schimbul unei plăţi monetare în Bitcoins, o monedă digitală. Cyberextortion poate fi profitabilă, astfel milioane de dolari anual sunt plătiţi ca răscumpărare. Din păcate, ca şi în cazul altor tipuri de deturnări de fonduri, plata nu garantează încetarea atacurilor cibernetice.

În ceea ce priveşte termenul de *terorism cibernetic*, acesta este puţin forţat din punctul nostru de vedere, deoarece este dificilă crearea de panică sau teroare prin intermediul calculatoarelor, cum de altfel definiţia în sine a terorismului caracterizează acest fenomen. Terorismul cibernetic creează prea puţine victime de agresiune fizică sau pierderi de vieţi omeneşti şi uneori deloc. Întradevăr se pot crea dificultăţi, pagube materiale şi financiare extrem de mari, însă efectul psihologic al terorii este creat asupra omului prin ameninţarea şi activarea instinctului de supravieţuire care duce la producerea de panică şi teroare. Deci ca să vorbim de teroare este necesar ca teroriştii cibernetici să producă pierderi de vieţi omeneşti sau cel puţin să amenințe cu acest lucru.

Ar fi posibilă şi realizarea acestor efecte, de exemplu prin identificarea unor grupuri de persoane, cum ar fi personal militar, politicieni, membrii ai unor companii sau instituţii care desfăşoară acţiuni ce contrazic doctrinele şi activităţile organizaţiilor teroriste, publicarea informaţiile personale cum ar fi date despre membrii familiilor, care vor fi ameninţaţi cu moartea, răpirea sau cu mutilarea, anexându-se totodată poze cu alte atrocităţi executate de către aceştia. Acest scenariu poate produce teamă şi panică în rândurile persoanelor implicate chiar dacă acest lucru ar fi greu de realizat.

Dacă luăm ca exemplu organizaţia teroristă Statul Islamic, aceasta are sau pretinde că are dezvoltată ”Divizia Hacking a Statului Islamic”. Aceasta a postat o listă cu 100 de nume şi informaţii personale despre care au susţinut că aparţin personalului militar al SUA. Hackerii au afirmat că deţin aceste date din compromiterea unor baze de date guvernamentale, dar lista a fost de fapt creată prin cercetarea surselor deschise. Conform statisticilor, aceste organizaţii ca ”Divizia Hacking a Statului Islamic” sau ”Cyber Califatul” deţin mijloace şi

personal cu grad scăzut de calificare folosindu-se de software-uri simple. Pericolul vine din partea altor state, care au interes să destabilizeze anumite companii sau instituţii guvernamentale din alte state. Acestea execută atacuri cibernetice complexe în numele acestor grupări teroriste. Un astfel de incident s-a produs, de exemplu, în aprilie 2015 când în numele Statului Islamic au fost compromise reţeaua de socializare, site-ul şi staţia televiziunii TV5 MONDE. Acest lucru s-a dovedit a fi, câteva luni mai târziu, orchestraţia hackerilor ruşi. Există posibilitatea ca aceştia să fi fost plătiţi de către Statul Islamic să execute aceste atacuri, având în vedere faptul că există o piaţă subterană înfloritoare şi astfel de acţiuni pot fi achiziţionate sau închiriate, ori au făcut-o în interes propriu sau al Rusiei.

Statul Islamic, probabil, nu este capabil să execute atacuri complexe în aria terorismului cibernetic, cum ar fi lovirea infrastructurilor critice, deşi şi-ar dori acest lucru. Până în prezent utilizarea spaţiului cibernetic de către această organizaţie s-a limitat în zona operaţiunilor psihologice şi de comunicare.

Ceea ce execută cu succes în mediul virtual organizaţiile teroriste sunt publicitatea acţiunilor sale, radicalizarea şi recrutarea de persoane. Binenţeles că acestea sunt parte componentă a acţiunilor teroriste deci pot fi considerate acte de terorism cibernetic chiar dacă nu produc victime în mod direct. Victimele şi teroarea sunt produse mai târziu prin acţiunile acelor persoane recrutate din mediul virtual şi prin ”îngrozirea” populaţiei civile datorită atrocităţilor la care sunt supuse victimele care ulterior sunt postate pe reţelele de socializare. Există date conform cărora, în ultima perioadă, aproximativ 30 000 de combatanţi străini s-au alăturat jihadiştilor în Siria, în Irak şi în alte ţări, majoritatea fiind contactaţi prin internet şi reţele de socializare.

Având în vedere progresul tehnologiei şi interesul depus atât de organizaţiile teroriste, cât şi de alte state puternice pentru dezvoltarea acestor gen de capabilităţi, în ianuarie 2008, NATO a elaborat pentru prima dată *”Politica NATO privind Apărarea Cibernetică”* punând bazele celor trei piloni ai politicii NATO în spaţiul cibernetic[6]:

1. *Subsidiaritatea*, prin care asistenţa este furnizată numai la cerere, altfel se aplică principiul responsabilităţii proprii purtate de statele suverane;
2. *Ne-duplicarea*, prin evitarea unei duplicări inutile la nivelul structurilor sau al capabilităţilor – la nivel internaţional, regional şi naţional;
3. *Securitatea*, de exemplu, cooperarea bazată pe încredere, luând în considerare sensibilitatea informaţiilor legate de sisteme care trebuie puse la dispoziţie şi posibilele vulnerabilităţi.

[6] http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.html

Astfel, s-au stabilit trei niveluri de ameninţare cibernetică[7]:

Nivelul 1 – „Garden variety" cu următoarele caracteristici: lipsit de experienţă; fonduri limitate; comportament oportunist; vulnerabilităţile ţintei cunoscute; foloseşte viruşi, viermi, troieni rudimentari şi bots; în căutare de senzaţii tari şi publicitate; uşor de detectat.

Nivelul 2 – „Mercenary" cu următoarele caracteristici: abilităţi de ordin superior; bine finanţaţi; activitate orientată/direcţionată; foloseşte viruşi, viermi, troieni, bots ca mijloc de a introduce instrumente mai sofisticate; ţinteşte şi exploatează date valoroase, detectabile, dar greu de atribuit.

Nivelul 3 – „Nation State" cu următoarele caracteristici: tradecraft foarte sofisticat; agenţii intel străine foarte bine finanţate; ţinteşte tehnologii precum şi info; utilizează o gamă largă de tradecraft; stabileşte o prezenţă sub acoperire pe reţelele sensibile dificil de detectat; livrează interdicţii/implanturi hardware.

Conform acestei clasificări, se poate observa cu uşurinţă că, până în prezent, cei mai puternici şi mai periculoşi actori în acest domeniu sunt statele-naţiuni. Nu există nici un dubiu asupra faptului că anumite ţări investesc masiv în capabilităţi de atac cibernetic care pot fi folosite atât pentru a executa acte de terorism cibernetic cât şi în scop militar, aducând beneficii atât de ordin strategic cât şi financiar. Prin faptul că sunt greu de detectat, acţiunile fiind de tip asimetric, agresorul poate să-şi păstreze anonimatul. Un exemplu în această direcţie o reprezintă Coreea de Nord, stat care şi-a dezvoltat, în ultima perioadă, foarte mult, capabilităţile de atac cibernetic. Acţiunile acestui stat au culminat cu atacul din 2014 a studiourilor cinematografice Sony Pictures, acţiune care a coincis cu lansarea filmului "The Interview" distribuit de Sony, în care este prezentat un complot al CIA pentru asasinarea liderului nord-coreean, Kim Jong-Un. Acţiunile au reuşit să creeze panică în rândurile angajaţilor studioului Sony Pictures din Los Angeles, aceştia fiind trimişi acasă şi sfătuiţi să nu se conecteze sub nici o formă la reţeaua informatică a companiei. Acest tip de atac a reprezintă o nouă provocare pentru SUA fiind afectate nu doar funcţionarea computerelor dar şi bazele de date, sistemele de operare şi companiile aflate în legătură cu Sony.

Concluzii:

Având în vedere ritmul de dezvotare al tehnologiei, credem că vom vedea în perioadele următoare atacuri teroriste cibernetice care vor avea ca efect pierderea de vieţi omeneşti, ceea ce va duce cu siguranţă la crearea de panică şi teroare. Cu toate acestea suntem de părere că atacurile cu un astfel de efect vor fi puţine ca număr şi vor provoca mai puţine victime decât ar produce un simplu atac cu o armă de foc.

[7] Idem.

Un alt aspect care trebuie luat în considerare este modul de gestionare al hackerilor. Aceştia sunt prezenţi peste tot şi nu pot fi opriţi. Însă aceştia pot fi exploataţi şi atraşi de partea instituţiilor. Un hacker sau un grup de hackeri poate crea probleme mari statelor şi companiilor. Ei se pot găsi fie de partea celor răi, fie de partea celor buni. De ce să nu facă parte din tabăra celor buni? Aceştia pot fi recrutaţi să lucreze pentru instituţiile guvernamentale, agenţii de informaţii sau pentru armată. Nu toţi hackerii sunt răi. Este bine cunoscut faptul că grupul Anonymus, care este considerat a fi un "Robin Hood" al mediului virtual, au acţionat de foarte multe ori împotriva organizaţiilor criminale sau teroriste. Astfel de cazuri în care au fost implicate grupuri de hackeri sunt multe. De ce să nu existe o bună colaborare între aceste organizaţii şi instituţii? În loc ca aceştia să fie arestaţi pentru încălcarea legii ei ar trebui stimulaţi pentru fiecare aport la bunul mers al lucrurilor. Suntem de părere că avem nevoie de hackeri. Aceştia pot reprezenta sistemul imunitar al internetului. Putem educa generaţiile viitoare de hackeri pentru a acţiona în folosul societăţii.

Latura neagră a mediului virtual şi anume criminalitatea şi terorismul cibernetic vor exista cu siguranţă şi de acum înainte aşa cum vor exista organizaţii criminale şi teroriste în mediul real. Acestea vor intenţiona să-şi dezvolte capabilităţile pentru a-şi îndeplini scopurile maliţioase de a induce teroare fără să fie nevoie de prezenţa lor fizică. Iar acest lucru este posibil numai în mediul virtual.

În concluzie, pentru a gestiona acest fenomen global, care nu are graniţe, statele trebuie să coopereze pentru dezvoltarea tehnologiilor necesare gestionării şi producerii de securitate cibernetică, pentru atragerea de partea lor a organizaţiilor active în mediul virtual şi pentru a educa generaţiile viitoare de hackeri.

BIBLIOGRAFIE

ENISA Threat Landscape 2012, disponibil la www.enisa.europa.eu;
Global Terrorism after the Iraq War (Special Report 111, October 2003);
How Modern Terrorism Uses the Internet, by Gabriel Weimann (Special Report 116, February 2004) disponibil la www.terror.net;
Raport cu privire la alertele de securitate cybernetică primite de CERT-RO în primele 6 luni ale anului 2013;
Strategia cibernetică de securitate a României, 2013;
Terrorism in the Horn of Africa (Special Report 113, January 2004);
The Diplomacy of Counterterrorism: Lessons Learned, Ignored, and Disputed (Special Report 80, January 2002);
http://searchsecurity.techtarget.com

http://www.botfree.ro/articles/pages/ro/2015-05-24-article-general-security-threats.html
http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm
https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html
www.cert-ro.eu
www.computerworld.ro
www.fortinet.com
www.infoworld.com.