MEDIUL DE SECURITATE INFORMAŢIONAL. ATACUL CIBERNETIC – AMENINŢAREA MODERNĂ A SECOLULUI XXI

Raisa Gabriela ZAMFIRESCU*

„The new century risks being overrun by both anarchy and technology. The two great destroyers of history may reinforce each other."
(Cooper, 2007)

Abstract

The 21st century began with remarkable discoveries in countless fields, it has brought along a technological evolution unheard of but together with the positive aspects the negative ones have appeared, the latter being defined by specialists as pervert aspects. Certainly one of the greatest challenges is the one in computing where, according to Eric Schmidt, CEO of Google, starting of 2010, in 48 hours there is produced as many information as before 2010, but it is not knowledge what it is being produced, most of the registered data being noise, reason for which, generally speaking, information services and security structures must reevaluate the paradigm, the operating mode, the working methodologies and instruments. This evolution had and it still has a powerful contribution in transforming and modernizing the risks and threats to the security of a state, asymmetry being presently a success feature for the malware attacks of the new century; most times it is this feature that succeeds in ensuring the necessary strategic advantage.

Keywords: security, intelligence, Digital Age, hybrid warfare, cyber-attack.

Introducere

Una din teoremele cunoscute ale sociologiei atunci când vine vorba de societate şi comunitate aparţine omului de ştiinţă Herbert Spencer care, în activitatea sa de cercetare atât în biologie cât şi în sociologie, a emis teoria conform căreia, societatea este asemeni unui organism biologic, anume aceasta se naşte/se formează, creşte/evoluează, se maturizează iar apoi moare/dispare (Enciclopedia Britannica, 2014).

Societatea este într-o continuă evoluţie şi schimbare, fapt pe care nu îl putem stopa ori înlătura nerămânându-ne decât să acceptăm, să înţelegem

* Academia Naţională de Informaţii „Mihai Viteazul".

şi să lucrăm pentru a preveni ceea ce se poate şi a menţine securitatea naţională, dar şi pentru a fi îndeplinit rolul pe care îl are statul nostru în parteneriatele bilaterale, alianţele şi structurile internaţionale din care este membru. Ceea ce a fost înainte de 1990 ne-a ajutat să înţelegem ameninţările convenţionale, să le putem clasifica şi defini, să formăm un cadru de bază şi un model de analiză la care să ne raportăm în prezent, în această încercare de a cataloga şi eticheta atipicul şi imprevizibilul. Nu este un pattern uşor de realizat însă este cert că se încearcă reactualizarea sa constantă, completându-se periodic prin cotidianul pe care îl definim ca stare de stabilitate şi prin acţiunile întreprinse ce nu se încadrează în constructul securităţii cu toate ramificaţiile sale.

Odată cu această evoluţie constantă a tehnologiei, societatea s-a văzut pusă în faţa unor noi provocări, mediul academic începând a studia şi dezvolta noi ramuri precum netnografia[1], cybercultura, etnografia digitală, în timp ce sectorul securităţii ia contact din ce în ce mai des cu atacuri maliţioase de natură cibernetică. Un bun exemplu îl poate constitui atacul cibernetic la adresa SONY Pictures Entertainment, întreprins la sfârşitul anului 2014, un caz ale cărui ramificaţii s-au extins dincolo de industria entertainment-ului şi de impactul asupra celor în cauză prin invadarea corespondenţei şi publicării informaţiilor cu caracter personal, ajungându-se treptat până la administraţia prezidenţială a Statelor Unite ale Americii, a semnării unui acord trilateral şi nu în cele din urmă la o serie de declaraţii ameninţătoare din partea Coreei de Nord.

Scopul acestui demers este de a puncta evoluţia mediului de securitate în secolul al XXI-lea şi noile ameninţări cu care ne confruntăm atât individual cât şi colectiv ca societate, punctând de asemenea elementele definitorii şi repercusiunile atacului de la SONY Pictures, o anchetă ce este încă în curs de desfăşurare şi un moment considerat critic, un moment ce a schimbat Hollywood-ul modern.

Mediul de securitate

Securitatea unui stat „este un drept imprescriptibil care derivă din suveranitatea deplină a poporului, se fundamentează pe ordinea constituţională (...) are ca domeniu de referinţă valorile, interesele şi

[1] Netnografia este ramura etnografiei care analizează comportamentul internauţilor în exprimarea online a acestora, considerându-se că prin gradul ridicat de anonimitate şi de accesibilitate, toate interacţiunile care se petrec în câmpul virtual sunt catalogate ca fiind mai profunde şi mai complexe decât cele reale, aspecte datorate în special lipsei de consecinţe. Termenul a fost utilizat prima dată de Robert V. Kozinets şi defineşte o metodă mai rapidă şi mai accesibilă pentru cercetători, mai naturală şi mai discretă decât multe alte metode de cercetare, oferind informaţii despre limbaj, comportament, obiceiuri, simboluri, sensuri şi varii perspective culturale.

obiectivele naţionale." (Strategia de Securitate Naţională a României, 2007, p. 7) Pe scurt, aceasta poate fi definită ca protecţie a valorilor, intereselor şi obiectivelor existenţei unui stat, însă, înainte de a o fixa în categoria drepturilor fundamentale, securitatea poate fi definită, pe scurt, ca o situaţie dependentă de structura fiecărui sistem, având un set de particularităţi şi o serie de paradigme care au rămas neschimbate în faţa evoluţiei umane şi a tranziţiei societăţii post-industriale la cea modernă, evoluând ulterior la cea informaţională, actualmente trecând la o societate a cunoaşterii – cu o serie de paradigme ce se regăsesc la nivelul întregii materii vii deoarece nu doar statul necesită securitate ci chiar şi individul, la nivel biologic.

La rândul său, mediul de securitate poate fi definit ca ansamblul de activităţi, acţiuni şi preocupări care evidenţiază starea de securitate, al cărui principal factor de influenţă este globalizarea, proces ce a condus şi încă conduce la evoluţia şi inovaţia riscurilor şi ameninţărilor naţionale şi internaţionale. În ultimii 25 de ani ameninţările din mediului de securitate contemporan şi-au modificat atât caracterul – posibilitatea unui atac din partea altor state democratice este una redusă motiv pentru care trebuie să luăm în considerare ameninţări venite din partea unor actori non-statali ori transfrontalieri –, cât şi forma de manifestare, aceasta din urmă fiind definită în special de inovaţie prin evenimente de tip Lebădă Neagră – evenimente neaşteptate şi neprevăzute din viaţa socială care să fie rare, să aibă un impact deosebit prin consecinţele ulterioare, dar şi un grad de predictibilitate scăzut (Taleb, 2010, pp. 5-17).

Unul din cele mai întâlnite exemple pentru acest tip de evenimente este reprezentat, cu siguranţă de atacurile de la 11 septembrie (9/11). Ceea ce s-a întâmplat pe 11 septembrie 2001 a generat numeroase urmări de proporţii pe toate palierele şi sectoarele societăţii americane şi, într-o lume modernă interconectată, schimbarea paradigmei de securitate la nivel mondial. De asemenea, difuzarea atentatelor în direct de către mass-media a condus la o expunere continuă a fenomenului atacurilor teroriste, provocând instabilitate atât în plan intern pentru Statele Unite ale Americii cât şi în plan extern, în relaţiile şi parteneriatele diplomatice şi strategice. Astfel, 9/11 a devenit un eveniment mediatic care a adus în lumina reflectoarelor Islamul alături de vulnerabilitatea epicentrului capitalismului mondial, ziua fatidică a Americii urmând a fi definită de unii experţi ca ziua în care civilizaţia occidentală s-a ciocnit cu cea musulmană. Prin expunerea excesivă şi agresivă, mass-media a reuşit să creeze noi prejudecăţi şi stereotipuri la nivel social, iar panica şi teroarea răspândită de teroriştii Al-Qaeda prin atentatele din 11 septembrie, dar şi prin alte acţiuni similare ulterioare, au condus la

catalogarea acestora de către John Graz drept „simbol al modernităţii şi un simptom al globalizării" (Barna, 2010, p. 9).

Aceste noi ameninţări atipice şi asimetrice nu pot fi combătute ori prevăzute de state doar în mod individual, iar dacă înainte de 1990 se cunoşteau caracteristicile unui atac armat convenţional, în prezent un stat poate fi atacat mult mai uşor prin lansare unor acţiuni care să vizeze infrastructura naţională economică şi/sau informaţională, acţiune care ar necesita doar achiziţionarea unor sisteme computerizate performante, costuri mult mai reduse decât ar necesita echiparea unei armate. Acesta este unul din motivele pentru care majoritatea ţărilor aderă şi se îndreaptă către alianţe şi parteneriate economice, politice şi/sau militare, formându-se astfel o nouă ordine mondială caracterizată prin fluidizarea graniţelor statale.

Mediul de securitate a evoluat, iar asimetria a devenit o trăsătură de succes pentru atacurile cibernetice ale noului secol şi mileniu, uneori chiar această caracteristică asigurând rezultatul scontat. Asimetria ori iregularitatea unui atac, indiferent de domeniul la care ne referim, oferă un avantaj strategic pentru cel care îl declanşează, elementul de noutate nefiind încadrat în niciunul din pattern-urile deja monitorizate.

Secolul XXI a deputat cu descoperiri remarcabile în nenumărate domenii, a adus cu sine o evoluţie tehnologică fără precedent însă o dată cu aspectele pozitive au apărut şi cele negative, ori cum le numesc specialiştii, efecte perverse. Una din cele mai mari provocări este cea din domeniul informaţional, unde, conform spuselor lui Eric Schimdt, CEO Google, începând cu 2010, în 48 de ore se produc tot atâtea informaţii câte s-au produs până în 2010, însă aceasta nu este cunoaştere, majoritatea datelor fiind zgomot, motiv pentru care serviciile de informaţii şi structurile de securitate în general trebuie să îşi reevalueze paradigma, modul de operare, metodologiile şi instrumentele de lucru, cele patru câmpuri de luptă devenind în prezent cinci: aer, apă, terestru, spaţiu şi cyberspaţiu.

O altă dimensiune a acestei evoluţii este redată de faptul că în prezent, securitatea nu mai este una pur militară, de tipul celei din trecut, când exista o relaţie de egalitate între securitate şi puterea militară, astfel că în prezent, când aducem în discuţie protejarea obiectivelor, valorilor şi intereselor naţionale evidenţiem un sistem amplu de procedee şi măsuri de apărare din care rezultă o clasificare a securităţii la nivel politic, militar, societal, economic, alimentar, informaţional, chiar şi la nivel de mediu înconjurător, biosfera fiind scena tuturor acţiunilor. Pare o modalitate eficace de a evidenţia tipurile de securitate, reuşind a se stabili elementele unei astfel de analize pentru fiecare clasă, având un obiect de referinţă şi o serie de actori implicaţi şi funcţionali la fiecare nivel, însă ele sunt elemente inseparabile ale

constructului securităţii naţionale, motiv pentru care nici atacurile nu mai sunt cele de altădată care să respecte reţeta de atac ori război convenţional, vorbind astfel de acţiuni hibride cu implicaţii la fiecare nivel şi pe fiecare palier al societăţii.

Chiar dacă nu este o modalitate nouă, acceptarea termenului de hibrid şi a unui cumul de acţiuni complexe ce aduce două state ori entităţi în conflict, fără a mai exista neapărat o declaraţie ori o întâlnire militară pe un câmp de luptă, a dat startul unor noi divergenţe. Taxonomia termenului este amplu dezbătută pentru a se putea stabili ce anume include acest nou termen, hibrid, pentru a se putea afla care sunt limitele permise şi de unde anume putem vorbi de încălcarea regulilor.

Până în momentul de faţă, războiul hibrid[2] este definit ca un tip de război fără limite, complex, cu acţiuni pe multiple dimensiuni şi tehnologie modernă ce încearcă a surclasa pregătirea militară, care îmbină războiul convenţional cu regulile şi limitele sale cu asimetria tipică secolului XXI, o formă modernă ce cuprinde mijloace de acţiune care îi permite agresorului să evite atribuirea/însuşirea acţiunilor, ele putând să devină atacuri clandestine (Hunter şi Pernik, 2015, p. 3).

Războiul hibrid se duce pe toate palierele societăţii, prin acţiuni şi sancţiuni economico-financiare (embargo, restricţionarea comerţului, amânarea ori anularea anumitor contracte, blocarea conturilor bancare), politice (excluderea din anumite organizaţii şi alianţe), diplomatice, militare şi nu în ultimul rând la nivel informaţional, **dimensiunea cyber reprezentând unul din punctele forte ale acestei noi forme de conflict.** Cu o societate din ce în ce mai tehnologizată şi mai dependentă de sistemele informaţionale era de aşteptat să apară şi ameninţările la acest nou stil de viaţă ales şi totodată impus.

Secolul XXI – o eră digitală

Sfârşitul Războiului Rece împreună cu globalizarea au dus la o revoluţie informaţională, conducând astfel la diversificarea paletei de riscuri şi de ameninţări pe care orice stat trebuie să le prevină şi să le combată, secolul XXI forţând mediul de securitate la o schimbare de paradigmă, la o îmbinare armonioasă şi eficientă a tradiţionalului cu modernul. Eric Hrovat (2001) a evidenţiat foarte bine că „războiul convenţional (tancuri, avioane, trupe la sol, submarine, rachete, sisteme de apărare) a început să fie înlocuit de *tirurile cifrelor binare*, într-un câmp de luptă diferit. Războiul informaţional

[2] Hibrid – entitate provenită din încrucişarea a doi indivizi de specii, de soiuri, de genuri sau de rase diferite.

este noua artă de subminare a adversarului în noile bătălii. Nu este nevoie să te afli pe câmpul de luptă" (Hrovat, 2001, p. 2), De remarcat este faptul că în trecut a apela la mijloace neconvenţionale de luptă te cataloga ca fiind un oponent slab ce luptă murdar, profitând de vulnerabilităţile adversarului, însă în prezent, tocmai ceea ce ducea la propria denigrare acum se consideră o strategie inteligentă.

Secolul în care trăim este unul digital iar informaţia este o armă ce poate ucide, puterea fiind de partea celui ce o deţine. Trăim într-o societate informaţională în care totul se face online, după noul rit modern, avem conexiune *wi-fi* oriunde ne-am deplasa, tabletele şi/sau smartphone-urile deja sunt un *must have* şi chiar dacă nu le utilizăm la adevărata lor capacitate, tot sunt nişte instrumente de nădejde atunci când vine vorba de reţelele de socializare şi de lipsa privaţiunii auto-indusă odată cu *check-in*-urile, ori cu pozele postate pentru a putea vedea prietenii (şi nu numai) cât de bine te distrezi, cum te plictiseşti, pe unde călătoreşti, care îţi sunt hobby-urile sau orice alt lucru mai mult sau mai puţin insignifiant la care te gândeşti. Unii ar spune că Internetul este un cadou de la Dumnezeu pentru psihopaţi şi persoane cu intenţii rele (criminali şi/sau hărţuitori), această evoluţie uşurându-le cu siguranţă *munca.* Pe baza acestor fapte se poate afirma că evenimentele din 11 septembrie 2001 au demonstrat cum aspectele pozitive ale globalizării, cu tot ceea ce prezintă Occidentul ca fiind evoluţie şi tehnologie modernă, pot fi folosite în sens negativ şi în mod distructiv de către teroriști pentru propria cauză. De asemenea, este de menţionat că una din strategiile lor de recrutare constă în prezentarea materialelor găsite în mediul online în care se regăsesc elemente de violenţă, corupţie, abuzuri, privarea de libertate a cetăţenilor în numele securităţii naţionale, distrugeri, oameni săraci lipsiţi de ajutor ori de vreun sprijin material, pe scurt, „imagini ale disperării" (Barna, 2010, pp. 7-20).

Piraţii Internetului: #GOP şi atacul SONY Pictures

Ultimul sfert de secol a condus la o dezvoltare tehnologică fără precedent, fapt ce a contribuit la formarea unei comunităţi cibernetice ce activează într-un spaţiu fără graniţe geografice/fizice, cyberspaţiul, al cărui câmp de luptă este reprezentat de Internet iar arsenalul, frecvent reactualizat, este redat de New Media (Ghidul OSINT, 2012). Dacă după atacurile din 11 septembrie 2001 presa a fost invadată de articole avându-i în centru pe piraţii aerului, în ultimii ani şi ca urmare a războiului global dus împotriva terorismului, notorietatea acestora a scăzut iar în lumina reflectoarelor au păşit piraţii Internetului, atacurile cibernetice înmulţindu-se considerabil.

Pentru acest nou domeniu s-a structurat rapid o taxonomie a termenilor cyber pentru a se încadra acţiunile *soldaţilor* noului câmp de luptă, astfel că majoritatea tehnicilor convenţionale au primit prefixul „cyber", creându-se astfel termeni precum cyberintelligence, cyberwarfare, cyber manipulation, cyber infiltration, cyber assault, cyber crime, cyber raid, cyber attack (Alford, 2000, p. 105).

Există, totuşi, o confuzie în definirea şi catalogarea atacurilor informaţionale şi a celor cibernetice de tip terorist, astfel că, chiar dacă ambele tipuri se desfăşoară pe acelaşi câmp de luptă, între ele există o serie de diferenţe considerabile, cea mai importantă fiind redată de caracteristica principală a unui atac terorist şi anume, producerea de victime umane. O definiţie completă pentru cyberterorism ce poate fi cotată ca principală distincţie între această formă modernă de terorism şi atacurile cibernetice este furnizată chiar de Biroul Federal de Investigaţii (FBI) care descrie cyberterorismul ca fiind „atacul premeditat, motivat politic împotriva informaţiei, sistemelor informatice, programelor informatice şi datelor, rezultând în violenţa împotriva ţintelor necombatante, de către grupuri subnaţionale sau agenţi clandestini" (Alford, 2000, p. 105).

Atacul cibernetic este una din cele mai grave ameninţări informaţionale ce vizează realitatea virtuală a acestui univers on/offline al secolului XXI, atac ce poate fi întreprins cu mijloace de software, cu produse specifice de atac al parolelor, codurilor de identificare, poştei electronice, acţiuni fără reguli prestabilite ce au ca scop modificare şi/sau distrugerea bazelor de date ori a diferitelor produse prin depistarea vulnerabilităţilor de sistem, a breşelor de securitate şi a furtului de date. Astfel, de atacuri cibernetice pot viza site-urile prezidenţiale (Ucraina, octombrie 2007)[3], bursiere, bancare, ale ambasadelor (august 1997)[4], ori pagini oficiale ale instituţiilor publice şi nu numai, atacuri ce pot escalada cu uşurinţă de la activism şi hacktivism, la cyberterorism dacă ar ataca infrastructuri critice, iar apoi ar bloca serviciile de urgenţă, dacă ar sabota reţelele informaţionale, financiare, electrice, de transporturi ş.a.m.d. De asemenea teroriştii se pot folosi de cyberspaţiu pentru a-şi amplifica efectele atacurilor convenţionale. Avantajele atacurilor cibernetice se pot regăsi în anonimatul atacatorului, în lipsa unor frontiere geografice, în accesibilitatea şi în costurile reduse ale aparaturii şi, nu în ultimul rând, în popularitatea care poate fi dobândită

[3] Ucraina, octombrie 2007: atacul cibernetic asupra site-ului preşedintelui Viktor Iuşcenko de către ramura tânără a Mişcării pentru Eurasia, atac ce a blocat website-ul timp de 3 zile.
[4] August 1997: blocarea site-urilor mai multor ambasade din Sri Lanka timp de două săptămâni de către Gruparea Tigrii Negrii, grupare legată de Tigrii Eliberării din *Tamil Eelam*, supraîncărcând poşta electronică cu peste 800 de e-mail-uri.

cu uşurinţă prin asigurarea unui public martor, o audienţă ce poate fi transformată rapid în ţintă.

Soldaţii noului *câmp de luptă* se împart în diferite categorii de genul hackerilor black hat/white hat[5], crackerilor[6], au un limbaj propriu (*leet*)[7], tehnici de luptă personalizate domeniului în care activează – phishing[8], spoofing[9], juice jacking[10] ş.a.m.d., şi nu în ultimul rând, instrumentele/armele necesare pentru atacul de malware – botnets, viruşi ori viermi informaţionali care profită de acele zero-day[11] din aparatura utilizată la nivel mondial. Deep Web ori Dark Web au devenit termeni cunoscuţi de majoritatea chiar dacă pătrunderea în aceste zone ale internetului necesită cunoştinţe în domeniu.

Unul dintre atacurile cibernetice care au ţinut prima pagină a ziarelor în Statele Unite ale Americii este cel la adresa Sony Pictures Entertainment de la sfârşitul anului 2014, la nici trei ani de la atacul Sony PlayStation, care a provocat serioase pagube financiare şi de imagine. Menţionam că astfel de atacuri s-au înmulţit, motiv pentru care trebuie amintit că, în septembrie 2014, Apple a fost ţinta unui atac cibernetic asupra contului deţinut de companie în sistemul iCloud, făcându-se publice mai multe poze (în mare parte nud) cu vedete celebre din cetatea filmului. Ameninţările au continuat, iar după ce, în data de 24 noiembrie, sistemul informatic SONY Pictures din Cluver City a fost blocat şi închis ulterior pentru motive de siguranţă şi investigaţii, angajaţii revenind la lucrul cu foaia şi creionul, de Crăciun, o altă entitate a atacat serviciul Playstation, dar şi consolele Xbox de la Microsoft. Stabilit fiind deja faptul că cele două atacuri au avut autori diferiţi, cele întâmplate în luna noiembrie 2014 au fost revendicate de grupul intitulat #GoP aka Guardians of Peace, iar în decembrie 2014 de Lizard Squad, o entitate virtuală despre care nu se cunoaşte pentru moment dacă este un

---

[5] Black hat hacker: persoană care pătrunde ilegal şi cu intenţii malițioase în software-ul unor device-uri. White hat hacker: persoană care pătrunde legal în software-ul unor device-uri fiind un expert în securitatea informaţională.

[6] Cracker: persoană care se ocupă exclusiv cu spargerea parolelor şi/sau schimbarea ulterioară a acestora.

[7] Noul alfabet *leet* folosit de comunitatea închisă de gameri şi de hackeri în spaţiul virtual pentru ca activitatea lor să fie mai greu de depistat.

[8] Phishing: acţiunea de a trimite e-mail-uri frauduloase pentru a infecta device-urile de pe care sunt accesate cu scopul de a fura informaţiile stocate.

[9] Spoofing: acţiunea prin care un program ori un device este manipulat să arate şi să se comporte ca un altul în scop fraudulos.

[10] Juice jacking: intruziune frauduloasă prin folosirea unui cablu de alimentare de tip USB, acţiune prin care se poate instala un malware şi/sau accesa, copia informaţii. Dispozitivele vulnerabile sunt cele de tip smart (telefon, tabletă) .

[11] Zero-Day: vulnerabilitate în soft-ul device-urilor necunoscută de producător, ce poate fi exploatată de hackeri.

grup ori un singur individ, însă se poate spune că este de cuvânt deoarece acesta a anunţat încă de la începutul lunii că urmează *un cadou* de Crăciun.

Pe scurt atacul de la Sony Pictures Entertainment, considerat ca cel mai mare atac informatic, a început în data de 24 noiembrie 2014, când angajaţii Sony Pictures din Culver City au primit un mesaj ce le-a blocat sistemul informatic (telefoanele, poşta electronică, computerele), pe desktop-ul calculatoarelor afişându-li-se o poză cu un schelet şi titlul „Hacked by #GOP" (fig. 1). Pentru moment aceştia nu au precizat motivul atacului, însă pagubele estimate s-au ridicat la furtul a aproximativ 10 TB (terabiţi) de date secrete şi strict secrete de pe serverele Sony Pictures.

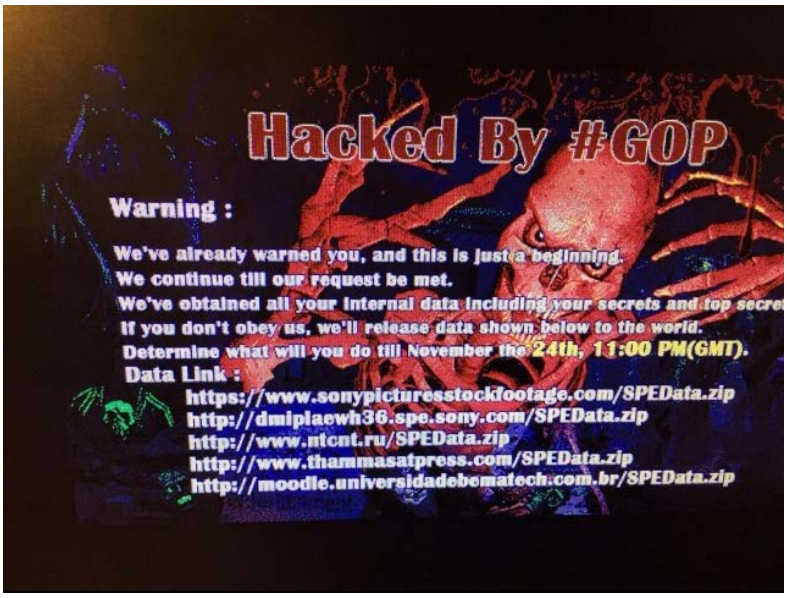

Figura nr. 1 – mesajul primit de angajaţii Sony Pictures în 24.11.2014
Sursa: https://pmcdeadline2.files.wordpress.com/2014/11/hacked-by-gop-sony-pictures-under-attack.png?w=970

După trei zile de tăcere, a urmat o nouă acţiune din partea hackerilor, GoP urcând pe hub-urile online, aka Torrente cinci filme noi ale studioului – acestea au fost extrase la atacul din 24 noiembrie, fiind versiuni de DVD de tip promoţional. Din cele cinci producţii Sony, doar unul a fost lansat până la acea dată, mai precis filmul cu Brad Pitt „Fury", producţia devenind rapid al doilea

cel mai piratat film cu peste 1 milion de download-uri cu adrese unice de IP. Alături de acesta au mai fost postate şi versiuni complete a patru filme în curs de apariţie: „Annie", „Mr. Turner", „Still Alice" şi „To Write Love On Her Arms".

În 28 noiembrie au apărut primele speculaţii conform cărora în spatele atacului cibernetic întreprins de gruparea intitulată Guardians of Peace s-ar afla chiar Coreea de Nord, făcându-se legătura cu premiera comediei „The Interview", iar pe 1 decembrie, Internetul a fost încă o dată bombardat de informaţii confidenţiale sustrase de pe serverele companiei Sony Pictures: bugete de producţie, parole, protocoale de securitate, informaţii despre vedete, pseudonime ale acestora pentru rezervări, date de naştere, adrese, numere de asigurare socială ale angajaţilor şi nu numai, salariile celor mai bine plătiţi 17 oficiali ai companiei, dar şi ale altor 47.000 de angajaţi şi colaboratori şi, nu în ultimul rând, o serie de e-mail-uri din cadrul unor conversaţii cu caracter ofensator la adresa unor nume celebre de la Hollywood, dar şi la adresa preşedintelui Barack Obama (potrivit Mediafax.ro).

După această acţiune, şefii Sony Pictures, Michael Lynton şi Amy Pascal, au făcut primele declaraţii oficiale catalogând atacul ca fiind unul maliţios, implicând totodată şi FBI-ul. Lucrurile au escaladat treptat, iar investigaţiile sunt în curs de desfăşurare, însă chiar dacă Coreea de Nord a continuat să nege vehement implicarea sa în atacul cibernetic întreprins de GoP, anchetatorii au reuşit să urmărească o serie de reziduuri virtuale identificându-le ca aparţinând strict de sistemele şi serverele accesibile doar în Coreea de Nord – informaţii furnizate la sfârşitul lunii decembrie într-o declaraţie a directorului FBI, James Comey (Agerpres.ro, 07.01.2015).

Piesa centrală a întregului atac cibernetic este producţia Sony Pictures, „The Interview", o comedie cu un buget de 44 milioane dolari SUA, ce prezintă o tentativă fictivă de asasinare a liderului nord-coreean Kim Jong-un. Filmul a fost unul controversat încă de la început, Phenianul solicitând încă din luna iunie a anului 2014 să fie blocat. Neacceptând cenzura impusă, Sony a amânat totuşi premiera din octombrie 2014, făcând o serie de modificări ale finalului privind moartea dictatorului. După patru variante modificate şi chiar acordul preşedintelui japonez Sony, Kazuo Hirai, producătorul şi actorul Seth Rogen a considera, într-un e-mail adresat co-preşedintei Sony, Amy Pascal, conversaţie făcută publică de GoP, că „acesta este acum povestea americanilor care schimbă filmul pentru a-i face fericiţi pe nord-coreeni. Este o poveste condamnabilă"(Mediafax.ro).

Decizia studioului de a nu amâna premiera a dus la o nouă serie de ameninţări din partea hackerilor, în urma cărora FBI a avertizat cinematografele de posibile atacuri şi astfel lansarea oficială a filmului a fost

anulată, acţiune ce a provocat un val de nemulţumiri la Hollywood dar şi în rândul administraţiei prezidenţiale, considerându-se un act de predare: ***„În curând, lumea va vedea ce film prost a făcut Sony Pictures Entertainment. Lumea va fi plină de temeri (...) Aduceţi-vă aminte de 11 septembrie 2001. Vă recomandăm să vă ţineţi la distanţă de acele locuri (în care va fi proiectat filmul). Iar dacă locuinţa voastră este în apropiere, ar trebui să plecaţi de acasă. Tot ce se va petrece în zilele viitoare va fi din vina SPE. Lumea întreagă va denunţa Sony*" (Mediafax.ro).**

Concluzii

Chiar dacă se credea că totul este pierdut, toată publicitatea şi controversa au pornit un adevărat război pentru libertatea de exprimare într-un stat democrat, iar filmul a reuşit să fie proiectat în peste 500 de săli de cinema independente din Statele Unite ale Americii. La 8 ianuarie 2015, acesta înregistra încasări din vânzarea biletelor de aproximativ 5 milioane dolari SUA şi era pus la dispoziţia publicului în mediul online pe cele mai cunoscute platforme, pentru închiriere ori achiziţionare. Site-urile care s-au înscris la streaming au fost GooglePlay, YouTube Movies, Xbox Video Microsoft şi pagina oficială www.seetheinterview.com, acestora adăugându-li-se în 28 decembrie Apple cu serviciul iTunes. Din difuzarea online, filmul a reuşit să strângă (prin preţurile de 5,99 dolari SUA şi 14,99dolari SUA), pînă la data de 8 ianuarie 2015, 31 de milioane dolari SUA, având încasări finale de 38 milioane dolari SUA. Astfel, „The Interview" devenea filmul online numărul unu al Sony Pictures.

Consecinţele nu au întârziat să apară, iar o serie de coincidenţe nu fac decât să întărească suspiciunile unora că totul a fost planificat. Chiar dacă mai sunt conspiraţionişti care plasează atacul ca pe o strategie de marketing Sony pentru promovarea unui film de mâna a doua (şi care a reuşit să împartă lumea criticilor în două tabere), escaladarea tensiunilor dintre Statele Unite şi Coreea de Nord, ca de altfel şi implicarea FBI, par a contrazice această ipoteză. În cadrul Sony Pictures Entertainment a avut loc o serie de demiteri, iar mai mulţi angajaţi au depus o plângere comună pentru că nu li s-au protejat informaţiile cu caracter personal şi confidenţial – mesaj postat pe site-ul oficial de către Sony (www.sonypictures.com).

La nivel oficial şi diplomatic au fost făcute o serie de declaraţii, preşedintele Barack Obama catalogând atacul cibernetic ca pe un act de vandalism care va aduce represalii pentru vinovaţi (luându-se în calcul chiar reincluderea pe lista statelor ce sprijină terorismul, listă de pe care Coreea de Nord a fost scoasă în 2008, după ce în ianuarie 2002 preşedintele de la acea vreme, George W. Bush, a nominalizat statul pe axa răului, alături de Iran şi

Irak), în timp ce liderul Kim Jong-un şi administraţia sa a declanşat o serie de ameninţări şi jigniri, motiv pentru care unii specialişti consideră că acesta este începutul unui război cibernetic între cele două naţiuni: *«Contraatacul nostru cel mai dur va viza Casa Albă, Pentagonul şi continentul american, fosa septică a terorismului, şi va depăşi cu mult „contraatacul simetric" anunţat de Obama».* – Comisia Națională de Apărare nord-coreeană (NDC) (Agerpres.ro, 21.12.2014).

O primă acţiune din partea SUA a fost întreruperea masivă a conexiunii la Internet şi reţele 3G dintre Coreea de Nord şi celelalte state, represalii nerecunoscute oficial însă acceptate chiar prin declaraţia purtătorului de cuvânt Maria Harf: „(...) printre răspunsurile noastre, unele vor fi vizibile, altele nu" (Agerpres.ro, 26.12.2014). Acestea au continuat cu semnarea unui acord trilateral între Statele Unite ale Americii, Japonia şi Coreea de Sud, acord privind schimbul de date confidenţiale la adresa proiectului nuclear al Phenianului, care prevede că orice informaţie cu caracter confidenţial să fie transmis celor două ţări asiatice prin intermediul Washington-ului (Agerpres.ro, 26.12.2014). O altă decizie luată de preşedintele Barack Obama, de această dată cu aplicabilitate internă, este revizuirea şi consolidarea strategiei cibernetice a Statelor Unite.

Investigaţiile continuă, Sony Pictures încearcă să remedieze ce se poate, lupta ducându-se acum la nivel de administraţii prezidenţiale. Este cert că atacurile cibernetice au devenit o mare problemă pentru societatea actuală, atacuri ce pot escalada în adevărate probleme globale, mai ales că mijloacele care pot fi utilizate ca principale arme de către piraţii Internetului sunt dispozitive indispensabile în viaţa cotidiană a secolului XXI, a erei digitale.

Referinţe bibliografice:

1. *Agerpres – Actualizează lumea*. *Sony Pictures*. http://www.agerpres.ro/views/site/pages/content/searchResults.html?q=sony+pictures [Online] (accesat în perioada 6-8.04.2015).
2. Agerpres.ro: http://www.agerpres.ro/externe/2014/12/21/phenianul-meninta- washingtonul-cu-represalii-daca-sua-vor-sanctiona-rpdc-in-scandalul-sony-18-47-42 .
3. Agerpres.ro: http://www.agerpres.ro/externe/2014/12/26/acord-sua-japonia- coreea-de-sud-pentru-schimb-de-date-confidentiale-vizand-programul-nuclear-nord-coreean-14-27-50.

4. Agerpres.ro: http://www.agerpres.ro/externe/2015/01/07/directorul-fbi-hackerii-au-fost-neglijenti-in-atacul-informatic-asupra-sony-si-au-folosit-servere-nord-coreene-20-39-27.
5. Alford JR., Lionel D. (2000). *Cyber Warfare: Protecting Military Systems.* [Online] http://www.dau.mil/pubscats/pubscats/AR%20Journal/arq2000/alford.pdf (accesat la 7.04.2015).
6. Antipa, Maricel (2010). *Triumviratul dezastrului global*, Bucureşti: Editura Monitorul Oficial.
7. *Analiza de intelligence.* (2013) Curs nepublicat, susținut în cadrul prelegerilor de Analiza Informațiilor: OSINT în cadrul Facultății de Sociologie și Asistență Socială, Universitatea din București.
8. Barna, Cristian (2010). *Terorismul, ultima soluție? Mărirea și decăderea Al-Qaīda*, București: Editura Top Form.
9. Cooper, Robert (2007). *Destrămarea națiunilor. Ordine și haos în secolul XXI*, Bucureşti: Editura Univers Enciclopedic.
10. Deadline.com (22 decembrie 2014). *Sony Hack:A Timeline.* [Online] http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ (accesat la 6.04.2015).
11. Encyclopaedia Britannica (2014). *Herbert Spencer*. [Online] http://www.britannica.com/EBchecked/topic/559249/Herbert-Spencer (accesat la 10.04.2015, 10:17).
12. *Ghid OSINT*. (2012) [Online] http://www.sri.ro/upload/Ghid_OSINT.pdf (Accesat la 4.04.2015).
13. Hrovat, Eric (2001). *Information Warfare: The Unconventional Art in a Digital World*. [Online] http://www.sans.org/reading_room/whitepapers/warfare/information-warfare-unconventional-art-digital-world_787 (accesat la 6.04.2015).
14. Hunter, Eva și Pernik, Piret (2015). *The Challenges of Hybrid Warfare.* [Online]http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf (accesat la 7.05.2015).
15. Kozinets, Robert V. (2010) *Netnography: Doing Ethnographic Research Online*, London: SAGE.
16. Mediafax.ro. *Sony*. http://www.mediafax.ro/tags/sony [Online], (accesat în perioada 6-8.04.2015).
17. Mediafax.ro: http://www.mediafax.ro/cultura-media/sony-pictures-incearca-sa-diminueze-unda-de-soc-dupa-atacul-informatic-asupra-serverelor-sale-13718290.
18. Mediafax.ro: http://www.mediafax.ro/life-inedit/filmul-despre-kim-jong-un-scena-mortii-liderului-nord-coreean-considerata-inacceptabila-si-modificata-de-mai-multe-ori-video-13723225.
19. Mediafax.ro: http://www.mediafax.ro/externe/piratii-cibernetici-au-amenintat-studiourile-sony-evocand-atentatele-din-11-septembrie-2001-13725818.

20. Petrescu, Stan, coord. (2007). *Asimetriile prezentului – Contraterorism vs. Terorism. Terorismul cibernetic*, Bucureşti: Editura Academiei Naţionale de Informaţii.
21. http://www.sonypictures.com/corp/notification/SPE_Cyber_Notification.pdf?#zoom=100.
22. *The 2014 Counterterrorism Calendar. Modus Operandi – cyber attack*. (2014) Bucureşti: Serviciul Român de Informaţii, 2014.
23. Taleb, Nassim Nicholas [2007] (2010). *Lebăda Neagră. Impactul foarte puţin probabilului*, Bucureşti: Editura Curtea Veche.