NR.31 | 2016

Intelligence

în serviciul tău

CYBERSPACE, NOUL TEATRU DE RĂZBOI

CTRL + ALT + SECURE!

CTRL+ALT+SECURE

DIRECTORUL SERVICIULUI ROMÂN DE INFORMAȚII
EDUARD HELLVIG

O nouă dimensiune a atacurilor *cyber* a devenit realitate la 23 decembrie 2015. Un grup de *hackeri,* cu o afiliere încă incertă, a scufundat în întuneric pentru câteva ore o regiune din vestul Ucrainei. Prin dezactivarea unei părți importante din infrastructura de electricitate a țării, obiectivul evident al acestui atac a fost să demonstreze vulnerabilitatea serviciilor publice în fața ingeniozității tehnologice folosite în scop distructiv.

Nu este primul semnal de alarmă al impactului pe care îl poate avea un atac cibernetic. În **aprilie 2015**, emisia postului francez de televiziune **TV5Monde**, concomitent cu site-ul și conturile de rețele sociale ale acestuia, au fost deturnate de un grup de *hackeri* afiliați **Daesh**. Jihadismul *online* nu mai are doar înfățișarea propagandei, ci și a agresivității războiului hibrid.

Amenințările *cyber* nu mai sunt, în acest fel, doar un concept abstract. Acest nou tip de agresiuni îi afectează fără discriminare nu doar pe aceia dintre noi care sunt conectați la spațiul *online,* ci și pe cei care nu folosesc tehnologii avansate. Orice societate devine vulnerabilă în fața acestui flagel.

Acestei realități îngrijorătoare și dinamice, profesionalismul specialiștilor în informații trebuie să îi răspundă printr-un schimb de informații susținut și o expertiză solidă. Ca instituție aflată în serviciul cetățenilor, avem datoria unei adaptări permanente a procesului de *intelligence* pentru a răspunde cât mai eficient amenințărilor cibernetice.

Suntem nevoiți, astăzi mai mult ca oricând, să abordăm diferit mediul de securitate, îndeosebi prin adaptabilitate și capacitate de reacție rapidă. Din păcate, trăim într-o lume în care cetățeanul constată că a devenit, el însuși, o țintă a unor amenințări care au atins cote alarmante.

Pentru **România**, apartenența la **NATO** și **UE** a redus riscul unui conflict armat pe teritoriul nostru. Însă pericolul nu a dispărut, ci s-a mutat în spațiul cibernetic, alimentat de evoluția inevitabilă a tehnologiilor.

Din fericire, țara noastră dispune de o resursă umană de excepție în domeniul informatic, după cum o demonstrează și tinerii de elită din echipa **Centrului Național Cyberint** al Serviciului Român de Informații. Grație expertizei în zona IT, Serviciul se bucură astăzi de o recunoaștere în plan internațional ca instituție de top în *cyberintelligence*. Acest fapt ne permite să ne consolidăm poziția în formatele multilaterale de cooperare din care facem parte, în **NATO** și **UE**.

Această performanță se datorează eforturilor susținute de optimizare în utilizarea resurselor. Menținerea acestui atu de care dispunem impune, în același timp, inovație și continuitate.

Spun inovație, pentru că securitatea cibernetică a României are, în primul rând, nevoie de o legislație pusă în acord cu epoca digitală. Nu ne putem permite să abordăm amenințările mileniului III cu instrumente legale concepute în secolul trecut, tributare unui mod de gândire convențional.

În ceea ce privește continuitatea, doar printr-un parteneriat durabil cu societatea românească, prin deschidere și comunicare publică putem spera să îi convingem pe cei mai potriviți profesioniști în IT că este o chestiune de onoare și mândrie să se alăture echipei noastre.

Experiența din *intelligence* ne arată că eficiența e posibilă doar în parteneriat cu cetățenii în serviciul cărora ne îndeplinim misiunile.

Intelligence
SUMAR

Nr. 31 / 2016

Intelligence

Redactor-Șef: Ferah Bănică
Art Director: Alex Revega
Editori: Marius Bercaru
Andreea Gheorghițescu
Ancuța Crăciun
Mihai Dinescu
Oana Veliciu
Fotografii: Victor Levițchi
Shutterstock
Arhiva SRI

Contact: intelligence@sri.ro
Difuzare: 0377.723.673
Adresa redacției: București, bd. Libertății, nr. 14

ISSN 1844-7244

SECURITATEA CIBERNETICĂ

DE LA „PERLA COROANEI“ ÎN IT SPRE „BUSINESS AS USUAL“ ÎN SOCIETATE

de general-locotenent Florian COLDEA

În ultimele două decade am fost martorii unui **alt fel de „revoluție”**, **a informației**. Este o revoluție prin care formidabila putere de calcul a calculatoarelor și a tot mai diversificatelor dispozitive fixe sau mobile este conectată în rețele de bandă largă, adevărate autostrăzi informaționale ce leagă întreaga lume. Aceasta a condus la folosirea tehnologiei informaționale (IT) în fiecare domeniu al activității umane, de la comunicare, comerț, divertisment, educație și socializare la management și guvernare.

Spațiul cibernetic s-a extins rapid, ajungând să se suprapună peste majoritatea sferelor „clasice” ale vieții fiecăruia dintre noi. Practic, mașinile pe care le conducem astăzi dispun de o capacitate de procesare a datelor mai mare decât cea pe care se puteau bizui vehiculele ce au dus primii oameni pe Lună. La sfârșitul anului 2015, 45% din populația întregii lumi, aproximativ 3,2 miliarde de persoane, are acces la Internet. În România, conform INS, peste jumătate dintre gospodării dețin un calculator cu acces la Internet, iar dintre acestea peste 70% sunt in mediul urban, iar numărul de utilizatori ai Internetului crește exponențial odată cu democratizarea accesului direct de pe telefoanele mobile. În plus, conform datelor existente în prezent, țara noastră dispune de o foarte bună viteză a rețelei, fiind printre cele mai rapide din Europa și chiar din lume.

Fiecare dintre noi poate să cumpere, să joace sau să caute *online* informațiile de care are nevoie – și poate face acest lucru chiar și de pe o bancă din parc, nemaifiind legați de „glia” computerului de birou sau a cablului de net.

Este evident și dincolo de orice contestare faptul că extinderea rețelei de Internet și a întregii game de servicii și posibilități pe care aceasta le aduce constituie un pilon important pentru dezvoltare. Există însă și **o provocare extrem de importantă** care este asociată acestei evoluții: **asigurarea securității** întregului spațiu cibernetic. Dacă nu se poate asigura circularea securizată a datelor dinspre și către milioanele de utilizatori, vom constata că odată cu spațiul cibernetic vor crește exponențial și spețele de criminalitate cibernetică, de spionaj cibernetic, de afectare a infrastructurilor ce depind de acest spațiu, precum și alte potențiale viitoare riscuri pe care în prezent probabil că încă nu reușim să le intuim.

Atunci când Internetul a fost creat, iar protocoalele pe care acesta se bazează au fost dezvoltate, nimeni nu și-a imaginat că se crea în fapt **încă un mediu de ducere a războiului**, alături de cele deja clasice: pământ, aer, apă și (cf. unor autori) spațiul extra-terestru. Este un mediu de luptă aparte, cu o anvergură revizuită a actorilor (de la state și până la indivizi), în care atacurile se duc prin biți, viruși sau troieni, în care spionajul urma să fie la ordinea zilei și în care nu doar oamenii pot fi „recrutați”, ci întregi sisteme IT pot fi puse sub control. Ca urmare a versatilității și mobilității specifice „armelor” sale, agresiunea cibernetică a devenit deja un element foarte important în **mixul operațional specific războiului hybrid**.

Spațiul cibernetic a fost proiectat astfel încât să funcționeze în mare măsură pe o **prezumție de încredere**, cea care a și făcut posibilă *upgradarea* sa succesivă de la câteva sute la miliarde de utilizatori, practic, pentru toate aspectele activității umane. Această caracteristică aparte face posibil ca odată cu gradul de interconectare al unei comunități sau națiuni să crească și nivelul de vulnerabilitate față de atacurile cibernetice.

Din acest punct de vedere, **chiar și cele mai puternice și avansate state sunt expuse riscurilor** generate de alte state sau chiar de grupări ori indivizi foarte motivați. În ceea ce privește direct **România**, s-au remarcat prin agresivitate atacurile cibernetice **Red October** și **MiniDuke** ori cel desfășurat prin intermediul **Wipbot/Epic** (și multe altele, necunoscute publicului larg, care au vizat instituții de stat și obținerea accesului la rețele informatice de interes național și exfiltrarea de date confidențiale). De asemenea, au atras atenția spionajul cibernetic, activitățile de criminalitate organizată informatică și, într-un plan secundar, *hacktivism*-ul, fiind identificați și arestați membrii mai multor grupări care au lansat atacuri informatice asupra instituțiilor din țara noastră.

LA NIVEL MONDIAL, 3,2 MILIARDE DE PERSOANE, AU ACCES LA INTERNET

Astfel, s-a ajuns în situația în care securitatea cibernetică și războiul cibernetic sunt adesea invocate chiar în aceeași propoziție. **Securitatea cibernetică** face trimitere la asigurarea viabilității unui mediu care a ajuns să fie vital pentru standardul de viață și chiar pentru stabilitatea societății moderne. **Războiul cibernetic** descrie acțiunea unor actori (adesea cu susținere statală) de a exploata vulnerabilitățile acestui spațiu în diferite scopuri, care ajung astfel să afecteze esența/natura însăși a spațiului cibernetic. Ceea ce complică și mai mult lucrurile este că nu există încă o definiție universal acceptată pentru *cyber warfare*, iar raportarea la această problematică variază de la convingerea că luptele cibernetice sunt inevitabile la opinia că riscurile și pericolele de acest tip ar primi o atenție disproporționată.

Însuși **conceptul integrator de securitate națională** a suferit o serie de **transformări** în ultimele decenii. Acesta nu mai echivalează cu securizarea frontierelor terestre, a spațiului aerian și a apelor teritoriale. Securitatea națională a evoluat către o abordare multidimensională ce acoperă securitatea militară, politică, economică, energetică, de mediu și cibernetică. Se subînțelege astfel că provocările aduse de spațiul cibernetic în planul securității naționale trebuie identificate, iar o serie de acțiuni specifice inițiate pentru a putea preveni sau limita transformarea acestora în amenințări la adresa valorilor și intereselor de securitate consacrate și protejate de societate. Acestea sunt cele care constituie coloana vertebrală a unei strategii sectoriale de securitate cibernetică.

Rămâne în continuare foarte puțin probabil ca problemele Internetului să poată fi rezolvate de o autoguvernare a comunității globale ce deține infrastructurile critice, respectiv sectorul privat, iar guvernele să se limiteze la jucarea unui rol minimalist. O componentă semnificativă a amenințării cibernetice este determinată de spionajul statal, de criminalitatea informatică susținută de unele state și de capabilitățile ofensive pe care acestea le dezvoltă, astfel încât, *nolens volens*, **nivelul statal trebuie să joace în continuare un rol esențial** în gestionarea acestei problematici.

Securitatea cibernetică este o dimensiune a securității naționale și a aplicării legii, iar responsabilitatea centrală a gestionării le revine statelor prin propriile servicii de informații și, *in extenso*, prin instituții de aplicare a legii. **Pentru serviciile de informații**, ca și pentru societate în general, este foarte important să își dezvolte capacitatea de a gestiona acest nou tip de amenințări. Caracterul schimbător al acestora, precum și capacitatea de a potența sau modifica modul de manifestare al amenințărilor deja clasice, presupun **o coerență aparte** pe latura de prevenire și contracarare, precum **și o acțiune concertată** pe mai multe planuri: tehnologic, organizațional și legal.

Din punct de vedere tehnologic, devine evident că a dispune de sisteme IT solide este esențial pentru securitatea cibernetică, pornind de la infrastructurile critice și până la soluțiile tehnice menite să conducă la creșterea rezilienței în fața unor atacuri de aceste tip.

Organizațional, securitatea cibernetică este mult prea importantă pentru a fi lăsată numai în responsabilitatea structurilor și a specialiștilor IT. Sunt foarte multe aspecte pe care cei din afara zonei de IT trebuie să le aibă în vedere, chiar dacă nu dispun de o înțelegere aprofundată sau specializată în domeniul tehnologiei. În fapt, întreg personalul trebuie format în sensul unui comportament profesional prudent din perspectivă cibernetică (*cyber-safe*), iar procesele organizaționale trebuie proiectate și configurate astfel încât să nu expună instituția sau organizația unor riscuri cibernetice inutile.

Legal, este nevoie de stabilirea unor reguli și limite de acțiune suficient de flexibile pentru a fi aplicabile unui domeniu în continuă evoluție, dar și suficient de clare pentru a nu expune arbitrariului și incertitudinii nici cetățenii, și nici instituțiile cu responsabilități.

Se acuză uneori faptul că preocuparea de asigurare a securității cibernetice ar putea limita potențialul inovator de dezvoltare, specific Internetului. Este drept că măsurile specifice presupuse de implementarea unor politici de securitate cibernetică vor aduce cheltuieli suplimentare, însă o astfel de perspectivă rămâne una profund limitată la aspectele economice ale dezvoltării Internetului. Pentru o mai bună punere în perspectivă, ar fi oportună și **observarea evoluțiilor similare din alte industrii** – creșterea măsurilor nu a împiedicat inovația sau dezvoltarea nici în domeniul aeronautic, și nici în domeniul automobilului. Iar dacă **valoarea pe care o dorim protejată** este acest potențial de inovație și dezvoltare adus de Internet, cred că este vitală menținerea unui acces facil și nediscriminatoriu, care să nu lezeze (spre exemplu) alte valori, precum cele legate de siguranța utilizatorilor, proprietatea intelectuală ori stabilitatea rețelei ca infrastructură esențială a unei economii cibernetice în continuă dezvoltare etc, toate extrem de importante atât pentru societate, cât și pentru fiecare dintre noi, ca indivizi ori cetățeni.

Așa cum o dovedesc și alte articole dedicate subiectului în acest număr al revistei *Intelligence*, **o abordare comprehensivă a securității cibernetice trebuie să aibă în vedere nu numai tehnologia, ci și procesele socio-economice și, mai ales, oamenii.** Subiectul nu mai ține de cercul restrâns al câtorva specialiști, ci privește întreaga societate, la modul profund, cotidian. *Cybersecurity* tinde spre *mainstream* și va deveni, mai devreme decât cred mulți dintre noi, un *business as usual* pentru întreaga societate.

ABSTRACT

In the last two decades we have witnessed a different kind of revolution, related to information and technology. The cyberspace quickly expanded and it is now integrated to almost any "classic" area of our lives, bringing not only progress, but also some related challenges or even threats. It has become a new kind of space where many actors – not only states, but also groups of hackers or even determined individuals – can and do engage in new kinds of aggressions against each other or against simple and honest citizens or the vital infrastructures they rely on. In this context, it is obviously a good idea to have state of the art IT systems and experts, but it is not enough. Not anymore.

Cyber security is too important so it cannot remain an affair between the IT experts. It involves everyone, as professionals, as citizens, as simple individual living in modern society. Cyber security is no longer the crown of the few, but the business as usual for all of us.

REVOLUȚIA TEHNOLOGICĂ MEGA TRENDUL ÎNCEPUTULUI DE SECOL XXI

de Arthur LAZĂR - MUREȘAN

Unul din cele mai importante trenduri ale sistemului internațional actual este reprezentat de **accelerarea schimbărilor în diferitele domenii științifice și tehnologice**. Evoluția tehnologiilor a atras după sine **creșterea exponențială a vitezei de circulație a informației**, aspect care ne-a schimbat fundamental viața și modul nostru de a trăi. Primul *website* a fost creat în 1991. În 1993 acestea au ajuns la 50, iar în 2000 au depășit cifra de 5 milioane. Primul *email* a fost trimis în 1971, în timp ce, din 2013, se trimit mai mult de 40 de trilioane de email-uri pe an. În plus, aproape că nu ne putem imagina viața fără accesul la un calculator, începând de la lecturarea curentă a presei în fiecare dimineață, consultarea email-ului și alte activități curente care fac deja parte din rutină. Toate aceste computere nu există, însă, de unele singure. Ele sunt legate între ele, creionând un imens *network*. Prin urmare, **interconectarea globală** este una dintre caracteristicile fundamentale ale așa-numitei „revoluții tehnologice".

1991
PRIMUL WEBSITE
1993
50 DE WEBSITE-URI
2000
5 MILIOANE DE WEBSITE-URI

Așadar, o concluzie certă se desprinde de aici: **o mare parte din viața noastră este direct dependentă de *gadgeturi* conectate prin Internet**. Prin urmare, se poate spune că **o mare parte din existența noastră nu se mai petrece exclusiv în spațiul fizic, ci în spațiul virtual**. O transformare similară este resimțită și în sfera puterii, privită din perspectiva relațiilor internaționale. Noua realitate are ca efect **schimbarea naturii puterii**. Distribuția acesteia este mult mai accentuată, în timp ce difuziunea ei a atins cote extrem de ridicate (actori aproape anonimi pot ajunge să dețină resurse informaționale semnificative care, convertite în putere efectivă, pot crea probleme inclusiv statelor naționale).

PUTEREA CIBERNETICĂ – DEFINIȚIE ȘI CARACTERISTICI

Apariția noului tip de realitate virtuală, ca un element intrinsec al vieții noastre, a avut o influență majoră în schimbarea caracteristicilor puterii și a generat, practic, apariția acestei noi categorii – **puterea cibernetică**. Una din cele mai complete definiții a termenului, general acceptată în literatura de specialitate, descrie *puterea cibernetică* drept *„abilitatea de a utiliza spațiul cibernetic pentru a crea avantaje și a influența elementele în toate mediile operaționale și peste toate celelalte instrumente ale puterii*".

Se impun a fi făcute, prin urmare, câteva precizări. În primul rând, **puterea cibernetică este o expresie firească a evoluției tipului de geografie**, rezultând un nou domeniu de manifestare a puterii. Acum 200 de ani puterea actorilor de pe scena internațională se exercita preponderent terestru. Armate întregi, infanterii, cavalerie grea sau ușoară duceau greul luptelor pe uscat. La începutul secolului XX, dezvoltarea tehnologiilor navale și apariția flotelor maritime mari au condus la exploatarea spațiului maritim. **Alfred MAHAN**, general american și profesor la Academia Navală de Război, a defilat în jurul lumii, la începutul anilor 1900, cu o imensă flotă americană de război, atrăgând atenția încă de pe atunci că o mare putere urma să apară: SUA. Ulterior, începând cu dezvoltarea tehnologiilor aviatice, spațiul aerian a început să fie utilizat ca resursă de putere. Se spune că al Doilea Război Mondial a fost câștigat ca urmare a contribuției decisive a flotei aeriene de care dispunea tabăra aliaților. În sfârșit, la începutul anilor '60-'70 și ulterior în perioada de apogeu din anii '80 a Administrației Reagan, odată cu începerea Războiului Stelelor și a cursei înarmărilor fără precedent, câmpul de luptă s-a mutat în extra spațiu. De dată mai recentă, în contextul exploziei Internetului, resursele spațiului cibernetic sunt din ce în ce mai utilizate spre a fi transformate corespunzător.

PUTEREA DEPINDE DE RESURSE, IAR PUTEREA CIBERNETICĂ DEPINDE ÎN PRIMUL RÂND DE RESURSELE CIBERNETICE ȘI MAI ALES DE CAPACITATEA DE TRANSFORMARE A ACESTOR RESURSE ÎN DIVIDENDE REALE DE PUTERE.

În al doilea rând, **puterea cibernetică nu prezintă valoare fără capabilități de proiecție**. În accepțiunea *behavioristă*, orice putere trebuie să aibă capacitatea de a se impune în fața alteia, de a produce efecte și de a modela și influența comportamente. Pentru aceasta este nevoie de capacitate de proiecție a puterii. Așa cum apariția flotelor navale facilita transportul trupelor, mărea mobilitatea infanteriilor, îmbunătățea capabilitățile logistice, și proiecția puterii cibernetice trebuie văzută în aceeași logică, capacitatea de proiecție fiind prin ea însăși o resursă de putere. În cazul puterii cibernetice, proiecția se realizează aproape instantaneu. Așa cum spunea un renumit strateg militar american, prin intermediul puterii cibernetice se pot produce pagube la adresa unor infrastructuri aflate la mii de kilometri depărtare într-o secundă, doar cu ajutorul unui *click* al unui *mouse*. Așadar, puterea cibernetică, deși asemănătoare la o primă vedere cu celelalte tipuri de putere (navală, aeriană sau spațială), este diferită de acestea și în același timp superioară lor.

Puterea cibernetică are cel puțin 4 dimensiuni manifestate în toate cele 4 tipuri de spații de care am vorbit (terestru-naval-aerian-cyber).

În al treilea rând, **puterea cibernetică nu este doar o expresie a noului tip de geografie sau a noului tip de spațiu**. Aceasta, asemenea celorlalte tipuri de putere (economică, militară, organizațională sau socială), este o **resursă sau o sumă de resurse care contează în indexul general al puterii**. Mai mult fiind o resursă care poate influența fundamental celelalte tipuri de putere, se pare că deține o pondere semnificativă în orice formulă menită să facă clasamente și să calculeze indexul general de putere.

Aceste sume de caracteristici ne deschid, practic, un nou orizont de interpretare. Fiind mai mult decât o expresie a spațiului cibernetic, puterea cibernetică înseamnă mult mai mult decât ce a însemnat puterea navală în era dezvoltării maritime sau puterea spațială în anii Războiului Stelelor. La momentul respectiv, nici una dintre acele puteri nu puteau fi considerate prin ele însele piloni ai puterii în general, ci cel mult indicatori care, de cele mai multe ori, aveau o reflexie în alte tipuri de putere, de cele mai multe ori militară sau economică. **Puterea cibernetică este, însă, o expresie a realității noastre zilnice, iar acest aspect alături de puterea economică, militară, organizațională și socială, o face un pilon al puterii generale. Puterea cibernetică potențează aceste tipuri de putere, fiind un factor multiplicativ al formelor tradiționale de putere**.

RESURSELE PUTERII CIBERNETICE

Puterea depinde de **resurse**, iar puterea cibernetică depinde în primul rând de **resursele cibernetice** și mai ales de capacitatea de transformare a acestor resurse în dividende reale de putere.

Paul KENNEDY, în studiul său legat de ascensiunea și decăderea marilor puteri, arată că **dinamica schimbării în sistem este impulsionată, în principal, de evoluțiile economice și tehnologice**. Aceste evoluții economico - tehnologice au depins de variate categorii de resurse. Structurile producției s-au schimbat de la perioadă la perioadă, iar acestea afectează în mod direct economia și tehnologia. Capacitatea de inovație tehnologică a făcut în toate perioadele istorice diferența. Prin urmare, **capacitatea de conversie a resurselor este fundamentală și oferă un anumit avantaj unor societăți în raport cu altele**. Apariția corăbiilor cu bătaie lungă și dezvoltarea comerțului în spațiul atlantic după 1500 a adus beneficii acelor state europene care au știut să le fructifice, după cum dezvoltarea ulterioară a motorului cu abur și resursele de cărbune și metal, pe care acesta se baza, a sporit masiv puterea relativă a unor națiuni, diminuând-o pe a altora.

Însă niciuna din aceste resurse de putere nu a avut o **influență multilaterală asupra celorlalte instrumente ale puterii,** așa cum se întâmplă cu resursele puterii cibernetice. Acestea au un rol esențial asupra puterii economice, după cum aceleași categorii de resurse influențează esențial modul în care se duc anumite războaie moderne. Secolul XXI este prin excelență un secol al resurselor de tip *cyber*. Globalizarea și revoluția informației generează noi resurse ale puterii. Controlul rețelelor și conectarea devin o sursă importantă de putere.

Există **trei mari categorii de resurse utilizate în cyberspațiu**, definitorii pentru puterea cibernetică a **resurselor fizice** (echipamentele făcute de om la care se adaugă infrastructura care permite ca informația să circule - fibre optice, sisteme de comunicații spațiale, infrastructuri critice, sisteme industriale), ***know how***–ul care face ca informația să circule și **factorul uman**. La aceste resurse, în funcție de context, se poate adăuga **informația**, ca resursă de putere, cyberspațiul fiind în sine un mediu informațional unde informația este creată, stocată și, ulterior, împărtășită. Cunoașterea care rezultă din acest proces și din aceste interacțiuni extrem de rapide este percepută ca resursă de putere și ajută, de exemplu, în *decision-making*.

Joseph NYE arată că și **puterea cibernetică ca tip important de putere are o dublă natură: hard și soft**. Totodată, aceasta se poate manifesta atât în interiorul cyberspațiului, cât și în exteriorul acestuia. Atacurile cibernetice care *vizează* o țintă reprezintă un tip de resursă hard, în timp ce o campanie de diplomație publică derulată prin Internet, menită să influențeze opinia publică, poate fi considerată o resursă blândă de putere cibernetică.

Provocarea majoră cu care ne confruntăm atunci când încercăm să analizăm puterea și resursele acesteia este reprezentată de evaluarea legată de **ponderea fiecărei resurse în indexul general de putere**. Și în cazul puterii cibernetice, fiecare resursă are desigur influență diferită în ecuația finală. Mai mult, acestea depind de un anumit context de manifestare, asemeni puterii în general.

Ar trebui adăugat că puterea cibernetică nu se exprimă doar prin capacitatea de proiecție. Cel puțin la fel de importante sunt capacitățile de protecție. **Există, așadar, două fațete ale puterii cibernetice sensibil corelate între ele: o componentă defensivă** – denumită în literatura de specialitate *cybersecurity* **și o componentă ofensivă** care ține mai degrabă de capacitatea de proiecție a puterii. Pentru ca un actor din sistem să dețină putere cibernetică semnificativă, nu doar că este nevoie să dețină capabilități în ambele sensuri, ci trebuie să identifice inclusiv un mecanism de balansare a acestor tipuri de resurse. Problema majoră în cazul puterii cibernetice este că, spre deosebire de formele tradiționale de putere, cele două fațete (ofensiv și defensiv) presupun apelul la tipuri diferite de resurse. Așa se face că vulnerabilitățile rezultate de pe urma unui sistem de protecție ineficient nu pot fi suplinite de capacități de atac.

ACTORII PUTERII CIBERNETICE

Atunci când discutăm despre actorii puterii cibernetice ne lovim de o barieră importantă: **imperceptibilitatea** acestora. Această caracteristică derivă din însăși natura spațiului cibernetic, care este din ce în ce mai permisiv și oferă posibilitatea de manifestare a altor actori (non statali), uneori mai activi decât statele. De sute de ani sistemul internațional a fost clădit în jurul noțiunii de stat. Indiferent de forma sistemului (unipolar, bipolar, multipolar), după încheierea păcii de la *Westphalia,* statele națiune au devenit piatra unghiulară a sistemului internațional. Puterea era, prin urmare, distribuită doar între acestea, iar diferențele de clasament se manifestau aproape exclusiv raportat la astfel de entități. Puterea statelor și resursele de care acestea dispuneau erau vizibile, măsurabile și se exprimau fie prin armate puternice, resurse naturale considerabile, tehnologii avansate sau economii eficiente. Puterea era oarecum perceptibilă!

În zilele noastre, difuziunea puterii se exprimă prin diluarea substanței actorilor. Nu doar că actorii non-statali pot acumula putere relativă, dar chiar indivizii pot pune probleme în cyberspațiu unor actori mult mai mari, precum statele și instituțiile acestora. Se deduce, așadar, în momentul de față că **„jucătorii" din sistem sunt distribuiți după o formulă care situează la un capăt indivizii, apoi agregatele sau grupurile de indivizi cu organizare relativă (grupuri non-statale, ONG-uri, *hackeri*), iar la celălalt capăt se află statul**.

Acest tip de clasificare, fără alte explicații, este totuși simplistă atunci când vorbim de distribuția puterii în sistemul internațional. Problema majoră care se pune este legată de acele tipuri de transformări care pot cu adevărat să producă efecte în cadrul sistemului. Întrucât discutăm de sistemul internațional și indexul general de putere, una din întrebările care se ridică este legată de acea categorie de actori, resurse și evenimente care pot, într-adevăr să influențeze clasamentul din sistem. Din acest motiv, **problema actorilor, ca element definitoriu pentru puterea cibernetică în sistemul internațional, trebuie tratată în corelație cu tipurile de amenințare, precum și cu consecințele și impactul acestor amenințări**. Nu în ultimul rând, **intențiile actorilor și tipul de resurse utilizate reprezintă un indicator al naturii entităților deținătoare de putere cibernetică** din interiorul sistemului internațional. Cu alte cuvinte, întrebările ar fi: *care este intenția adversarului, care sunt țintele sale, care este impactul amenințării?* Aceste noțiuni de clasificare sunt importante și le regăsim și în sistemul formulelor tradiționale de putere. În cazul puterii cibernetice, ele sunt cu atât mai importante pentru că ajută în procesul de atribuire.

Aspectul corelativ al acestui proces se referă la **problema conținutului resurselor antamate**. Cu alte cuvinte, accesul sau permisivitatea tuturor actorilor din sistem se manifestă uniform în privința tuturor categoriilor de resurse? Toți actorii, indivizi ori grupuri mai mult sau mai puțin organizate, au acces la cablurile de fibră optică care traversează oceanele sau sunt capabili să utilizeze resurse extrem de scumpe de tip „0 day"? Evident nu! Făcând analogia

cu formele tradiționale ale puterii, entitățile care puteau cu adevărat să mobilizeze sume considerabile de resurse erau statele. Utilizarea unui anumit tip de resurse (o escadrilă de bombardiere, de exemplu) nu numai că era extrem de costisitoare, dar era atributul exclusiv al statelor. Escadrila de avioane nu era deținută nici de grupări

consolidate *ad-hoc* și nici de indivizi răspândiți în cele mai îndepărtate locuri pe glob. Mai mult, utilizarea acelui tip de resursă producea efecte în planul exercitării puterii din sistem. În cazul puterii cibernetice lucrurile sunt oarecum diferite. Permisivitatea accesului la resurse și rapiditatea transformărilor poate face ca mai devreme sau mai târziu o categorie largă de entități să le poată utiliza aproape după bunul plac. În fine, intențiile și consecințele care decurg din manifestarea unei amenințări pot, într-adevăr, influența sau schimba puterea celuilalt? În formele tradiționale de putere, intenția era reprezentată preponderent de dorința actorilor din sistem de a obține poziții dominante în raport cu ceilalți actori, de regulă adversari. Se schimbă situația în cazul puterii cibernetice?

Includerea unor elemente de interpretare legate de **intenții, valori, forme organizaționale** ne aduc în zona teoriilor constructiviste și, la o primă vedere, pot complica mecanismul de evaluare a puterii cibernetice cel puțin din punct de vedere al potențialității sale. Realitatea arată că **intenția poate fi un corelativ extrem de important atunci când încercăm exerciții de atribuire a actorilor deținători de putere cibernetică**. Intențiile ne pot oferi indicii suplimentare legate de calitatea actorului. Spre exemplu, un *hacker* situat în Singapore poate să își dorească să obțină *„credențialele"* cardurilor câtorva clienți din cadrul unei bănci pentru a le putea fura banii. În alte situații, un grup organizat de *hackeri* ar putea să încerce să atace o companie pentru a vinde secretele concurenței. Este puțin probabil, însă, ca aceste tipuri de activități și consecințele care decurg de aici să producă efecte majore în sistemul internațional. Dacă, însă, un grup de *hackeri* reușește să paralizeze sistemul bancar dintr-o țară într-o perioadă de criză, atunci este cu totul altceva. Dacă acea criză este asociată și cu un context militar încordat, atunci avem indicii suplimentare legate de potențiala identitate a actorilor implicați. Dacă atacul în cauză implică acces considerabil la resurse, atunci este rezonabil să luăm în calcul faptul că în spatele atacurilor respective ar putea fi un actor statal.

Concluzia care se desprinde de aici este că, **deși puterea este din ce în ce mai distribuită în sistem, totuși deținătorii cei mai importanți de resurse rămân în continuare statele**. Aceștia nu sunt doar cei mai importanți ci și *„cei mai periculoși"*. Experiența demonstrează că **cyberspionajul și cybersabotajul intră, prin excelență, în apanajul statelor, singurele care pot și au, cel puțin deocamdată, resursele, dar și intențiile și motivațiile pentru a derula astfel de activități**. Dar cum putem spune dacă o armă cibernetică este utilizată de un stat sau de un grup de *hackeri* independent? Sau care sunt criteriile in funcție de care putem spune asta? Dacă o armată este vizibilă și măsurabilă, atunci ea poate fi ușor legată de o anumită putere. Armele cibernetice, însă, sunt dificil de perceput. Rămâne în sarcina specialiștilor de *cyberintelligence* să rafineze criteriile de atribuire. Până atunci, putem doar să încercăm să găsim criterii plauzibile de atribuire.

CONCLUZII

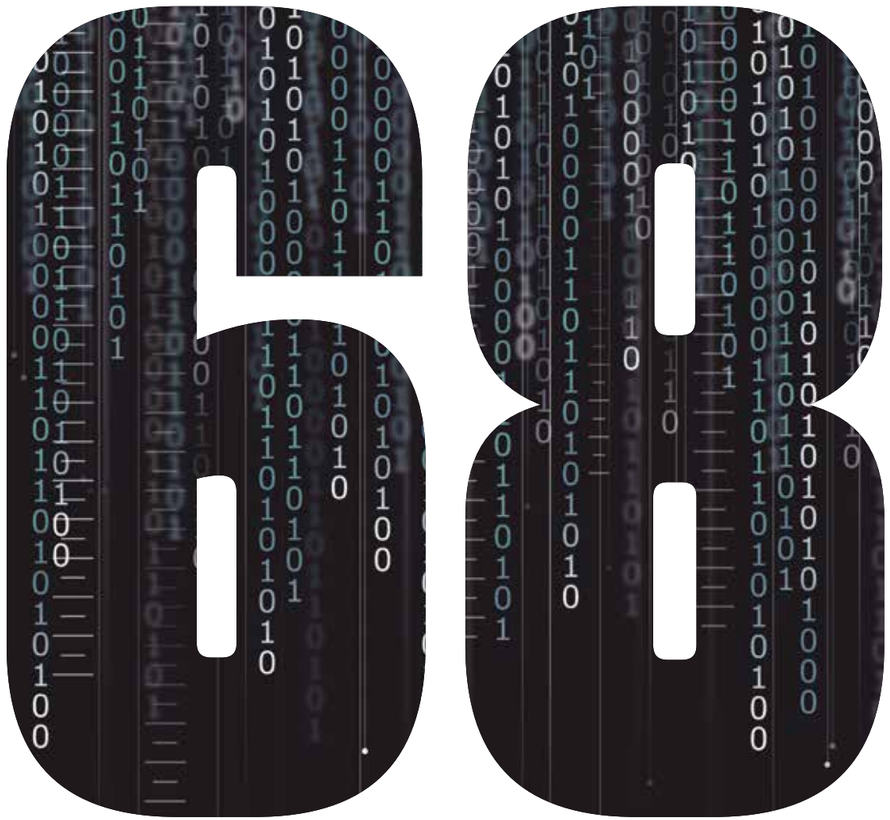
Puterea cibernetică este o expresie a noului tip de spațiu care a apărut concomitent cu explozia Internetului și a mijloacelor de comunicație moderne. Este fundamental diferită de celelalte forme de putere, în primul rând prin ingredientele sale, dar și prin influența pe care o exercită asupra tuturor celorlalte. Difuziunea sa, forța de propagare și imperceptibilitatea o fac de multe ori aproape imposibil de contracarat. De aceea, puterea cibernetică poate lovi fără dificultăți actori mari din sistem fără ca aceștia să perceapă din timp acest lucru.

Însă, atât timp cât resursele spațiului fizic sunt încă importante, puterea cibernetică și resursele sale nu pot substitui resursele tradiționale de putere. Cu certitudine le pot amplifica importanța și, de cele mai multe ori, pot face diferența. Din acest motiv, puterea cibernetică este un pilon al puterii generale, iar ponderea sa în indexul general de putere este semnificativă. Asemenea puterii tradiționale, și puterea cibernetică este contextuală, cumulativă și reînnoibilă. Actorii care vor putea să maximizeze aceste caracteristici ale puterii cibernetice vor avea șansele cele mai mari să ocupe pozițiile de sus ale clasamentului.

Deși resursele sale sunt mult mai accesibile pentru o plajă largă de actori, realitatea ultimilor ani arată că doar statele pot cu adevărat să acceseze acele instrumente care pot face cu adevărat diferența. Se deduce, astfel, că puterea cibernetică ca pilon al puterii în sistemul internațional este un atribut „smart" al statelor „smart". De felul în care vor combina actorii din sistem toate tipurile de resurse și le vor transforma în putere efectivă va depinde nu doar modul de exercitare a acesteia, ci și felul în care va fi distribuită în cadrul sistemului internațional.

ABSTRACT

Cyberpower has become one of the most sophisticated issues on the international relationships agenda. It is an expression of a new type of space which has emerged once both the Internet and modern technical communication systems have flourished. It is fundamentally different from other types of power in terms of internal ingredients and an expression of an overall influence exerted among them. It is the main reason why cyberpower should be considered a pillar of general power index. Similar to traditional types of power, cyberpower is contextual, cumulative, and renewable. The actors that will succeed in maximizing these features would eventually have the biggest chances to go up to the top of power ranking. It is the smart feature of smart states!



DE MILIOANE DE ALERTE CIBERNETICE

de Marius BOSTAN

Atunci când se vorbește despre securitate cibernetică, profesioniștii sunt de acord cu cel puțin două axiome: „Marea majoritate a companiilor și a instituțiilor cred că ele nu vor suferi niciodată un atac cibernetic” și „Nu există soluție infailibilă”.

În **2015** au fost generate cel puțin **68 de milioane de alerte cibernetice**, care au implicat 2,3 milioane de adrese IP. Circa 78% din alerte se referă la sisteme vulnerabile, 21% au fost infectate și 17 mii din domeniile .ro au fost compromise, conform unui raport **CERT-RO**. Deocamdată avem cunoștință, la nivel național, că s-au efectuat furturi și compromiteri de date – unele de importanță majoră, blocarea funcționării unor structuri cibernetice sau compromiterea în lanț a unor sisteme. Dar cine ne poate garanta că totul se va limita doar la atât? Cine ne poate garanta că prin calculatoarele compromise nu se vor produce catastrofe, cu pierderi de vieți omenești?

Este important să fim conștienți că **tehnologia este inertă din punct de vedere moral**. Ea poate fi folosită bine sau rău. Important este ca persoana, cu interesele sale, demnitatea sa, să fie pusă în centrul preocupărilor noastre. Totul depinde de cum și de către cine este folosită această putere enormă.

Noi românii știm să prețuim libertatea, pentru că am fost lipsiți de ea, individual și ca nație, înainte de 1989. Am văzut ambele sisteme și am ales fără ezitare calea libertății, democrației și economiei de piață. Dorim ca știința și tehnologia să ajute libertatea, accesul la informații, dezvoltarea economică, siguranța persoanei și comunităților, protejarea informațiilor private. Știm, din istoria noastră și a altor țări, că excesul de putere în mâna statului poate însemna dictatură, corupție, ineficiență. Știm că, aflate la dispoziția unui guvern totalitar, progresele științei și cele ale industriei IT pot deveni instrumente de opresiune.

ATACURI CU UN GRAD RIDICAT DE COMPLEXITATE ÎN ANUL 2016

Experții în securitate cibernetică ai ***Bitdefender*** au analizat principalele tendințe în materie de amenințări cibernetice pentru anul 2016, anticipând atacuri cu un grad ridicat de complexitate și infractori interesați să câștige cât mai mult din infracțiunile comise și care nu exclud un posibil atac terorist cibernetic cu consecințe catastrofice, care să paralizeze sistemele de control al traficului aerian sau să vizeze centralele nucleare.

O compromitere a sistemelor de dirijare a traficului în metrou ce ar duce la coliziunea intenționată a trenurilor de călători, în special în locuri și la ore deosebit de aglomerate, nu sunt scenarii de *science-fiction*. Ecluzele unor lacuri și baraje de acumulare deschise în mod intenționat prin sisteme cibernetice compromise ar duce, de asemenea, la pierderi de vieți omenești. Dar este, de asemenea, plauzibilă și varianta unui atac terorist condus din spatele unor calculatoare controlate de la distanță, despre care proprietarii legitimi să nu știe nimic, dar care să ofere protecția anonimatului *intruderilor* ce desfășoară activități de terorism. Asta ca să nu aducem în discuție ce ar însemna compromiterea sistemelor unor unități precum centrala nucleară de la Cernavodă, a echipamentelor electronice de control trafic aerian dintr-un aeroport sau preluarea controlului sistemelor cibernetice ale unor rafinării sau depozite de stocare a combustibililor.

Lumea trebuie să se pregătească pentru a face față unui posibil atac terorist cibernetic cu consecințe catastrofice, avertizează chiar **Eugene KASPERSKY**, CEO al companiei rusești de securitate informatică ***Kaspersky Lab,*** relatează Agenția *EFE*. „Poate fi vorba despre atacuri asupra matricei Sistemului Interconectat al unei țări, care să paralizeze sistemele de control al traficului aerian sau să vizeze centralele nucleare; este doar o chestiune de timp”, a subliniat Kaspersky într-un interviu acordat agenției spaniole de presă. O declarație interesantă, care ar trebui citită și prin prisma faptului că este făcută de o companie rusească.

De altfel, primul atac cibernetic care a provocat o pană de curent a fost executat la **23.11.2015** contra Ucrainei, cu probabilitate mare ca acesta să fi fost inițiat de pe teritoriul Rusiei. Astfel, conform Ministerului ucrainean al Energiei, citat de *Reuters*, *„hackerii, care pe 23 decembrie 2015 au atacat rețeaua de energie electrică a Ucrainei și care au provocat întreruperea furnizării de electricitate într-o zonă din partea de vest a acestei țări, au folosit serviciile unui furnizor de Internet din Rusia și au avut convorbiri telefonice pe teritoriul rus, ca parte a atacului coordonat*”. Aceștia au implantat un virus, printr-o operațiune de *phishing* (înșelăciune electronică care constă în obținerea unor date confidențiale folosind tehnici de manipulare a datelor identității unei persoane sau a unei instituții), susține societatea ***ESET France,*** care a monitorizat luni la rând acest virus. Societatea ucraineană de furnizare de energie electrică ***Prikarpattiaoblenergo*** a confirmat că, pe data de 23 decembrie, o mare parte a regiunii Ivano-Frankivsk a rămas complet fără curent electric timp de câteva ore. Pana a fost provocată de *„intervenția unor persoane neautorizate (...) în sistemul de comandă de la distanță, iar tehnicienii au reușit să restabilească manual furnizarea energiei electrice*”, se explică într-un comunicat difuzat de această companie.

În Republica Moldova, la **20 ianuarie a.c.**, operatorul național ***Moldtelecom*** a emis un comunicat, unde a explicat din ce cauză emisia a șapte posturi TV a fost sistată. Motivul ar fi atacul cibernetic asupra companiei, asemănător celor la care au fost supuse mai multe instituții de stat în aceeași perioadă a anului 2015. *„În seara zilei de 20 ianuarie anul curent au fost constatate probleme tehnice în difuzarea unui șir de canale TV din grila de emisie IPTV a companiei. Din momentul apariției deficiențelor în difuzare și până în prezent se depune efort maxim pentru înlăturarea problemei. Analiza preventivă arată că compania a devenit ținta unui atac cibernetic asemănător atacurilor cibernetice la care au fost supuse mai multe instituții de stat în aceeași perioadă a anului 2015 (...)”*, se explică în comunicat.

Am exemplificat aici doar evenimente de la granița țării noastre. Dar aceste exemple ar putea fi completate cu multe altele. Concluzia generală e că **atacurile cibernetice nu se mai rezumă doar la compromiteri de date. Modul de operare devine tot mai sofisticat, iar rezultatele atacurilor afectează în mod clar viața reală, nu doar cea virtuală.**

Sursele amenințările cibernetice sunt diverse: *hackerii*, persoanele frustrate, organizațiile criminale, grupurile politice extremiste, mișcările religioase fanatice, serviciile ostile de informații, grupările teroriste. Conform raportului de investigare asupra încălcărilor de securitate a datelor, realizat de compania americană ***Verizone*** pe 2014, a rezultat că **95% dintre atacatori sunt agenți externi, grupări activiste, 4% angajați și personal propriu din interior, iar sub 1% reprezintă partenerii de afaceri**.

Interesantă este și **evoluția în timp** a acestor amenințări. Dacă între anii **1996 și 2003** atacurile cibernetice vizau întreruperea sau blocarea serviciilor folosind viruși, viermi și atacuri pentru blocarea distribuită a serviciului (DdoS), între **2004 și 2005**, atacurile vizau obținerea profitului, apărând noțiunea de *cybercrime*. În această perioadă apar mesajele *spam* cu conținut *malware* și amenințările de tip *scamware*. Peisajul cibernetic se schimbă din nou, între anii **2007 și 2008**, fiind orientat în special spre zona de spionaj cibernetic. Apar, astfel, primele versiuni de amenințări cibernetice avansate persistente ***ZeuS*** și ***Stuxnet***. După anul **2010,** complexitatea atacurilor crește vertiginos, într-un singur atac fiind încorporate atât elemente de inginerie socială, cât și de *software* nociv. Specific atacurilor din această perioadă este exploatarea vulnerabilităților *zero-day*, furtul certificatelor digitale și puterea de polimorfism a aplicațiilor *malware*.

La început, soluțiile de securitate tradiționale, precum *firewall* sau antivirus, păreau suficiente, dar pe măsură ce atacurile au devenit mai sofisticate, soluțiile s-au dovedit a fi ineficiente întrucât se bazează pe informații despre atacurile anterioare cu mod de lucru cunoscut. De aici s-a născut ideea unor soluții proactive, de avertizare timpurie, cu scopul de a proteja și a detecta orice tentativă de atac neautorizat, în timp real. Una dintre metodele cele mai cunoscute este folosirea *honeypot*-urilor.

LEGEA SECURITĂȚII CIBERNETICE, PRIORITATE ZERO

Așadar, avem o problema reală – **creșterea exponențială a atacurilor cibernetice**. Nu se întâmplă punctual într-o anumită țară, ci global, chiar și la nivelul unor companii care declară că și-au luat măsuri de securitate. Dacă nu există soluții perfecte trebuie să acționăm pe cel puțin două paliere. În primul rând, la nivelul educației administratorilor de rețele și a utilizatorilor obișnuiți. Profesioniștii au statuat șase principii obligatorii: integritatea persoanelor, înțelegerea fenomenelor, respectarea procedurilor, *back-up* permanent al datelor, o atitudine care să pună totul sub semnul întrebării, formalitate în comunicare pentru minimizarea riscurilor. În al doilea rând, la nivel legislativ. Și aici intervine **Legea securității cibernetice**. Această lege nu expune suplimentar utilizatorii onești de sisteme cibernetice, sisteme de calcul, portabile, telefoane mobile și mini/micro *gadgeturi*, ci îi protejează de posibile abuzuri, prin stipularea clară a condițiilor și modalităților de abordare în cazul sistemelor compromise (cum, cine, în ce condiții, mandat judecătoresc etc). Articolul 2 specifică foarte clar că legea nu se aplică persoanelor fizice. Pentru companiile mari și cele ce prelucrează date personale, măsurile propuse de Legea securității cibernetice sunt deja implementate, acestea având structuri ce aplică deja propriile politici și măsuri de securitate, de regulă superioare condițiilor minimale stipulate de prezenta lege. În cazul societăților comerciale mici este de dorit să se aplice asemenea măsuri de securitate minimale, dar care să nu ducă în mod obligatoriu la costuri substanțiale sau nesustenabile. Pentru acestea există sisteme gratuite de tip antivirus sau *firewall,* care fac parte din suita de măsuri minimale ce trebuie luate preventiv sau pentru a limita daunele în cazul unor atacuri cibernetice. De asemenea, în sprijinul acestor societăți comerciale mici, microîntreprinderi sau pentru persoanele fizice, **MCSI** a elaborat **Ghidul securității cibernetice**, ghid ce cuprinde un set de recomandări minimale și bune practici de securitate cibernetică, reguli de prevenție, precum și modalități de reacție în cazul unor atacuri de acest tip.

BIG DATA, CLOUD, INTERNET OF THINGS

În mod evident, proiectul de lege nu este perfect. Încercăm să-l îmbunătățim cu ajutorul sugestiilor venite din partea societății civile, a ONG-urilor interesate de acest subiect și a cetățenilor ce își doresc o lege a securității cibernetice mai bună, mai aplicabilă și în sprijinul cetățenilor fără a impieta asupra intimității lor și a drepturilor cetățenești. Este legitimă și obligatorie intervenția statului împotriva furtului, spionajului și atacurilor cibernetice. Securitatea cibernetică trebuie să privească în mod egal atât instituțiile guvernamentale, cât și societățile comerciale, iar un parteneriat public-privat trebuie încurajat atât în centre de inovare și cooperare, cât și prin metode de asigurare, audit și subvenționare directă. Încercăm să ținem cont de toate opiniile pertinente și relevante venite din partea tuturor celor interesați, deoarece scopul nostru comun este să facem această lege cât mai bună, în așa fel încât să garanteze protejarea drepturilor și libertăților fundamentale ale cetățenilor în spațiul cibernetic.

Vorbim despre *Big Data, Cloud, Internet of Things* și tehnologii noi cu caracteristici care în urmă cu câțiva ani erau doar vise. Nu putem construi infrastructură cibernetică fără să ne asigurăm că este folosită în mod corect și în interesul cetățenilor. Nu putem folosi banii publici să construim infrastructuri, putere de calcul și capabilități, iar ele să fie compromise de atacatori care sunt adversarii democrației, adevărului și libertății, valori pe care noi toți vrem să le apărăm. Trebuie să ne asigurăm că această putere nu este folosită în mod contrar drepturilor fundamentale ale omului. Deoarece problematica securității cibernetice este una globală, este necesar să ne preocupe permanent unificarea forțelor cu toți aliații și chiar să inițiem cât mai multe programe de cooperare, regionale și globale.

ABSTRACT

When talking about cyber security we must remember that there is no foolproof solution. It is important to be aware that technology can be used good or badly, depending on the entity using it. This is why the person and its safety and well-being must be the center of our concerns. Cyber-attacks have grown exponentially, so the problem is real. It does not happen punctually, in a particular country, but globally, even with companies that claim they have taken security measures. As there is no perfect solution, we must act on at least two levels. First, in educating network administrators and ordinary users, and second, at the legislative level. A cyber security law does not additionally expose the honest users of cyber systems, computers, mobile phones, and mini/ micro gadgets, but it protects them from possible abuses by laying down clear terms and conditions of compromised system approach.

CINE SUNT AGRESORII CIBERNETICI

de Oana IORDAN

Societatea secolului al XXI-lea este puternic influențată de dezvoltarea fără precedent din domeniul IT&C, marcând începutul erei informaționale. „Democratizarea" tehnologiei și accesul liber la informație reprezintă o schimbare majoră comparat cu era industrială, când puterea economică a unui stat reprezenta un element esențial.

Intensificarea gradului de utilizare a Internetului generează, pe de o parte, creștere economică și schimbări sociale importante, dar este asociată și cu o intensificare a activităților ilegale derulate în spațiul cibernetic.

Spațiul cibernetic, considerat în prezent de teoreticieni drept al cincilea domeniu în care se poate desfășura un război, după sol, mare, aer și spațiu, oferă agresorilor cibernetici o mare diversitate de obiective și o serie de caracteristici specifice - dinamism extrem, conectivitate, anonimat, lipsa de trasabilitate - care fac dificilă atribuirea agresiunilor.

Amenințarea cibernetică reprezintă una dintre cele mai dinamice amenințări actuale la adresa securității naționale și poate veni din partea unei diversități de agresori cibernetici care folosesc metode adaptate permanent evoluțiilor tehnologice.

Principalele forme de manifestare a amenințărilor cibernetice la adresa securității naționale a României sunt reprezentate de agresiunile cibernetice derulate de patru categorii de agresori cibernetici - **actori statali, grupări de criminalitate cibernetică, grupări extremiste (*hacktiviste*)** și **grupări teroriste**.

De altfel, principalele categorii de actori care generează amenințări în spațiul cibernetic sunt prezentate și în *Strategia de securitate cibernetică a României*, care se referă în acest context la:

- „persoane sau grupări de criminalitate organizată care exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale;
- teroriști sau extremiști care utilizează spațiul cibernetic pentru desfășurarea și coordonarea unor atacuri teroriste, activități de comunicare, propagandă, recrutare și instruire, colectare de fonduri etc. în scopuri teroriste;
- state sau actori non-statali care inițiază sau derulează operațiuni în spațiul cibernetic, în scopul culegerii de informații din domeniile guvernamental, militar, economic ori al materializării altor amenințări la adresa securității naționale".

> **„CUNOAȘTE-ȚI INAMICUL ȘI CUNOAȘTE-TE PE TINE ÎNSUȚI; DINTR-O SUTĂ DE BĂTĂLII NU TE VEI EXPUNE NICIUNEI PRIMEJDII.**
> SUN TZU

Agresorii cibernetici dețin **capabilități tehnologice și resurse diferite** folosite pentru derularea de atacuri cibernetice, având **motivații diferite: politice, economice sau ideologice**. Astfel, dacă vorbim de actori statali, aceștia au resursele necesare pentru derularea unora dintre cele mai sofisticate atacuri cibernetice și, de cele mai multe ori, au și timpul necesar pentru a derula campanii de infiltrare în sisteme informatice de interes, în timp ce la polul opus se situează grupările extremiste și teroriste care dețin un nivel tehnologic redus, derulând de regulă atacuri cibernetice care nu afectează grav infrastructurile cibernetice atacate, ci creează mai mult prejudicii de imagine.

Amenințarea reprezentată de actorii statali are cel mai ridicat nivel de impact asupra securității naționale. Atacurile cibernetice derulate de actori statali au ca țintă domenii strategice: afaceri externe, apărare și securitate națională, economie, cercetare, energetic și re-

surse naturale. Sunt vizate îndeosebi instituții ale statului (ministere, reprezentanțe diplomatice, structuri guvernamentale, servicii de informații, structuri militare), dar și companii naționale sau private de interes strategic, trusturi media etc.

Motivația acestor atacuri este una politică, urmărindu-se preluarea și menținerea sub control a infrastructurilor cibernetice atacate, accesarea și exfiltrarea de informații sensibile sau confidențiale relevante care să ofere atacatorului avantaje politice, economice, militare, de securitate etc. (*spionaj cibernetic*).

Atacurile cibernetice desfășurate de actori statali au un nivel crescut de complexitate tehnologică, fiind, de regulă, de tip *APT* (*Advanced Persistent Threat*), sunt focalizate pe ținte exacte, de interes, și se caracterizează prin preocuparea pentru disimularea implicării statului, un aspect important urmărit fiind ca atacul să rămână nedescoperit pe o durată cât mai mare, fără a afecta funcționalitatea infrastructurii cibernetice compromise, pentru a permite exfiltrarea cât mai multor date de interes.

AȘA CUM SE STIPULEAZĂ ȘI ÎN RAPORTUL CERT-RO CU PRIVIRE LA ALERTELE DE SECURITATE CIBERNETICĂ PROCESATE ÎN ANUL 2014, „ENTITĂȚI DIN ROMÂNIA AU FOST ȚINTA UNOR ATACURI INFORMATIVE DIRECȚIONATE ȘI COMPLEXE, DE TIP APT, LANSATE DE CĂTRE GRUPURI CARE AU CAPACITATEA ȘI MOTIVAȚIA NECESARĂ PENTRU A ATACA ÎN MOD PERSISTENT O ȚINTĂ ÎN SCOPUL OBȚINERII ANUMITOR BENEFICII (DE OBICEI, ACCES LA INFORMAȚII SENSIBILE)”.

Atacurile cibernetice derulate de grupări de criminalitate cibernetică au un nivel mediu în ceea ce privește impactul asupra securității naționale și vizează cu predilecție domeniul financiar-bancar și al economiei digitale. Acest tip de atacuri s-a diversificat în ultima perioadă, atât în ceea ce privește țintele vizate (instituții ale statului, de la entități financiar-bancare, operatori de comunicații și, nu în ultimul rând, persoane fizice), modul de operare, nivelul tehnologic, cât mai ales în ceea ce privește gradul de automatizare al atacurilor, permițând acestor grupări să își extindă aria de manifestare și să își maximizeze câștigurile.

Motivația acestor atacuri este exclusiv economică, obiectivul grupărilor de criminalitate cibernetică fiind reprezentat de obținerea de beneficii financiare imediate sau obținerea de informații care să le asigure câștiguri financiare pe viitor. Atacurile vizează compromiterea confidențialității datelor gestionate de sistemele informatice asociate serviciilor financiar-bancare și fraudarea platformelor de comerț electronic.

Pentru derularea atacurilor cibernetice, grupările de criminalitate cibernetică folosesc din ce în ce mai mult rețele de tip *botnet*. În conformitate cu același *Raport al CERT-RO*, „46% din alertele de securitate cibernetică primite de instituție vizează sisteme informatice din România, victime ale unor atacatori care au reușit preluarea de resurse în cadrul unor rețele de tip *botnet* prin exploatarea unor vulnerabilități tehnice și infectarea sistemelor cu diverse tipuri de aplicații *malware*”.

De asemenea, în ultima perioadă a fost constatată o tendință accentuată de creștere a utilizării atacurilor de tip *ransomware*, care vizează nu doar utilizatorii individuali, ci și entități publice sau private și pot avea un impact major asupra victimelor.

Următoarele două categorii de agresori cibernetici - grupările *hacktiviste* și grupările teroriste - sunt caracterizate prin derularea unor atacuri cibernetice motivate ideologic, care în prezent au un impact scăzut asupra securității naționale. Atacurile cibernetice motivate ideologic se remarcă prin puternic impact mediatic, dat fiind că acestea nu sunt atacuri persistente, disimulate, ci sunt atacuri cibernetice asumate și expuse mediatic.

ATACATORII VIZEAZĂ ACCESAREA ILEGALĂ A SISTEMELOR INFORMATICE

Evoluția grupărilor *hacktiviste* este una dinamică, potențată de existența unor evenimente pe scena politică, economică sau socială care prezintă interes pentru agenda acestor grupări, atacurile derulate de către aceste grupări fiind o reacție la astfel de evenimente. Acest tip de grupări dispun de potențialul necesar pentru a se relansa și coagula rapid în jurul unor idealuri comune.

Țintele vizate sunt diverse, fiind predilecte infrastructurile informatice și paginile web aparținând unor instituții publice și guvernamentale, instituții de învățământ, dar și cele ale unor entități private.

Prin derularea de atacuri cibernetice, atacatorii vizează accesarea ilegală a sistemelor informatice și a bazelor de date asociate, indisponibilizarea acestora, exfiltrarea unor date confidențiale și publicarea acestora în mediul *online*, precum și alterarea conținutului paginilor web prin inserarea de imagini și mesaje. Atacurile cibernetice derulate de asemenea grupări, de regulă de tip *defacement* sau *DoS* (*Denial of Service*), nu au un grad ridicat de complexitate și nu necesită cunoștințe avansate de *hacking*, de cele mai multe ori, membrii acestor grupări folosind instrumente disponibile liber în mediul *online*.

În ceea ce privește ultima categorie de agresori cibernetici – **grupările teroriste**, trebuie precizat că în țara noastră **nu s-au înregistrat agresiuni cibernetice efectuate de către acestea,** spațiul cibernetic fiind îndeosebi utilizat pentru activități de propagandă, radicalizare, recrutare și finanțare.

Forma de manifestare identificată până în prezent este reprezentată de atacurile cibernetice de tip *defacement* realizate de *hackeri* sau grupări de *hackeri* simpatizanți ai ideologiilor islamist-radicale sau care provin de pe spații cu religie preponderent musulmană.

Astfel de atacuri au urmărit afectarea disponibilității și integrității rețelelor, prin alterarea conținutului, paginilor web atacate, cu scopul de a promova, sub diferite forme, mesaje și imagini de propagandă, de tip *graffitti cibernetic*.

Țintele acestor atacuri cibernetice, caracterizate printr-un nivel de complexitate redus, sunt reprezentate de paginile web ale unor entități private, dar și ale unor instituții publice locale, caracterizate printr-un nivel scăzut de securitate cibernetică, cel mai probabil criteriu de selecție fiind dat de tipurile de vulnerabilități identificate și exploatate de agresori, ca urmare a derulării unor operațiuni de scanare.

Concluzionând, trebuie subliniată importanța pe care o cunoaștere comprehensivă a agresorilor cibernetici (motivație, mod de operare, capabilități deținute și folosite și, implicit, ținte vizate) o poate avea în evaluarea corectă a amenințării cibernetice și a riscurilor conexe, inclusiv în realizarea unei politici eficiente de prevenire, combatere și contracarare, căci, așa cum spunea Benjamin Franklin, *„investiția în cunoaștere aduce cea mai bună dobândă”*.

ABSTRACT

The increased level of use of cyberspace generates economic growth and important social changes, but it is also associated with an increase in the illegal activities carried out in the cyberspace by different cyber aggressors, be they state or non-state actors. The most important threats to Romania's cyber security are the cyber attacks perpetrated by four categories of cyber aggressors: state actors, cyber criminal organizations, extremist (hacktivist) groups, and terrorist groups.

CUM TE PROTEJEZI ÎN ONLINE

de Daniel RĂDAN

Despre **securitate în mediul virtual** s-au scris mulți *Terrabytes* de informații și se vor mai scrie încă. De ce? Pentru că vorbim de un **mediu dinamic**, aflat în permanentă schimbare. Pentru că tehnologiile folosite sunt înlocuite, actualizate și modificate constant, apărând astfel noi și noi **provocări**. Și pentru că nivelul de ***awareness*** al utilizatorilor de Internet este încă unul foarte **scăzut**.

Mediul *online* are din ce în ce mai multe conexiuni cu spațiul fizic. Iar multe dintre lucrurile pe care le facem în primul au implicații în cel de-al doilea. Astfel, când securitatea este compromisă în spațiul virtual, utilizatorii pot avea parte de consecințe dintre cele mai neplăcute în spațiul fizic: de la stresul creat prin simpla funcționare greoaie a computerului, la dispariția sau afectarea integrității unor materiale personale (fotografii, videoclipuri, creații artistice) la prejudicii de imagine și/ sau financiare.

În general, utilizatorii de Internet care sunt conștienți de riscuri adoptă unele măsuri care, în opinia lor, ar trebui să fie suficiente pentru o bună protecție. Cel puțin experiențele anterioare le-au dovedit că au fost suficiente. Tu te-ai întrebat vreodată dacă măsurile tale de securitate sunt suficiente pentru a te proteja în *online*? Departe de a oferi garanția unei securități impenetrabile, întrebările următoare și comentariile aferente fiecăreia te vor ajuta să înțelegi mai bine multiplele fațete ale securității în spațiul virtual.

Instalezi *softuri* pe care nu le-ai căutat în primă instanță?

Principiul ar fi următorul: dacă nu l-ai căutat de la început, nu-l instala! Multe amenințări *online* vin sub forma de cereri de a da *click* pe un anumit link sau de a deschide atașamentul unui mesaj e-mail. Altele îți deschid niște ferestre *pop-up* foarte enervante care îți cer sa rulezi un extraordinar *scanner* de securitate sau să instalezi un *codec* ori un *player* cu ajutorul cărora poți vizualiza diverse conținuturi. Evită să dai curs unor asemenea cereri. Dacă dorești totuși să instalezi o astfel de aplicație, fă o verificare înainte (gândește-te că și atunci când cumperi un produs *online*, în prealabil te documentezi cu privire la calitățile și performanțele acestuia). Iar dacă e necesar să instalezi acel *soft*, încearcă să îl descarci direct de la sursă și nu de pe terțe *website*-uri.

Actualizezi *softurile* pe care le-ai instalat?

Dacă nu faci asta încă, ar trebui. Fie că e vorba de sistemul de operare în sine ori de alte *softuri* adiacente. De multe ori, atacatorii exploatează vulnerabilități ale unor aplicații de tip vizualizator de documente, *player* de conținut multimedia etc.. Majoritatea acestor produse primesc în mod constant actualizări din partea producătorilor. Instalează-le cât mai curând posibil!

Dezinstalezi aplicațiile de care nu mai ai nevoie?

Daca nu mai ai nevoie de un anumit *soft*, dezinstalează-l! Astfel, vor fi mai ușor de urmărit aplicațiile care necesită a fi actualizate, iar de multe ori va permite o executare rapidă a sarcinilor de către calculator (sunt frecvente aplicațiile de mici dimensiuni și *add-on*-urile care se instalează împreună cu diverse *softuri* și care pornesc odată cu computerul, ocupând memoria acestuia și afectându-i performanțele).

Folosești o singură parolă pentru toate conturile tale *online*?

Deși e simplu de utilizat, o parolă unică nu e cea mai bună idee din punct de vedere al securității. Utilizează parole dificil de intuit de către atacatori, formate din cifre, litere, caractere speciale. Și urmează principiul: conturi diferite, parole diferite. Poate părea complicat, dar în cazul în care un atacator obține parola de la contul personal de *e-mail*, nu va putea compromite și contul de e-mail de serviciu și pe cele de **Facebook, PayPal, Tweeter, MyBanking** etc.. De asemenea, este o măsură de siguranță suplimentară folosirea modalităților de autentificare în mai mulți pași (ex: parolă + *token*, parolă + cod transmis prin SMS etc.).

Îți protejezi conexiunea la Internet?

Dacă folosești un *router* pentru a te conecta la Internet, asigură-te că ai schimbat parolele implicite ale acestuia (de cele mai multe ori, astfel de dispozitive au parole standard de genul „1234”, „0000”, „admin”, „root”). De asemenea, actualizează *firmware*-ul și instalează *patch*-urile de securitate. Asigură-te că *router*-ul este configurat să ofere conexiuni criptate (tehnologia de criptare WPA2 este cea mai puternică formulă disponibilă în majoritatea *router*-elor moderne). Urmând acești pași, vei reduce considerabil șansele ca agresorii cibernetici să preia sub control conexiunea ta de Internet, folosind-o pentru a-ți compromite computerul, pentru a-ți afla „*credențialele*” de acces la diferite conturi sau pentru a o folosi ca paravan („*proxy*”) pentru derularea altor atacuri informatice.

Cât de relaxat ești când te conectezi la rețele *Wi-Fi* publice?

Ideal ar fi să nu te conectezi niciodată la rețele *Wi-Fi* sau *hotspot*-uri publice. Dar dacă situația o impune, odată conectat nu accesa conturi personale sau profesionale sensibile. De multe ori, conexiunile gratuite fie sunt compromise de infractori cibernetici care obțin astfel „*credențialele*” celor conectați la rețeaua respectivă, fie sunt create tocmai în acest scop.

Folosești programe de tip antivirus?

În ciuda sloganurilor cu care sunt promovate de către unii producători, programele antivirus nu asigură protecție 100%. Ele sunt eficiente sau chiar foarte eficiente în a identifica produse *malware* cunoscute, dar performanța lor scade considerabil când apar mostre noi de *malware*. Cu toate acestea, este important să ai un produs antivirus instalat. Aplicația antivirus ar trebui să funcționeze ca unul dintre straturile de protecție ale computerului tău. Și, fie că e vorba de o variantă cu plată sau de una gratuită, asigură-te că primește la timp toate actualizările și este activă permanent (în lipsa actualizărilor, un program antivirus oferă o protecție nu cu mult mai mare decât oferă un joc de cărți sau o aplicație de desenat).

Ești atent la datele tale personale?

Nu completa formulare primite via *e-mail*, prin care ți se cer date cu caracter personal, parole, coduri secrete sau *PIN*-uri. Când vine vorba de date sensibile, instituțiile publice, băncile sau marile companii sunt mai... conservatoare și nu solicită să le fie transmise prin banalul *e-mail*. Așa că, cel mai probabil, acel mesaj prin care ți se spune că banca ta dorește să actualizeze datele clienților și are nevoie și de ale tale, inclusiv numărul cardului bancar, codul PIN și parola de conectare la contul ***MyBanking*** - ai ghicit! - nu e de la bancă!

Observi cu ușurință schemele de inginerie socială?

În ce constă ingineria socială? Păi... în acel banner unde scrie că este nevoie doar să dai *click* pe un *link* dacă vrei să afli cum s-a produs cel mai recent accident aviatic ori să vezi în ce ipostaze incendiare a fost surprinsă o celebritate. Tot inginerie socială este și atunci când ești anunțat că tocmai ai câștigat o sumă de bani, o excursie sau o cină romantică, în urma unei extrageri la care nu îți amintești să te fi înscris, apoi ești rugat să transmiți datele personale ori să depui ceva bani într-un cont pentru a intra în posesia premiului. Indiferent de promisiune, ingineria socială îți va cere ceva: să deschizi un fișier atașat în *e-mail* sau transmis prin *instant messaging*, să urmezi un *link*, să instalezi un *soft*, să completezi cu datele tale un formular. Privește cu suspiciune astfel de cereri și nu te lăsa atras în schemă!

Asigurarea unui nivel ridicat de securitate în online nu este o sarcină ușoară. Dar costurile insecurității se pot dovedi a fi mult mai greu de suportat. Așadar, informează-te permanent cu privire la evoluțiile în materie de securitate IT! Implementează mai multe soluții/metode de protecție, nu te baza pe o singură aplicație. Și, cel mai important, fii vigilent!

ABSTRACT

The connections between the virtual environment and the physical space are ever more increasing. A low level of security of your virtual world could translate into a lot of real stress, loss of personal content or money. The awareness of the average Internet user is still close to ground level. In this article the author raises a few questions designed to increase security awareness, describing a few ways to have a safer cyber existence.

Long story short: use strong passwords, install security patches, keep your AV up to date and beware of social engineering scams. When it comes to cyber security, it is difficult to talk in terms of totally safe or 100% secure. So, be reasonable, keep yourself up to date with the latest in matters of IT security and be careful where you click!

INTERVIU

FLORIN COSMOIU

șeful Centrului Național Cyberint din cadrul SRI

„ÎN ULTIMII ANI, ATACURILE LA ADRESA SISTEMELOR INFORMATICE REPREZINTĂ O AMENINȚARE EMERGENTĂ LA NIVEL INTERNAȚIONAL“

MARIUS BERCARU: Cât de semnificativă este amenințarea din spațiul cibernetic pentru state, în general, și pentru România, în particular?

FLORIN COSMOIU: În ultimii ani, atacurile la adresa sistemelor informatice reprezintă o amenințare emergentă la nivel internațional, derularea acestora fiind conexată evenimentelor cu impact asupra statelor sau comunităților din cadrul societății.

Din această perspectivă, se poate afirma că spațiul cibernetic a devenit o reflexie a conflictelor și stărilor de tensiune pe plan mondial.

În caz particular, raportându-ne la calitatea țării noastre de membru NATO și UE, alături de poziția geografică, resursele de care dispune și obiectivele strategice pe care le are, România are statutul de țară vizată de atacuri cibernetice, în scopul principal de exfiltrare de informații strategice.

Putem să ne gândim că pagubele unui atac cibernetic sunt comparabile cu cele ale unui atac cu armată clasică?

Pagubele acestor tipuri de acțiuni sunt dificil de comensurat, în special prin prisma efectelor pe termen lung pe care le implică fiecare dintre ele. De altfel, este bine știut că una dintre caracteristicile amenințării cibernetice o reprezintă caracterul asimetric, acesta însemnând o relație de invers proporționalitate între investițiile într-un atac și valoarea pagubelor produse.

Cu toate acestea, în ultima perioadă se poate observa o tendință tot mai accentuată cu privire la realizarea de atacuri „*cyberkinetice*”, cu efect asupra spațiului fizic.

În acest sens, putem exemplifica prin atacul de la sfârșitul anului 2015 din Ucraina, într-o regiune situată la granița cu România, când agresorul cibernetic a preluat sub control infrastructura de furnizare a energiei electrice. Rezultatul în acest caz a fost încetarea furnizării de energie electrică timp de câteva ore în regiunea respectivă.

Totodată, în cazul în care entitățile teroriste și-ar dezvolta capabilitățile tehnologice în realizarea unor atacuri cibernetice de amploare, acestea pot avea un impact devastator asupra societății.

Se vorbește foarte des de atacuri cibernetice realizate de actori statali. Care ar putea fi scopul acestor atacuri? Ce își propune acest gen de atacuri?

Atacurile cibernetice realizate de actori statali vizează în principal infrastructurile cibernetice de interes național, urmărind preluarea controlului asupra acestora, în scopul sustragerii de informații confidențiale, de natură strategică, circumscrise domeniilor afaceri externe, economico-financiar, energetic, apărare, ordine publică și securitate națională.

Cum putem să deosebim un atac al unui actor statal de cel cu intenții criminale?

Principala diferență între cele două tipuri de atacuri cibernetice o constituie motivația atacatorului.

Așa cum menționam anterior, agresorii statali vizează exfiltrarea de informații strategice din sferele de interes, în timp ce principalul resort motivațional în cazul atacurilor cibernetice criminale îl reprezintă obținerea de foloase financiare ilicite.

De asemenea, agresiunile cibernetice de natură statală sunt mai dezvoltate din punct de vedere al nivelului tehnologic.

Care sunt principalele tipuri de atacuri criminale?

Activitățile subsumate criminalității informatice vizează cu predilecție domeniul economiei digitale, prin compromiterea confidențialității datelor gestionate de platformele de comerț electronic (care au rămas ținte predilecte) și fraudarea conturilor/ fondurilor clienților acestora.

De asemenea, în derularea acestui tip de atacuri, sunt vizați atât utilizatorii serviciilor de banking online, cât și infrastructurile cibernetice ale instituțiilor bancare.

Grupările infracționale recurg la crearea și utilizarea de rețele de boți, ca instrumente pentru derularea altor atacuri cibernetice, însă predominanta ultimilor ani a fost dată de utilizarea și distribuirea de malware, în special a celui de tip ransomware (CryptoLocker).

Atacurile derulate prin utilizarea de ransomware au un impact major asupra victimelor în situația, foarte frecventă, în care acestea nu au măsuri minimale de protecție (back-up al datelor și un program antivirus). În plus, până în prezent nu a fost identificată o soluție pentru recuperarea cheii private necesară pentru decriptarea datelor, fără a plăti recompensa. Relevant este faptul că plata recompensei nu garantează recuperarea datelor.

În cel fel afectează atacurile cibernetice utilizatorii de acasă, cetățenii în general?

Calculatorul unui cetățean poate fi ținta unui atac sau poate fi folosit pentru a derula un atac cibernetic. Spre exemplu, prin distribuirea de aplicații malițioase către o țintă, agresorii cibernetici pot dobândi accesul la sistemul informatic vizat și obține controlul asupra acestuia, în scopul utilizării unei părți din capacitatea de procesare a sistemului în derularea de activități infracționale. Totodată, atacatorii vizează obținerea datelor personale din calculatoarele țintă, cum ar fi credențialele de conectare la diverse platforme online, în vederea obținerii unor foloase financiare ilicite sau în scopul de a șantaja victima.

Există estimări cu privire la numărul de computere din România infectate într-un fel sau altul?

Nicio instituție nu deține date exacte cu privire la numărul de calculatoare infectate la nivelul României. Raportându-ne la cele trei categorii de utilizatori, respectiv utilizatori casnici, persoane juridice de drept privat și instituțiile de drept public, este greu să stabilim cu exactitate numărul sistemelor informatice infectate.

Ca date statistice, potrivit raportului cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2014, au fost implicate în cel puțin o alertă de securitate cibernetică un număr de 2.4 milioane de IP-uri unice, aproximativ 24% din totalul alocat spațiului cibernetic românesc.

Numărul real de calculatoare infectate este mai scăzut, dar este greu de estimat, în special din cauza alocării dinamice a IP-urilor, existând totodată și situații în care un utilizator se poate conecta cu același sistem informatic la Internet atât prin rețeaua de acasă sau de la locul de muncă, cât și prin intermediul unui *hotspot wireless* dintr-un spațiu public.

Cum își pot proteja instituțiile rețelele de computere? Dar cetățenii, ce măsuri își pot lua pentru laptopul de acasă? Vă rugăm să sintetizăm pentru cititori cele mai importante 5 sfaturi pentru cetățeni și instituții.

În vederea asigurării securității cibernetice a infrastructurilor cibernetice pe care le dețin sau le au în responsabilitate, persoanele juridice de drept public sau privat ar trebui să implementeze un set de politici și planuri de securitate care să respecte un set de cerințe minime de securitate cibernetică, să realizeze – anual sau când este necesar – audituri de securitate cibernetică, să implementeze un sistem de management al incidentelor de securitate cibernetică, să nu permită accesul neautorizat la datele deținute la nivelul acestor infrastructuri și să desemneze persoane responsabile în ceea ce privește coordonarea activităților de securitate cibernetică.

În privința persoanelor fizice, acestea ar trebui să folosească sisteme de operare și programe software cu licență, să actualizeze permanent sistemului de operare și *browser*-ul utilizat, să folosească soluții antivirus actualizate zilnic și să efectueze scanări periodice ale sistemului

pentru identificarea posibilelor fișiere cu conținut malițios. Nu în ultimul rând, este foarte important ca utilizatorii să nu acceseze linkurile primite prin e-mailuri care solicită actualizarea informațiilor personale, întrucât entitățile legitime nu cer niciodată furnizarea sau verificarea unor informații sensibile printr-un mijloc nesigur, precum e-mailul.
În spațiul cibernetic, utilizatorul reprezintă primul filtru în prevenirea contactului cu aplicații malițioase.

Au existat cazuri de instituții românești atacate? Care sunt instituțiile statului care gestionează astfel de cazuri?
Bineînțeles, luând în considerare rolul pe care România îl are în arhitectura de securitate a UE și NATO, instituțiile românești au fost și vor fi vizate de atacuri cibernetice cu un înalt nivel tehnologic.
În ceea ce privește cunoașterea, prevenirea și contracararea atacurilor cibernetice desfășurate de actori statali la adresa instituțiilor din România, Serviciului Român de Informații îi revine un rol important în domeniu.
Trebuie să reținem, totuși, faptul că demersul național principal de consolidare a capabilităților de apărare cibernetică l-a reprezentat constituirea Sistemului Național de Securitate Cibernetică și a Consiliului Operativ de Securitate Cibernetică, entități prevăzute prin Strategia de Securitate Cibernetică a României.
Conform Strategiei, Sistemul Național de Securitate Cibernetică reprezintă cadrul general de cooperare pentru asigurarea securității cibernetice, care reunește autorități și instituții publice cu responsabilități și capabilități în domeniu. Acesta acționează pe componentele de *cunoaștere*, *prevenire*, *cooperare și coordonare*, *contracarare*, toate acestea realizându-se prin informare, monitorizare, diseminare, analizare, avertizare, coordonare, decizie, reacție, refacere și conștientizare, adoptare de măsuri proactive și reactive.
Organismul prin care se realizează coordonarea unitară a SNSC, desemnat prin această Strategie, este COSC (din care fac parte, în calitate de membri permanenți, reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Telecomunicații Speciale, Serviciului de Informații Externe, Serviciului de Protecție și Pază, Oficiului Registrului Național pentru Informații Secrete de Stat, secretarul Consiliului Suprem de Apărare a Țării).

Nu putem evita proiectul legii securității cibernetice. De ce este necesară o astfel de lege?
Din punct de vedere strategic, la nivelul României trebuie continuate eforturile de creare și dezvoltare a unui cadru legislativ eficient, care să asigure condițiile necesare printr-o cooperare strânsă cu entitățile afectate a atacurilor cibernetice.
Cadrul național actual de reglementare legislativă și nivelul de operaționalizare a instituțiilor și structurilor cu atribuții în domeniul securității cibernetice din România nu permit, în prezent, prevenirea și contracararea eficientă a unor atacuri cibernetice la scară națională.
O lege a securității cibernetice ar stabili cadrul general de reglementare a activităților în domeniul securității cibernetice și obligațiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice.
De asemenea, un astfel de act normativ ar institui cadrul legislativ care să permită instituțiilor statului cu atribuții în domeniul *cyber* să cunoască, prevină și contracareze amenințările cibernetice, să diminueze vulnerabilitățile infrastructurilor cibernetice și să asigure exercitarea neîngrădită a drepturilor și libertăților fundamentale ale persoanelor în spațiul cibernetic.
În absența posibilității de descurajare sau diminuare directă a nivelului de agresivitate a atacurilor cibernetice, măsurile de reacție necesare trebuie să aibă în vedere limitarea / eliminarea vulnerabilităților create de cadrul legal insuficient dezvoltat în acest domeniu și de nivelul precar al culturii de securitate cibernetică la nivelul entităților publice și private.

> **INSTITUȚIILE ROMÂNEȘTI AU FOST ȘI VOR FI VIZATE DE ATACURI CIBERNETICE CU UN ÎNALT NIVEL TEHNOLOGIC**

Există voci care, în cursul dezbaterii publice cu privire la noul proiect de lege a securității cibernetice, au afirmat că instituțiile statului vor putea controla online-un românesc. Care sunt garanțiile de respectare a drepturilor cetățenești în acest caz?
Constat la nivelul societății civile o preocupare majoră, în ceea ce privește instituțiile statului și modul în care activitatea acestora pot afecta dreptul la intimitate prin introducerea acestei legi, aspect absolut legitim, susținut de poziția SRI, potrivit căreia datele cu caracter privat pot fi accesate decât prin mandat emis de judecător.
Nu observ, însă, aceeași îngrijorare cu privire la faptul că datele personale ale cetățenilor pot fi accesate și folosite de către persoane rău voitoare, grupări de criminalitate informatică, entități străine sau de către agresori cibernetici.
Legea securității cibernetice a României statuează clar faptul că, numai în cazurile în care există indicii temeinice privind afectarea securității cibernetice, drepturile cetățenilor pot fi restrânse doar prin mandat judecătoresc.

James Clapper, directorul Comunității americane de informații, avertiza recent în cadrul unei audieri în congres despre un nou pericol: "In the future, intelligence services might use the Internet of Things for identification, surveillance, monitoring, location tracking, and targeting for recruitment." Domnule Cosmoiu, cum anticipați securitatea cibernetică a viitorului, mai ales în contextul marcat de dezvoltarea programelor analitice de big data și de ceea ce numim Internet of Things?
Indiferent de modul în care evoluează tehnologia, dreptul la viață privată a utilizatorului trebuie să primeze, iar ca acesta să fie asigurat, trebuie să existe o legislație clară privind exercitarea acestui drept în spațiul cibernetic. În acest sens, legislația trebuie să conțină reglementări care să oblige producătorii / dezvoltatorii de tehnologii la implementarea unor măsuri de protecție adecvate a utilizatorilor, în raport cu orice terț.

CINE ȘI CUM NE ATACĂ TELEFONUL MOBIL

de BITDEFENDER

Într-o piață care însumează aproximativ **2 miliarde de telefoane mobile inteligente *(smartphones),*** protejarea datelor salvate în terminalele mobile devine o problemă serioasă, mai ales că acestea nu mai sunt folosite de mult doar pentru a suna sau a trimite mesaje prietenilor. Între timp au devenit niște **mini-calculatoare** folosite pentru a stoca date, fotografii, pentru a accesa conturi de *e-mail*, rețele sociale, jocuri, sau multimedia. De cele mai multe ori, telefoanele sunt legate nu numai de viața privată a cuiva, ci și de locul de muncă al posesorului telefonului. Astfel, o vulnerabilitate sau un atac asupra telefonului mobil poate afecta nu doar individul, prietenii, dar și compania pentru care acesta lucrează.

Vă prezentăm câteva dintre **cele mai des întâlnite atacuri asupra telefoanelor mobile**, **posibilele implicații la nivel personal și nu numai,** cât și o serie de metode de protejare împotriva escrocilor care folosesc dispozitivele mobile pentru a înșela oamenii, a le fura banii și chiar pentru a pătrunde în organizațiile și firmele unde aceștia au acces.

TIPURI DE AMENINȚĂRI CARE VIZEAZĂ TERMINALELE MOBILE

În mai puțin de 10 ani, telefoanele mobile și-au schimbat total înfățișarea și funcționalitatea. Interesul crescut al producătorilor și al utilizatorilor a atras atenția atacatorilor care au văzut în telefoane și tablete un nou domeniu de exploatat.

Una dintre cele mai răspândite metode de atac asupra terminalelor mobile sunt **amenințările care apelează sau trimit SMS-uri pe ascuns la numere cu supra-taxă**. Utilizatorul va înțelege că ceva nu este în regulă cu telefonul sau tableta sa abia la prima factură, când va trebui să plătească mult mai mult decât anticipase sau dacă este pe cartelă, va termina creditul mult mai repede. Dacă vă întrebați cum ajung aceste aplicații malițioase pe dispozitivele utilizatorilor, răspunsul este simplu: atacatorii iau o aplicație legitimă, o modifică adăugând cod periculos și o deghizează într-o aplicație populară. Apoi, folosind diferite tehnici de inginerie socială conving utilizatorii să descarce și să instaleze aplicația pe telefon sau pe tabletă. Aceste aplicații periculoase pot de asemenea fura și alte informații din telefon, cum ar fi datele de identificare ale dispozitivului, coordonate GPS, lista de contacte, adrese de *e-mail* sau *e-mail-uri*.

Foarte multe aplicații periculoase (exemplu: ***Android.Trojan.FakeInst)*** pretind că instalează *browsere*, antiviruși și aplicații de *chat* pe mobile când de fapt păcălesc utilizatorul și trimit SMS-uri la numere cu supra-taxă. Unele au nevoie ca utilizatorul să le configureze manual, pe când altele se instalează singure odată ajunse în dispozitivele mobile, și eventual își schimbă iconița la un interval de timp pentru ca utilizatorii să nu le detecteze prezența.

O altă categorie generoasă de aplicații periculoase pretind că țin în viață **bateria dispozitivului** pentru mai mult timp. În schimb, ele spionează în fundal tot ce face utilizatorul cu telefonul sau tableta, culeg date și le trimit pe *serverele* atacatorilor.

Unele aplicații de mobil procedează într-un mod similar cu **programele false de securitate** de pe PC. Odată ce utilizatorul instalează o astfel de aplicație, aceasta îi spune că dispozitivul are probleme cu durata de viață a bateriei, care se descarcă mult prea repede. Îi sugerează să acceseze un *website* de unde să descarce un utilitar. Dar pe *site* utilizatorul va gasi un instrument care spionează de fapt activitățile utilizatorului.

Utilizatorii trebuie să se ferească și de **aplicațiile false de video *player,*** care odată instalate trimit mesaje la un număr cu supra-taxă care ajung să coste până la 5 dolari SMS-ul. **Android.Trojan.FakePlayer**, de exemplu, păcălește utilizatorul să-i dea permisiunea să modifice sau să șteargă cardul de memorie al telefonului, să acceseze informații de pe telefon fără a cere alte permisiuni.

Odată cu creșterea constantă a numărului de aplicații din piețele oficiale **Google Play** și **AppStore**, dezvoltatorii au început să adauge tot **mai multe funcții** în aplicațiile făcute de ei pentru un plus de competitivitate. Dacă ne uităm atent la sutele de mii de aplicații care stau la dispoziția utilizatorilor de telefoane mobile și tablete, vedem că unele dintre aceste aplicații pot pune probleme de securitate posesorilor de dispozitive mobile atunci când transferă date din telefon – nume de utilizator și parole folosind rețele nesecurizate, în timp ce altele activează fără permisiunea posesorului de mobil funcția de GPS pe lângă furtul de contacte, adrese de *e-mail*.

PEISAJUL ACTUAL AL AMENINȚĂRILOR CARE VIZEAZĂ TERMINALELE MOBILE

Amenințările care vizează terminalele mobile sunt tot mai răspândite și se modifică foarte repede în contextul dezvoltării accelerate a pieței de mobile. Astfel, amenințările informatice care vizează furtul datelor personale și al detaliilor de autentificare în conturile bancare câștigă din ce în ce mai mult teren în peisajul virușilor pentru terminale mobile cu Android. Dacă virușii care trimit SMS-uri la numere *premium* sunt în continuare în top din punct de vedere al numărului de atacuri, noile amenințări, mai complexe, de tip *ransomware* – ce blochează terminalul și solicită plata unei amenzi – înregistrează creșteri susținute.

Chiar daca nu sunt la fel de avansați din punct de vedere tehnologic comparativ cu amenințările pentru **Windows**, **aplicațiile *ransomware* pentru Android** pot cauza probleme prin indisponibilizarea telefonului sau a datelor de pe acesta. Telemetria Bitdefender confirmă faptul că familia de *ransomware* **Slocker** e cea mai frecvent răspândită amenințare în România, UK, Germania și Australia.

Reclamele agresive afișate utilizatorilor de aplicații gratuite sunt cunoscute pentru faptul că adună date personale pentru a adapta conținutul în funcție de utilizator. Agențiile de marketing apreciază drept foarte valoros acest tip de informație care face campaniile promoționale mai eficiente și mai profitabile.

Una dintre cele mai recente amenințări mobile analizate în laboratoarele **Bitdefender** vizează **reclamele periculoase care promit soluții de antivirus**, dar creează în schimb abonamente la servicii cu supra-taxă care livrează imagini pentru ecran și *screensavere*.

Specialiștii **Bitdefender** au identificat *bannere* de reclamă în diverse aplicații legitime de **Android**, care lansează atacuri menite să păcălească utilizatorii să cumpere un produs fals de securitate. Printre reclamele livrate de platforma **InMobi** s-a strecurat un *banner* care afișează pe ecranul *smartphone*-ului un mesaj care informează că dispozitivul este infectat cu viruși. Ca să-l dezinfecteze, utilizatorul trebuie să acceseze un *link* ca să descarce soluția de AV. De fapt, în loc de soluția AV, utilizatorul este păcălit să-și facă un abonament de 3 sau 4 euro pe săptămână prin care pot avea acces la tonuri de apel *premium* și *wallpapere*. Abonamentul poate fi întrerupt doar manual.

Dacă nu aveți nicio soluție de securitate instalată pe *smartphone* sau tabletă, nu ar trebui să vi se afișeze niciun mesaj de tip *pop-up* care să vă informeze cu privire la diverse infecții. Nu vă grabiți să urmați instrucțiunile din aplicație. Dacă însă folosiți o soluție antivirus dedicată, trebuie să știți că nicio aplicație legitimă nu vă

cere bani în plus pentru a curăța sistemul de viruși.

În acest caz particular, dezabonați-vă imediat trimițând **un SMS la numărul menționat în secțiunea „Termeni și Condiții”**. Trebuie doar să mergeți în josul paginii unde v-ați abonat inițial. Dezinstalați aplicațiile pe care le-ați descărcat recent. O soluție AV care să blocheze paginile este de asemenea foarte utilă. **Bitdefender** recomandă folosirea *software*-ului **Clueful**, care vă informează la ce tip de informații au acces aplicațiile pe care le instalați și care sunt riscurile pe care vi le asumați instalându-le.

Un studiu recent al companiei noastre a dezvăluit că **multe jocuri și aplicații pentru copii monitorizează locația copiilor** în ciuda reglementărilor **COPA** (*Children's Online Privacy Protection Act*), care prevede ca dezvoltatorii de *soft* să nu acceseze date cu caracter personal fără acordul prealabil și explicit al părinților. În ciuda acestor prevederi, există însă jocuțe și *soft* educațional, precum **Kids ABC Games** and **Educational Puzzles** care monitorizează locația copiilor și accesează funcția de geo-locație. Dat fiind faptul că profilul aplicațiilor nu justifică o astfel de funcție, cel mai probabil dezvoltatorii colectează aceste date pentru a le trimite unor terțe-părți care foloses aceste informații în scopuri publicitare. Alte aplicații pentru copii încearcă deasemenea să acceseze istoricul căutarilor pe net sau ID-ul unic al dispozitivului.

FENOMENUL BYOD ÎN COMPANII

BYOD face referire la obiceiul angajaților de a aduce la locul de muncă și de a folosi atât în interes de serviciu, cât și în interes personal dispozitivele mobile proprii, precum telefonul, tableta sau *laptopul*. Această practică poate pune în pericol siguranța informațiilor unei companii dacă angajații și firma nu iau măsuri de protecție serioase care să le apere datele.

În primul rând, toate dispozitivele mobile personale trebuie înregistrate atunci când accesează rețeaua companiei. Punctele de acces (*Hotspots*) neautorizate trebuie interzise cu desăvârșire în cadrul rețelei companiei, iar un dispozitiv care se conectează la *wi-fi*-ul autorizat de companie trebuie sa permită doar autentificarea bazată pe datele de conectare din domeniu sau cu certificate digitale. Angajații trebuie să înțeleagă responsabilitatea pe care o poartă atunci când manevrează date sensibile ce țin de companie pe dispozitive personale în afara spațiului firmei. Dacă pierd, rătăcesc sau li se fură un telefon mobil sincronizat cu *e-mailul* de serviciu, multe informații aparent inofensive pot ajunge pe mâini necunoscute și pot constitui un prim pas într-un atac de lungă durată care întotdeauna începe cu colectarea de date.

METODE DE ÎMBUNĂTĂȚIRE A SECURITĂȚII TERMINALELOR MOBILE

În afara casei, telefoanele mobile și tabletele devin cele mai utilizate dispozitive electronice, iar provocările și amenințările asociate acestora sunt diferite și necesită o abordare specială. Principalele probleme care pot apărea sunt furtul sau pierderea dispozitivelor, descărcarea de aplicații ce conțin viruși, ce fură informații sensibile și direcționează utilizatorii către site-uri și documente compromise.

FIȚI ATENȚI CE APLICAȚII DESCĂRCAȚI ȘI DE UNDE!
Descărcați aplicații numai din magazinele oficiale ale operatorilor și producătorilor precum Google Play și Apple App Store. Softurile provenite de la distribuitorii neoficiali vă pot infecta telefonul sau tableta și pot trimite mai departe, unor terțe părți informații private. În zone necunoscute, ați putea fi tentați să descărcați aplicații care să vă ajute să găsiți diferite locații precum restaurante, hoteluri sau muzee. Aveți însă încredere doar în cele care provin din surse autorizate. Pentru a evita descărcarea aplicațiilor nesigure din greșeală, verificați configurația terminalului accesând SETĂRI, SECURITATE și asigurându-vă că opțiunea SURSE NECUNOSCUTE este nebifată.

ACCESAȚI DOAR HOTSPOTURI SIGURE!
Hotspoturile wireless publice sunt vulnerabile interceptărilor de trafic și răspândirii virușilor, întrucât nu sunt protejate de parole și pot fi accesate de oricine. Imaginați-vă că cineva aflat în apropiere vă interceptează pachetele de date și vede tot ce faceți pe internet. Asigurați-vă că opțiunile de infraroșu, Wi-Fi și Bluetooth-ul sunt oprite atunci când nu le utilizați. Acestea vor consuma bateria și pot facilita accesul neautorizat la datele de pe dispozitivul mobil.

OPRIȚI SERVICIUL DE DATE MOBILE ATUNCI CÂND NU ÎL UTILIZAȚI!
Dacă sunteți în afara țării, nu uitați că serviciile de internet în roaming sunt foarte scumpe, iar o aplicație a unei rețele sociale care încearcă să se actualizeze la fiecare cinci minute va costa mai mult decât întregul plan de date achiziționat.

NU PUBLICAȚI PE PLATFORMELE SOCIALE DETALII REFERITOARE LA LOCAȚIA ÎN CARE VĂ AFLAȚI!
Dacă vă actualizați regulat conturile de social media și împărtășiți cu toată lumea unde sunteți și ce faceți, iar profilul dumneavoastră nu este accesibil exclusiv prietenilor, ați putea ajunge să spuneți unor persoane complet străine că nu sunteți acasă. Ați fi de acord să puneți afișe mari prin tot orașul prin care să faceți public locul în care vă aflați?

FIȚI ATENȚI LA OFERTELE PREA BUNE PENTRU A FI REALE!
Dacă primiți dintr-o dată oferte incredibil de avantajoase cu hoteluri de lux la prețuri foarte mici, rezervări de apartamente sau oferte de reîncărcare a telefonului mobil, ignorați-le. Un click pe linkurile incluse în emailuri pot infecta telefonul sau tableta sau vă pot atrage să completați formulare cu informații personale.

PROTEJAȚI-VĂ TERMINALUL CU PAROLE ȘI OPȚIUNI DE CRIPTARE!
În cazul în care cineva vă fură sau vă găsește telefonul mobil, îngreunați-i accesul la informațiile stocate. De asemenea, criptați datele cu ajutorul unui software dedicat sau – dacă dispozitivul o permite – cu ajutorul opțiunii de criptare disponibilă în terminal. Folosiți programe anti-theft pentru a vă găsi telefonul, a-l bloca sau a șterge informațiile de pe el de la distanță.

TRANZACȚIILE ONLINE FOLOSIND HOTSPOTURI NESECURIZATE SUNT RISCANTE!
Autentificarea în orice cont de bancă implică date sensibile. Tastarea datelor sensibile în timpul conexiunilor nesecurizate este riscantă, întrucât traficul poate fi urmărit de persoane neautorizate. Pentru tranzacții bancare sigure puteți folosi un laptop, iar dacă acesta rulează Windows, o soluție dedicată precum Safepay vă ajută să efectuați tranzacții bancare în siguranță.

NU ACCESAȚI LINK-URILE SAU DOCUMENTELE ATAȘATE ÎN EMAIL-URI VENITE LA ÎNTÂMPLARE!
La fel ca și pe computer, e-mailurile pot avea documente atașate care conțin viruși pentru terminale mobile, iar un click pe un astfel de link vă poate instala software periculos pe telefon.

INSTALAȚI UN PROGRAM DE PROTECȚIE ANTIVIRUS!
Instalarea unei soluții antivirus și a unei soluții de protecție a datelor personale este imperativă. Alegeți însă o sursă reputată și urmăriți furnizorii care oferă și soluții de securitate pentru PC pentru a evita soluțiile de securitate false.

MENȚINEȚI SOFTWARE-UL ACTUALIZAT!
Menținându-vă sistemul de operare și aplicațiile actualizate, vă asigurați că aveți cele mai recente versiuni de software pentru a face față celor mai recente amenințări.

Pentru protecția terminalelor mobile cu Android, Bitdefender recomandă folosirea soluției complete de securitate Bitdefender Mobile Security.

ABSTRACT

In a market that totals approximately 2 billion smartphones, protecting the data saved in them becomes a major issue, given the fact that they are used for more than just calling and texting. These smartphones have become mini-computers and are used to save data and photos, to access e-mail accounts, social networks, websites, and online games. In most cases phones are used for personal and professional purposes, which makes it possible for an attack against a terminal to affect the individual, his/ her friends and acquaintances, but also his/her co-workers and the company he/ she works for. The various types of threats can be addressed by several methods of protection, but alongside a few healthy habits, smartphone users should employ dedicated software for this purpose.

TRATEAZĂ TELEFONUL MOBIL CA PE UN COMPUTER

de Mihai GEORGESCU

Dispozitivele mobile au transformat în mod semnificativ felul în care putem să interacționăm cu informația. Avem la dispoziție, în propriul buzunar, toate informațiile de care avem nevoie în desfășurarea activităților cotidiene. Prin intermediul dispozitivelor mobile, avem acces nelimitat și instantaneu la orice carte, revistă, articol, film sau *show* de televiziune, facilitându-ne radical modul de viață. Interacționăm direct cu persoane din colțuri opuse ale lumii, schimbăm informații, idei și gânduri, prin simple atingeri ale dispozitivelor pe care le utilizăm.

La sfârșitul anului 2015, la nivel global funcționau mai mult de 2.6 miliarde de dispozitive mobile, iar potrivit raporturilor de evaluare realizate, se estimează că, până la începutul anului 2020, vor fi utilizate 6.1 miliarde de dispozitive.

CUM AVANTAJELE NU VIN NICIODATĂ SINGURE...

În mai puțin de 10 ani, dispozitivele mobile și-au schimbat total funcționalitatea și înfățișarea. Interesul tot mai ridicat, atât din partea producătorilor, cât și din partea utilizatorilor, a atras atenția persoanelor rău intenționate, care au văzut în astfel de dispozitive o nouă arie de exploatat. Peste 85% dintre utilizatorii de dispozitive mobile inteligente din România nu utilizează aplicații mobile pentru securitatea dispozitivelor proprii, fiind astfel predispuși la compromiterea datelor de pe *device*-uri. Infractorii așteaptă și pot specula orice pas greșit al utilizatorilor care nu își securizează datele pe dispozitivele mobile, în scopul obținerii unor *credențiale* de conectare la conturi personale de *e-mail*, date privitoare la carduri de credit și conturi bancare, și chiar *exfiltrarea* datelor personale, în scopul folosirii acestora pentru obținerea de foloase ilicite. Astfel, prin simpla instalare de aplicații nedorite sau ascunse (*malware*) pe *smartphone*, tabletă, laptop sau alte dispozitive mobile, atacatorii pot obține acces la datele noastre personale.

LA NIVEL MONDIAL, CEA MAI FOLOSITĂ PAROLĂ ESTE 123456 ÎN ANUL 2015

Mulți utilizatori ar putea considera faptul că securitatea dispozitivelor mobile este mai puțin importantă decât securitatea unui PC, însă în primul rând trebuie să ne raportăm la datele existente pe aceste categorii de dispozitive. În afara casei, telefoanele mobile și tabletele devin cele mai utilizate dispozitive electronice, iar provocările și amenințările asociate acestora sunt diferite, necesitând o abordare specială. Principalele probleme care pot apărea sunt furtul sau pierderea dispozitivelor, descărcarea de aplicații ce conțin viruși, care fură informații sensibile și direcționează utilizatorii către *site*-uri și documente compromise.

În ceea ce privește măsurile de securitate la nivelul dispozitivelor mobile, acestea au devenit o preocupare tot mai importantă în anul 2015. Potrivit specialiștilor din cadrul companiei furnizoare de soluții antivirus ***McAfee Labs,*** numărul aplicațiilor malițioase pentru dispozitivele mobile a crescut cu 112% în anul 2014, cu 5 milioane de semnături *malware* identificate doar în trimestrul 3 al anului respectiv.

CE VULNERABILITĂȚI SUNT EXPLOATATE

Pentru a ne securiza dispozitivele mobile, trebuie să cunoaștem câteva date privitoare la cele mai comune vulnerabilități ce pot fi exploatate de o aplicație rău intenționată.

Deseori, utilizatorii dispozitivelor mobile nu își activează măsurile elementare de siguranță, cum ar fi blocarea pe bază de parolă, amprentă digitală sau model grafic, iar, în situațiile în care acestea sunt active pe dispozitiv, parolele sunt de forma „0000” sau „1234”. Fără să ținem cont de aceste măsuri minimale de securizare a propriilor dispozitive, datele existente pe acestea vor fi cu siguranță compromise în cazul pierderii sau furtului acestora.

Utilizatorii dispozitivelor mobile pot descarcă aplicații cu conținut malițios (*malware*) în necunoștință de cauză, întrucât acestea pot fi ușor disimulate în jocuri, actualizări de securitate ale sistemului de operare, utilitare sau orice altă aplicație ce poate capta atenția – în acest caz persoanele rău intenționate folosindu-se de ingineria socială. Este dificil pentru orice utilizator să facă diferența între o aplicație legitimă și una care are conținut malițios.

De asemenea, de multe ori, utilizatorii se feresc să actualizeze *software*-ul existent pe dispozitiv, versiunile mai vechi ale acestora fiind mult mai vulnerabile din punct de vedere al securității. Totodată, dispozitivele care au o vechime mai mare de aproximativ un an și jumătate nu mai primesc actualizări ale sistemului de operare din partea producătorului, majoritatea încetând furnizarea de suport odată cu apariția noilor tipuri de dispozitive din gamă.

Comunicațiile în sistem *wireless* nu sunt întotdeauna criptate, iar de cele mai multe ori aplicațiile pe care le utilizăm în transmiterea mesajelor către alte persoane nu criptează conținutul conversațiilor. Atât timp cât aplicațiile nu criptează conținutul, informațiile transmise sunt foarte ușor de interceptat de o persoană rău intenționată.

O altă vulnerabilitate importantă o reprezintă faptul că utilizatorii pot folosi dispozitive mobile cu sisteme de operare care au suferit modificări neautorizate. Astfel, în cazul terminalelor care folosesc sistemul de operare *Android*, ne raportăm la conceptul de *rooting*, iar în cazul dispozitivelor *Apple* (*iOS*) la termenul *jailbreak*. Astfel de sisteme de operare permit utilizatorilor să instaleze funcții ale sistemului de operare sau ale aplicațiilor existente care nu sunt autorizate de către producător, facilitând în acest fel și accesul aplicațiilor *malware*.

CONSECINȚELE POT FI SEVERE

La momentul actual, cele mai dăunătoare coduri pentru dispozitivele mobile sunt programele *trojan*, aplicații aparent legitime. Rapoartele realizate de companii de specialitate relevă faptul că, în cursul ultimilor doi ani, atacurile cu astfel de aplicații malițioase au fost concentrate aproape exclusiv pe platforma *Android*.

Aplicațiile malițioase pot transforma orice dispozitiv mobil în membrul unei rețele de dispozitive ce pot fi controlate de către un atacator (*botnet*). Aceste tipuri de *malware* pot trimite informații despre dispozitiv către atacator, acesta dobândind în mod facil accesul la dispozitiv. Mai mult, astfel de aplicații pot ajunge în orice sistem informatic conectat la dispozitivul mobil infectat.

În magazinele *online* de aplicații aferente platformelor *iOS*, *Windows Phone*, *Blackberry*, și în special *Android*, există aplicații periculoase care pretind că prelungesc durata de viață a dispozitivului mobil sau că instalează *browsere*, sisteme antivirus și aplicații ce facilitează comunicarea interpersonală. În fapt, în spatele interfeței vizibile de către utilizator, aplicațiile malițioase obțin informații în fundal cu privire la activitatea acestuia și trimit datele către serverul atacatorului, astfel atât dispozitivul, cât și datele personale ale celui care îl utilizează devenind vulnerabile.

FURTUL DATELOR PERSONALE

Amenințările care vizează terminalele mobile sunt extrem de răspândite și au o dinamică foarte complexă în contextul dezvoltării foarte rapide a pieței de profil. Astfel, amenințările cibernetice care vizează furtul datelor personale și al detaliilor de autentificare în conturile bancare câștigă din ce în ce mai mult teren în peisajul virușilor pentru terminalele mobile, în special acelea care folosesc sistemul *Android*. Dacă virușii care trimit SMS-uri la numere cu supratarxă sunt în continuare în top din punct de vedere al numărului de atacuri, sunt într-o creștere semnificativă și noile amenințări, de nivel tehnologic ridicat, de tip *ransomware,* care criptează conținutul prezent pe spațiul de stocare al dispozitivului și solicită plata unei răscumpărări a datelor compromise, prin intermediul monedei virtuale Bitcoin, în vederea anonimizării acestuia.

În general, virușii bancari care vizează dispozitivele mobile pretind a fi actualizări ale certificatelor digitale și păcălesc astfel utilizatorii să îi descarce și să îi instaleze. *ZitMo* este cel mai cunoscut virus bancar de pe dispozitivele *Android*, prezent chiar și pe dispozitivele mobile din România. Astfel de viruși primesc comenzi de la un server de comandă și control, către care pot exfiltra toate SMS-urile pe care utilizatorul le primește pe mobil. Astfel, agresorii informatici pot intercepta numărul de autentificare al tranzacțiilor imediat ce utilizatorii le inițiază.

Una dintre cele mai recente amenințări mobile analizate de către specialiști vizează reclamele periculoase care recomandă utilizatorului instalarea de soluții antivirus, în realitate acest gen de aplicații creând abonamente la servicii cu supratarxă. De asemenea, au fost identificate *bannere* de reclamă în diverse aplicații legitime disponibile pe platforma *Android*, care lansează atacuri menite să păcălească utilizatorii să cumpere un produs fals de securitate. Dacă pe dispozitivul propriu nu există soluții de securitate instalate, pe acesta nu ar trebui să fie afișat niciun avertisment cu privire la eventuale infecții sau aplicații malițioase prezente. În caz contrar, trebuie reținut faptul că nicio aplicație legitimă pentru securizarea datelor de pe dispozitiv nu percepe taxe adiționale pentru curățarea sistemului de aplicații malițioase.

CUM NE SECURIZĂM DISPOZITIVELE MOBILE

ÎN VEDEREA ASIGURĂRII SECURITĂȚII PROPRIILOR DISPOZITIVELOR MOBILE, SE IMPUN CÂTEVA REGULI DE BAZĂ:

- Asigurarea unor măsuri de securitate privind rețeaua *wireless* proprie printr-o parolă sau cheie de securitate poate preveni accesul wireless neautorizat la dispozitivele noastre.
- Utilizatorii trebuie să folosească parole complexe și puternice pentru blocarea dispozitivului. În cazul în care cineva ne fură sau ne găsește telefonul mobil, trebuie să îi îngreunăm pe cât posibil accesul la informațiile stocate. De asemenea, criptarea datelor existente cu ajutorul unui *software* dedicat sau – dacă dispozitivul o permite – cu ajutorul opțiunii de criptare disponibile la nivelul sistemului de operare al dispozitivului este o soluție eficientă. Totodată, putem folosi aplicații de tipul „anti-theft” pentru a găsi telefonul, a-l bloca sau a șterge informațiile de pe el de la distanță.
- La momentul instalării aplicațiilor pe dispozitivele mobile trebuie să examinăm cu atenție ce permisiuni solicită acestea sistemului de operare instalat. Aplicațiile solicită accesul la anumite facilități ale telefonului atunci când sunt instalate, însă mulți dintre utilizatori nu acordă atenție acestor detalii, astfel că este ușor pentru atacatori și pentru dezvoltatorii de aplicații malițioase să convingă utilizatorii să ofere permisiuni care nu sunt neapărat necesare aplicației, creându-se astfel o breșă de securitate.
- *Hotspot*-urile *wireless* publice sunt vulnerabile interceptărilor de trafic și răspândirii virușilor, întrucât nu sunt protejate de parole și pot fi accesate de oricine, astfel pachetele de date și activitatea online ne pot fi interceptate oricând suntem conectați la o astfel de rețea. Se recomandă ca funcțiile *Wi-Fi* și *Bluetooth* să fie oprite atunci când utilizatorul nu le folosește. Pe lângă consumul ridicat al bateriei, aceste module pot facilita accesul neautorizat la datele existente pe dispozitiv.
- În ceea ce privește achiziționarea unei soluții antivirus pe dispozitivul mobil utilizat, chiar dacă aceasta nu reprezintă o investiție semnificativă, orice proces care rulează în fundal, inclusiv un antivirus, afectează performanța acestuia. Mai mult, putem spune că primul filtru în prevenirea contactului cu aplicațiile malițioase îl reprezintă utilizatorul. Atâta timp cât acesta este informat și citește cu atenție sporită toate permisiunile pe care o aplicație le solicită sistemului de operare înainte ca aceasta să fie instalată, riscurile se diminuează semnificativ.

ABSTRACT

We hear it every day, on television, on the radio, at the grocery store, and in the movies – that our world is getting smaller. We can be anywhere in the world within a day, by jumping on a plane, and by means of Skype, Google Hangouts or Apple's Face Time we can talk face to face to almost anyone in the world during the time it takes to turn on the computer or other mobile device.

Almost any and all information that we could possibly ever need or want is available to us at the speed of electricity, and our lives are infinitely better in uncountable ways. Research and practice in medicine, science, health, art, and a myriad other domains have increased exponentially as a direct consequence of the immediate availability of information that we take for granted in the 21st century.

On the other hand, criminals can get hold of passwords and access sensitive information when users install unwanted, hidden software (malware) on their computer, tablet, telephone, or other mobile device that they increasingly take for granted as members of the information age. Criminals can also critically compromise the information technology, infrastructure, and systems of large corporations to steal their customers' critical financial data and access their personal records.

Today's mobile devices are as powerful and connected as any personal computer or laptop, so we must take the same precautions on our mobile devices as we do on our computer regarding messaging and online safety.

CONSENS
UTILIZATORUL, ORGANIZAȚIA ȘI STATUL

de Radu-Mihai CORBEANU

În contextul în care fenomenul agresiunilor cibernetice cunoaște o amplificare constantă, susținută de aproape perfecta anonimizare specifică spațiului virtual și de cadrul legal lacunar de impunere a măsurilor sancționatorii, securitatea cibernetică devine un deziderat tot mai greu de atins.

Construcția și aplicarea unui sistem eficient de securitate cibernetică a devenit un proces complex, multifațetat, ce necesită o abordare multidisciplinară și implicarea conjugată a statului, organizației/ companiei și utilizatorului (din dubla sa perspectivă, de angajat al organizației și de utilizator independent). În vederea susținerii acestui demers, de importanță critică este identificarea scopului comun, a intereselor convergente ale celor trei actori, în contextul în care pot exista perspective diferite asupra conceptului de protecție, a relevanței acesteia pentru satisfacerea intereselor generale, precum și asupra implicațiilor conexe generate.

Utilizatorul, organizația și statul oferă cele trei abordări asupra procesului de asigurare a securității cibernetice, interferența acestora reprezentând soluția optimă pentru inițierea construcției unui sistem preventiv și reactiv eficient, orientat spre securitate comună și edificarea unei strategii defensive exhaustive.

Interdependența perspectivelor pornește de la principiul conform căruia securitatea cibernetică nu este rezultatul exclusiv al aplicării unei soluții *software*, ci al intercorelării atribuțiilor și responsabilităților entității statale, organizației și utilizatorului pe acest palier. Astfel, acesta din urmă are nevoie de ceilalți doi actori fie pentru crearea unui cadru legislativ protectiv și coerent (de către stat), fie pentru inițierea unor proceduri și metodologii de lucru (de către organizație). Pe de altă parte, organizația are nevoie de cultura de securitate a utilizatorului și de stat, unicul actor care deține sau ar trebui să dețină instrumentarul sancționatoriu capabil a determina diminuarea acestei amenințări cu caracter de fenomen și fundamentarea unui sistem preventiv. În acest scop, entitatea statală solicită implicarea celorlalți actori, deoarece fiecare deține partea sa de responsabilitate în cazul unei infectări cu *malware* a infrastructurilor cibernetice de interes pentru securitatea națională.

STATUL – COORDONATOR AL PROCESULUI DE SECURIZARE A AMENINȚĂRII CIBERNETICE

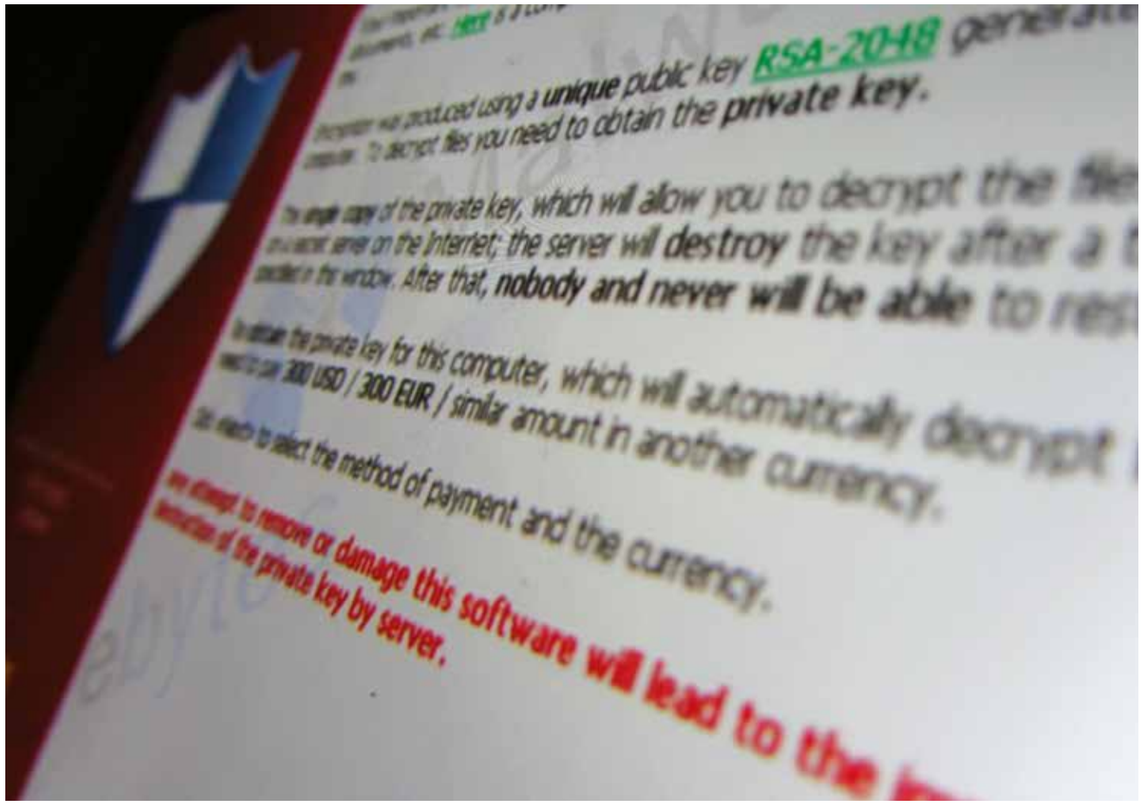
Responsabilitatea superioară, prin prisma complexității atribuțiilor implicate, este cea a entității statale, garant al securității organizației și utilizatorului, al informațiilor vehiculate la nivelul infrastructurilor cibernetice de interes pentru securitatea națională, dar și al fiecărei rețele informatice, indiferent de relevanța informațiilor vehiculate la nivelul acesteia.

La nivel guvernamental se realizează reglementarea normelor generale de securitate cibernetică, se stabilesc strategii și se promovează abordări unitare ale unor concepte și perspective evolutive, aplicate și dezvoltate de organizații, care se confruntă în mod direct cu efectele atacurilor cibernetice.

Statul propune o serie de soluții, conforme strategiei și intereselor naționale/ supra-naționale, în vederea constituirii unor mecanisme eficiente de prevenție și reacție, un ansamblu coerent de acte normative și decizii care vizează reducerea riscurilor specifice *cyberspace-ului*.

O abordare incoerentă a ciclului preventiv-reactiv-sancționatoriu de către entitatea statală poate reprezenta o vulnerabilitate de securitate cibernetică pe care orice agresor va căuta să o speculeze în vederea derulării de activități ilegale în spațiul virtual.

Totodată, construcția cadrului conceptual, organizatoric și acțional, necesar asigurării securității cibernetice, prezintă relevanță și din perspectiva conturării unor cerințe minimale de securitate pentru infrastructurile cibernetice ale fiecărei organizații.



Astfel, deținătorii de infrastructuri cibernetice ar trebui să adopte și să pună în aplicare politici (norme interne) de securitate cibernetică, cu respectarea unor cerințe minime stabilite la nivel național, care să le permită identificarea și implementarea măsurilor tehnice și organizatorice adecvate pentru gestionarea eficientă a riscurilor inerente spațiului virtual.

ORGANIZAȚIA ȘI ROLUL SĂU ÎN SUSȚINEREA SECURITĂȚII CIBERNETICE

Atacurile cibernetice pot genera pierderea unor date de importanță critică pentru companie, proprietate intelectuală sau relevante pentru valoarea comercială, situații de natură a afecta avantajul competitiv al entității respective. Mai mult, un studiu al *Oxford Economic* a demonstrat faptul că agresiunile cibernetice prezentate în spațiul public (mass-media) determină un impact imediat asupra cotațiilor bursei de mărfuri, „sensibile" la afectarea reputației companiei-victimă, aspect de natură a implica importante pierderi financiare pentru aceasta.

Interesele organizației impun tranziția de la modul clasic în care este abordată securitatea cibernetică, focusat exclusiv pe reacție și control, la o abordare inovativă, care să includă și elemente de prevenție, bazată pe riscuri și o strictă ierarhizare a intereselor critice ale entității.

În scopul detectării rapide a intruziunilor cibernetice și identificării unor reacții defensive eficiente la acestea, organizațiile trebuie să își reconfigureze politicile de securitate printr-o conexare eficientă a tehnologiilor, proceselor și competențelor umane cu activitățile specifice de risc management.

În esență, finanțarea proceselor care integrează capabilitățile predictive, preventive, de detectare și de reacție reprezintă soluția optimă în vederea diminuării impactului agresiunilor cibernetice. O strategie eficientă va necesita cunoașterea adversarului, a motivelor acestuia, resurselor, metodelor de atac, implicând asigurarea monitorizării și analizei amenințărilor, colaborarea cu spațiul public și cel privat, specializat în soluții IT, sau cu alte entități ale căror cunoștințe pot fi angrenate în acest proces, precum serviciile de *intelligence*.

În definitiv, nu există o politică de securitate cibernetică perfectă, fiind însă deosebit de importante corecta corelare a acesteia la specificul organizației și a mediului în care își desfășoară activitatea și integrarea rolului pe care utilizatorul infrastructurilor cibernetice îl joacă în acest demers.

UTILIZATORUL, FACTOR DECISIV AL SUCCESULUI POLITICII DE SECURITATE CIBERNETICĂ

Nicio politică de securitate cibernetică nu produce efectele scontate fără o implementare corectă și o aplicare la toate nivelurile organizației. Necunoașterea și dezinteresul utilizatorului primar determină neaplicarea regulilor fundamentale de securitate cibernetică, situație care reprezintă o vulnerabilitate a organizației și care, cel mai probabil, va fi speculată de agresorii cibernetici. Așadar, de o importanță critică pentru organizație este aplicarea politicii de asigurare a securității cibernetice, cu strictețe, de către fiecare angajat în parte. În lipsa concretizării măsurilor și soluțiilor trasate, politica de securitate devine nefuncțională, astfel încât utilizatorul reprezintă factorul decisiv pentru determinarea succesului/ insuccesului acesteia.

ÎN IUNIE 2015, AU FOST RAPORTATE ÎN SUA APROXIMATIV 1.000 DE VICTIME ALE CRYPTOWALL. COSTURILE ESTIMATE ALE UTILIZATORILOR PENTRU OBȚINEREA CHEII PRIVATE NECESARE DECRIPTĂRII DATELOR AU FOST DE 18 MILIOANE DE DOLARI.

Există o multitudine de reguli și bune practici în ceea ce privește rolul utilizatorului în procesul de asigurare a securității cibernetice, toate focusându-se pe importanța fundamentală a responsabilizării acestuia pentru fiecare acțiune derulată de pe stațiile de lucru ale organizației.

Din perspectiva sa de utilizator independent, acesta poate aplica aceleași principii vehiculate în mediul organizațional în lipsa constrângerilor specifice statutului de angajat, ci exclusiv din convingerea că respectarea regulilor și normelor de accesare a serviciilor *online* poate determina diminuarea riscurilor de infectare cu *malware*.

Astfel, dezvoltarea fenomenului *ransomware* la o scară exponențială determină necesitatea ca utilizatorul să devină un jucător activ pe componenta securității cibernetice, în caz contrar interesele sale imediate (atât cu privire la securitatea datelor, cât și de ordin financiar) fiind serios periclitate.

Conform datelor furnizate mass-mediei de FBI în iunie 2015, au fost raportate, pe teritoriul american, aproximativ 1.000 de victime ale *CryptoWall*, una dintre cele mai recente forme de *ransomware*, în doar primele trei luni de activitate ale acestui *malware*. Costurile estimate ale utilizatorilor pentru obținerea cheii private necesare decriptării datelor au fost de 18 milioane de dolari. Însă, nu întotdeauna achitarea recompensei solicitate de agresor garantează recuperarea fișierelor.

PERSPECTIVE PENTRU CONSTRUCȚIA CONSENSULUI

Responsabilitatea convergentă a statului, organizației și utilizatorului în ceea ce privește asigurarea securității cibernetice reprezintă soluția indispensabilă menținerii funcționalității fiecărui actor în spațiul virtual. Defectarea acestei triade poate genera repercusiuni incomensurabile pentru fiecare membru în parte, astfel încât interdependența determină nevoia de cooperare și directare unitară a efortului de securizare.

Disfuncționalitățile în activitatea fiecăruia afectează întregul proces de asigurare a securității cibernetice, astfel încât este necesară o atentă analiză a potențialelor surse generatoare de inconveniențe și identificarea, de comun acord, a unor soluții eficiente.

În construcția și implementarea unui sistem de securitate cibernetică eficient, corelat la necesitățile fiecărui actor din spațiul virtual, este fundamentală edificarea unui parteneriat strategic public-privat, în urma căruia atât statul, cât și compania să obțină satisfacerea propriilor interese printr-o abordare comună. Decidentul politic trebuie să se folosească de expertiza mediului privat, în special a companiilor IT ce dețin importante centre de analiză *malware* sau de inovare pe componenta tehnologică, dar și a marilor firme ce și-au construit sisteme de protecție cibernetică eficiente, pentru a identifica vulnerabilități, soluții și a prognoza evoluția amenințărilor cibernetice. De asemenea, partenerul privat poate apela la sprijinul instituțiilor cu responsabilități în domeniul *cybersecurity*, în vederea stabilirii unor mecanisme de notificare în caz de incident cibernetic, efectuării unor teste de penetrare, a schimbului de informații și expertiză cu privire la agresiunile cibernetice, precum și susținerii demersului de instruire a personalului.

Utilizatorul poate și trebuie să susțină acest proces, responsabilizarea sa fiind imboldul necesar demarării proiectelor de securizare și nu rezultatul acestora.

Interdependența acestor interese poate reprezenta scheletul construcției unei strategii naționale de identificare a consensului în domeniul securității cibernetice, coordonate de către stat, care ar putea fi constituită din trei elemente:

- politică de inițiere/ dezvoltare a culturii de securitate cibernetică a utilizatorului;
- campanii de conștientizare a riscurilor cibernetice la care este supusă infrastructura cibernetică a organizației și care afectează îndeplinirea obiectivelor acesteia;
- demersuri de promovare a parteneriatului public-privat în domeniul securității cibernetice.

În definitiv, membrii triadei stat-organizație-utilizator trebuie să conștientizeze că orice moment de întârziere în procesul de identificare a intereselor comune în planul securității cibernetice produce pagube însemnate, de ordin financiar și/ sau în planul securității naționale. În vederea transformării acestei triade într-un garant al securității cibernetice, soluția optimă ar fi identificarea și negocierea elementelor disonante, a piedicilor în calea construcției consensului.

ABSTRACT

Building and applying an efficient cybersecurity system require the joint contribution of the state, organization, and user, having a critical impact on the identification of the common goals and convergent interests of all three stakeholders.

Considering the complexity of the assigned attributes involved in this process, the main responsibility rests with the state, as a guarantor of the organization's and user's cybersecurity.

The organization's main objective is to implement the transition from the classic pattern of cybersecurity, entirely focused on reaction and control, to an innovative approach based on prevention, risks, and a strict classification of the entity's critical interests.

The user's ignorance and lack of interest are the main causes for breaking fundamental cybersecurity rules and can represent an organization's vulnerability most likely to be exploited by hackers.

The interdependence of the three stakeholders' interests can represent the most important element in the construction of a national strategy, which can be coordinated by the state based on three primary elements: an innovative user's policy of cybersecurity culture, an awareness strategy of cyber risks for the organization's cyberinfrastructure, and a public/ private partnership in cybersecurity field.

CONNECTED

PE PIAȚA DE LARG CONSUM - O OPORTUNITATE

de Mihnea COSTOIU

Ultimul deceniu - și cu precădere ultimii ani - ne-au arătat că **direcția viitorului apropiat stă în automatizări și în controlul tehnologiei la nivel cibernetic**. Iar odată cu explozia spațiului cibernetic dincolo de granițele propriilor noastre case și spații de lucru, utilitatea acestui fenomen tehnologic a căpătat și o **dimensiune macro**. **Spațiul cibernetic este acum *mass-market.*** Tehnologia este în viața noastră, a tuturor. Fiecare casă, fiecare familie și fiecare organizație sunt astăzi parte din revoluția tehnologică. Producția de energie electrică, producția de autovehicule, de gaze naturale, de jucării, de produse alimentare, toate sunt super-tehnologizate, având componente IT în ciclul de producție. Distribuția de energie electrică, de gaze naturale, transportul pe calea ferată, transportul aerian sunt coordonate cu ajutorul sistemelor inteligente și ale soluțiilor *software* specializate.

MEDIUL CIBERNETIC TREBUIE SĂ FIE FUNCȚIONAL ȘI SIGUR

Pe scurt, fiecare automobil modern, fiecare jucărie, aproape fiecare articol electrocasnic modern, toate sunt produse cu ajutorul unor soluții *software* - fundamentul funcțional al mediului cibernetic. Iar acest fenomen evoluează și se dinamizează de la an la an. Gândind prin intermediul acestei paradigme - care este o realitate - este ușor de văzut cum viața noastră este nu doar îmbogățită, ci și condiționată de avantajele soluțiilor *software* și a mediului cibernetic. Ele îndeplinesc o nevoie, dar reprezintă și o necesitate pentru că implică atât de multe dintre aspectele vieții noastre de zi cu zi. Pentru a putea avea o societate funcțională, mediul cibernetic trebuie să fie și el funcțional și sigur. Iar în acest caz nu este de mirare că **pentru anul 2016 cea mai importantă tendință a dezvoltării în tehnologie este securitatea cibernetică**. Bugete crescute, vulnerabilități care pot costa organizațiile din ce în ce mai mult, un mediu virtual tot mai efervescent, toate acestea sunt ingredientele unui fenomen care cere clar niște direcții de securitate la nivel național. Iar aceste direcții există deja.

În acest context, atât în ceea ce privește apărarea națională, cât și în ceea ce privește mediul de business, securitatea cibernetică devine o necesitate - nu o opțiune. Statele investesc din ce în ce mai mult în securitatea cibernetică, iar rezultatele sunt concretizate în mediul cibernetic relativ stabil pe care acestea reușesc să îl mențină. Însă conștientizarea la nivel social trebuie să crească pentru că **gradul de utilizare al Internet-ului în România este crescut** și pentru **că infrastructura noastră de *Internet*** și comunicare - una dintre cele mai noi și mai performante din lume - promite să lărgească și mai mult orizontul tranzacțiilor ***online.*** Iar aceasta înseamnă nu doar că miza este mare, ci că mai are mult loc să crească. Un asemenea fenomen generalizat impune și niște reguli de utilizare pentru că dacă miza este mare, interesul pentru găsirea vulnerabilităților este și el.

Țările au organizații naționale care se ocupă cu găsirea vulnerabilităților de acest fel, iar aceste organizații au un rol deosebit de important la nivelul securității cibernetice naționale, însă pentru a putea acoperi întregul fenomen este nevoie de un întreg curent de educație și conștientizare care să crească permeabilitatea societății la acest tip de informații. Să luăm ca exemplu unul dintre mesajele publicate de **Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)** - instituția centrală în România care se ocupă cu asigurarea securității cibernetice la nivel național:

„Marți, 3 martie 2015, un grup de cercetători a descoperit o nouă vulnerabilitate SSL/TLS (CVE-2015-0204), denumind-o FREAK, acronim pentru Factoring RSA Export Keys. Această vulnerabilitate permite atacatorilor să intercepteze conexiuni de tip HTTPS între clienții vulnerabili și serverele web, forțându-i să utilizeze criptografia de tip «export-grade».”

*** BUGETE CRESCUTE, VULNERABILITĂȚI CARE POT COSTA ORGANIZAȚIILE DIN CE ÎN CE MAI MULT, UN MEDIU VIRTUAL TOT MAI EFERVESCENT, TOATE ACESTEA SUNT INGREDIENTELE UNUI FENOMEN CARE CERE CLAR NIȘTE DIRECȚII DE SECURITATE LA NIVEL NAȚIONAL.**

Sunt sigur că un astfel de mesaj, unul din numeroasele publicate de **CERT-RO** pe pagina lor, nu sunt destul de conștientizate de mediul social, iar aici mă refer la un spectru semnificativ de oameni care ar trebui să urmărească aceste vulnerabilități: de la administratori de rețea, programatori sau alți specialiști în domeniul IT, până la angajați ai firmelor care își derulează diferite activități prin mediul online, inclusiv comunicații, *banking*, *online business* sau simple organizații care fac ori acceptă plăți *online*. Spectrul de oameni este amplu, iar permeabilitatea nu este încă suficient de mare, chiar dacă tot **CERT-RO** anunța în urmă cu ceva timp apariția unui virus troian orientat spre 12 instituții financiar-bancare din România sau un altul spre sisteme de operare mobile folosite la scara largă.

Instituții specializate ale statului lupta cu atacurile cibernetice, iar sumele investite în securitatea cibernetică devin tot mai semnificative. Însă pentru mediul privat, a permite ca informațiile clienților să fie „pierdute” nu este productiv. Iar companiile au conștientizat din ce în ce mai mult acest lucru, însă este și acesta un proces care probabil va mai dura. Un atac cibernetic poate păta reputația organizațională a unei firme și, la fel de important, poate reduce confortul publicului în a împărtăși informații relevante *online*. Aceasta este o problemă pentru că **parte din atomicitatea proceselor de comunicare din societatea noastră se bazează pe încrederea utilizatorului în mediul *online.*** Devine clar, așadar, că trebuie să investim în această direcție. Dar cum?

Cred că una dintre oportunitățile relevante în acest moment trebuie să se bazeze pe educația în privința securității cibernetice. Și este important ca acest lucru să se întâmple la toate nivelurile societății: de la sistemul de învățământ la sistemul de training al angajaților din cadrul organizațiilor private. Acest context cred că poate deveni o oportunitate la nivel național pentru că avem capacitatea de a oferi acest tip de educație. Un argument în acest sens este chiar faptul că avem specialiști IT de calibru în universități, iar instituții ale statului fac deja acest lucru. România a desfășurat proiecte prin care a antrenat specialiști pentru investigații de securitate cibernetică în Sri Lanka. Dacă putem extinde un astfel de serviciu spre beneficiul societății, de ce să nu o facem? O structură în care acest lucru ar putea să capete formă ar fi ca universități din România, împreună cu instituții ale statului, să vină în sprijinul operatorilor economici prin cursuri și *training*-uri. Mulți dintre specialiștii produși de Universitatea Politehnica din București urmează cariere de experți în domeniul securității cibernetice. Așadar, printr-un parteneriat stabil cu instituții ale statului, numărul de servicii direcționate în acest sens ar putea să crească în beneficiul societății românești.

BUGETE URIAȘE ÎN DOMENIUL SECURITĂȚII ONLINE

Este adevărat că unele dintre marile corporații investesc bugete uriașe în domeniul securității *online* și că au drept angajați unii dintre cei mai buni specialiști în acest sens, însă este bine de ținut minte că exact acestea sunt și unele dintre companiile care au avut cel mai mult de pierdut de pe urma vulnerabilităților cibernetice. Cu alte cuvinte,

în mod cert cei mai buni specialiști în domeniul securității cibernetice se găsesc tot în mediul privat, însă pentru un fenomen *mass-market* este nevoie de un val de educație care să poată vorbi unui număr din ce în ce mai mare de oameni.

Companiile mari își alocă bugete importante pentru dezvoltarea infrastructurii de IT și cu precădere a infrastructurii de securitate, și nu doar în domenii precum *e-Commerce* sau *banking* ci și în *retail*. Însă cu puțină creștere a nivelului de conștientizare, cred că putem atrage atenția asupra faptului că investițiile în training-uri de specialitate sunt la fel de importante pentru asigurarea securității propriu-zise pentru că de multe ori eroarea nu este la nivel digital, ci, uman. Multe dintre vulnerabilitățile existente cer aprobarea utilizatorului într-un fel sau altul pentru a putea accesa informații personale sau de serviciu. Și cred că acest detaliu este un indiciu foarte relevant.

VULNERABILITĂȚILE VOR PROVOCA PIERDERI DIN CE ÎN CE MAI MARI

Concluzia directă: avem **nevoie de educație** în acest sens. Sigur, investițiile în infrastructură vor rămâne la fel de mari, însă cu cât **mediul cibernetic va deveni mai extins și mai necesar vieții noastre cotidiene, vulnerabilitățile cibernetice vor putea provoca pierderi din ce în ce mai mari**. Suntem obișnuiți cu faptul că Internetul predomină societatea noastră și facem eroarea de a presupune că îi cunoaștem și regulile. Însă multe dintre vulnerabilitățile existente ne dovedesc exact opusul.

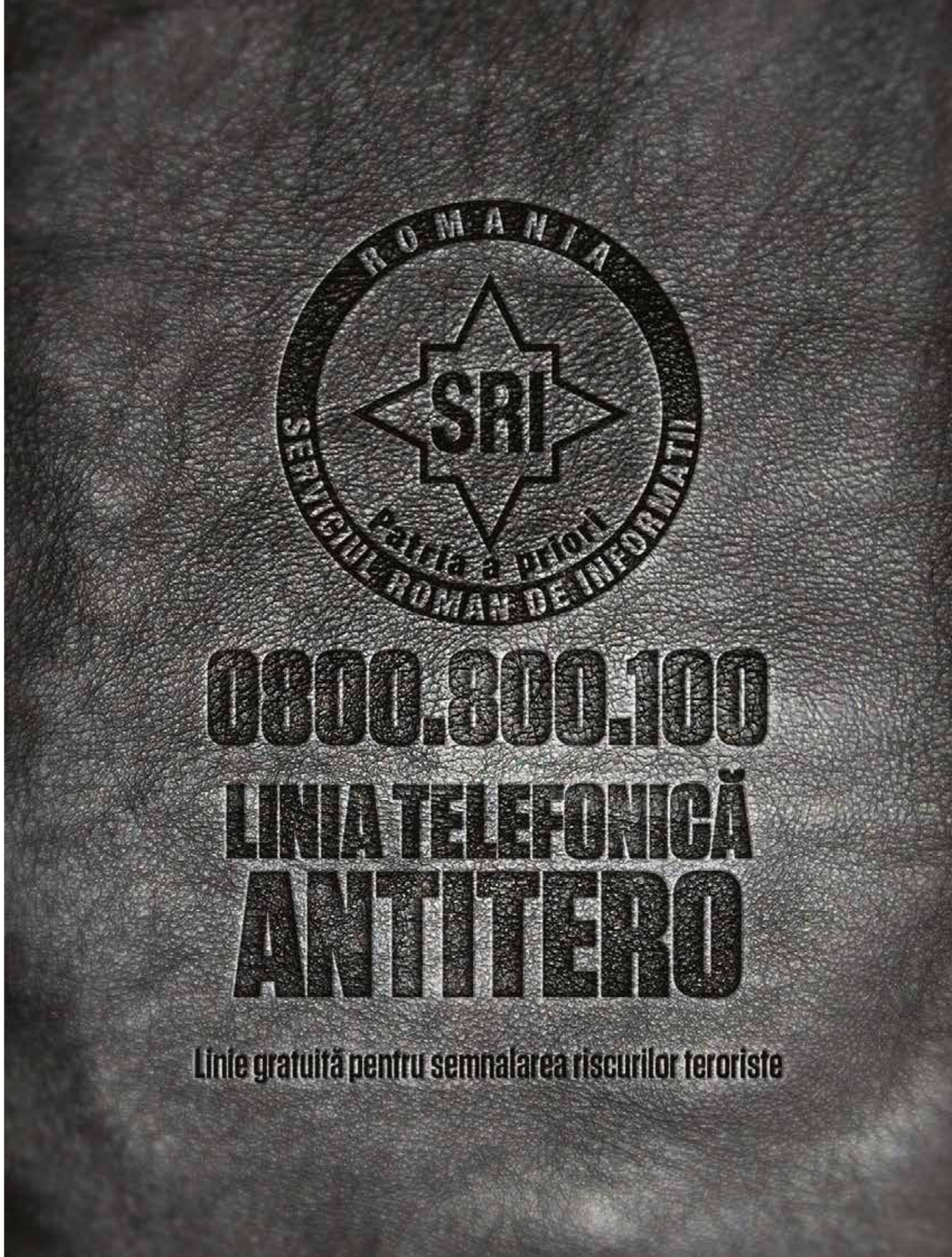
Cred că **2016 va fi un an important în schimbarea de paradigmă a societății în ceea ce privește securitatea cibernetică** pentru că se vor aloca bugete din ce în ce mai importante pentru soluționarea acestor vulnerabilități prin educație, iar acest lucru va crea o direcție clară de dezvoltare și la nivel național. În același timp, inovațiile tehnologice promit să extindă interacțiunea umană cu mediul cibernetic, ceea ce dinamizează și mai mult o piață în continuă expansiune și schimbare. Nevoia de stabilitate cel puțin în ceea ce privește securitatea este din ce în ce mai bine conturată.

Desigur, instituțiile specializate în acest sens fac eforturi importante pentru a acoperi o cerere din ce în ce mai mare, însă este clar că implicarea trebuie să vină din mai multe direcții pentru a putea reuși să ținem pasul cu evoluția tehnologiei. România are instituții importante în acest domeniu care sunt sigur că vor primi din ce în ce mai multă atenție în viitorul apropiat. Însă pentru ca educația în securitate cibernetică să poată fi popularizată la nivel național la același nivel cu mediul *online*, este nevoie de un număr din ce în ce mai mare de inițiative și de capacitatea de a aduce expertiza din zona de securitate cibernetică (la nivel național sau militar) în mediul civil.

Pentru a contribui la acest obiectiv național și social, **Universitatea Politehnica din București și-a propus crearea unui centru de securitate cibernetică destinat zonei civile în parteneriat cu universități militare sau alte instituții specializate**. Este o inițiativă care sper să marcheze un început, dar care, mai mult decât orice, reprezintă o invitație la colaborare, pentru că dacă am învățat ceva din numeroasele proiecte pe care universitatea noastră le-a desfășurat până în prezent, aceasta este că progresul este imposibil fără colaborare.

ABSTRACT

The last couple of years have shown that the near future is directed towards automation and technological control at a cybernetic level. The expansion of cyber space beyond the limits of our own homes and workplaces gives a macro dimension to the utility of this technological phenomenon. Cyber space is now mass market. In order to have a functional society, cyber space itself has to be functional and safe. Cyber security has become the number one trend in technological development, becoming a necessity, not an option in both matters regarding national security and the business environment. Investments in infrastructure are significant. Still, vulnerabilities can cause extreme damage, the larger cyber space becomes. We are used to the idea that the Internet is present in every aspect of our lives and we assume we know its rules. Vulnerabilities prove us wrong and the best way to protect ourselves is to get educated in the matter.



PLANIFICAREA STRATIFICATĂ A SECURITĂȚII CIBERNETICE LA NIVELUL UNEI ORGANIZAȚII

de Sebastian CAMINSCHI

În contextul unui mediu informațional dinamic și predispus atacurilor cibernetice de amploare, este important ca fiecare organizație, fie că vorbim de companii mai mari sau mai mici sau de instituții publice și agenții guvernamentale, să adere la implementarea unor acțiuni bine puse la punct de securitate cibernetică. Astfel, devine o misiune în sine identificarea responsabilă a vulnerabilităților sistemelor informatice, atât pentru protecția datelor cu valență strategică, cât și pentru asigurarea unei bune funcționări a infrastructurilor organizației.

ATENȚIE LA TRANSFERUL DE DATE

Securitatea datelor este crucială pentru toate organizațiile. Informațiile despre consumatori și clienți, informațiile despre plăți, dosarele personale, detaliile conturilor bancare - toate aceste informații sunt adesea imposibil de înlocuit în cazul în care sunt pierdute și sunt periculoase dacă ajung în mâinile atacatorilor. Modul în care sunt manipulate și protejate este esențial pentru securitatea organizației și așteptările de confidențialitate ale clienților, angajaților și partenerilor. Fie că vorbim despre resurse umane, fie despre resurse materiale sau tehnologice angrenate în asigurarea securității cibernetice, este important ca, la nivelul organizației, acestea să fie inventariate pentru a putea realiza o balanță echilibrată între valoarea datelor protejate și performanța resurselor necesare.

Experții în securitate consideră că **datele sunt supuse riscului atunci când sunt transferate**. Dacă toate datele organizației s-ar afla într-un singur computer sau *server* care nu este conectat la alte sisteme și nu ar părăsi niciodată acel computer, ar fi probabil foarte ușor de protejat. Însă, majoritatea activităților necesită ca datele să fie transferate și utilizate în întreaga companie, trebuie să fie accesate de angajați, analizate și cercetate în scopuri de marketing, utilizate pentru a contacta clienții și chiar accesate împreună cu partenerii-cheie. De aceea, la nivelul organizației trebuie să existe **un plan și o politică** - un set de linii directoare - despre cum trebuie protejat fiecare tip de date, în funcție de unde sunt plasate și cine le va utiliza.

Politica de confidențialitate trebuie să descrie informațiile protejate și trebuie să conțină referiri din care să rezulte faptul că protecția informațiilor este o prioritate, iar nerespectarea confidențialității poate aduce penalizări costisitoare pentru clienți sau angajați. Conducătorii organizației sunt direct răspunzători de ceea ce solicită și ceea ce oferă în politica de confidențialitate; de aceea, este important ca politica să fie adaptată nevoilor, iar regulile și așteptările să fie împărtășite către toți angajații și partenerii care pot veni în contact cu acele informații. De asemenea, **crearea copiilor de rezervă** este foarte importantă pentru protecția datelor în cazul în care datele sunt furate, alterate de *hackeri* sau chiar șterse accidental de către un angajat.

Orice organizație trebuie să-și facă un plan pentru situații neașteptate, cum ar fi pierderea sau furtul de date, ce pot expune afacerile la un risc semnificativ de litigii, plan care va face mai ușoară lansarea unui răspuns rapid și coordonat, indicând partenerilor cât de pregătită este organizația pentru a face față agresiunilor cibernetice.

SECURITATEA REȚELEI LA NIVELUL UNEI ORGANIZAȚII

Rețeaua internă a unei organizații ar trebui să pună la dispoziția angajaților doar acele servicii și resurse care sunt esențiale pentru activitatea și nevoile lor de zi cu zi.

Elementele necesare pentru definirea celor mai bune metode de securizare a rețelei informatice constau în: identificarea tuturor echipamentelor și conexiunilor din rețea, stabilirea limitelor dintre sistemele organizației și cele la care se interconectează, impunerea controalelor împotriva accesului neautorizat, respectiv identificarea evenimentelor de refuz de servicii. Din practică s-a constatat că cele mai eficiente metode de securizare a unei rețele constau în separarea de Internetul public prin mecanisme solide de autentificare a utilizatorilor și sisteme de impunere a politicilor de acces implementate prin paravane de protecție, dublate de mecanisme de filtrare a traficului *web*. De asemenea, soluțiile suplimentare de monitorizare și securitate, cum ar fi programele antivirus și sistemele de detecție a intruziunilor, trebuie să fie utilizate pentru a identifica și stopa încercările de accesare neautorizată a resurselor. După identificarea punctelor limită din rețeaua companiei, fiecare terminație trebuie evaluată pentru a determina ce tipuri de controale de securitate sunt necesare, respectiv *routerele* trebuie să permită realizarea traficului spre și de la adresele IP publice ale companiei și să realizeze partajarea lățimii de bandă pe care o oferă furnizorul de servicii de Internet. Paravanele de protecție trebuie să permită realizarea traficului doar către și de la setul minim de servicii necesare, iar sistemele de detecție a intruziunilor trebuie configurate pentru a monitoriza activitatea suspectă ce trece prin perimetrul rețelei protejate.

Dacă la nivelul organizației este necesară operarea unei rețele fără fir pentru utilizarea Internetului către clienți, invitați și vizitatori, este important ca această resursă să fie păstrată separat de rețeaua principală a companiei, astfel încât traficul din rețeaua publică să nu poată interfera cu sistemele interne. Accesul în rețeaua nepublică trebuie restricționat la dispozitivele și utilizatorii specifici organizației în cea mai mare măsură posibilă, îndeplinind în același timp și necesitățile de afaceri. De asemenea, dacă necesitățile impun ca anumite dispozitive să se conecteze atât la rețeaua publică, cât și la cea nepublică, trebuie luate măsuri de interzicere prin mecanisme de ordin tehnic a conectării simultane, iar dacă anumite ramuri ale rețelei nepublice funcționează în tehnologie fără fir este obligatoriu ca acestea să fie protejate prin criptare cu acces protejat. În cazul în care resursele din rețeaua internă trebuie accesate de la distanță, utilizând mediul Internet, unul dintre mecanismele cele mai solide este utilizarea rețelelor virtuale private însoțită de autentificare cu

doi factori, pe bază de certificate digitale.

Totodată, utilizatorilor trebuie să li se furnizeze *„credențiale”* de acces unice, cu date de expirare presetate, iar politicile de parole trebuie să determine angajații să utilizeze cele mai solide parole posibile, fără a crea nevoia sau tentația de a reutiliza parole sau de a le scrie. Toate sistemele și *software*-urile, inclusiv pentru echipamentele din rețea, trebuie să fie actualizate la timp, prin utilizarea serviciilor de actualizare automată, în special pentru sistemele de securitate precum aplicațiile împotriva *software*-urilor rău intenționate, instrumentele de filtrare *web* și sistemele de prevenire a intruziunilor.

În regulamentul informatic ce guvernează utilizarea rețelei trebuie să fie făcute precizări clare privind utilizarea mediilor de stocare externe, iar acolo unde nu există implementate mecanisme tehnice de limitare și control a accesului, utilizatorii trebuie instruiți să nu introducă niciodată suporți de memorie proveniți din surse necunoscute și să nu deschidă fișiere cu care nu sunt familiarizați.

SECURITATEA SITE-URILOR WEB

Serverele web, care găzduiesc date sau alt conținut disponibil clienților în Internet, sunt adesea cele mai vizitate și atacate componente ale rețelei unei companii. Infractorii cibernetici caută în permanență *site*-uri *web* securizate în mod necorespunzător pentru a le ataca, în timp ce mulți clienți consideră că securitatea *site*-urilor este un criteriu de top atunci când aleg, de exemplu, să facă cumpărături *online*. Consecințele neimplementării unor măsuri adecvate de protecție sunt în general mari și țin de pierdere de profituri, prejudicierea credibilității în fața clienților și uneori răspunderea judiciară. În general, atacatorii caută să exploateze vulnerabilitățile *software* din *serverul web*, care au la bază sistemul de operare sau conținutul activ, pentru a obține accesul neautorizat la serviciile sistemului sau la sistemul de fișiere și compromiterea acestuia prin executarea de comenzi, instalarea de *software*-uri rău intenționate, blocarea anumitor servicii, înlocuirea conținutului legitim sau utilizarea capabilităților pentru anonimizare în derularea altor atacuri.

Concomitent cu implementarea funcționalităților *site*-ului trebuie avute în vedere și problemele de securitate, care trebuie apreciate ca un compromis între utilitate, performanță și risc. Configurațiile *hardware* și *software* implicite sunt, de obicei, setate de producători pentru a scoate în evidență caracteristicile, funcțiile și ușurința utilizării în detrimentul securității, motiv pentru care, pornind de la sistemele de operare pe care se bazează *serverele web* și continuând până la nivelul bazelor de date, administratorii trebuie să transpună în parametrii adecvați cerințele de securitate. Principiul primordial este instalarea cantității minime de servicii ale *serverului web* și eliminarea oricăror vulnerabilități cunoscute, prin *patch*-uri sau *upgrade*-uri.

Site-urile *web* sunt adesea unele dintre primele locuri în care infractorii cibernetici caută informații valoroase, ceea ce presupune existența unui proces sau politică de publicare care să determine ce tip de informații se publică în mod deschis, ce informații se publică cu acces restricționat și ce informații ar trebui să nu fie publicate în oricare din depozitele accesibile publicului. Fără implementarea autentificării corespunzătoare a utilizatorilor, organizațiile nu pot restricționa în mod selectiv accesul la informații specifice; în plus, fără anumite procese de autentificare a *serverului*, utilizatorii nu vor putea determina dacă *serverul* este autentic sau o versiune contrafăcută, operată de un infractor cibernetic.

Infrastructura rețelei (ex. paravanele de protecție, *router*-ele, sistemele de detecție a intruziunilor) care sprijină *serverul web* joacă un rol critic de securitate, de aceea, în majoritatea configurațiilor, aceste echipamente vor fi prima linie de apărare între un *server web* public și Internet. Arhitectura rețelei nu poate proteja singură un *server web*, din cauza complexității și varietății atacurilor, de aceea securitatea serviciilor *web* trebuie implementată prin mecanisme diversificate de protecție stratificate, a căror întreținere necesită efort constant, resurse și vigilență în ceea ce privește configurarea, protejarea și analiza fișierelor jurnal, crearea de copii de rezervă pentru informațiile critice, testarea și aplicarea *patch*-urilor de securitate și, nu în ultimul rând, testarea periodică a nivelului de securitate cibernetică.

SECURITATEA E-MAILULUI

E-mailul a devenit o parte critică a activității de zi cu zi, începând de la managementul intern și până la asistarea directă a clienților. Beneficiile asociate cu *e-mailul*, ca un instrument de afaceri primar, sunt mult mai mari decât aspectele negative, de aceea o platformă *e-mail* de succes începe cu principiile de bază ale securității privind confidențialitatea, protecția clientului și a informațiilor de afaceri.

E-mailul este metoda primară pentru răspândirea virușilor informatici, a *software*-urilor rău intenționate, dar, totodată, este una dintre cele mai facile căi de protecție împotriva acestora. Aplicațiile de filtrare a *e-mailurilor* nesolicitate și nedorite reprezintă una dintre componentele importante ale unei strategii solide antivirus, care, dacă sunt actualizate și analizate cu regularitate, constituie o linie de apărare tehnologică importantă împotriva intruziunilor de la nivelul rețelei.

Angajații trebuie să utilizeze *e-mailul* în mod responsabil pentru ca eforturile organizației împotriva riscurilor cibernetice să creeze un mediu de lucru educat în protejarea intereselor de afaceri. Aici trebuie avut în vedere faptul că *e-mailul* nu este conceput pentru a fi sigur, incidentele de adresare greșită sau redirecționare pot conduce la scurgerea accidentală de date.

Un alt aspect care trebuie avut în vedere, pornind de la stocare și *back-up* până la cerințele legale și de reglementare, este cel al retenției *e-mailurilor* și implementarea de controale de bază pentru a ajuta angajații să le rețină doar atât timp cât susțin activitățile desfășurate.

CONCLUZII

Abordarea stratificată a metodelor de protecție împotriva software-urilor rău intenționate reprezintă calea ce trebuie urmată împotriva amenințărilor la adresa securității rețelei unei organizații. Protecția eficientă împotriva virușilor informatici, a troienilor sau a altor aplicații software rău intenționate trebuie să vizeze o combinație de tehnici, soluțiile antivirus fiind o necesitate, însă nu trebuie să fie singura linie de apărare.
De asemenea, utilizarea mediilor de stocare externe poate constitui calea de acces în sisteme țintă pentru o serie de aplicații rău intenționate, care pot afecta integritatea, disponibilitatea și confidențialitatea datelor companiei.
Combinând metode ca utilizarea filtrării web, protecția prin semnături antivirus, protecția proactivă împotriva software-urilor rău intenționate, paravane de protecție, păstrarea actualizată a versiunilor aplicațiilor instalate, se reduce riscul de infecție, iar prin instituirea unor politici solide de securitate și instruirea utilizatorilor va crește semnificativ siguranța sistemelor.

ABSTRACT

In the context of a dynamic informational environment prone to cyber-attacks, it is important that organizations, whether they are companies, public institutions or government agencies, adhere to the implementation of well-developed cyber security actions. The layered approach of network protection methods is the way forward against cyberspace threats which, together with the establishment of solid security policies and user training, will significantly increase the safety of the systems.

SECURITATEA CIBERNETICĂ EUROPEANĂ

CĂTRE O PIAȚĂ DIGITALĂ UNICĂ

de Mihai DINESCU

În mod incontestabil, prosperitatea și libertatea societății contemporane depind într-o proporție covârșitoare de tehnologiile digitale. Avansul așa-numitului „Internet al lucrurilor” (*Internet of things*) ilustrează tocmai modul în care sistemele și rețelele informatice tind să ne acapareze viața cotidiană. Chiar și recenta ediție a **Forumului Economic Mondial de la Davos** a stat sub semnul tehnologiilor inovatoare precum inteligența artificială, imprimarea 3D, nano- și bio-tehnologia, vorbindu-se tot mai mult despre „a patra revoluție industrială”. Având una dintre cele mai avansate economii din lume, **Uniunea Europeană (UE)** nu poate ignora avansul tehnologic și riscurile de securitate pe care le presupune dependența de tehnologia informațională. Mai mult, chiar unele modele de afaceri de succes pornesc astăzi tocmai de la premiza accesului constant la Internet.

În același timp, rețelele și sistemele informatice pot fi afectate într-o măsură tot mai mare de incidente care cresc în amploare, frecvență și complexitate, provocate atât prin atacuri malițioase, cât și prin erori umane, dezastre naturale sau pur și simplu prin eșecuri tehnice. Toată această multitudine de amenințări cibernetice au determinat Uniunea să conștientizeze că un nivel ridicat al securității cibernetice este în măsură să mențină atât încrederea consumatorilor în economia europeană, cât și să consolideze piața internă și creșterea economică.

Ținând cont de această evoluție, instituțiile centrale ale UE și statele membre și-au asumat în ultimii ani o serie de direcții de acțiune pentru consolidarea securității în mediul *online* european.

Primul pas a constat în elaborarea unor documente programatice care definesc acțiunile **UE** în domeniul securității cibernetice și al combaterii criminalității cibernetice, înscrise în marja **Agendei Digitale a UE**. Aceasta din urmă stabilește **7 domenii de acțiune esențiale pentru ameliorarea gradului de reziliență în fața atacurilor cibernetice**, domenii ce au în vedere:

- **realizarea pieței digitale unice** - ținând cont de faptul că tot mai mulți dintre cetățenii europeni își gestionează viața cotidiană cu ajutorul resurselor *online*, obiectiv pentru care este nevoie de uniformizarea serviciilor digitale de înaltă calitate la nivelul întregii Uniuni;
- **stimularea interoperabilității sistemelor informatice și a standardizării tehnologice** - pentru ca dispozitivele, aplicațiile, serviciile și rețelele informatice să poată funcționa în orice stat membru UE;
- **consolidarea încrederii și a securității *online*** - prin combaterea criminalității cibernetice și a breșelor în securitatea datelor cu caracter personal;
- **promovarea accesului nediscriminatoriu la Internet de mare viteză** - acesta urmând să fie asigurat tuturor cetățenilor europeni la prețuri accesibile și competitive;
- **investiții în cercetare și inovare** - pentru o creștere economică sustenabilă, inclusiv prin parteneriate între sectorul public și cel privat;
- **promovarea alfabetizării digitale** - având în vedere că unii dintre cetățenii europeni nu sunt expuși mediului digital, cu toate că Internetul este tot mai prezent în viața noastră de zi cu zi;
- **exploatarea potențialului tehnologiilor IT&C** - în domenii precum schimbările climatice, îmbătrânirea populației, digitalizarea conținutului sau sistemele inteligente de transport.

În continuarea principiilor asumate de către **UE** prin **Agenda Digitală**, legislația europeană a dobândit în ultimii ani **două acte normative de o importanță deosebită**, respectiv **Strategia de securitate cibernetică a UE** și **Proiectul Directivei privind securitatea rețelelor și a informației** (*Network and Information Security*/ NIS). Ambele documente au ca obiectiv principal stabilirea măsurilor legale și a stimulentelor necesare pentru ca mediul *online* din Europa să devină unul dintre cele mai sigure din lume.

O STRATEGIE PENTRU SECURITATEA CIBERNETICĂ A UE

Adoptată în **2013**, **Strategia de securitate cibernetică a UE** este în primul rând rezultatul conștientizării schimbărilor profunde pe care le-a produs evoluția tehnologică în societățile europene. Spațiul cibernetic deschis și liber a produs deja efecte tangibile în termeni de incluziune socială și politică în întreaga lume, a înlăturat o mare parte din simbolismul frontierelor dintre state, comunități și cetățeni și a permis schimbul liber de idei și informații la nivel global. Mai mult, Internetul a permis crearea unui spațiu de exprimare liberă și de exercitare a drepturilor fundamentale, schimbare vizibilă în fenomene precum Primăvara arabă.

În acest nou context tehnologic, a devenit evident faptul că **UE** trebuie să aplice inclusiv *online* valorile și principiile pe care le apără *offline*, precum respectarea drepturilor fundamentale, a democrației și a statului de drept. Libertatea *online* necesită un nivel constant de securitate cibernetică, motiv pentru care, în viziunea Strategiei, guvernele statelor membre sunt cele care trebuie să își asume rolul central în protecția împotriva incidentelor și a activităților malițioase. Doar în acest fel ne putem propune garantarea eficientă a drepturilor fundamentale în spațiul cibernetic. Pe de altă parte, Strategia recunoaște rolul important al sectorului privat, care deține sau operează o parte semnificativă a infrastructurilor ce susțin mediul *online*.

Cu toții conștientizăm faptul că Internetul a devenit coloana vertebrală a creșterii economice. Tehnologia informațională este astăzi una dintre resursele critice de care depind toate celelalte sectoare economice-cheie, precum sistemul financiar, cel energetic și de transport. Mai mult, o mare parte dintre noile modele de afaceri pornesc tocmai de la premiza furnizării neîntrerupte a serviciilor de Internet.

Pe de altă parte, **Strategia de securitate cibernetică a UE** amintește de faptul că, potrivit „*2012 Special Eurobarometer 390 on Cybersecurity*”, aproximativ o treime dintre cetățenii europeni nu au încredere în folosirea Internetului pentru servicii bancare sau de cumpărături *online*. Mai mult, majoritatea cetățenilor europeni evită să își divulge datele personale *online* din rațiuni ce țin de securitatea cibernetică. Potrivit statisticilor europene, peste 10% dintre utilizatorii europeni au fost deja victime ale fraudelor *online*.

Cifrele îngrijorătoare ale anvergurii criminalității cibernetice ilustrează tocmai modul în care digitalizarea societăților dezvoltate aduce atât beneficii economice enorme, cât și vulnerabilități neașteptate la adresa unor servicii publice esențiale precum rețelele de apă, sănătatea publică, furnizarea energiei electrice sau telecomunicațiile.

ÎN ABSENȚA LIMITELOR SPAȚIULUI CIBERNETIC, ESTE LESNE DE ÎNȚELES CUM UN STAT EUROPEAN CU UN NIVEL SCĂZUT DE SECURITATE CIBERNETICĂ POATE FI O VULNERABILITATE PENTRU CELELALTE STATE MEMBRE ȘI CHIAR PENTRU UNIUNE ÎN ANSAMBLU.

O DIRECTIVĂ UE PENTRU UN MEDIU ONLINE MAI SIGUR

Ca urmare a adoptării **Strategiei de securitate cibernetică a UE**, în iunie 2013, **Comisia Europeană (CE)** a demarat procedura de adoptare a unei directive care să asigure un nivel comun de securitate cibernetică în toate statele membre. Practic, **Directiva NIS** este principala linie de acțiune a Strategiei de securitate cibernetică a **UE**. Pe lângă încurajarea cooperării dintre statele membre și a gradului de pregătire la nivel național pentru incidente de securitate cibernetică, Directiva își propune să introducă inclusiv obligativitatea operatorilor de infrastructuri critice de a notifica incidentele de securitate către autoritățile naționale competente. Astăzi, o mare parte dintre incidentele **NIS** nu ajung la cunoștința autorităților și nu pot conduce la adoptarea măsurilor adecvate pentru contracararea amenințărilor cibernetice.

Propunerea de directivă pornește de la două premise îngrijorătoare: pe de-o parte, se poate constata cu ușurință ineficiența demonstrată până în prezent de către mecanismele voluntare de raportare a incidentelor cibernetice în statele membre, iar pe de altă parte, aceleași state membre înregistrează grade diferite de pregătire în privința securității cibernetice.

Mai mult, Internetul nu cunoaște frontiere geografice. În absența limitelor spațiului cibernetic, este lesne de înțeles cum un stat european cu un nivel scăzut de securitate cibernetică poate fi o vulnerabilitate pentru celelalte state membre și chiar pentru Uniune, în ansamblu.

Astfel, fără un mecanism european coerent pentru o cooperare eficientă și pentru un schimb de informații bazat pe încredere, **CE** estimează că Uniunea va continua să se confrunte cu reglementări necoordonate și cu standarde divergente. În consecință, ne-am putea confrunta în continuare cu un nivel tot mai scăzut al securității cibernetice. Mai mult, fără un nivel adecvat de protecție în fața incidentelor de această natură, este posibilă chiar re-apariția unor bariere în interiorul pieței unice europene, fragmentare care va aduce costuri suplimentare pentru cetățenii europeni și pentru companiile care activează în mai multe state membre.

ABSTRACT

The rise of the “Internet of things” and the unavoidable “4th industrial revolution” determine the EU to aim for a better regulation of the cyberspace. As IT networks and systems are increasingly targeted by more frequent, wide and complex incidents, the EU common market can stay functional only through a proper level of cybersecurity.

Given the constant technological evolution and the fact that an increasing number of European start-ups are based on a business model that takes the Internet for granted, the EU has undertaken several steps along the European Digital Agenda. In practice, this approach has led to the adoption of an EU Cybersecurity Strategy and an EU Directive for Network and Information Security (NIS).

PROIECTUL EUROPEAN DE PROTEJARE A INFRASTRUCTURILOR CRITICE

de Alexandru GHIȚĂ

26 ianuarie 2016, orele 22:00. Varianta *online* a „The Times of Israel” publică știrea frapantă a unui atac cibernetic asupra rețelei IT deținute de un departament din cadrul Ministerului Energiei din Israel. Conținutul știrii redă o cuvântare susținută în dimineața aceleiași zile la conferința *Cybertech* din Tel Aviv prin care ministrul Yuval STEINITZ asigura audiența atât de existența incidentului cibernetic, cât și de capabilitățile statului israelian de a stopa efectele malițioase ale *malware*-ului idenficat. Ceea ce pare să fie surprinzător nu este contrastul dintre dominanța Israelului pe piața soluțiilor de securitate cibernetică și realitatea întâmplării, ci creșterea în frecvență a relatărilor publice ce au la bază un astfel de subiect.

Cu mai puțin de două săptămâni înaintea acestei știri, ediția *online* a *Reuters* relata existența unui alt incident cibernetic, de data aceasta în Ucraina, unde autoritățile au descoperit un calculator infectat în rețeaua informatică a aeroportului Boryspil din capitala Kiev. Codul malițios era similar cu cel pe care compania de securitate *ESET* într-o analiză de specialitate îl identificase ca fiind suspectul principal al penei de curent din 23 decembrie 2015, pană ce a afectat zona orașului Ivano-Frankivsk din Ucraina și, implicit, infrastructura companiei din domeniu, *Prykarpattyaoblenergo*.

Statistica atacurilor avansate ce țintesc infrastructura unei entități (*advanced targeted attacks*) sau care exploatează vulnerabilități necunoscute publicului larg (*zero-day exploits*) ne spune că, cel mai adesea, momentul detecției survine mult după ce s-a realizat deja infectarea rețelei. Putem presupune, deci, că știri ca cele prezentate mai sus sunt efecte ale unei posibile campanii îndelungate și planificate.

Pe o scară gradată a nivelului de insecuritate cibernetică, absența unei infrastructuri IT ne duce direct la bază, acolo unde suntem protejați chiar și de cel mai complex atac cibernetic ce ar putea exista vreodată, dar ce se întâmplă în cazul unei societăți informaționale care trebuie să asigure necesitățile cetățeanului conform epocii în care trăiește? În situația unei societăți ce își propune să ofere servicii publice eficiente, transparente și cel puțin disponibile *online*, nevoia

de asigurare a securității cibernetice devine un subiect intrinsec.

Întrebările firești care se nasc în acest context sunt dacă România ca stat este cel puțin pregătită să identifice un astfel de atac cibernetic la nivelul propriilor infrastructuri informatice? Dar și care sunt pașii necesari a fi urmați în asigurarea acestui deziderat? Fără a ne opri asupra carențelor legislative curente, un posibil răspuns pentru ultima întrebare îl putem identifica în conținutul Strategiei Naționale de Securitate Cibernetică aprobate prin HG nr. 271/2013.

În concordanță, Serviciul Român de Informații și-a propus, în prima parte a anului 2013, realizarea unui proiect cu fonduri europene nerambursabile care să implementeze prevederile a două din direcțiile de acțiune stabilite prin strategia amintită, respectiv [1] *Dezvoltarea capacităților naționale de management al riscului în domeniul securității cibernetice și de reacție la incidente cibernetice în baza unui „Program național" vizând [...] consolidarea, la nivelul autorităților competente, potrivit legii, a potențialului de cunoaștere, prevenire și contracarare a riscurilor asociate utilizării spațiului cibernetic [simultan cu] creșterea nivelului de reziliență al infrastructurilor cibernetice* și [2] *Promovarea și consolidarea culturii de securitate în domeniul cibernetic [prin] derularea unor programe de conștientizare a [...] administrației publice și a sectorului privat cu privire la vulnerabilitățile, riscurile și amenințările specifice utilizării spațiului cibernetic, [inclusiv prin] formarea profesională adecvată a persoanelor care își desfășoară activitatea în domeniul securității cibernetice, promovarea pe scară largă a certificărilor profesionale în domeniu [și] includerea unor elemente referitoare la securitatea cibernetică în programele de formare și perfecționare profesională a managerilor [...]*, oferind suportul informațional, analitic și decizional necesar funcționării *Sistemului Național de Securitate Cibernetică*.

EVOLUȚIA PROIECTULUI

În **decembrie 2013,** lua naștere proiectul **Sistem Național de Protecție a Infrastructurilor IT&C de Interes Național împotriva Amenințărilor Provenite din Spațiul Cibernetic**, încadrat în Axa Prioritară III „Tehnologia Informației și Comunicațiilor pentru sectoarele privat și public", Domeniul Major de Intervenție 2 „Dezvoltarea și creșterea eficienței serviciilor publice electronice", Operațiunea 2 „Implementarea de sisteme TIC în scopul creșterii interoperabilității sistemelor informatice".

Scopul *a priori* al proiectului a fost de a asigura **consolidarea sistemelor de securitate cibernetică existente la nivelul infrastructurilor critice naționale și a infrastructurilor guvernamentale**, având ca substrat dezvoltarea pe trei coordonate principale: actualizarea sau, după caz, completarea tehnologiilor de securitate existente în infrastructurile de securitate IT beneficiare, instruirea resursei umane responsabile cu administrarea acestor rețele și implementarea unui mediu colaborativ absolut necesar în contextul cibernetic actual.

O analiză anterioară derulării proiectului atrăgea atenția asupra unui **spectru variat de implementări a conceptului de securitate la nivelul instituțiilor de stat**, existența unor elemente IT neinteroperabile chiar în cadrul aceleiași infrastructuri, lipsa unor mijloace sau indicatori care să asigure analiza nivelului de securitate și, nu în ultimul rând, pregătirea deficitară a personalului cu responsabilități în domeniul în cauză. Toate aceste ipostaze ale nivelul de protecție existent la momentul realizării studiului reprezentau vulnerabilități în cunoașterea și conștientizarea prezenței unui posibil atac cibernetic în derulare la nivelul infrastructurii, fără a se mai lua în discuție eventuale capabilități de prevenire.

Revenind la statistică, majoritatea amenințărilor cunoscute ce țintesc infrastructuri IT, publice sau private, folosesc ca vector de infectare *site*-uri vulnerabile sau create special cu conținut malițios camuflat în codul paginilor *web*, mesageria electronică prin transmiterea unor mesaje cu atașament infectat, dar și orice dispozitiv mobil (laptop, telefon sau *stick* de memorie) ce poate fi inserat în rețeaua vizată. Pe fondul vulnerabilităților născute din politici de securitate precare, din lipsa unor metode de inspecție a fluxurilor de date menționate și din capabilitățile reduse de reacție ale resursei umane responsabile, acești vectori de infectare se transformă în adevărate riscuri la adresa securității cibernetice.

O privire exhaustivă asupra infrastructurii de rețea propuse de proiect cuprinde o gamă amplă de soluții de securitate delimitate în două zone ce au fost denumite generic **DMZ** și **INTERN**. În timp ce în arealul **DMZ**-ului sunt plasate sistemele ce iau contact cu mediul exterior și asigură accesul utilizatorilor interni la resursele din Internet, în zona **INTERNĂ** sunt gestionate informații specifice fiecărei organizații în parte.

Limitându-ne doar la o enumerare sumară a sistemelor achiziționate prin proiect, aceste **soluții de protecție împotriva atacurilor cibernetice** pot fi categorisite în funcție de rol:

CU ROL DE INSPECȚIE A TRAFICULUI PE BAZĂ DE SEMNĂTURI

- ***Mail Gateway*** - produs cu capabilități anti-*malware* și anti-*spam*, necesar verificării conținutului malițios al mesajelor din mesageria electronică;
- ***Unified Security Management*** - produs cu funcționalități integrate ce permit inspecția IDS/IPS, setări de *firewall* și de politici de securitate;
- ***Web Gateway*** - produs necesar inspectării traficului generat pe utilizatorii interni la accesarea *site*-urile din Internet;
- ***Web Application Firewall*** - produs destinat protecției serviciilor *web* expuse în Internet împotriva atacurilor cunoscute, precum ***Integer Overflows, Remote File Inclusion, Format String, Cross-Site Scripting, Cross-Site Request Forgery, SQL Injection*** ș.a.;
- **Soluție de Antivirus**;

CU ROL DE ANALIZĂ A TRAFICULUI PE BAZĂ DE COMPORTAMENT

- ***Soluție de analiză într-un mediu virtual*** - produs destinat analizei comportamentale a fișierelor executabile, *script*-urilor, DLL-urilor și a URL-urilor identificate în traficul *http* și *smtp*;

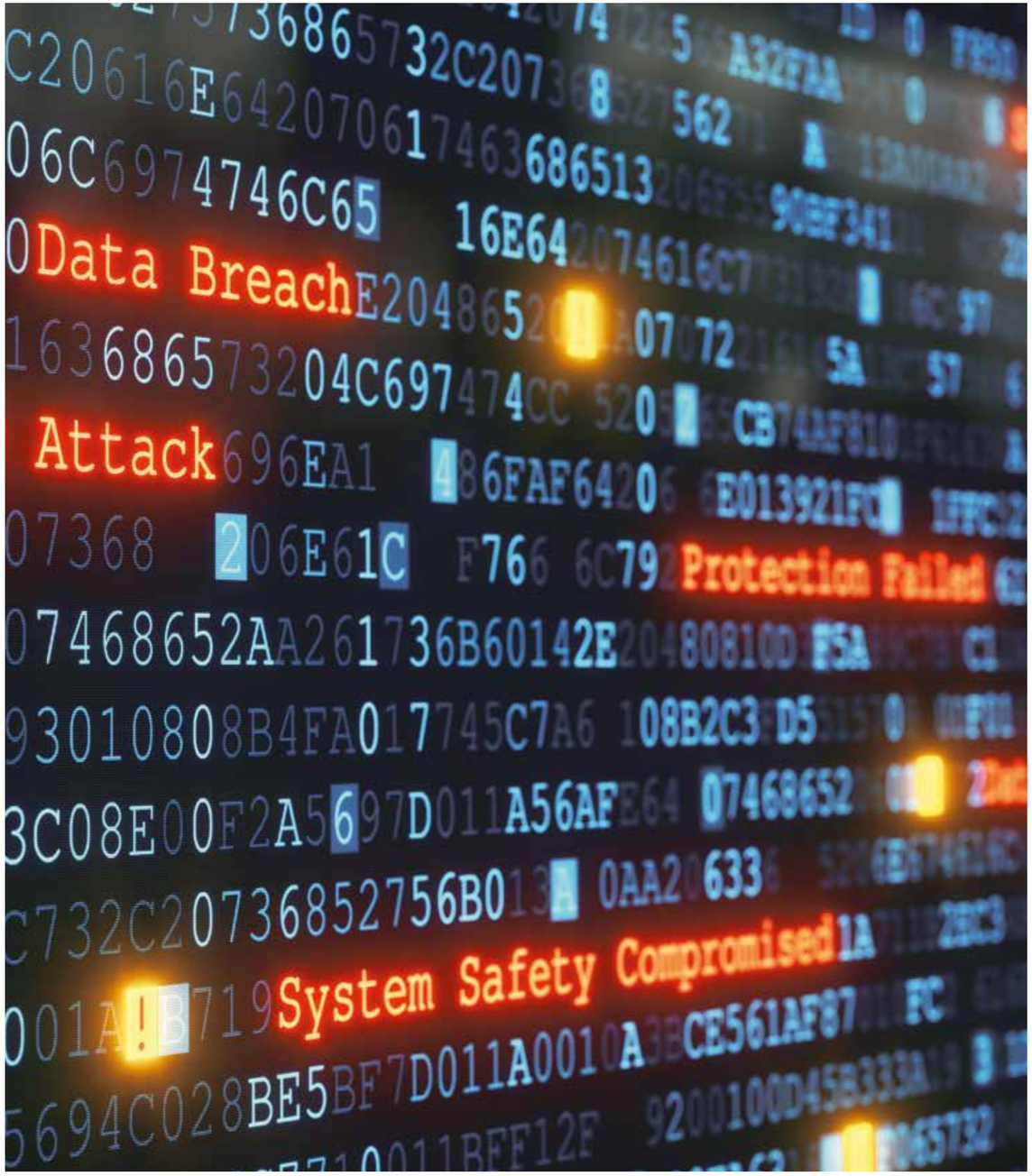
CU ROL DE EVALUARE ȘI MANAGEMENT AL VULNERABILITĂȚILOR

- ***Vulnerability Management*** - sistem de evaluare a securității sistemelor de operare și a aplicațiilor (*web* sau de altă natură) aflat la dispoziția administratorului de securitate local;
- ***Security Information and Event Management*** - produs ce are ca funcții colectarea centralizată, agregarea, normalizarea și corelarea evenimentelor de securitate generate de echipamentele de rețea și de securitate.

Toate soluțiile achiziționate au fost însoțite de cursuri de formare profesională cu scopul de a asigura instruirea angajaților responsabili cu administrarea și exploatarea tehnologiilor la nivelul fiecărei instituții.

Suplimentar asigurării cunoștințelor necesare de administrare, instruirea în domeniu prin aspectele sale sociale a favorizat și crearea unui mediu colaborativ, iar specializarea unui număr cât mai mare de oameni nu poate reprezenta decât un câștig în problematica spațiului cibernetic, orice abordare individuală în această arie având șanse reduse de succes.

Finalitatea proiectului a venit odată cu noiembrie 2015 și chiar dacă parcurgerea celor 23 de luni îngăduite implementării a cunoscut adesea momente de impas cauzate fie de inerția specifică, fie de resursa umană deficitară prin număr, astăzi putem afirma că un prim pas pentru protejarea infrastructurilor critice a fost făcut, lasând viitorului apropiat un alt pas, la fel de mare, spre dezvoltarea culturii tehnologice în mediul cibernetic.



ABSTRACT

City power outage and cyber security, is there at least one common feature to name? Nowadays we call it cyber-attack and it seems to be an increased presence in our monthly news. What can it be done to improve our infrastructures' protection against breakdowns, information leakage or any kind of cyber threat? As a good start, along with a trained human resource, it will be a minimum of cyber tools for inspection, investigation, and audit events in critical IT infrastructures. Those are the milestones that SRI achieved with the National Project for IT&C Infrastructure Protection against Threats Emanating from Cyberspace.

Intelligence

COOPERAREA INTERNAȚIONALĂ PENTRU UN CYBERSPACE SIGUR

de Miruna COCOLAN

Lumea globalizată este caracterizată de **interdependențe complexe**. Asistăm astăzi la dezvoltarea tehnologiilor și mijloacelor de comunicații într-un ritm fără precedent, proces cu un impact semnificativ atât asupra societății, cât și asupra indivizilor. Această dezvoltare aduce, pe lângă multitudinea de beneficii incontestabile, o serie de provocări.

Datorită avansului tehnologic, **mediul de securitate** devine din ce în ce **mai dinamic**, **vulnerabilitățile și amenințările depășind barierele spațiului fizic și manifestându-se, deseori, în mediul virtual**. Întrucât spațiul cibernetic este definit de absența frontierelor, prevenția și contracararea amenințărilor necesită adaptarea și inovarea metodelor și instrumentelor destinate îndeplinirii acestor scopuri. Potrivit lui Wolfgang ROHRIG și Rob SMEATON în „Cyber security and cyber defence in the European Union. Oportunities, synergies and challenges.", utilizarea din ce în ce mai frecventă a tehnologiilor moderne de comunicații produce schimbări sociale majore și conduce la dezvoltare economică, însă creează și un cadru favorabil desfășurării de activități ilegale.

Amenințările provenite din spațiul cibernetic sunt caracterizate de **dinamism și asimetrie**, având caracteristici globale. Aceste trăsături le fac greu de identificat și neutralizat prin măsuri izolate ale statelor. Astfel, devine pregnantă necesitatea de **cooperare** a tuturor entităților cu rol în asigurarea securității cibernetice, atât din spațiul public, cât și din cel privat. Cooperarea trebuie intensificată atât pe plan național, cât și pe plan internațional în vederea asigurării unor răspunsuri adecvate la amenințările provenite din mediul virtual.

ACORD DE NEAGRESIUNE CIBERNETICĂ SUA-CHINA

În ceea ce privește **activitatea de cooperare internațională**, aceasta joacă **un rol fundamental în prevenirea și combaterea riscurilor și amenințărilor la adresa securității naționale în toate domeniile de manifestare**. Când vorbim însă de amenințările emergente în spațiul virtual, a cărui caracteristică esențială este lipsa frontierelor, rolul acesteia devine tot mai pregnant.

Din ce în ce mai mult, statele pun accent pe intensificarea eforturilor de colaborare cu alte țări ori cu organizații internaționale pe subiectul amenințărilor cibernetice. **Statele Unite ale Americii (SUA)** sunt un participant activ la întâlniri ale **Organizației Națiunile Unite (ONU)** în domeniu, dezvoltând și planuri de cooperare bilaterală cu alte state pentru asigurarea securității cibernetice (v. *Council on Foreign Relations, Cyber Threats and International Cooperation, Workshop Summary Report, Washington DC, 26.02.2015*). În septembrie 2015, **SUA** au anunțat semnarea unui acord de neagresiune cibernetică cu **Republica Populară Chineză (RPC)**, subiect abordat de Adam SEGAL în „*The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement*". Ca urmare a demersurilor întreprinse în acest domeniu, au constatat însă că, pentru a ține pasul cu evoluția rapidă a amenințărilor provenite din mediul virtual, este nevoie de un efort orientat spre stabilirea unor norme de utilizare a spațiului cibernetic, dezvoltarea unor standarde de asumare a responsabilității pentru derularea de atacuri cibernetice statale și identificarea unor bune practici pentru prevenirea și apărarea împotriva agresiunilor cibernetice realizate de către actori non-statali.

Totodată, **organismele supranaționale** abordează din ce în ce mai des această problematică. **Organizația Tratatului Atlanticului de Nord (NATO)** deține propria infrastructură cibernetică și majoritatea statelor membre împărtășesc concepția conform căreia amenințările la adresa securității cibernetice reprezintă un motiv de îngrijorare, însă nu toate au aceeași percepție în ceea ce privește prioritățile strategice. **Neil ROBINSON** susține în „*Cyber Security Strategies Raise Hopes of International Cooperation*" - Rand Review, 2013, că **NATO** nu are autoritate asupra infrastructurilor destinate sectorului privat și societății civile din cadrul statelor membre, o nuanță importantă ținând cont că, de cele mai multe ori, când vorbim de amenințări cibernetice, limitele acestor sectoare nu sunt clar delimitate.

Când vorbim despre **Uniunea Europeană (UE)**, responsabilitățile în materie de securitate cibernetică sunt, în general, prerogative ale organismelor statelor membre. Deși nu există o abordare unitară la nivelul statelor asupra politicilor cibernetice în opinia lui **Neil ROBINSON**, a fost elaborată **Strategia UE pentru securitate cibernetică**, ce „reprezintă viziunea globală a UE asupra celor mai bune modalități de a preveni și de a gestiona perturbările și atacurile cibernetice" (v. „Problematica securității cibernetice în cadrul organizați-

PREȘEDINTELE SUA, BARACK OBAMA, ÎMPREUNĂ CU PREȘEDINTELE CHINEI, XI JINPING

DEZVOLTAREA COOPERĂRII INTERNAȚIONALE REPREZINTĂ O NECESITATE ȘI LA NIVEL NAȚIONAL, FIIND CUPRINSĂ ȘI ÎN STRATEGIA DE SECURITATE CIBERNETICĂ A ROMÂNIEI, ADOPTATĂ ÎN 2013.

ilor internaționale și implicarea României ca membru al acestora", www.mae.ro). Documentul statuează că Uniunea va coopera cu parteneri internaționali, cu sectorul privat și cu societatea civilă în ceea ce privește accesul liber la Internet și prevenirea amenințărilor provenite din mediul virtual. Una dintre prioritățile Strategiei vizează „stabilirea unei politici internaționale coerente a Uniunii Europene privind spațiul cibernetic și promovarea valorilor fundamentale ale UE", iar o măsură destinată implementării este „cooperarea internațională în domeniul spațiului cibernetic".

Dezvoltarea cooperării internaționale reprezintă o necesitate și la nivel național, fiind cuprinsă și în **Strategia de securitate cibernetică a României**, adoptată în 2013. **Principalele direcții de acțiune** în acest sens statuate de document sunt:

- încheierea unor acorduri de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;
- participarea la programe internaționale care vizează domeniul securității cibernetice;
- promovarea intereselor naționale de securitate cibernetică în formatele de cooperare internațională la care România este parte (*Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, Anexa nr. 1*).

România transpune direcțiile de acțiune incluse în Strategie prin implicarea în diferite **formate de cooperare internațională**, atât bilaterale cât și multilaterale. Statul nostru contribuie la formularea unor politici de securitate cibernetică în vederea constituirii unui cadru organizat de identificare, cunoaștere și prevenire a vulnerabilităților spațiului virtual. Totodată, statutul de membru al organizațiilor internaționale semnifică deținerea unui rol activ în eforturile internaționale de creare a unei abordări coerente și eficiente a oportunităților și provocărilor generate de spațiul cibernetic.

Amenințările întâlnite în spațiul cibernetic evoluează rapid. Apar metode noi de compromitere a datelor, de accesare ilegală a informațiilor, de obținere de date despre comportamentul utilizatorilor ori de îndeplinire a unor obiective contrare securității naționale. În vederea identificării unor metode adecvate de apărare în fața unor asemenea agresiuni, este necesară înțelegerea acestora.

Astfel, rolul pe care cooperarea internațională îl deține în procesul de asigurare a securității cibernetice este conferit și prin **prisma naturii amenințărilor generate în mediul Internet**, respectiv: amenințări cibernetice de sorginte statală, amenințări generate de actori non-statali, amenințări generate de grupări de criminalitate informatică, amenințări de natură extremist-teroristă. Toate aceste activități pot viza atingerea unor obiective împotriva securității naționale, pot avea ca efect afectarea disponibilității, confidențialității și integrității infrastructuri critice cibernetice ale statelor ori pot implica constituirea de către entități statale a unor capacități și capabilități ofensive cibernetice ce pot fi utilizate în agresiuni cibernetice.

Observăm că amenințările expuse anterior au în comun faptul că nu sunt delimitate de granițele teritoriale ale unui stat anume. Actorii se pot situa pe teritoriul uneia sau a mai multor țări, iar țintele nu se regăsesc, de cele mai multe ori, în același areal geografic. Astfel, planificarea, realizarea și producerea rezultatului unei agresiuni cibernetice sunt caracterizate de un caracter transnațional. Totodată, infrastructura necesară derulării agresiunilor de acest tip poate fi situată pe teritoriul mai multor state.

Identificarea unor modalități adecvate de răspuns la agresiunile cibernetice este dificilă întrucât atribuirea acestora necesită consumarea unor resurse mari de timp, precum și din cauza anonimității infractorilor în spațiul cibernetic. Aceste agresiuni nu au amploarea necesară pentru a necesita un răspuns de tip militar, însă au potențialul de a produce pagube semnificative pe termen lung, pot afecta economiile țărilor și pot pune dificultăți factorilor de decizie în adoptarea unui răspuns adecvat.

IMPORTANȚA CANALELOR DE COMUNICARE

În vederea formulării unei **reacții corespunzătoare la o agresiune de tip cibernetic** este necesară, în primul rând, identificarea atacatorului. Din cauza dificultății acestui proces de atribuire a atacului, există riscul indicării eronate a agresorului și, astfel, posibilitatea generării unui conflict bilateral. Astfel, rezultă necesitatea existenței unor canale de comunicare, respectiv dezvoltarea cooperării internaționale între entitățile cu rol în asigurarea securității cibernetice în scopul clarificării elementelor de interes și a realizării unei atribuiri corecte a atacului.

Amenințările la adresa securității cibernetice au produs **modificări în natura conflictelor**. Cele convenționale au loc în spațiul fizic (pe uscat, pe ape, în aer) și, totodată, presupun utilizarea unor instrumente palpabile. Emergența spațiului cibernetic însă a condus la extinderea zonelor de conflict, prin eliminarea barierelor geografice și creșterea numărului de participanți. Costurile reduse de derulare a unei agresiuni cibernetice au permis actorilor de tip non-statal să întreprindă atacuri cibernetice chiar și împotriva unor ținte cu un nivel tehnologic avansat. Deși atacurile la scară mai mare necesită resurse de tip financiar și capabilități avansate, cele la scară limitată pot fi realizate prin intermediul instrumentelor disponibile deja pe piața de profil.

În procesul de identificare și prevenire a agresiunilor cibernetice este necesară o analiză constantă a vulnerabilităților, amenințărilor, atacatorilor și metodelor utilizate. Surprinderea acestor elemente, necesare în procesele de evaluare a riscului și de dezvoltare a politicilor de securitate cibernetică, reprezintă o provocare raportată la dezvoltarea dinamică a acestui domeniu. Astfel, captarea lor într-un timp scurt este posibilă doar prin intermediul unei strânse cooperări internaționale, ce necesită depunerea de efort susținut la nivel național, european și global.

ABSTRACT

Nowadays the world is marked by the rapid evolution of communication and information technologies, which brings important opportunities but also serious challenges. In the borderless realm of cyberspace, the nature of the conflict has changed. The actors are spread beyond geographical boundaries and hard to identify, so it is a certainty that cyber security cannot be achieved by each state on its own. Only by building and maintaining a strong international cooperation can we answer the question: "How can we ensure the security of cyberspace?".

Intelligence

SECURITATEA CIBERNETICĂ ÎN NATO

de Camelia UNGUREANU și Eugen POPESCU

Securitatea cibernetică este **o temă tratată cu prioritate din ce în ce mai mare în cadrul Organizației Tratatului Atlanticului de Nord (NATO)**, având în vedere viteza cu care societatea globală își însușește tehnologia ca pe un instrument de uz cotidian și ușurința cu care autori rău intenționați o implementează pentru a-și atinge scopurile. Pentru a veni în întâmpinarea riscurilor de securitate emergente, **previziunile NATO pe termen mediu și lung** au luat în calcul **dezvoltarea capabilităților comune de apărare cibernetică și pregătirea de personal specializat** care să asigure continuitate și performanță în utilizarea tehnologiei, cu scop defensiv.

În mediile politice și militare se vorbește adesea despre **conceptul NATO** cunoscut sub denumirea de ***Smart Defence*** - o viziune în baza căreia statele aliate sunt încurajate să coopereze pentru dezvoltarea, obținerea și menținerea capabilităților militare, abordând problemele de securitate curente și venind în acord cu noul concept strategic al **NATO**. **Proiectele în format multinațional** reprezintă ilustrarea concretă a noii perspective de consolidare a securității, oferind o formulă de interconectare a țărilor membre ale Alianței și de rentabilizare a investițiilor, într-un context global de austeritate economică, aflat în continuă schimbare. Urmând această idee, **conceptul *Smart Defence* se canalizează în sensul cumulării eforturilor, precum și al cooperării cu mediile industrial și academic**, construind punțile necesare între inițiativele naționale și cele internaționale.

În aria securității și apărării cibernetice sunt integrate viziunile statelor membre **NATO** pentru implementarea a trei astfel de **proiecte**: ***Multinational Cyber Defence Capability Development*** **(MNCD2)**, ***Malware Information Sharing Platform*** **(MISP)** și ***Multinational Cyber Defence Education and Training*** **(MNCD E&T)**.

MNCD2

Propus în anul **2012**, proiectul a pornit de la **ideea dezvoltării capabilităților comune de apărare cibernetică la nivelul statelor membre NATO prin intermediul unor contribuții naționale echitabile** în scopul asigurării prevenirii, detecției, răspunsului și recuperării în cazul atacurilor ce pot afecta confidențialitatea, integritatea sau disponibilitatea informațiilor. Urmând o viziune unitară, **MNCD2** a fost **un model de bune practici pentru inițierea și conceperea viitoarelor proiecte similare**, respectând principii simple și eficiente. Produsele, standardele și activitățile de cercetare sunt dezvoltate în cele mai avantajoase condiții economice, iar implicarea în mod centralizat a industriei naționale a statelor partenere contribuie decisiv la adaptarea soluțiilor create și la integrarea de arhitecturi interoperabile.

Direcțiile principale pe care le urmează proiectul prevăd crearea de produse pentru eficientizarea schimbului de informații despre incidentele de securitate cibernetică, dezvoltarea de instrumente optime pentru informarea factorilor decizionali și a managerilor IT cu privire la atacurile cibernetice și implementarea unor capabilități de identificare și investigare a amenințărilor persistente avansate (*Advanced Persistent Threat*/ **APT**) la adresa securității informatice organizaționale și statale.

Inițial, MNCD2 a fost **structurat sub forma a trei subproiecte** (ulterior, fiind definite continuări ale acestora sau propuneri noi, aflate încă în stadiul de evaluare în incubatorul de cercetare pe domeniul securității cibernetice, care a devenit în prezent MNCD2):

Work Package 1 **(WP1) -** ***Technical Information Sharing,*** urmărind **realizarea unei capabilități destinate schimbului eficient de informații între echipele naționale de răspuns la incidentele din zona securității cibernetice** (**CSIRT**). Aplicația rezultată, ***Cyber Information and Incident Coordination System*** **(CIICS)**, a fost finanțată de 3+1 națiuni, respectiv **România**, **Canada**, **Olanda,** ca membre ale **MNCD2**, dar și de către **Finlanda**, prin intermediul unui mecanism de finanțare directă la nivelul ***NATO Communications and Information Agency*** (**NCIA**).

CIICS reprezintă o modalitate de partajare a informațiilor atât în interiorul organizațiilor, cât și între acestea, având integrată posibilitatea adaptării la procedurile naționale specifice; platforma urmează a fi făcută interoperabilă cu alte sisteme de partajare a informațiilor (cum ar fi **MISP**).

Activitățile de implementare, operare și mentenanță aferente federației de state partenere sunt asigurate prin intermediul **NCIA**, formalizate în cadrul unui pachet de lucru separat, **WP5**. În perspectiva aderării mai multor națiuni la această federație, **NCIA** a propus un model de licențiere și de co-deținere a **CIICS** de către țările care nu au finanțat dezvoltarea produsului, acestea putând avea fie calitatea de simpli utilizatori ai federației, fie statutul de contributor la dezvoltarea **CIICS**.

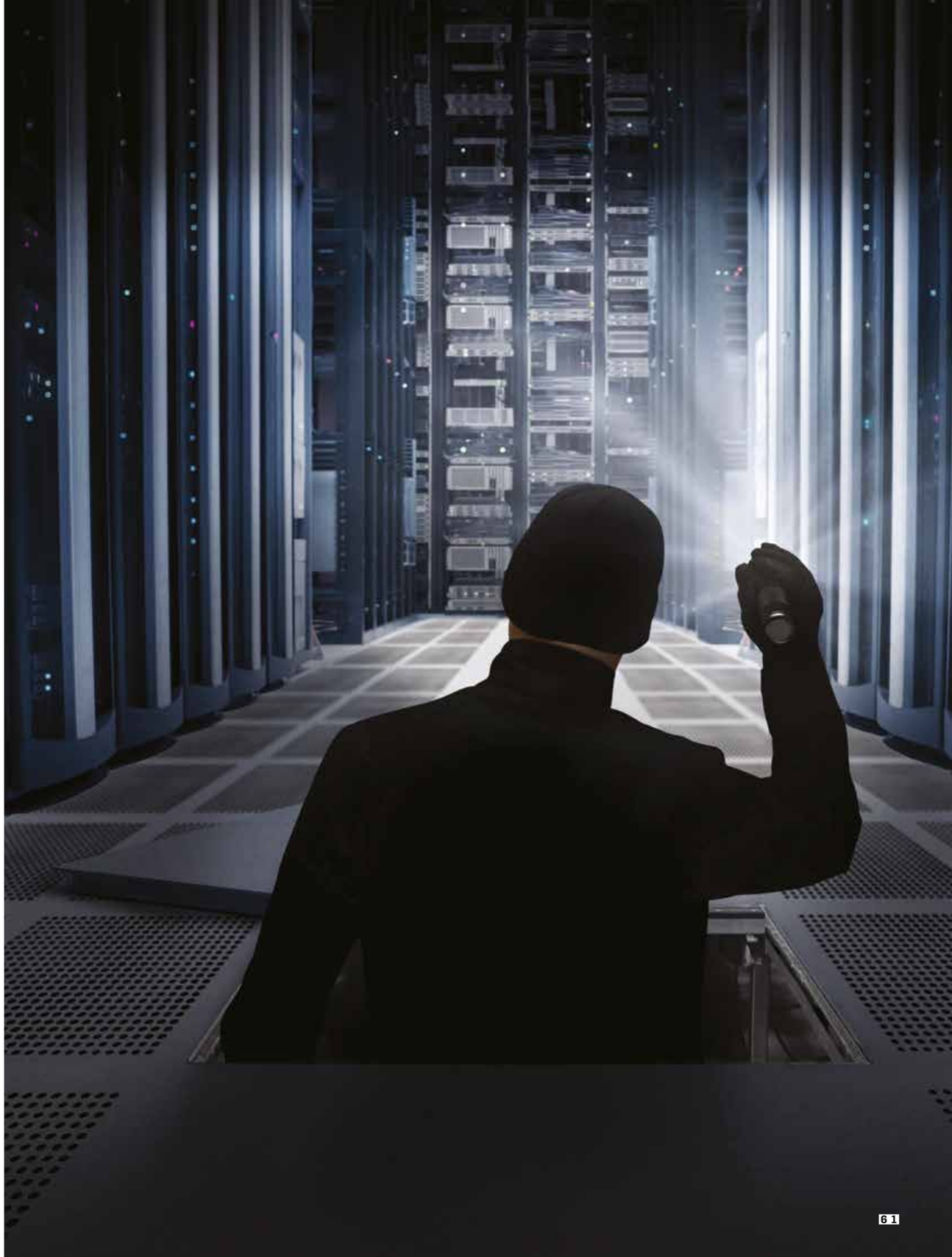
Aplicația a fost instalată la nivel național în cadrul proiectului „**Sistem național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic**”. Echipele de reacție rapidă la incidente de securitate cibernetică din cadrul instituțiilor vor putea colabora prin intermediul acesteia atât cu **Centrul Național Cyberint** sau **CERT-RO**, cât și cu entități de tip **CERT** din cadrul **Ministerului Apărării Naționale (MApN)**, **Ministerului Afacerilor Interne (MAI)** sau **Serviciului de Telecomunicații Speciale (STS)**.

De asemenea, nu trebuie omis succesul înregistrat de **CIICS** în cadrul exercițiilor ***Cyber Coalition*** din anii 2014 și 2015, concretizat în mai multe solicitări ale unor națiuni de a utiliza aplicația în cadrul unei perioade de testare a capabilităților acesteia.

Work Package 2 **(WP2) -** ***Cyber Defence Situational Awareness,*** având drept scop **crearea unui instrument destinat deopotrivă factorilor decizionali și managerilor IT în vederea îmbunătățirii capabilităților de avertizare situațională de tip *enterprise* puse la dispoziția acestora, cât și operatorilor CSIRT pentru sporirea abilității de a proteja comunicațiile și sistemele informatice împotriva atacurilor cibernetice**. Conceptele urmărite se referă la monitorizarea rețelelor și a evenimentelor de securitate, exploatarea sistemelor de alertare prezente, estimarea implicațiilor unui atac cibernetic prin intermediul unei analize de risc, precum și posibilitatea evaluării efectelor execuției controlate a contra-măsurilor. **WP2** este finanțat în comun de **Canada, Olanda, Norvegia și România**, ca membre ale **MNCD2**, precum și de **Finlanda**, prin același mecanism paralel utilizat și pentru finanțarea **CIICS**.

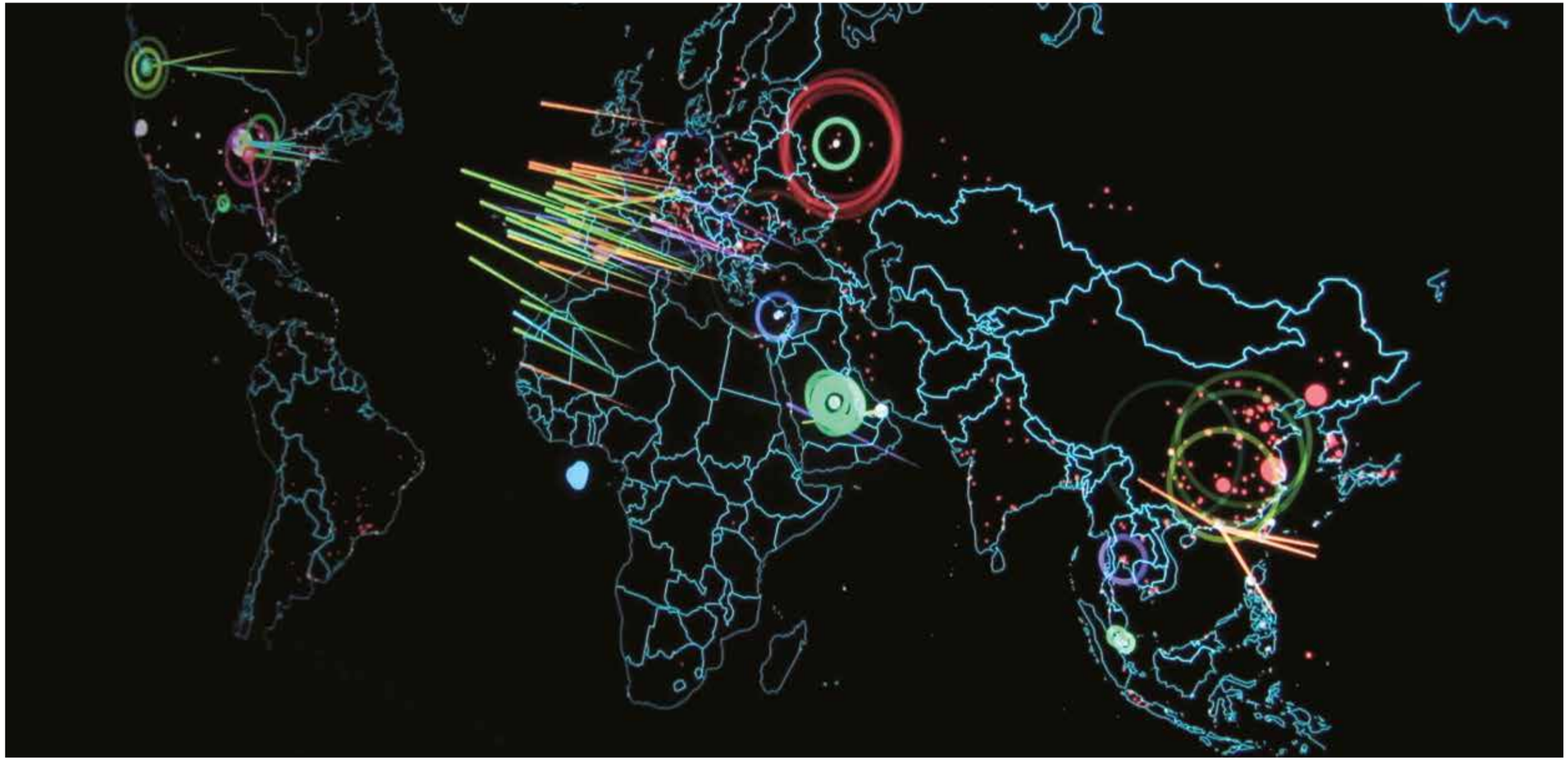
Inițial au fost colectate, analizate și consolidate cerințele națiunilor, întocmindu-se un document de referință pentru implementarea proiectului. Strategia aleasă de **NCIA** este selectarea unor companii care pot dovedi abilitatea de a duce la bun sfârșit acest proiect complex prin intermediul unor implementări cu caracter demonstrativ, dar suficient de elaborate pentru a asigura potențialii clienți de capacitatea tehnică de a realiza o implementare operațională. La finalul procesului

*** SMART DEFENCE - O VIZIUNE ÎN BAZA CĂREIA STATELE ALIATE SUNT ÎNCURAJATE SĂ COOPEREZE PENTRU DEZVOLTAREA, OBȚINEREA ȘI MENȚINEREA CAPABILITĂȚILOR MILITARE**



Intelligence

*** ROMÂNIA A DEVENIT UNUL DINTRE PRINCIPALII ACTORI CARE INFLUENȚEAZĂ DEZVOLTAREA DE CAPABILITĂȚI ÎN DOMENIUL SECURITĂȚII CIBERNETICE ÎN CADRUL ALIANȚEI.**



de selecție, vor fi disponibile patru alternative pentru implementarea unei soluții viabile. Selectarea celor patru companii care vor prezenta la sfârșitul anului 2016 implementări demonstrative s-a făcut și cu sprijinul nemijlocit al unei echipe de specialiști din cadrul Centrului Național Cyberint, care a evaluat, dintr-o perspectivă tehnică, răspunsurile transmise de 15 companii internaționale de prestigiu în domeniul securității cibernetice, la un document de tip *Request for Information* (RFI), elaborat de **NCIA**. În cadrul acestui document, NCIA a prezentat sintetic și structurat cerințele inițiale, prin intermediul a trei scenarii. Contribuția României la succesul acestui proiect amplu s-a materializat și prin organizarea la București în, luna septembrie 2015, a unei conferințe ce a urmărit identificarea de elemente suplimentare în cadrul soluțiilor comerciale ale companiilor invitate de **NCIA**.

Work Package 3* (WP3) - *Distributed Multi-sensor Collection and Correlation Infrastructure* (DMCCI)**, având drept scop **crearea unei capabilități destinate identificării și investigării amenințărilor de tip APT la nivelul unei rețele complexe, de dimensiune *enterprise*.** Propunerea inițială referitoare la crearea unui sistem complex de analiză a datelor existente în cadrul unor rețele de tip ***enterprise în vederea identificării amenințărilor de tip APT a fost redirecționată către crearea de subsisteme independente care ar putea conduce în final la implementarea unui sistem precum cel propus inițial.

Complexitatea, costurile ridicate ale proiectului, precum și dificultatea de a fi implementat și exploatat în condițiile unor rețele slab interconectate, care dispun de resurse umane reduse numeric și pregătite la un nivel insuficient, a determinat schimbarea modalității de abordare. Acest fapt s-a datorat și contribuției *in-kind* a României, care a întocmit un studiu privind fezabilitatea implementării proiectului în forma sa inițială, prin analiza în detaliu a tehnologiilor disponibile la ora actuală și prin dezvoltarea și analiza unui număr de 10 scenarii în care un vector de infecție de tip APT poate pătrunde în rețeaua unei organizații. Studiul de fezabilitate a arătat că resursele existente pe piață pot conduce doar la implementări cu caracter demonstrativ pentru o investiție financiară rezonabilă, abordarea fiind de succes doar dacă investițiile sunt considerabile, iar exploatarea sistemului este în acord cu restricțiile existente la nivelul fiecărei organizații sau legislații naționale.

MISP

Proiectul MISP a pus **bazele unei comunități de experți analiști în securitate cibernetică** (*community of trust*) **din statele membre NATO**, uniți printr-o relație de încredere și printr-o platformă de schimb de informații cu privire la aplicațiile malițioase complexe. Provocările care au determinat dezvoltarea colaborării în acest domeniu au fost desprinse din zona experiențelor practice cu care s-au întâlnit specialiștii în identificarea și gestionarea amenințărilor persistente avansate, întrucât acestea vizează cel mai adesea ținte de talie națională și internațională și nu sunt detectabile de produsele comerciale de protecție în spațiul cibernetic.

Printre liniile de interes ale proiectului se numără crearea unor proceduri de colaborare internațională, realizarea unor instrumente tehnice performante pentru schimbul de informații și interconectarea cu proiectul MNCD2 pentru alinierea și conjugarea eforturilor depuse.

MNCD E&T

Pentru concretizarea viziunii de adaptare a răspunsului la amenințările cibernetice, **actuala școală de instruire în domeniul IT&C, *NATO Communications and Information Systems School* (NCISS), se reinventează**: își extinde domeniul de expertiză înglobând formarea de specialiști în apărare cibernetică, își mută sediul într-un complex de clădiri modern și dotat pe măsura necesităților și își schimbă numele în **NCIS&CS**, prin adăugarea terminației *Cyber*. Toate aceste schimbări relevă importanța oferită mediului cibernetic în cadrul Alianței și sunt concretizate printr-un proiect de amploare denumit **MNCD E&T**.

În completarea paletei de proiecte de tip *Smart Defence*, **MNCD E&T** angajează eforturile statelor membre **NATO** pentru dezvoltarea de capabilități de educație și instruire în domeniul apărării cibernetice într-un format unitar, bazat pe colaborare și interoperabilitate. Stabilește un registru de înțelegere comună a conceptelor și a metodologiei de educație specifică, identifică necesitățile de instruire existente la nivelul națiunilor partenere și realizează demersuri pentru satisfacerea acestora, prin intermediul parteneriatelor cu mediile academic și privat.

Astfel, începând cu anul **2017**, vor fi disponibile **cursuri de specializare în apărare cibernetică**, livrate atât pentru angajații NATO și pentru cei ai structurilor de apărare ale națiunilor partenere, cât și pentru studenți sau personalul angajat în mediul privat. Respectând standarde înalte de calitate educațională, serviciile de instruire vor fi furnizate sub diverse forme de prezentare, cuprinzând atât sesiuni de scurtă durată (modulare, punctuale, de perfecționare), cât și programe de lungă durată (fundamentale, de formare, precum studiile de master). Riscurile emergente necesită a fi echilibrate prin răspunsuri pe măsură; dezvoltarea de instrumente și abilități comune pentru contracararea acestora demonstrează gradul ridicat de conștientizare și vigilență existente la nivelul statelor membre NATO. **România** a devenit **unul dintre principalii actori care influențează dezvoltarea de capabilități în domeniul securității cibernetice în cadrul Alianței**. Dovedind profesionalism și seriozitate de-a lungul cooperării internaționale pe acest tronson, țara noastră a oferit și continuă să ofere expertiză în implementarea și consolidarea unor domenii de nișă, cum este cel al apărării active.

ABSTRACT

Smart Defence is a concept that encourages Allies to cooperate in developing, acquiring, and maintaining military capabilities to meet current security problems in accordance with the new NATO strategic concept. Therefore, NATO's Smart Defence means pooling and sharing capabilities, setting priorities, and coordinating efforts better.

Multinational projects are a concrete illustration of the Smart Defence initiative, a new way of cooperating among NATO nations. The concept reveals a renewed emphasis on multinational cooperation in order to provide cost-effective security in a period of economic austerity. NATO's Smart Defence requires an innovative approach in order to enhance its military capability development process. In line with this idea, Cyber defence - related projects are strongly committed to join efforts and work together with industry and academia, building the necessary bridges between international and national initiatives.

RESPONSABILIZARE ÎN MEDIUL VIRTUAL

de George STAN

Efectele unei conduite mai mult sau mai puțin responsabile în mediul virtual par la prima vedere a se limita la acesta. Trebuie, însă, să avem în vedere riscurile la care ne expunem prin implicarea noastră din ce în ce mai mare în activități realizate pe internet. Implicarea fiecăruia dintre noi în mediul online trebuie să țină cont și de aspectul responsabilizării noastre, prin orice formă ne-am implica ca utilizatori ai acestor resurse.

Granițele și dimensiunea lumii virtuale sunt deja din ce în ce mai greu de definit, mediul virtual devenind o „prelungire", o altă formă de reprezentare, sau doar o simulare a lumii reale. De cele mai multe ori, acțiunile din mediul virtual se transpun în efecte în dimensiunea reală, iar orice formă din lumea reală are deja o reprezentare în mediul virtual, oamenii fiind deja preocupați din ce în ce mai mult de imaginea profilelor lor virtuale.

Internetul ne influențează viața din ce în ce mai mult. Serviciile pe care ni le oferă de cele mai multe ori gratuit, opțiunile personale privind conținutul accesat, gradul de expunere și cât de mult Internet „consumăm", toate acestea trebuie să fie completate de un nivel minim de responsabilizare în mediul virtual, atât din partea celor care participă ca simplii „consumatori" cât și din partea celor care „produc", adaugă conținut, oferă un serviciu.

INTERNETUL ESTE LIBER, IEFTIN ȘI BUN

Ne bucurăm cu toții de beneficiile Internetului, costul lunar al unei conexiuni la Internet fiind deja echivalent cu prețul combustibilului necesar unui automobil pentru a parcurge o distanță de 100 de km. Prin utilizarea Internetului eliminăm adesea distanțe mult mai mari.

De cele mai multe ori, regăsim informațiile de care avem nevoie căutând răspunsul pe Internet, ne documentăm, ne amuzăm și socializăm din ce în ce mai mult în fața unui calculator.

Toate aceste aspecte pozitive, servicii pe care le regăsim în mediul *online*, forme de divertisment, căi de socializare, trebuie să țină cont și de amenințări la care, de multe ori, ca simpli utilizatori ne supunem ca urmare a unor acțiuni mai mult sau mai puțin responsabile sau ca urmare a unor forme de pasivitate, a unei culturi de securitate mai puțin avute în vedere în mediul virtual.

O MULTITUDINE DE SERVICII DIN INTERNET SUNT GRATUITE

Câți dintre noi **nu** folosesc un serviciu gratuit de e-mail de la Google, Yahoo, Microsoft etc.? Un serviciu gratuit poate fi însă o strategie de motivare a unui utilizator să folosească și alte servicii ale companiei, iar, în special în cazul acestor mari furnizori de servicii de e-mail, spre exemplu, principalele surse de venit vin din serviciile de marketing oferite sau alte servicii premium.

MARKETING. ONLINE MARKETING. CYBERMARKETING

Marketing-ul este în accepțiunea generală „știința și arta de a convinge clienții să cumpere". Dacă, la început, această activitate se concentra pe produse, acum se axează pe analiza de piață și determinarea nevoilor clienților față de un produs sau serviciu. Activitățile cele mai importante în marketing, respectiv identificarea de noi clienți și administrarea sau menținerea clienților existenți, par a fi găsit în mediul *online* instrumentele ideale pentru dezvoltarea cât mai eficientă a activității de *online* marketing. Astfel, a apărut termenul de *cybermarketing*, prin care se înțelege marketing-ul care folosește ca principal canal de comunicare Internetul.

Aflat la intersecția a trei mari domenii: marketing, economie și tehnologie, *cybermarketing*-ul gravitează în jurul clientului (consumatorului), principalele instrumente folosite pentru acest tip de marketing fiind *e-mail-ul*, publicitatea *online*, *newsletter-ul*, *site-uri etc*.

Internetul devine, astfel, și locul ideal de întâlnire între un producător sau vânzător și consumator.

Nivelul de expunere la *cybermarketing* depinde astfel foarte mult de serviciile utilizate, de conținutul accesat prin navigarea în mediul virtual.

PERSPECTIVA IoT (INTERNET OF THINGS)

Este clar faptul că Internetul a devenit motorul care ne angrenează în prezent pe toți. Internetul este un lucru „atât de bun" încât tendința este de a gândi un viitor conectat din ce în ce mai mult la Internet. Mașini, electrocasnice, sisteme de iluminat, dispozitive mobile etc. ar putea fi toate parte a unei rețele unice. Această conectivitate va permite controlul, comunicarea și partajarea datelor între dispozitive, toate acestea realizându-se de la nivelul unui sistem de control gestionat de către utilizator. Se preconizează, astfel, un management eficientizat al resurselor, o creștere a productivității angajaților, ceea ce va duce la generarea de noi venituri cât și creșterea beneficiilor pentru utilizatori.

Deja există sisteme automate de control a temperaturii ambientale, controlabile de la nivelul unui *smartphone*, care poate fi, de asemenea, conectat cu un *smartwatch*. Iluminatul public ar putea să nu mai aibă nevoie de sesizarea din partea unei persoane a unei disfuncționalități, prin implementarea unor senzori în cadrul rețelelor de iluminat putând fi raportată orice disfuncționalitate, în mod automat, la un sistem de monitorizare și control. Același principiu poate fi aplicat și la rețeaua de semafoare a unui oraș.

Dezvoltarea și implementarea conceptului *IoT* poate reprezenta un pas înainte pentru cei angrenați în *cybermarketing*, în special pentru furnizorii de reclame *online*.

IMPORTANȚA SECURIZĂRII PRIN RESPONSABILIZARE

Marile companii de *online* marketing vor câștiga din ce în ce mai mult de pe urma expunerii noastre în mediul virtual. Încercările unor acțiuni de tip *cybercrime* vor fi, de asemenea, într-un număr crescător și din ce în ce mai ample. Și pentru că Internetul este și contribuția fiecăruia dintre noi, vă supun atenției următorul scenariu.

Foarte multe persoane dintre cele care au un site web personal (chiar și multe companii care oferă servicii de *web design, development*) utilizează platforme gratuite de tip *CMS* (*Content Management System*). Preocuparea este foarte mare pentru conținutul promovat pe site, însă foarte puține persoane sunt preocupate de securitatea platformei utilizate. Grupări mari de *cybercrime* pot utiliza aceste platforme, prin compromiterea lor și adăugarea de conținut malițios, atât în acțiuni de tip ***BlackHat Seo*** (acțiuni de îmbunătățire a volumului traficului către un anumit domeniu, utilizând tehnici ilicite, în scopul creșterii gradului de expunere a respectivului domeniu în Internet în lista rezultatelor unei căutări efectuate pe Internet), cât și în acțiuni ample, de anonimizare a unor operațiuni complexe cum ar fi cele de distribuire a unor fișiere malițioase. Situațiile întâlnite indică, în urma infectării, posibilitatea obținerii controlului sistemului infectat și, de ce nu, modificarea fișierelor personale ale utilizatorului, utilizând elemente tehnice deținute doar de atacator, în vederea cererii unei recompense pentru remedierea fișierelor (acțiunea descrie un tip de *malware* ce poartă denumirea de ***ransomware).***

De asemenea, în situația în care fișierele malițioase ajung în cadrul unui sistem informatic cu ajutorul unor reclame malițioase, distribuite prin intermediul rețelelor de distribuție a reclamelor *online* (în necunoștință de cauză pentru compania care se ocupă cu distribuirea de reclame *online*, procesul de infectare fiind facilitat și de un sistem informatic neactualizat sau utilizarea unor aplicații neactualizate), vorbim despre ***malvertising.***

În încheiere, este relevant să punem în lumină importanța fiecărui utilizator de Internet și necesitatea de a avea în vedere anumite aspecte ce țin de o minimă responsabilizare a fiecăruia dintre noi în momentul în care suntem în mediul virtual.

ABSTRACT

The boundaries and the size of the virtual world have already become hard to define, virtual environment becoming an "extension", another form of representation or just a simulation of the real world. More and more often actions from virtual environment translate into effects in actual life, and any form of real world has already a representation in the virtual environment. People are already concerned over their virtual representation. The Internet influences our lives more and more. The services that we access on the Internet are mostly free. The way we choose the content we access, the exposure and how much Internet "we consume", must be supplemented by a minimum level of responsibility.

JENS STOLTENBERG, NATO - EU ENHANCE CYBER DEFENCE COOPERATION

NESIGURANȚA ÎNTR-O LUME MULTIPOLARĂ

de dr. Cristian IORDAN

Termenul de „nesiguranță” descrie poate cel mai bine sistemul internațional actual. Am fost martorii ridicării altor puteri, dar toate au fost sau sunt încă afectate în proporții variabile de criza economico-financiară și dezechilibre interne, schimbându-le astfel evoluția către statutul de mari puteri. Prin urmare, teoriile multipolarității sau policentricității sunt încă discutabile.

Este adevărat că unica superputere, **Statele Unite ale Americii**, a cunoscut **provocări** la adresa rolului și puterii sale pe fondul problemelor economice interne și a evoluțiilor globale. Totuși, există un număr considerabil de **atuuri** pentru a contrabalansa: adaptabilitate și flexibilitate economice, perspectiva independenței energetice și creșterea economică rezultantă, tendințe demografice pozitive, alianțe și parteneriate viabile, cele mai bine cotate universități din lume, atractivitate (un atribut *soft power* prin excelență, potrivit lui **Joseph NYE** în *„The Future of Power”*). Tot **Joseph NYE** în „Soft Power and European-American Affairs, in Hard Power, Soft Power and the Future of Transatlantic Relations” subliniază faptul că proiecțiile economice nu sunt totul pentru a accede la statutul de mare putere, ci combinația de atribute *hard power* și *soft power*, denumită de autor *smart power*.

De cealaltă parte a Atlanticului, **continentul european**, câmp de bătălie pe durata câtorva secole, a reușit să depășească acest episod din istoria sa, atingând prin blocul comunitar cea mai lungă perioadă de pace și stabilitate și devenind astfel un model și un susținător vocal al democrației, al drepturilor omului și al soluționării pașnice a conflictelor. Aceste rezultate provin incontestabil și din relația transatlantică a securității pe care a asigurat-o. Vehiculul cel mai vizibil și cu o durată de viață de apreciat a fost reprezentat de Alianța Nord-Atlantică.

Astăzi **NATO** se confruntă cu o abordare de tipul „să facem mai mult cu mai puțin” – inevitabilul subiect al scăderii bugetelor din zona de securitate și apărare. Abordarea este diversificată, **NATO** acordând o atenție tot mai mare amenințărilor emergente de securitate.

Astfel, subiectul amenințărilor cibernetice devine relevant atunci când state și organizații internaționale se confruntă cu un număr tot mai mare al încercărilor (reușite sau nu) de a obține date sensibile sau informații clasificate, venite din partea unor entități diverse (statale, criminale, *hacktiviste* etc.). Cooperarea în domeniul *cyber* este o obligație a părților pentru a învăța și a progresa în protejarea valorilor în format binar, dar devine astfel și o oportunitate de a consolida alianța, construind pe eforturile și experiența existente și aducând o dimensiune nouă mecanismelor de securitate existente. Și de ce nu, mai multă profunzime... Potrivit lui **Wade WILLIAMSON** în articolul *„Combating Emerging Threats Through Security Collaboration”* din *„Security Week”* (17.12.2012), continuarea acestor demersuri poate reprezenta un mod în care să transformăm societățile deschise în care trăim și cultura colaborativă într-un avantaj competitiv, inclusiv prin parteneriat public-privat, pentru a limita, opri și, poate cel mai important, preveni pierderile de date și informații și chiar atacuri.

„Parteneriatele militare (n.n.- și nu numai) de astăzi sunt mai importante decât oricând înainte. Strategia națională a Americii, alături de problemele fiscale și politice fac improbabilă desfășurarea unilaterală de forțe pentru a răspunde provocărilor de securitate ale secolului XXI.”, scrie **James HOWCROFT** în articolul *„Things Americans Need to Know: How to Be Better Partners”* din *„Small Wars Journal”* (25.06.2013). Este un moment în care zone mai discrete de cooperare ar putea înregistra o evoluție ascendentă.

ACORD TEHNIC PENTRU PROTECȚIA REȚELELOR

SUA și **Europa** se văd în continuare în situația de a conlucra, de a învăța unii de la ceilalți, de a se susține reciproc, cu atât mai mult cu cât condițiile geopolitice ale secolului XXI fac imposibile sau extrem de dificile gesturile unilaterale pe scena globală. Chiar dacă este dificil să ajungi la un nivel de echilibru, relația transatlantică încă este inevitabilă, susține încă din **2006 Vittorio PARSI** în *„The Inevitable Alliance: Europe and the United States Beyond Iraq”*. Iar un echilibru și o articulare dezirabile între **NATO** și **UE** ar reprezenta cu siguranță un avantaj extrem de valoros. Cele două organizații se află într-un proces de creștere a sinergiei, două evenimente susținând această idee. Mai întâi este vorba de semnarea pe **10 februarie 2016** a unui **„Acord tehnic pentru protecția rețelelor în fața atacurilor cibernetice”** (*„NATO - EU Enhance Cyber Defence Cooperation”*), un semn al conștientizării la un nivel superior a provocărilor comune cu care se confruntă cele două organizații. Apoi, vorbim de anunțul din **11 februarie** privind implicarea **NATO** în patrularea zonelor maritime migratorii pentru prevenirea traficului cu persoane.

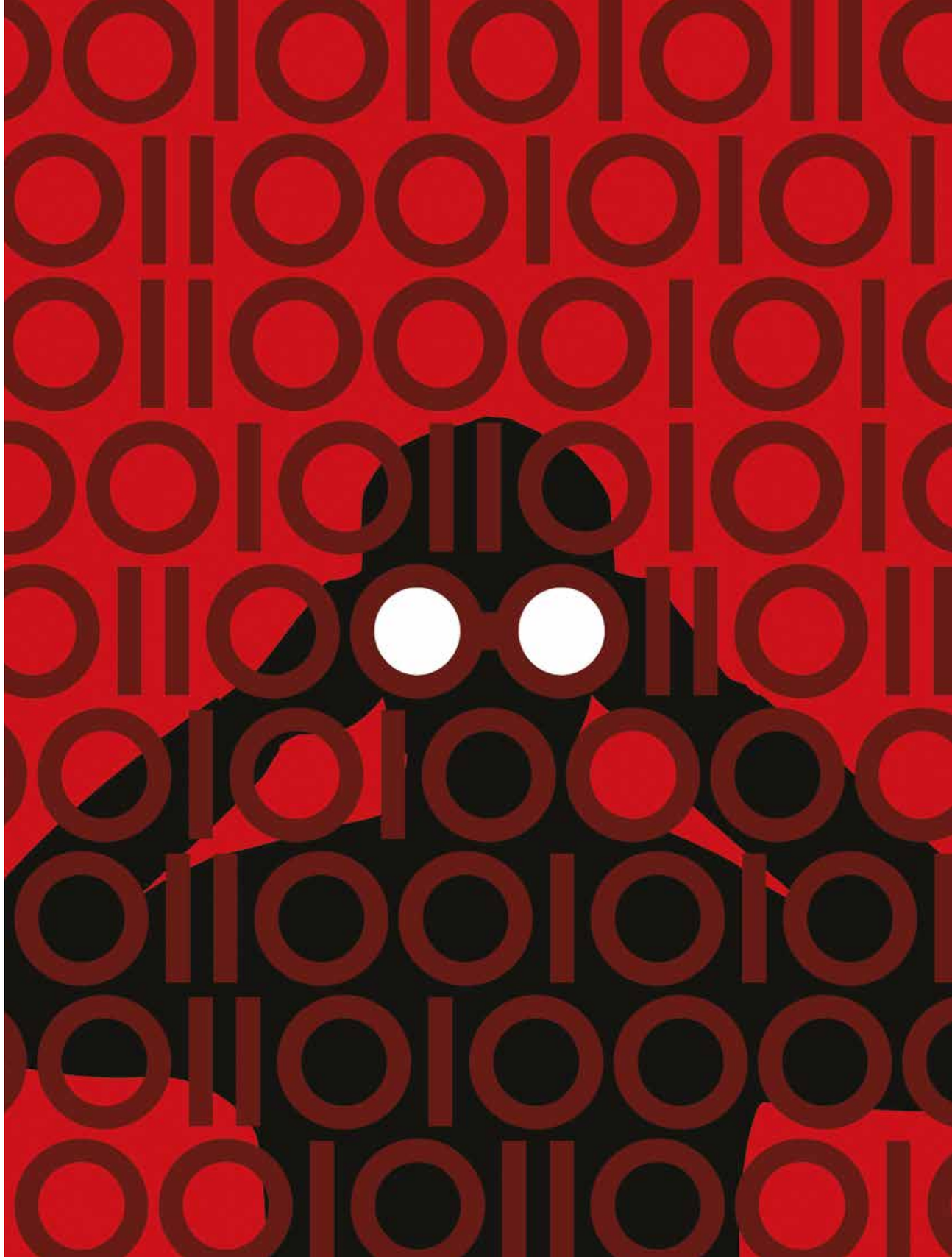
În concluzie, trăim vremuri de schimbare, de modificări strategice, dar alegerile pe care le facem acum ne modelează viitorul. Poate că așa-numitul „declin al Occidentului” nu este atât de aproape... Dacă cea mai mare provocare pentru europeni și americani este să continue ceea ce au inițiat împreună, trebuie aprofundat parteneriatul? Motivele sunt numeroase: nu trebuie să subestimăm puterea valorilor lor comune, încrederea, civilizația și obiectivele comune. Doar astfel vom putea face față unor amenințări precum cea cibernetică. Relația noastră, chiar dacă înregistrează fluctuații, trebuie să meargă mai departe.

ABSTRACT

In an age of uncertainty, numerous challenges arise to the current security establishment. The emerging challenges, such as cyber, have the potential to strengthen, not weaken, the transatlantic relation.

ACTORII CIBERNETICI STATALI – O CONTINUĂ PROVOCARE ÎN CYBER INTELLIGENCE

de Iulian ALECU



Cine ne atacă? De ce ne atacă? La ce să ne așteptăm? Sunt doar câteva din **întrebările la care un ofițer de informații care lucrează în domeniul *cyber intelligence* este solicitat să răspundă**. Iar răspunsurile nu sunt deloc ușor de dat.

De ce? Pentru că, spre deosebire de lumea fizică, **spațiul cibernetic oferă mult mai multe și complexe variante și forme de disimulare a intențiilor și acțiunilor unui atacator cibernetic**. Mai mult, **problematica atacurilor cibernetice** prezumate a fi derulate de actori statali **depășește cadrul „tehnic" al investigației**, fiind încadrată în contextul geopolitic și economic în care se află la un anumit moment țara vizată de un anumit atac.

Așadar, cu ce ne confruntăm? **Prima problemă** este determinată de **definirea „valorii de apărat"**. *De ce trebuie să definim acest concept?* Pentru că **dinamismul atacurilor cibernetice, care a crescut exponențial în ultimii ani, în același timp cu complexitatea metodelor de penetrare a infrastructurilor cibernetice și de asigurare a „**nedetectabilității**" prezenței malițioase, a determinat în mod dramatic schimbarea paradigmei „zidului de apărare care nu poate fi spart" în „asumarea faptului că infrastructurile cibernetice sunt deja penetrate"**. Este un adevăr pe care trebuie să-l acceptăm și să ni-l asumăm. **Nu există sisteme de protecție perfecte**, dar cu siguranță există atacatori foarte determinați să obțină accesul în anumite infrastructuri cibernetice, indiferent cât de bine protejate sunt acestea. Iar această determinare îi face să conceapă și să perfecționeze, în mod continuu, *tool*-urile de care dispun, astfel încât să poată obține ceea ce își doresc: accesul neautorizat și controlul infrastructurilor cibernetice vizate.

NU VOM PUTEA ȚINE PASUL CU ATACATORII NICIODATĂ

Întrucât există milioane de astfel de infrastructuri, începând de la cele care deservesc entități mici sau private, a căror activitate nu afectează securitatea națională, până la cele care deservesc entități de stat sau private a căror activitate se încadrează în ecuația securității naționale, este important să definim care este **„valoarea de protejat" din perspectiva securității naționale**. Resursa de care dispunem este limitată, nu vom putea ține pasul cu atacatorii niciodată, iar, dacă ne propunem să protejăm totul, ne vom găsi foarte curând în situația în care vom fi copleșiți.

Odată rezolvată problema „valorii de protejat", facem pasul spre **a doua problemă** cu care ne confruntăm: **identificarea atacurilor cibernetice**. Spre deosebire de atacurile de tip criminal sau extremist, **cele prezumate a fi de origine statală sunt mai dificil de detectat**. *De ce?* Pentru că, așa cum arătam mai sus, **atacatorii sunt foarte determinați să obțină accesul neautorizat în infrastructurile cibernetice țintă**, dar sunt cel puțin la fel de **determinați să își asigure prezența nedetectată în aceste infrastructuri pentru o perioadă îndelungată**. Iar aici ne referim la **ani**, nu zile sau luni.

De ce? Simplu. Să ne închipuim infrastructura cibernetică a unui minister de externe, din orice țară a lumii. Accesul neautorizat într-o astfel de rețea este o mină de aur pentru un atacator statal: acces la toate informațiile zilnice referitoare la obiective, strategii, acțiuni, parteneriate ale statului respectiv și nu numai. Accesul și controlul asupra unei rețele informatice permite și utilizarea respectivei rețele în susținerea sau derularea altor atacuri cibernetice... un exercițiu de imaginație ne poate arăta în câte moduri poate un atacator să acționeze în acest sens...

Așadar, cum detectăm atacurile? Printr-un **proces tehnic, analitic și de *intelligence* continuu și dinamic**, care integrează informațiile furnizate de diverse surse specializate. Este un proces care necesită cel puțin aceeași determinare, inteligență și minuțiozitate pe care o au atacatorii atunci când își propun să obțină accesul într-o infrastructură cibernetică țintă.

Odată depășit și acest obstacol, trecem spre **a treia problemă**, și anume, **determinarea încetării atacului și investigarea acestuia**. Din momentul în care atacatorul a obținut accesul în rețeaua informatică vizată, el va urmări să își extindă prezența și controlul în rețea, astfel încât să aibă acces la toate informațiile de interes și, la nevoie, să le poată *exfiltra*. Este un proces complex care presupune o adaptare și perfecționare continuă a aplicațiilor malițioase folosite, astfel încât motoarele de detecție antivirus și investigatorii să nu descopere prezența atacatorului. În această situație, cei care investighează atacul au de rezolvat o primă sarcină dificilă: **identificarea tuturor stațiilor infectate din rețea, urmată de „curățarea" lor, asigurându-se că infecția nu mai este prezentă în rețea**. Pentru un timp, de obicei destul de scurt. *De ce?* Pentru că atacatorii statali, așa cum spuneam, sunt foarte determinați să dețină accesul neautorizat în anumite infrastructuri și, în astfel de situații, își vor rafina și mai mult variantele de atac și persistență pentru a fi și mai greu de detectat.

Acest aspect ne ajută să observăm **diferența de esență dintre amenințările din spațiul fizic și cele din spațiul cibernetic**: dacă în spațiul fizic acțiunile și prezența amenințării este ceva mai ușor de identificat, **în spațiul cibernetic, mai ales atunci când vorbim de atacatori statali, prezența și activitățile acestora pot trece foarte ușor neobservate, dar cu repercusiuni de multe ori greu de cuantificat**.

Și, prin această observație, facem pasul spre ceea ce înseamnă **investigarea atacului cibernetic**. Îndrăznesc să spun că acest proces are un **caracter continuu**. Da, pare ciudat, mai ales dacă un atac încetează! Și totuși... **Un atac cibernetic statal presupune multe resurse înalt specializate din partea atacatorului** pentru: stabilirea și studierea țintelor, crearea, gestionarea și adaptarea infrastructurilor de atac și *exfiltrare*, conceperea modalităților de infectare, derularea propriu-zisă a etapei de infectare, validarea țintelor infectate, asigurarea persistenței în toate sistemele informatice validate ca fiind de interes, căutarea și *exfiltrarea* informațiilor de interes, depozitarea acestora, transmiterea către solicitant, analiza și prelucrarea acestora. **Investigația unui atac cibernetic** urmărește, analizează și încearcă să înțeleagă toate aceste procese complexe. Iar acest lucru necesită timp și resurse. Pe de altă parte, același atacator statal, care, poate, a încetat un atac cibernetic, va iniția un altul, însă o investigație anterioară poate constitui **o lecție învățată** în ceea ce privește *modus operandi* al atacatorului. **Atacatorii sunt oameni**, oamenii nu sunt perfecți, iar acest lucru poate fi în avantajul investigatorului...

ATRIBUIREA ATACULUI CIBERNETIC

Ajungem astfel la **cea mai dificilă problemă cu care se confruntă cei care investighează atacurile cibernetice statale**: **atribuirea atacului cibernetic**. *De ce este una dintre cele mai dificile probleme?* Pentru că **spațiul cibernetic oferă posibilități aproape nelimitate de disimulare**, astfel încât un actor cibernetic poate să pară foarte ușor a fi un altul. *Și atunci?*

Să facem un exercițiu: să luăm trei state pe care le vom denumi A, B și C. A și C sunt prietene, dar B este inamic. B, însă, dispune de capacități cibernetice înalt dezvoltate și poate iniția un atac cibernetic care, datorită posibilităților de disimulare, are toate caracteristicile unui atac ce provine din țara prietenă lui A, respectiv C. Ce poate urma este ușor de imaginat.

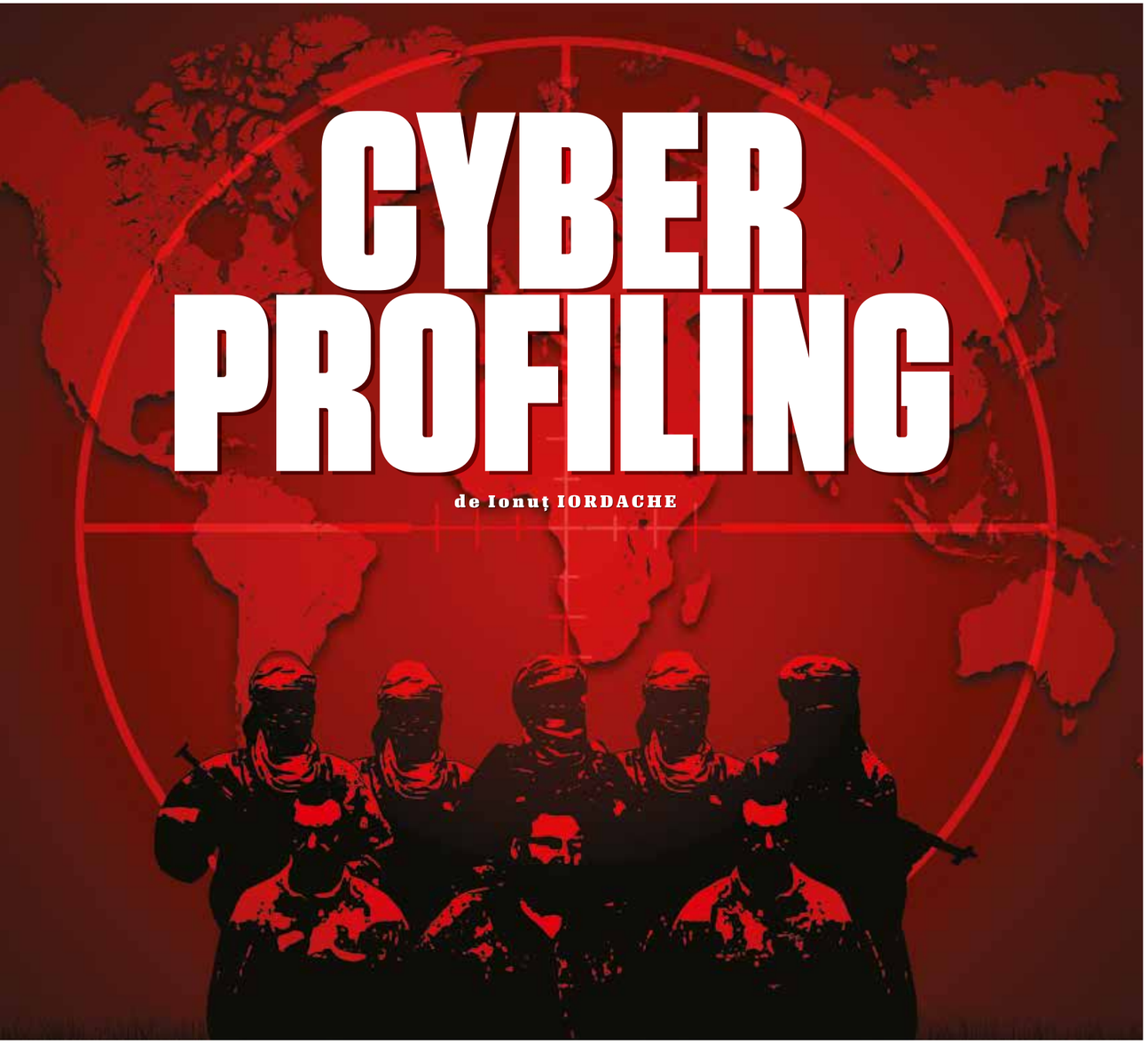
Atribuirea făcută doar în baza unor presupuneri sau suspiciuni ne expune la un risc mare de autodezinformare și, de asemenea, de dezinformare a partenerilor cu care lucrăm. Acesta este, practic, un alt motiv pentru care investigația unui atac cibernetic este un proces

continuu: este vital să înțelegem cine este în spatele unui atac cibernetic. Iar acest lucru înseamnă **studiul atent al tuturor indiciilor pe care le furnizează investigația, dar și contextul internațional de la momentul derulării atacului**. Astfel, atunci când vorbim despre România și vrem să înțelegem motivele care au determinat includerea țării noastre pe „lista" țărilor vizate de un atacator, este important să începem de la statutul țării noastre de membru NATO, UE și al parteneriatelor politico-economice din care este parte, alături de poziția geografică, resursele de care dispune și obiectivele strategice pe care le are ca stat. Această **analiză contextuală** are un **caracter dinamic**, determinat de însuși dinamismul situației geopolitice și economice, și solicită un efort constant al ofițerilor de informații din *cyber intelligence* și al analiștilor care au datoria de a observa „elementele de finețe" în schimbările care au loc zilnic pe scena geo-economico-politică, asigurând în acest fel „ancorarea în prezent" a investigației atacului cibernetic.

În loc de încheiere, propun spre reflecție un citat din Sun Tzu, „Arta Războiului", capitolul referitor la Strategia Ofensivă, paragraful 4: „**Supremul rafinament în arta războiului este de a dejuca planurile inamicului**".

ABSTRACT

A well-known proverb captures the essence of intelligence: In the land of the blind, the one-eyed man is king. One who is better informed than his adversaries will have the advantage. Intelligence powers everything we do and it can power everything you do as well. When it comes to cyber intelligence, we must gather information about adversary's behaviour, capabilities, and intentions. More importantly, by understanding the events that shape the beliefs and motivations of threat actors, it is possible to comprehend what drove the adversaries to behave as they did and perhaps to understand what this means for the future.



CYBER PROFILING

de Ionuț IORDACHE

Evoluția spațiului virtual, a comunicării și a rețelelor sociale au favorizeazat apariția unor entități (indivizi și grupări) interesate de inițierea și promovarea propriilor obiective de tip criminal, extremist sau terorist. Totodată, accesul facil la tehnica de calcul, disponibilă la prețuri scăzute, a deschis orizonturile persoanelor rău intenționate să dezvolte un nou tip de amenințare la adresa infrastructurilor cibernetice de interes național. Coroborat cu expansiunea multitudinii de programe informatice și a sistemelor de operare, majoritatea având vulnerabilități exploatabile de persoane cu un nivel mediu de cunoștințe în domeniul *hacking*-ului, s-a creat **un spațiu *web* nesigur și, de cele mai multe ori, periculos pentru utilizatorul neexperimentat**. În context, atacurile cibernetice orientate asupra sistemelor informaționale, atât civile, cât și guvernamentale, pot produce o serie de consecințe negative în plan financiar, operațional, legal sau strategic.

Pe lângă atacurile cibernetice de tip criminal, în **2015** s-a coagulat o **recrudescență a fenomenului terorist pe spațiul Uniunii Europene** fapt ce a generat și **o creștere la nivel internațional a numărului de agresiuni cibernetice motivate ideologic și de actori implicați în realizarea acestora**, în special pe palierul grupărilor de *hacking* islamiste.

De fapt, ce reprezintă **o amenințare cibernetică**? Am putea descrie în linii generale o astfel de stare ca fiind **o persoană sau organizație care intenționează prin instrumentele deținute ori prin nivelul tehnic specializat să genereze prejudicii entității țintă**. Concret, însă, o amenințare cibernetică este **generată de o entitate rău voitoare**, indiferent că este vorba despre un singur individ sau o organizație întreagă, cu obiective politice, sociale sau personale, în funcție de motivația celui care o dezvoltă. **Mediul de propagare a amenințării este o rețea informatică**, ce conține pe suporții de stocare informații de interes pentru atacator, fie el actor statal sau simplu hacker cu un nivel minimal de cunoștințe tehnice (utilizator al unor softuri prietenoase cu capacități ofensiv-distructive).

În prezent, în literatura de specialitate se identifică amenințări informatice compuse din **trei piloni**:

- **Intensitatea** - este determinată, în mod prioritar, de perseverența unei amenințări în contextul atingerii obiectivului. Intensitatea impune și necesită pragul maximal pe care îl poate atinge nevoia concretizării amenințării, cât de mult este dispus atacatorul să riște pentru a-și atinge scopul;
- **Discreția** - abilitatea unei amenințări de a-și menține un nivel acceptabil de confidențialitate pe întregul proces, până la atingerea obiectivului.
- **Timpul** - intervalul optim în care inițiatorii unei amenințări planifică, dezvoltă și implementează metodele pentru atingerea obiectivului. În cazul unui atac cibernetic complex, se impune acceptarea obiectivă a unui interval de timp necesar pentru ca toți pașii, de la implementare până la execuția propriu-zisă, să fie realizați cu minuțiozitate.

Referitor la atributele de tip **posibilități tehnice**, au fost identificate următoarele elemente necesare:

- **Personalul tehnic** - persoane care sunt implicate direct în fabricarea programelor informatice cu potențial distructiv, precum și cele care le utilizează, dispunând de cunoștințe/aptitudini IT. Un număr ridicat al membrilor personalului tehnic va genera accelerarea proiectării și realizării planurilor de atac ale amenințării, dar va crește nivelul de risc contrainformativ și probabilitatea de penetrare a organizației de către instituții cu atribuție pe această linie;
- **Palierul tehnologic** - reprezintă nivelul de competență teoretico-practică și existența prealabilă a unui transfer de *know-how* între grupări în vederea atingerii obiectivului. Cu cât nivelul de cunoștințe din spatele amenințării este mai mare cu atât probabilitatea ca atacul cibernetic să-ți atingă obiectivul scontat este mai reală, eficiența acestuia fiind cuantificabilă prin raportul eficient dintre intervalul de timp mai scurt și nivelul de resurse minim utilizat.
- **Accesul** - reprezintă capacitatea unei amenințări de a plasa un membru al celulei ofensive în cadrul unui sistem restricționat. Acesta se definește ca fiind orice sistem informatic sau fizic în care este permis accesul pe baza unor privilegii sau acreditări.

În decursul timpului, **profilul actorilor amenințărilor** a cunoscut o diversificare a obiectivelor urmărite, sens în care aceștia s-au coagulat pe diverse **interese** astfel:

***Hackerii* individuali** sunt cei care de cele mai multe ori lucrează în mod solitar la implementarea unor amenințări și atingerea obiectivului. Datorită existenței și diseminării nerestricționate pe forumurile de securitate cibernetică a unei multitudini de programe informatice cu capacități ofensive, aceștia și-au îmbunătățit abilitățile tehnice și și-au îndreptat atenția de la atacarea unor sisteme mici și vulnerabile către rețele informatice cu mult mai importante, cum sunt cele ce aparțin mediului financiar sau guvernamental. În majoritatea cazurilor, acești actori ai spectrului criminal utilizează acțiunile de *defacement* sau injecția de cod malițios în cadrul *site*-urilor ce aparțin instituțiilor sau persoanelor cu notorietate publică. Motivația de intruziune a *hackerilor* individuali poate include și colectarea de informații cu privire la conturile bancare, furtul de informații cu caracter confidențial ori alterarea conținutului paginilor *web* țintă.

Grupurile de *hackeri* sunt acele celule care colaborează pentru atingerea unui deziderat comun, cum ar fi cel asimilat fenomenului de *hacktivism*, context în care atacurile realizate de aceștia sunt aparent bazate pe convingerile politice sau dorința de a contesta autoritatea și/sau legitimitatea organizațiilor sau guvernelor țintă. În prezent, cea mai cunoscută celulă de acest gen se identifică de obicei cu numele de **Anonymous**, dar conform analizelor realizate de firmele de specialitate s-a stabilit că nivelul acestor aderenți la curentul anterior indicat au capacități tehnice limitate. Analitic, se constată faptul că distribuția agresiunilor realizate de aceste grupări nu relevă un tipar anume, fiind vizate entități cu obiecte de activitate diverse, fără a se urmări în mod specific afectarea instituțiilor guvernamentale sau a unor organizații/societăți comerciale de importanță strategică.

Atacurile cibernetice statale sunt orchestrate exclusiv de entități statale ce au ca principal obiectiv identificarea vulnerabilităților umane și tehnologice ale unui alt stat țintă în vederea exploatării acestora. Scopul acestui tip de agresiuni, care poate avea și o caracteristică de tipul spionajului (clasic sau economic), este generat de nevoia agresorului de a cunoaște capabilitățile, resursele naturale și energetice ale entității țintă. Modul de anonimizare al unui astfel de amenințări se realizează prin utilizarea de către agresori a unor servere aflate pe teritoriul altor state, prin care își direcționează traficul de Internet.

Totuși, pe lângă aceste entități individuale, grupate sau statale, în prezent un alt fenomen are o ascensiune rapidă în spectrul amenințărilor și este cunoscut sub numele de terorism cibernetic. Amenințările de acest tip sunt direct corelate cu situația geopolitică, evoluțiile și conflictele din Orientul Mijlociu (expansiunea grupării teroriste **Daesh**, „războiul rece” cu Iranul, războiul civil din Siria, relațiile tensionate dintre Israel și Autoritatea Palestiniană etc.). Concomitent cu diversificarea țintelor vizate de agresiuni cibernetice, s-a dezvoltat vizibilitatea grupărilor de *hacking* islamiste și a acțiunilor acestora. Obiectivul unui terorist cibernetic implica perturbarea funcțiilor guvernamentale, alterarea integrității sistemului de apărare, distrugerea sau furtul de informații cu caracter clasificat și, cel mai grav, perturbarea infrastructurilor critice cu consecințe ce se pot încadra în spectrul pierderilor de vieți omenești.

ABSTRACT

As organizations all over the world become increasingly dependent on computer information systems, the issue of security of these systems against the cyber-attacks is becoming increasingly important. The technology evolves by the day and new methods of breaking networks and computers information systems are developed by these entities that we just discussed about.

Threats can be of different types and may pursue different objectives. Depending on the environment of a computer systems or network is and type of information that is hosted on it, different classes of threats will have an interest in trying to get different types of information or access, based on their particular capabilities.

Actors threats were attackers may be represented in several general categories:

Individual hackers, who always worked individually;

Groups of hacker who collaborate with other hackers to achieve their goals;

Cyber terrorism cells who aimed to disrupt government functions, defense departments and critical infrastructure disruption.

DARK WEB UNIVERSUL HACKERILOR

de Mirela CERNAT și Marius-Ștefan MUNTEANU

CYBERSPACE - ULTIMA FRONTIERĂ

Dacă explorarea spațiului cosmic era, în anii ’70, expresia maximă a progresului științific și tehnologic, în prezent un nou spațiu, creat de om, cel virtual, a devenit „noua frontieră extremă ce trebuie cucerită”. Și armele, și actorii sunt diferiți în cele două situații, însă scopul a rămas același: nevoia omului de supremație, de a controla resurse, de a-și testa capabilitățile și de a încerca să își depășească în mod constant limitele.

În acest nou context, *hacking*-ul a devenit un fenomen greu controlabil, mai ales din cauza faptului că este considerat de cei care-l practică o cultură, un mod de viață. Nu se afișează public, se ascund după identități false în locuri greu accesibile autorităților, care le urmăresc modul de atacare a infrastructurilor informatice pentru a reduce astfel vulnerabilizarea și compromiterea securității persoanelor și a comunităților.

HACKERII ÎN DARK WEB

Fenomenul devine tot mai periculos pe măsură ce se accentuează tendința, în *Dark Web*, de înființare a grupurilor de *cybermercenary*, organizații criminale care prestează „servicii la comandă”, cum ar fi executarea de atacuri cibernetice sau crearea de viruși informatici.

Recrutarea hackerilor pentru astfel de misiuni se face pe forumuri *underground* în *Dark Web* - o „realitate ascunsă”, unde sunt găzduite *site*-uri ilegale, magazine *online* pentru droguri, arme, asasini plătiți, mărfuri contrafăcute, acte de identitate și carduri bancare falsificate, conturi furate, servicii de *hacking* sau chiar *servere* cu baze de date ascunse ale băncilor și ale serviciilor secrete din întreaga lume.

Piața *Dark Web* înflorește pe baza anonimității oferite de protocoalele de comunicare implementate în această zonă a Internetului, specialiștii în securitate IT avertizând asupra tendinței în creștere a vânzărilor acestui tip de servicii.

Un suport tehnic suplimentar - interfețe prietenoase, email și *Internet Relay Chat* (serviciu de transmitere a mesajelor în timp real) - simplifică navigarea în *Dark Web*.

SERVICII DE HACKING ÎN DARK WEB

Cele mai des întâlnite servicii disponibile în *Dark Web* sunt: executarea unor atacuri de *tip DDoS, malware, spam, kituri* de exploatare vulnerabilități, servicii de *botnet* (*software* ce permite preluarea controlul acestora fără cunoștința proprietarilor de drept și să le utilizeze pentru a lansa atacuri cibernetice asupra unor terți), *doxing* (culege informații de pe Internet despre o anumită entitate) ori *crypter* (program care folosește mai multe limbaje de criptare pentru a putea face un *server* creat de utilizatorul respectiv nedetectabil de antivirus). Pentru a închiria, de exemplu, un *botnet*, utilizatorii plătesc de la 2-5 dolari / lună (pentru atacuri limitate ca număr și durată) până la 100-200 dolari / lună pentru atacuri mai complexe. *Kiturile* de exploatare au prețuri mult mai mari (20.000-30.000 dolari), motiv pentru care utilizatorii le închiriază pentru perioade limitate (500 dolari / lună).

Plata se poate face, în general, prin utilizarea criptomonedelor, precum **Bitcoin** sau **Litecoin**, rareori fiind acceptate plățile prin **PayPal**, **Western Union** sau alte sisteme publice. Sunt preferate monedele digitale, pentru că la asemenea tranzacții nu se poate oferi un cont bancar, atașat invariabil unei identități. Pentru a ușura calculele, există și un curs valutar al **Bitcoin**-ului, dar și case de schimb. Cei care nu dispun de fondurile necesare își pot cumpăra *exploituri*, viruși destinați obținerii de **Bitcoin**.

În *Dark Web* există câteva **comunități de *hacking,*** abordabile prin intermediul protocoalelor de anonimizare. Multe dintre acestea sunt accesibile numai pe baza unei invitații, fiind specializate pe anumite

topicuri (atacuri de tip troian), dar există și comunități generice (ex. forumuri de *hacking*) în care membrii discută probleme legate de acest domeniu, cu excepția fraudelor bancare (ex. carduri false, alte fraude financiare).

De asemenea, *Dark Web*-ul găzduiește multe **forumuri și chat-uri dedicate activității de *black hacking,*** dar vânzarea produselor și serviciilor se realizează pe piața neagră.

Principalele magazine *online* pentru produsele și serviciile de *hacking* sunt: **Alpha Bay**, **Silkroad 3.0**, **TheRealDeal**, **DreamMarket**, **MRNiceGuy**, **Outlaw**, **Majestic Garden**, care folosesc platforme/instrumente de criptare precum **Tor**, ce codifică toate datele utilizatorilor în straturi și le trimite spre o rețea de servere aparținând unor voluntari răspândiți în toată lumea. **Tor** alege, în mod aleator, un nod prin care intră în rețea, printr-o conexiune criptată. Acesta se conectează cu un alt nod, printr-o altă conexiune criptată și așa mai departe. Nodul de ieșire se conectează la destinație. La fiecare zece minute, nodul de intrare se modifică, astfel că orice încercare de restabilire a traseului și, implicit, de localizare este sortită eșecului. Informația este cifrată multiplu, prin intermediul altor utilizatori anonimi, fiecare dintre aceștia fiind, la rândul său, un canal de transmitere a datelor de la și către alte persoane. Pachetele de date sunt divizate și criptate și trec prin nenumărate servere până la destinația finală și înapoi. Un alt instrument de criptare utilizat pentru a-și ascunde identitatea, locația și adresa IP accesabil prin *browserul* Tor este **I2P**. Acesta oferă permanent două straturi de criptare, fiind mai rezistent atacurilor care vizează scoaterea de sub anonimat a utilizatorilor.

Una din problemele majore în comunitățile de *hacking* din piețele negre este încrederea, utilizatorii implementând în acest sens un mecanism de stabilire a reputației unui vânzător bazat pe *feedback*-ul cumpărătorilor.

În rețeaua Tor, există și *hackeri* care își oferă serviciile prin intermediul propriilor *site*-uri, dar utilizează forumurile magazinelor *online* pentru a menține contactul cu clienții, având astfel și beneficii precum posibilitatea de a-i fi verificată reputația de către viitori colaboratori prin parcurgerea *feedback*-urilor primite în timp, dar și protecția identității sale și a celor cu care vine în contact.

În acest sens pot fi menționate **magazinele *online*** „**TheRealDeal**” care oferă un mediu propice pentru comercializarea kiturilor de exploatare și serviciilor de *hacking* (atacuri *DDoS*, *malware*), dar și tutoriale pe teme conexe activității de hacking, respectiv „**Nucleus**” - specializat mai mult pe produse (ex. malware, carduri clonate) și mai puțin pe servicii.

Din punctul de vedere al efectelor atacurilor executate, există două mari comunități de *hackeri*: ***white hacking* sau *white hats***, cei care descoperă fisurile din programele informatice fără a profita de ele (de obicei aceștia au contract cu o organizație care îi plătește pentru a descoperi aceste vulnerabilități și a le repara), și ***black hacking* sau *black hats***, categorie în care intră *crackerii* (adevărații pirați informatici) și *phisherii*, care construiesc, de exemplu, anumite *site*-uri pentru a fura bani sau informații despre cărțile de credit.

Cât privește fenomenul ***white hacking***, acțiunile derulate în **Dark Web** nu vizează numai persoane, companii, autorități oficiale, transformându-se uneori, mai ales în actualul context geopolitic, într-o „formă virtuală de luptă împotriva extremismului” (Maria STEINER, 2015). Relevant în acest sens este atacul grupului de *hackeri* **GhostSec**, afiliat **Anonymous**, asupra *site*-ului **Isdrat**, administrat de organizația jihadistă **Stat Islamic** în **Dark Web**, înlocuind conținutul cu reclame la unele medicamente uzuale.

Un alt exemplu de *white hacking* este cel al organizatorilor Primăverii Arabe din Egipt care au folosit rețeaua **TOR** pentru a nu fi descoperiți de autorități care blocaseră accesul la toate platformele de socializare de pe teritoriul țării (Sullivan John, 2011). Grație

Tor, aceștia au devenit anonimi și păreau că accesează Internetul dintr-o altă zonă a lumii, putând astfel să își continue planul care a dus la căderea regimului **MUBARACK**. De altfel, **The Tor Project** a primit **Premiul pentru Proiecte în Beneficiul Social** pentru „impactul social benefic asupra lumii”, acordat de **Free Software Foundation**.

Revenind la ***black hacking***, observăm cum sunt afectate economii sau linii de business întregi și, totodată, viețile atâtor oameni! Datele personale a mii de oameni - nume, adrese, parole, coduri PIN, date medicale - sunt în mod constant subtilizate și vândute pe *site*-urile din **Dark Web**, care a devenit astfel o piață uriașă pentru comerțul cu date furate, mai profitabil chiar decât traficul de droguri.

În septembrie 2014, experții de la **Kaspersky Lab** au descoperit o campanie de *hacking* condusă de atacatori din Brazilia care vizau *routerele* domestice prin intermediul unui atac *web* (Paganini PIERLUIGI, 2015). Prin tehnici de inginerie socială și prin utilizarea unor *site*-uri *web* malițioase, au schimbat setările *DNS* ale *routerelor* domestice, ceea ce le-a permis atacatorilor să redirecteze victimele către *site*-uri *web* false pentru a fura *credențialele* clienților băncilor braziliene.

Hacking-ul a devenit un fenomen dificil de controlat prin prisma faptului că ofertele sunt tot mai numeroase, iar prețurile acestor servicii scad în mod constant, ceea ce constituie o vulnerabilitate cu o dezvoltare exponențială din perspectiva activităților de prevenire și contracarare.

Destructurarea acestor grupări devine o altă poveste fără sfârșit: ce eliminăm azi, apare mâine sub o altă formă, mai sofisticată și mai greu de găsit, atât timp cât va exista o piață pentru absolut orice se poate tranzacționa, legal sau ilegal.

Tur virtual al grupărilor de hackeri în Dark Web

Putem demara un tur virtual al comunității de *hacking* cu prezentarea unor pagini *web* dedicate:

„RENT-A-HACKER”

- **administrat de un singur utilizator;**
- **oferă servicii specializate în domeniu, capabile „să distrugă o afacere sau viața unei persoane” (fiind, probabil, administratorul unui *botnet* prin intermediul căruia execută atacuri de tip DDoS);**
- **„capabil să deruleze campanii de spionaj și urmărire *online*”, să culeagă informații de natură privată.**

„HACKER FOR HIRE”

- **oferă o gamă largă de servicii ofensive, de la fraude cibernetice la *hacking*, dar și de tip defensiv, pentru victimele actelor de criminalitate *online*.**

„HELL”

- **conține câteva secțiuni în care se regăsesc instrumente de *hacking*, tutoriale, iar la rubrica „Joburi”, oferte de servicii din partea hackerilor, care pot fi contactați pentru negocierea ofertelor.**

ABSTRACT

The famous dark web is a space for illicit marketplaces where anyone can buy anything, including, but not limited to, hackers for hire. Hackers, cyber criminals and whistleblowers are attracted to communities on the dark web. Such communities allow them to share information and make business deals without fear of reprisal. There are also dark web hacking forums where hackers and cybercriminals share stolen data and hacking tips, where users can buy and sell hacked data, as well as share their hacking techniques and tutorials. Finally, authorities turn to hacking methods for tracking IP addresses on the Dark Web, deploying hacking tools known internally as network investigative techniques for shutting down a wide range of illegal activities.

REȚELE DE „BOȚI”

OFENSIVA ARMATELOR DE ZOMBI ALE INTERNETULUI

de Radu STRATULAT

Rețelele de tip *botnet* sunt **una dintre cele mai periculoase amenințări la adresa securității Internetului**, problema fiind globală prin natura ei.

Un *botnet* reprezintă **o rețea de calculatoare infectate (prin exploatarea unor vulnerabilități sau prin inginerie socială) cu o aplicație *malware* care permite infractorilor cibernetici să le poată controla de la distanță**, fără ca proprietarii de drept să fie conștienți de acest lucru. Calculatoarele compromise (boți, *zombi* sau drone) sunt controlate de o persoană sau de un grup de atacatori (*Botmaster*) prin intermediul unor centre de comandă și control (**C&C**). Aceștia pot utiliza puterea cumulată a mai multor calculatoare *zombi* pentru a amplifica exponențial impactul atacurilor cibernetice derulate, dimensiunea unei astfel de rețele putând ajunge de la o mie la câteva zeci de mii de calculatoare infectate. Un studiu efectuat la nivelul anului 2008 arăta că aproximativ 40% din cele 800 de milioane de calculatoare conectate la Internet într-o zi normală făceau parte dintr-o rețea de tip *botnet*.

Rețelele *botnet* reprezintă coloana vertebrală a operațiunilor cibernetice având în vedere rolurile multiple ce le pot fi alocate, cum ar fi: culegerea de date personale, parole, detalii ale cardurilor de credit, adrese și numere de telefon, acestea putând fi utilizate ulterior în diferite activități infracționale ce vizează furtul de identitate, fraudele bancare, *spam*-ul, ingineria socială, accesul de la distanță pe sistemele țintă sau distribuția de *malware*. De asemenea, pot fi utilizați în lansarea de atacuri de tip **DDoS** (*Distributed Denial of Service*) asupra *site*-urilor *web* sau rețelelor informatice, respectiv în activități de spionaj industrial sau guvernamental.

Infractorii cibernetici identifică permanent noi metode care să facă rețelele *botnet* mai robuste, mai greu de identificat, pentru a putea rămâne active perioade mai mari de timp, adaptându-le capabilitățile de a ascunde datele extrase în timpul atacurilor. Spre exemplu, prin găzduirea unui centru de comandă și control într-o rețea de tip *Tor*, se poate ascunde locația serverului, acesta devenind mult mai greu de identificat și de scos din funcțiune. Rețelele *botnet* sunt create astfel încât comportamentul lor să fie aproape similar cu cel al unor aplicații legitime, detecția lor necesitând astfel un efort mai mare și un timp mai îndelungat. Aceste rețele devin tot mai sofisticate, cu boți care comunică direct unul cu altul (*peer-to-peer*), fără a avea nevoie de intermedierea unui *C&C*. Dacă un *bot* este descoperit, un altul îi va lua locul, extinzând durata de viață a rețelei de boți și asigurând continuitatea activităților ilegale derulate.

Un efort susținut a fost derulat într-o operațiune globală coordonată de Interpol pentru a înlătura *botnet*-ul **Simda**, responsabil pentru infectarea a cel puțin 770.000 de calculatoare (peste 90.000 fiind infectate doar la începutul anului 2015) din peste 190 de țări, cele mai afectate fiind SUA, Marea Britanie, Canada și Rusia. Activ timp de câțiva ani, *botnet*-ul Simda a fost rafinat permanent pentru a exploata orice vulnerabilitate cu noi versiuni tot mai greu de depistat, generate și distribuite la intervale foarte scurte de timp (de câteva ore). În prezent **Kaspersky Lab's** deține o colecție de peste 260.000 de fișiere executabile aparținând diferitelor versiuni ale *botnet*-ului Simda.

Botnet-ul **Coreflood** a reușit infectarea a mai mult de 2 milioane de calculatoare în toată lumea. *Botmaster*-ii au utilizat sistemul pentru a „exfiltra” peste 500 GB de informații bancare sensibile, rezultând pierderi financiare enorme, atât pentru instituțiile bancare, cât și pentru persoanele fizice.

Rețelele *botnet* reprezintă infrastructura perfectă pentru lansarea atacurilor de tip **DDoS**, în cursul cărora un număr foarte mare de computere compromise atacă o singură țintă, sistemele vizate fiind determinate să nu mai poată răspunde la comenzi din cauza indisponibilizării sau blocării resurselor. Caracteristica ultimei perioade este magnitudinea volumetrică a acestor atacuri, generată de implicarea unor rețele *botnet* de mare calibru, țintele vizate fiind de regulă corporații (șantajate ulterior de către atacatori), însă au fost derulate și o serie de atacuri motivate politic.

*** BOTNET-UL COREFLOOD A REUȘIT INFECTAREA A MAI MULT DE 2 MILIOANE DE CALCULATOARE ÎN TOATĂ LUMEA.**

Hackeri neidentificați au încercat să saboteze chiar și rețeaua Internet. Între 30 noiembrie și 1 decembrie 2015, o entitate neidentificată a inițiat și derulat cel mai puternic atac **DDoS** asupra celor 13 servere **DNS** (*Root Name Servers*) ce fac parte din infrastructura de bază a Internetului, inundându-le cu trafic de pe mai multe adrese **IPv4**, serverele primind mai mult de 5 milioane de cereri pe secundă și peste 50 de miliarde de interogări în cele două zile. În comparație, în ultimii doi ani, cele mai multe cereri recepționate într-o zi normală pe serverele **DNS** nu au depășit cifra de 10 milioane. Din fericire, atacul nu a reușit să blocheze serverele **DNS**, deoarece operatorii acestora au realizat devierea traficului suplimentar înspre o serie de servere aflate în rezervă. Dată fiind însă magnitudinea atacului, doar o entitate foarte puternică ar dispune de resursele necesare susținerii unui astfel de atac cibernetic, coordonat pe o perioadă de 48 de ore, existând suspiciuni că în spatele atacului s-ar afla un actor statal.

În luna ianuarie 2016, un atac **DDoS** revendicat de gruparea *hacktivistă* **New World Hacking** a fost îndreptat împotriva *site*-ului **BBC**. Gruparea susține că atacul a avut magnitudinea de 602Gbps, ceea ce-l plasează pe primul loc în istoria atacurilor de acest tip, depășind de aproape două ori recordul precedent de 334Gbps din anul 2015 asupra rețelei **Arbor Networks**. Pe lângă site-ul **BBC**, **New World Hacking** a atacat în aceeași zi și *site*-ul candidatului la alegerile prezidențiale din SUA, **Donald TRUMP**, gruparea afirmând că toată operațiunea a fost doar un test pentru ceea ce va urma.

Pe viitor, amenințările *online* vor evolua mai mult înspre a stăpâni **psihologia din spatele fiecărei combinații inițiate**, decât înspre stăpânirea aspectelor tehnice ale operațiunii în sine. Atacatorii vor continua să utilizeze **teama** ca și instrument principal, ce s-a dovedit a fi deosebit de eficient în trecut. În ultima perioadă, infractorii cibernetici au făcut uz de *crypto-ransomware* pentru a convinge utilizatorii *online* să plătească răscumpărări în vederea obținerii accesului la cea mai importantă resursă a unui sistem, propriile date. Ne putem aștepta deci la noi metode, mai elaborate, de direcționare a psihicului victimelor în direcția dorită de atacatori, prin noi trucuri ce folosesc ingineria socială pe post de momeală.

BOTNEȚII ȘI MOBILITATEA

Explozia de *smartphone*-uri și adaptarea lor în creștere la cerințele pieței, precum și nevoia de mobilitate și putere de procesare sunt tendințe care nu au trecut neobservate de către autorii de *malware*. Ca urmare, aceștia și-au concentrat atenția pe dispozitivele mobile, fapt ce a condus la o creștere abruptă a *malware*-ului mobil în ultima perioadă.

Smartphone-urile sunt practic niște minicalculatoare la purtător. Le folosim nu numai pentru a efectua apeluri, ci și pentru operațiuni bancare, cumpărături *online*, poștă electronică, navigare pe Internet etc. Cei mai mulți dintre utilizatori păstrează o mare parte dintre datele importante sau personale pe telefonul mobil. Creșterea exponențială a numărului de aplicații descărcate, partajate sau instalate, face ca aceste telefoane inteligente să devină tot mai vulnerabile la diverse tipuri de *malware*. Operațiunile bancare derulate de pe dispozitivele mobile au devenit tot mai populare, fără însă a beneficia de mecanisme de protecție comparabile cu cele de pe PC-uri, încurajând astfel criminalitatea informatică.

În ceea ce privește criminalitatea cibernetică, este întotdeauna dificil de previzionat ce se va întâmpla peste un an sau peste 10 ani de acum înainte. Peisajul amenințărilor mobile a suferit schimbări dramatice în ultimii 10 ani, iar comunitatea infracțională continuă să identifice noi metode, tot mai ingenioase, de a utiliza aceste atacuri pentru un singur scop, cel financiar. Având în vedere explozia de telefoane inteligente și a multor altor tehnologii mobile, o previziune rezonabilă pentru viitorul nu foarte îndepărtat ar fi legată de convergența *malware*-ului mobil cu cel specific PC-ului. Cum totul devine mobil, putem preconiza că și *malware*-ul va migra în această direcție, devenind „mobil”.

PRIETENII IMPERSONALI

Nici rețelele sociale nu au fost trecute cu vederea de către autorii de *malware*, în urmă cu câțiva ani **Panda Security** atrăgând atenția pentru prima dată asupra existenței unei rețele care comercializa *boți* specializați în *targetarea* rețelelor sociale și conturilor *webmail*. *Boții* erau oferiți spre vânzare prin intermediul paginilor *web*, oferta conținând un portofoliu amplu de programe ce aveau ca țintă rețelele sociale și serviciile *webmail*, incluzând **Twitter**, **Facebook**, **Hi5**, **MySpace**, **MyYearBook**, **YouTube**, **Tuenti**, **Friendster**, **Gmail** și **Yahoo**.

O echipă de cercetători de la Departamentul de Etică și Ingineria Computerelor din cadrul Universității Columbia Britanică (*The University of British Columbia/**UBC***) au descoperit faptul că grupuri de așa-ziși *„boți* sociali” ar putea să însemne dezastrul unor rețele precum **Facebook** sau **Twitter**. Acești boți sociali mimează foarte bine utilizatorii *online*, adăugând posturi care par a veni de la ființe umane, dar, în secret, promovează produse sau puncte de vedere, iar unii pot să se folosească de noile conexiuni pentru a intra în posesia informațiilor private ale utilizatorilor respectivi. Coordonați de un *botmaster* abil, aceștia pot aduna în scurt timp o cantitate mare de informații private de diferite tipuri. Cercetătorii UBC au calculat că o rețea de boți are nevoie de doar 1000 de prieteni umani însumați pentru a deveni profitabilă, dacă scopul acesteia este furtul de informații. „Complexitatea rețelelor de boți sociali face dificilă realizarea unei politici unitare împotriva lor.”, afirmă cercetătorii UBC.

În 2015, **Facebook** a anunțat că a identificat peste 170 milioane de conturi false, în marea lor majoritate *boți* sociali, compania fiind nevoită să declanșeze o adevărată ofensivă în vederea eliminării acestora.

INTERNETUL TUTUROR LUCRURILOR - O NOUĂ PROVOCARE

Internetul de bandă largă devine tot mai răspândit, costurile de conectare scad tot mai mult, tot mai multe echipamente sunt create cu senzori și capabilități *Wi-Fi* incluse, costurile de producție scad, iar invazia telefoanelor inteligente este în continuă creștere. Toate acestea creează ambientul perfect pentru **Internetul Tuturor Lucrurilor** (*Internet of Things* / **IoT**).

Dincolo de dispozitivele mobile, cel mai probabil obiectiv viitor pentru infractorii cibernetici îl va reprezenta **IoT**. Este extrem de dificil de prognozat numărul de obiecte conectate ce vor exista pe piață în următorii 5 ani, **Gartner** estimându-l la peste 30 de miliarde, în timp ce **IDC** estimează că piața va depăși 200 de miliarde. Mai simplu spus, **IoT** este practic un concept ce se referă la un viitor în care obiecte, oameni, sisteme și procese sunt conectate între ele cu ajutorul Internetului. Aceasta include totul, de la telefoane sau alte dispozitive mobile, automobile, espressoare, *routere*, mașini de spălat, frigidere, sisteme de închidere sau de iluminat, sisteme multimedia și aproape orice altceva ne putem imagina. **IoT** reprezintă o transformare majoră în lumea digitală, având potențialul de a afecta direct orice persoană sau afacere. **Cisco** și **General Electric** estimează dimensiunea **IoT** la peste 10.000 miliarde de dolari, iar **International Data Corporation** estimează că la nivelul anului 2020 peste 40% din datele tranzitate în întreaga lume vor fi rezultate ale comunicațiilor dintre aceste echipamente / sisteme interconectate.

Anul **2015** a marcat unele incidente în care au fost implicate dispozitive compromise sau nesigure, variind de la televizoare inteligente până la automobile. Chiar dacă utilizatorii au devenit tot mai conștienți de riscurile de securitate generate de conectarea diverselor dispozitive la Internet, interesul public față de tehnologia *smart* este în continuă creștere. Dată fiind diversitatea de sisteme de operare și lipsa unor reglementări solide pentru aceste dispozitive inteligente, un atac cibernetic de amploare asupra acestora pare de neevitat.
Cum tot mai mulți producători și furnizori de servicii vor să valorifice oportunitățile de afaceri generate de această piață, este rezonabil să presupunem că securitatea nu a fost primul lucru luat în considerare în procesul de dezvoltare a acestor noi produse. Oare va fi Internetul Tuturor Lucrurilor următoarea mare provocare pentru infractorii cibernetici?

ABSTRACT

Zombie computer networks, also known as botnets, have been for several years the most important infrastructural component in the world of cybercrime actors. In a reality where the purchase and sale of services information theft or campaign spreading ransomware are facilitated by them, botnets play a central role in the world of cybercrime.

In other words, hundreds or thousands of computers, smartphones or IoT devices, that are part of such networks, rivaling the power of today's most powerful cloud computing platforms, are used for sending spam, launching Denial of Service attacks and performing other malicious actions.

* ÎN 2015, FACEBOOK A ANUNȚAT CĂ A IDENTIFICAT PESTE 170 MILIOANE DE CONTURI FALSE, ÎN MAREA LOR MAJORITATE BOȚI SOCIALI

FORUMURILE DE CRIMINALITATE CIBERNETICĂ

UN MOTOR AL ECONOMIEI SUBTERANE

de Octavia POPA

Societatea contemporană este caracterizată, printre altele, prin asediul informațional zilnic la care este supusă. În spatele acestui flux continuu de imagini, sunete și semne funcționează un sistem socio-profesional a cărui complexitate și anvergură sunt nebănuite.

Evoluția tehnologică și apariția Internetului au determinat o serie de mutații în ceea ce privește viața cotidiană a individului, ajungând să influențeze majoritatea acțiunilor sale. În realitatea zilelor noastre, se remarcă atât o dezvoltare a tehnologiei, cât și o diversificare a metodelor de comitere a infracțiunilor de tip informatic. La începutul anilor 2000, s-au remarcat atacurile de tip *phishing*, fraudele informatice și atacurile prin intermediul rețelelor de tip *botnet*, pentru ca, actualmente, atacurile cibernetice să atingă un nivel nemaiîntâlnit de tehnologizare.

În acest context al diversificării și creșterii nivelului de complexitate al agresiunilor cibernetice s-a resimțit nevoia apariției unor spații exclusiviste care să îi permită individului, în condiții de anonimat, relaționarea și schimbul de informații, servicii sau produse specifice unei anumite tematici. Apariția acestor medii cibernetice, cunoscute sub denumirea de forumuri, a condus la modificarea modului de interacțiune între grupările de criminalitate organizată, prin prisma atât a eliminării necesității întâlnirilor față în față cât și a „garanției" anonimizării activităților infracționale derulate.

Forumurile de criminalitate informatică sunt organizate, în majoritatea cazurilor, pe model ierarhic, membrii fiind împărțiți în categorii în funcție de diferite criterii precum vechimea, expertiza, notorietatea sau veniturile realizate din derularea de agresiuni cibernetice.

Înțelegerea acestor medii este dificilă datorită răspândirii geografice ample, diversității culturale, măsurilor complexe de anonimizare, respectiv criptării comunicațiilor între utilizatori, ceea ce a determinat ca aceste platforme să fie ermetice iar accesul în interior să fie unul foarte restrictiv.

STUDIU DE CAZ - FORUMUL DARKODE

Un foarte bun exemplu în sensul celor prezentate este forumul de criminalitate informatică „Darkode.com", destructurat în luna iulie 2015, ca urmare a unor eforturi internaționale comune ale instituțiilor de aplicare a legii din aproximativ 20 de state. *Darkode* a reprezentat o platformă on-line exclusivistă, ai cărei membri sunt persoane cu preocupări în domeniul criminalității informatice ce provin, cu precădere, din state foste componente ale Uniunii Sovietice dar și din țări precum România, Marea Britanie, China, India, Algeria sau Brazilia. În anul 2015 „darkode.com", datorită nivelului foarte avansat al expertizei deținute de către utilizatori, era considerat unul dintre cele mai importante forumuri de criminalitate informatică din lume.

Comunitatea era una ermetică, formată din aproximativ 400 de membri. Accesul se realiza în baza unei invitații din partea unui membru cu notorietate și a unui interviu în care fiecare potențial „candidat" trebuia să își dovedească expertiza în domeniul criminalității informatice, respectiv să ofere o descriere amănunțită atât a activităților derulate, a intereselor sale, precum și a elementelor de actualitate (tehnici, resurse, aplicații malițioase) ce pot aduce plusvaloare comunității. Aceste metode de securizare erau impuse pentru a preveni accesul în forum a unor reprezentanți ai legii sau investigatori sub acoperire. În ceea ce privește structura organizatorică, forumul era structurat pe trei paliere ierarhice, după cum urmează:

„Nivel -1" - în cadrul căruia activau noii membri, care aveau acces în forum dar nu au realizat nicio tranzacție cu ceilalți utilizatori. Acești utilizatori nu aveau acces la resursele forumului și nu beneficiau de facilitatea de a invita alte persoane în cadrul comunității;

„Nivel 1" – destinat membrilor care au inițiat/ finalizat tranzacții cu membri mai vechi și au primit *feedback* pozitiv din partea acestora. Acești utilizatori aveau acces doar la discuțiile purtate în cadrul „Nivelului 1" și puteau lansa un număr limitat de invitații către alți potențiali membri;

„Nivel 2" – reprezenta cea mai importantă zonă (numărul de membri pentru această categorie era de ordinul zecilor), unde tranzacțiile realizate erau de ordinul zecilor și sutelor de mii de dolari. Accesul în cadrul „Nivelului 2" se realiza după ce se obținea aprobarea a cel puțin cinci membri de „Nivel 2" iar numărul invitațiilor ce puteau fi lansate către potențiali noi membri era nelimitat.

În cadrul forumului au fost comercializate atât produse specializate (aplicații de tip *botnet* destinate furtului de date bancare, vulnerabilități informatice, servicii de *hosting*, servicii destinate anonimizării) cât și date aferente conturilor bancare a milioane de persoane, în special din SUA, Marea Britanie, Canada și Australia.

BOTNEȚII BANCARI

Rețelele de boți (*botnet*) sunt alcătuite din sisteme informatice infectate, aflate în locații diferite pe glob, controlate de la distanță de către alte persoane sau entități decât deținătorii legitimi ai acestora.

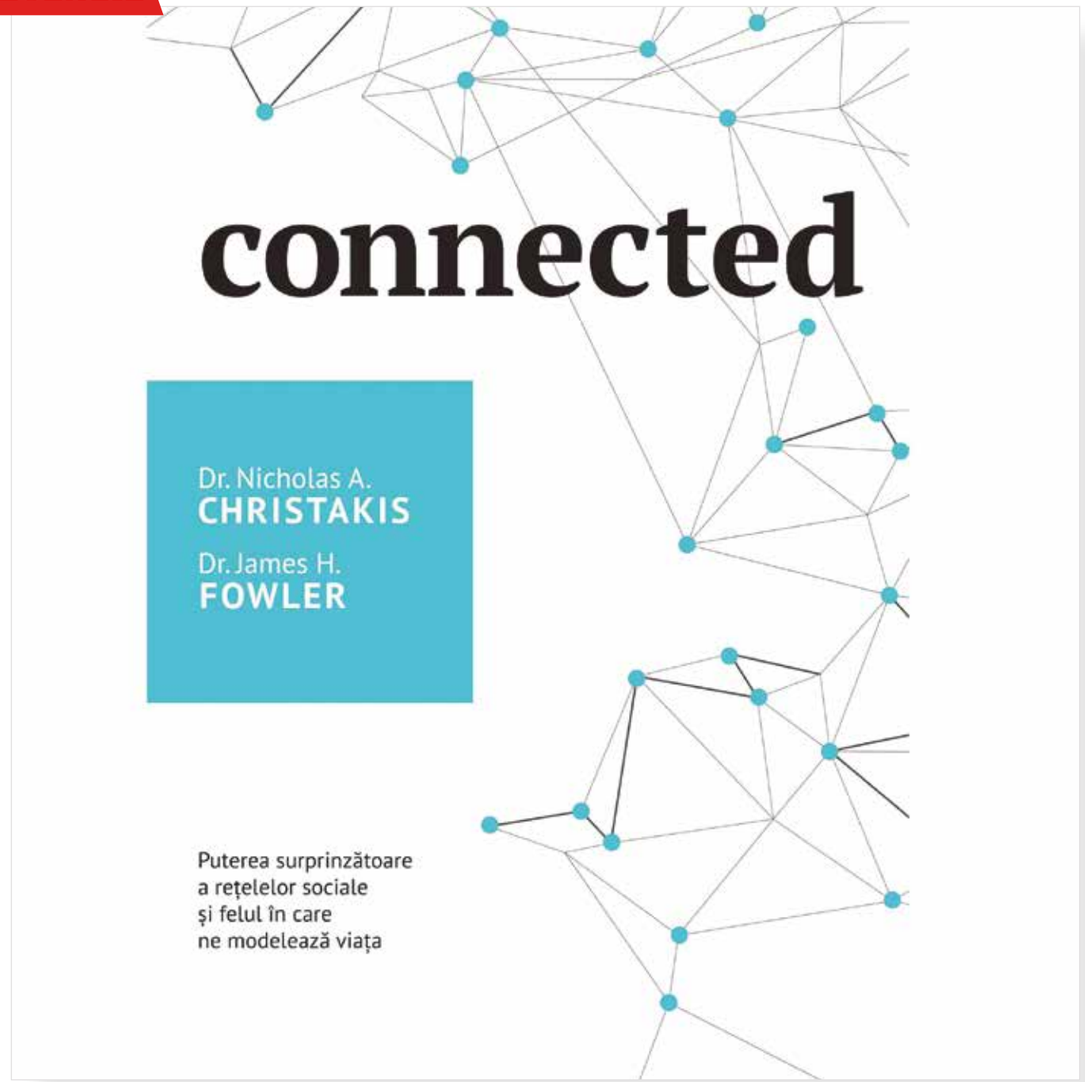
Creșterea exponențială înregistrată în domeniul criminalității informatice poate fi explicată de adoptarea în cadrul forumurilor de criminalitate informatică a modelului „crime-as-a-service". Acest concept definește procesul de transformare al forumurilor de criminalitate informatică în platforme de comerț ilegal cu servicii sau instrumentele, prin intermediul cărora, orice persoană, cu sau fără cunoștințe tehnice, poate derula atacuri cibernetice.

Astfel în 2010, Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) menționa, în cadrul unei lucrări științifice, că prejudiciul generat de aplicații malițioase, la nivel global, era de aproximativ 10 miliarde USD. În 2014, directorul adjunct al FBI, Joseph DEMAREST, afirma că rețelele de boți generau doar în SUA, un prejudiciu de 9 miliarde USD, iar la nivel internațional, suma urca până la 110 miliarde USD.

Importanța amenințării determinate de rețelele de boți este reflectată în Raportul cu privire la alertele de securitate cibernetică procesate de CERT-RO în cursul anului 2014, în care a fost menționat faptul că „rețelele de tip *botnet* reprezintă cea mai importantă problemă existentă în spațiul cibernetic național deoarece aceste computere compromise pot fi utilizate în derularea de atacuri cibernetice asupra altor ținte din România sau din spațiul extern țării noastre".

ABSTRACT

Nowadays the society faces new challenges in terms of threats. The development of the Internet provides new opportunities for the organized crime groups due to the advantages offered by the "online world", like anonymity, increased efficiency, and the possibility to launch cross-border attacks. The increased use of the Internet in public institutions generates risks and vulnerabilities in terms of cyber security. In this context cyber security has become a national security priority as a part of the national security strategy. A wide variety of methods like phishing, spamming, social engineering, skimming, carding as well as other sophisticated techniques - bank botnets, creating and spreading specialized malware and bulletproof hosting are used by cyber criminals. These groups are seeking to obtain substantial financial gains with less effort and reduced costs. The losses generated by cyber criminality are at a high level worldwide.



CONNECTED

PUTEREA SURPRINZĂTOARE A REȚELELOR SOCIALE ȘI FELUL ÎN CARE NE MODELEAZĂ VIAȚA

de Daniela LUCA

Connected, o carte despre puterea rețelelor sociale asupra oamenilor, reprezintă un rezultat al interconectării activității a doi cercetători, Dr. Nicholas A. CHRISTAKIS și Dr. James H. FOWLER. „Numeroși oameni cu care suntem conectați au jucat un rol decisiv în apariția acestei cărți", susțin autorii care subliniază că un prieten comun a inițiat „un lanț lung de prezentări ce au conectat oameni care, anterior, se aflau la distanță unii de ceilalți".

Specialist în medicină și sociologie, Dr. CHRISTAKIS este profesor de sociologie medicală și medicină la *Harvard Medical School*, respectiv profesor de sociologie la *Harvard Faculty of Arts and Sciences*. De mai bine de 15 ani, Dr. CHRISTAKIS cercetează modul în care factorii sociali și interacțiunile sociale afectează sănătatea și longevitatea, fiind recunoscut pentru studiile sale despre formarea și funcționarea rețelelor sociale. În anul 2009, Dr. CHRISTAKIS a fost nominalizat de revista **Time** drept una dintre cele mai influente personalități ale lumii.

Dr. FOWLER este politolog, profesor asociat la *University of California* și la *Center for Wireless and Population Health Systems*, fiind recunoscut pentru studiile despre rețelele sociale, economia comportamentală, implicarea politică și genetica politică.

Interese comune, conexe, au unit doi specialiști care nu se cunoșteau si care se aflau la distanță, în susținerea ideii că „întregul este mai bun decât suma părților implicate".

Connected a apărut în 2009, fiind tradusă ulterior în aproape 20 de limbi. Cartea a fost considerată cea mai bună a anului în topul *Best Innovation and Design Books*, a obținut premiul *Books for a Better Life* și a beneficiat de o prezentare specială în *New York Times Magazine*.

Connected a fost tradusă în limba română în anul 2015, fiind inclusă în colecția *„Outliers"* a editurii Curtea Veche Publishing, colecție în care se regăsesc cărți ale autorilor care se remarcă pentru că sunt mereu cu un pas înaintea tuturor, dezvăluind tendințele societății, economiei mondiale, culturii globale și digitale.

O SINTEZĂ MULTIDISCIPLINARĂ

Deși poate fi percepută ca un studiu sociologic al relațiilor interumane, al rețelelor sociale, cartea reprezintă o sinteză multidisciplinară (sociologie, medicină, psihologie, politologie, teologie, tehnologie/ mediul *online*) prin care autorii atrag atenția cu privire la puterea rețelelor sociale și analizează modul în care acestea ne modelează viața.

Pentru a realiza fundamentul acestei argumentații, autorii identifică cinci reguli în funcție de care se formează rețelele și se produce influența în rețea: 1. Noi ne modelăm rețeaua; 2. Suntem modelați de rețeaua noastră; 3. Prietenii ne influențează; 4. Prietenii prietenilor noștri ne influențează; 5. Rețeaua are propria viață.

Deși este general acceptată teoria cu privire la faptul că prieteniile nu sunt întâmplătoare și că relațiile sociale depind de factori precum cultura, limitele geografice, apartenența politică, statutul socio-economic sau chiar factori genetici, autorii aduc argumente, exemple și date statistice care să susțină ideea. „Dacă ești bogat, vei atrage și mai mulți prieteni, iar dacă ai mai mulți prieteni, vei găsi mai multe căi de a te îmbogăți", este o afirmație ilustrativă în acest sens.

Conexiunea și **contaminarea** sunt două aspecte fundamentale ale rețelelor sociale. Cu toate că a fost demonstrat (Stanley Milgram) că există șase trepte distanță între oricare două persoane (prietenul tău se află la o treaptă distanță de tine, prietenul prietenului este la două trepte ș.a.m.d.), autorii argumentează că influența în rețea se realizează doar la trei trepte. Pornind de la ideea că tot ceea ce facem și spunem tinde să se transmită în rețeaua noastră, influențându-ne prietenii (o treaptă), apoi pe prietenii prietenilor noștri (două trepte) și pe prietenii prietenilor noștri (trei trepte), cercetătorii identifică trei motive posibile pentru limitarea influenței: deteriorarea acurateței informației pe măsura transmiterii, evoluția incontrolabilă a rețelei în sensul inconsecvenței conexiunilor, biologia evoluționistă al cărei istoric susține faptul că oamenii au evoluat în grupuri mici.

Autorii fac referire la un studiu asupra fericirii care argumentează capacitatea rețelelor sociale de a influența emoțiile oamenilor. Oamenii fericiți preferă compania celor asemenea lor și transmit același sentiment și altora. Probabilitatea de a fi fericit crește cu 15% dacă te afli la o treaptă de influență de un prieten fericit, cu 10% pentru cea de-a doua treaptă de influență și cu 6% pentru cea de-a treia. De asemenea, probabilitatea ca oamenii să fie fericiți crește odată cu numărul prietenilor. În schimb, oamenii care se simt singuri vor pierde 8% dintre prieteni pe parcursul unui an.

CONTAMINAREA PRIN REȚEAUA SOCIALĂ

Ideea de contaminare în cadrul rețelei sociale se sprijină pe tendința oamenilor de a se imita unii pe alții. Obezitatea poate fi transmisă în cadrul unei rețele sociale la fel cum decizia de a slăbi poate fi determinată de hotărârea unui prieten al prietenului tău de a ține o cură de slăbire. Contaminarea prin rețeaua socială este argumentată pornind de la exemple precum crizele de râs, durerile de spate, sinucidere, practici sexuale sau idei politice.

Deși autorii susțin că „încă nu știm dacă Internetul va crește viteza sau extinderea contaminării în general" la o scară mult mai mare, fenomenul contaminării poate fi lesne observat și în zilele noastre, un exemplu elocvent în acest sens fiind criza imigranților din Siria. Extinderea rețelei Internet, accesul la platforme de socializare precum *Facebook* sau *Twitter*, fluxul informațiilor prin intermediul diferitelor forme media au făcut ca persoane aflate la distanță de evenimente să fie influențate chiar și la nivel emoțional. Mai mult, influența fenomenului se poate observa și în reacțiile și deciziile unor guverne occidentale.

> **„ALTRUISMUL, COOPERAREA, DORINȚA DE A PEDEPSI ȘI DE A PROFITA DE PE URMA ALTORA NE SUNT ÎNSCRISE ÎN ADN**

Multe exemple, chiar și istorice (de pildă, „mania dansului", fenomen înregistrat în Europa secolului al XIV-lea), studii și rezultate ale unor cercetări sunt prezentate pentru a susține că fenomenul contaminării există la nivelul rețelelor sociale, autorii identificând argumente pentru producerea acestuia, dar fiind mai puțin preocupați de modul în care se propagă.

Dr. CHRISTAKIS și Dr. FOWLER afirmă că tendința de a forma rețele sociale face parte din moștenirea noastră biologică, creierul uman fiind construit în acest sens. Dacă unui om i se induce ideea că va sfârși deconectat, credința lui în forțele supranaturale, în Dumnezeu, va crește. „Credințele religioase sunt parțial înrădăcinate în creierul nostru și se leagă de dorința noastră de a avea o conexiune socială cu ceilalți, nu doar o conexiune spirituală cu Dumnezeu". Religia este percepută ca o modalitate de a crea rețele sociale, putând fi înțeleasă doar prin studierea rolului pe care îl are în funcționarea rețelelor sociale. „Nu există atei în tranșee, mai ales dacă ești singur în tranșee", susțin autorii.

Mai mult, rețelele sociale ne sunt înscrise în gene. Numărul de prieteni, localizarea în centrul sau la periferia rețelei sunt stabilite genetic. Omul este, de fapt, *Homo dictyous* (omul rețelelor), altruist, cooperant, dar și egoist și răzbunător, diferit de *Homo economicus* (John Stuart Mill), care își urmărește doar propriul interes pentru a obține câștiguri personale maxime cu cel mai mic cost posibil. „Altruismul, cooperarea, dorința de a pedepsi și de a profita de pe urma altora ne sunt înscrise în ADN", susțin autorii.

Susținând că teoria conform căreia individul acționează rațional și din interes propriu nu poate fi validă pentru că „nu lasă loc pentru altruism” și „nu studiază deloc felul în care oamenii ajung să-și dorească ceea ce își doresc”, CHRISTAKIS și FOWLER construiesc o nouă teorie a *Homo dictyous*, care pare a fi inspirată de teoria economică a *mâinii invizibile* formulată de Adam Smith, potrivit căreia, prin urmarea propriului interes, indivizii stimulează indirect economia. În capitalism, urmărirea propriului bine contribuie la binele societății. Prin apartenența la o rețea socială, omul își urmărește propriul interes, luând în considerare și bunăstarea celorlalți – „vrem ceea ce vor și alte persoane la care suntem conectați”.

Dacă oamenii au fost creați pentru a trăi interconectați, iar rețeaua socială din care fac parte influențează emoțiile, comportamentul și atitudinile lor pentru a schimba ceva din toate acestea în existența unui om, înțelegerea rețelei din care face parte este determinantă, susțin autorii. Soluționarea unor probleme s-a dovedit a fi mai eficientă în cazul în care abordarea acestora se realizează la nivel de grup și nu individual sau la nivelul comunității ca întreg.

Un factor important care a intervenit în modul în care oamenii trăiesc în cadrul rețelelor sociale este evoluția tehnologică. Conectarea în rețelele de socializare *online* (*Facebook*, *Twitter* ș.a.), viețile virtuale din mediul *online*, fie ele și jocuri (*World of Warcraft* sau *Second Life*), site-uri de informații colective (*Wikipedia*, *eBay*) sau site-urile matrimoniale, pot avea efecte serioase asupra modului în care oamenii își modelează și condiționează reciproc comportamentul.

Dr. CHRISTAKIS și Dr. FOWLER susțin că, de fapt, „hiperconectarea” realizată prin spațiul cibernetic respectă tendința ancestrală a oamenilor de a se conecta cu alți oameni. Mai mult, conform unui studiu al paginilor de *Facebook* ale unei facultăți, rețelele sociale *online* seamănă încă foarte mult cu cele *offline*. Numărul total de prieteni este, în medie, 150, iar numărul de prieteni apropiați este de 6.6, față de 4 prieteni în cazul rețelelor *offline*. Pe de altă parte însă, rețelele de socializare *online* oferă oportunități noi precum redefinirea calității de prieten sau posibilitatea de a urmări relațiile pe care le au ceilalți membri ai rețelei.

EFECTE NEGATIVE

Autorii afirmă că „în mediul *online* nu colaborăm unii cu alții pentru că ne forțează un stat sau o autoritate centrală”, ci spontan, datorită abilității noastre de a ne înțelege unii cu alții și a forma „grupuri cu destine conectate și scop comun”. Un exemplu în acest sens este *Wikipedia* care funcționează prin realizarea unei rețele sociale în jurul fiecărui subiect.

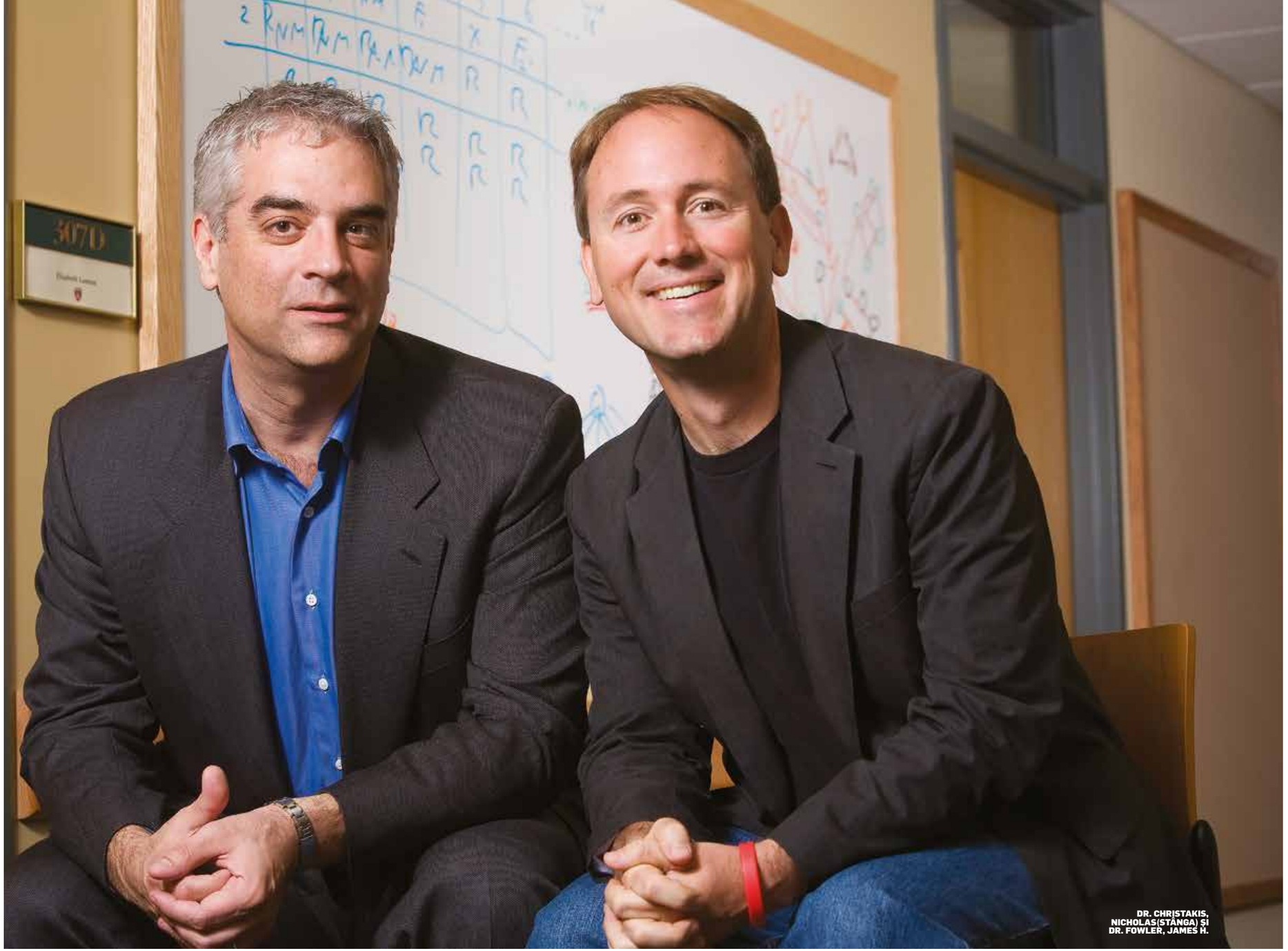
Internetul este cea mai complexă și mai extinsă dintre rețelele existente până acum, oferind capacitatea de a colabora la o scară mult mai mare decât aceea pe care am trăit-o anterior. Cu toate acestea, apartenența la rețelele sociale poate avea și efecte negative, autorii reliefând ideea prin explicarea comportamentului criminal: „pe măsură ce infractorii acționează într-un anumit moment și loc, ei cresc probabilitatea ca și alte persoane din apropiere să comită delicte, astfel încât au loc mai multe infracțiuni decât în mod normal”.

Ideea că rețelele sociale pot avea și efecte negative se susține și în zilele noastre, un exemplu în acest sens fiind fenomenul ISIS (platformele de socializare, Internetul facilitând, în general, efortul grupării de a se promova și chiar de a recruta noi membri).

Chiar și în această perspectivă, autorii îndeamnă la conectare, susținând că transmiterea comportamentelor negative și a altor fenomene nefavorabile „sunt doar efectele secundare pe care trebuie să le suportăm pentru a profita de avantajul rețelelor”. Influența pe care și noi o avem asupra celorlalți și faptul că „atunci când îi combini pe oameni în grupuri cu o anumită configurație, aceștia pot face lucruri mai multe și chiar diferite de ceea ce ar face fiecare individual” sunt considerentele pentru care conectarea are mai multe beneficii decât dezavantaje.

Connected atrage atenția asupra importanței ***hiperconectării*** într-o lume în care Internetul oferă nenumărate posibilități de informare și conexiune. Luările de poziție în raport cu guvernele (de pildă, Primăvara arabă), redimensionarea rapoartelor economice (prin formarea rețelelor profesionale *online*), organizarea de proteste (platformele de socializare *online* au făcut posibilă mobilizarea în cazul incendiului de la clubul **Colectiv**), implicarea în diverse cauze fără a ține seama neapărat de apartenența socio-economică, profesională sau culturală sunt doar câteva exemple în acest sens.

Dr. CHRISTAKIS, Nicholas A., Dr. FOWLER, James H.
Curtea Veche Publishing, București, 2015



DR. CHRISTAKIS, NICHOLAS(STÂNGA) ȘI DR. FOWLER, JAMES H.

ABSTRACT

Connected: The surprising Power of Our Social Networks and How They Shape Our Lives is the huge research of two scholars - Nicholas A. CHRISTAKIS, MD, PhD and James H. FOWLER, PhD. By analyzing the social networks through medicine, sociology, psychology, philosophy, theology, public policy, technology, the authors argue the *homo dyctious* theory. Understanding the human behaviour and attitude means analyzing and understanding social networks because their power on our lives is significant. We, all humans, are part of a superorganism, we are all hyperconnected.

Intelligence

INTELIGENȚA ARTIFICIALĂ

ȘI SECRETELE ȘTIUTE ALE VIITORULUI

de Marius BERCARU

În luna ianuarie 2016, revista *Nature*, titlu profilat în principal pe aducerea la lumină a noutăților din domeniile avangardiste ale științei, așeza pe copertă știrea conform căreia cercetătorii de la *DeepMind*, companie a gigantului Google, au reușit crearea unui *software* capabil să performeze în străvechiul joc de Go. Informația cuantificabilă era că programul, numit sugestiv *AlphaGo*, l-a învins în cinci meciuri din cinci pe campionul european de Go, stârnind admirație și curiozitate atât în rândul pasionaților disciplinei, cât și între pionierii și promotorii inteligenței artificiale. Evenimentul poate părea minor dacă ne amintim că în urmă cu exact 20 de ani, supercomputerul construit de IBM, *DeepBlue*, reușea să îl învingă într-un meci de șah pe campionul mondial Garry Kasparov. Însă Go este ceva mai mult decât șah. Conține mai multe posibile mișcări asociate fiecărui moment și se bazează și pe un alt soi de combustibil în afară de calcul și inteligență. Algoritmul *AlphaGo* nu numai că reușește să calculeze probabilistic cea mai bună dintre posibilele soluții, dar se bazează pe învățare (*deep learning*) așa cum este termenul interpretat și utilizat de oameni. Oamenii de la *DeepMind* au făcut mai mult decât să programeze o mașină să joace Go, ei au reușit să antreneze o inteligență artificială care să rezolve probleme în maniera situată la granița dintre inteligență rece și isteține umană. De fapt, se introduce în universul simulării de rețele neuronale un nou termen.

INTUIȚIA ARTIFICIALĂ

Numărul de posibile configurații ale jocului de Go depășește numărul atomilor din univers, astfel încât o abordare „de forță", prin încercare și eroare, pentru a determina cea mai bună dintre mișcări ar fi ceva indeterminat în timp, peste puterea de calcul a oricărui *cloud* existent sau care ar putea fi gândit la această oră. Principiul de construcție a creierului cibernetic Alpha Go este acela de studiu. *Antrenamentul* a constat în analiza a peste treizeci de milioane de poziții din jocuri la nivel expert jucate în întreaga lume, urmate de un *cantonament* în care AlphaGo a jucat cu alte softuri similare existente pe piață, reușind peste 99% victorii.

Definită drept capacitatea de a descoperi spontan, pe cale rațională, a sensului unei probleme, intuiția părea până la acest moment un atribut exclusiv uman. Malcolm Gladwell, autor canadian, afirmă în cartea sa, *Blink*, faptul că drumul către luarea celor mai bune decizii nu este dat de cunoaștere, ci mai degrabă de înțelegere. Cu alte cuvinte, nu este necesar un flux uriaș de informații, ci doar conectarea cu perspicacitate antrenată a acelor puncte care duc la atingerea scopurilor.

Calea către aplicațiile utile problemelor din lumea reală este deschisă. Tratarea cancerului, identificarea resurselor de apă potabilă în regiuni secetoase, inechitatea socială pot fi abordate inclusiv prin metode analitice intuitive la nivel automatizat.

ANAF CIBERNETIC?

Cercetătorii laboratorului de cibernetică și inteligență artificială (CSAIL) de pe lângă Massachusetts Institute of Technology (MIT) au contribuit la dezvoltarea unui sistem echipat cu inteligență artificială capabil să detecteze fraudele fiscale prin care corporațiile americane „ascund" anual aproximativ 91 de miliarde de dolari. Corporațiile internaționale sunt în esență structuri complexe și ultraramificate. În combinație cu folosirea „parteneriatelor", a „firmelor paravan", devine extrem de greu de urmărit care din raportările de venituri conduc la rezultate legale și care pot fi catalogate drept procese fiscale abuzive.

Software-ul dezvoltat pune bazele unei analize bazată pe inteligență artificială a incertitudinii în fluxurile financiare. Operațiunile companiilor sunt analizate pe nișe foarte înguste, apoi combinațiile cu potențial evazionist sunt identificate și aduse la lumină pentru a fi tratate separat. O activitate care, pentru o armată de contabili, ar însemna ani de muncă și rezultate parțiale.

BIG DATA ȘI PSIHOLOGIA CIBERNETICĂ

De câțiva ani, cantități uriașe de date rezultă din sprintul tehnologic și digitalizarea aspectelor vieții. Big Data este denumită categoria atât de mare și de complexă încât nu poate fi analizată cu instrumente tradiționale. Dimensiunile uriașe, de negândit la începutul mileniului, diversitatea, utilitatea strategică și comercială au reclamat în mod natural apariția unor instrumente care să poată realiza automat o separare a concluziilor utile din halda de steril informațional aparent. Iar exemplul cel mai la îndemână este rețaua de socializare Facebook.

Astăzi, se estimează că FB are 1,2 miliarde de utilizatori care sunt activi cel puțin o dată pe lună. Câteva sute de miliarde de fotografii generate de acești utilizatori se află stocate pe serverele companiei. Informații încrucișate între oamenii din întreaga lume sunt la dispoziția analiștilor. Butonul Like a introdus o nouă unitate de măsură pentru diverse comportamente umane - preferințe, gusturi, interacțiuni, decizii.

Un studiu realizat de Universitate Stanford și Universitatea din Cambridge a revelat faptul că se pot reconstitui cu precizie chiar trăsăturile de personalitate ale unui individ doar din interpretarea unui număr rezonabil de Like-uri pe rețeaua de socializare. Concluzia la care au ajuns cercetătorii este aceea că judecățile computerizate privind personalitatea indivizilor, realizate exclusiv pe baza amprentei online trasate de Like-uri, sunt mai precise decât portretul psihologic realizat de apropiați (prieteni, rude, familie). Mai mult, într-un număr semnificativ de cazuri, profilul psihologic obținut în mod digital a fost chiar mai precis decât propria opinie despre sine a subiecților, pe indicatori extrem de personali - sănătate, abuz de substanțe interzise, preferințe politice. Toate concluziile, validate științific prin metode tradiționale, au un punct comun foarte important - accesul la un volum uriaș de date care permite elaborarea de scheme logice, de arbori utili în determinarea *patternurilor* corecte. Tocmai cantitatea de date oferă relevanță unor concluzii care altfel ar reprezenta doar *fapte diverse*.

JURNALISM AUTOMATIZAT

Quakebot este un software scris de un jurnalist american din Los Angeles, zonă din SUA des afectată de cutremure. Programul preia în mod automat datele geofizice privind evenimentul seismic de la *US Geological Survey* și le transformă într-o scurtă știre de presă care ar putea oricând să treacă drept generată de o minte umană. Standardizarea tot mai accentuată a mesajelor media, goana tot mai acută după relevanță, concizie și, mai ales astăzi, viteză, face ca modelul să fie perfect viabil în mult mai multe domenii decât acela al cutremurelor. Dar, ca să menținem exemplul, putem cerceta ultimele o sută de relatări de presă, indiferent de canalul de difuzare, și vom constata că par structurate simetric de o entitate dotată cu AI. Ne putem imagina, în egală măsură, frustrarea jurnaliștilor juniori care sunt nevoiți ca duminică seara să preia toate rezultatele din diviziile inferioare ale campionatului național de fotbal și să redacteze știri mici pentru pagina opt din jurnalul sportiv.

Cuplarea la diverse surse de informație brută, nestructurată și interpretarea ei într-un mod util va fi probabil viitorul meseriei de jurnalist cu suflet și neuroni. Punerea în ecuație a tabelelor interminabile de rezultate financiare pe o perioadă de 10 ani și extragerea într-o formă validă editorial a concluziilor poate fi un exemplu de mod în care o profesie se poate modela la impactul cu noile tehnologii.

Sentience (Simțire) este titlul lucrării care extrage toate aceste concluzii. Dar *Sentience* poate fi și un frumos joc de cuvinte care combină fericit termenul *Sentence* (propoziție) cu cel de *Science* (știință).

O FOTOGRAFIE CÂT O MIE DE CUVINTE

Se estimează că în prezent pe Internet sunt postate în jur de 1,8 miliarde de fotografii în fiecare zi. Multe sute de miliarde în fiecare an. În afară de cele reprezentând pisici sau felicitări. Rămâne însă o cantitate greu de cuprins de informație care trebuie prelucrată, catalogată, indexată, informație care nu este structurată sub formă de text. Ce colectiv uman ar putea gestiona un asemenea aflux de date și metadate? Nici măcar în condiții teoretice, fără a ține seama de eficiență economică, această sarcină nu ar putea fi îndeplinită în condiții de perpetuitate.

Rețelele de socializare Pinterest și Tumblr, cu un succes considerabil în rândul internauților, au ca principal element de comunicare informația grafică. Se estimează că doar pe Tumblr, intrată relativ recent în portofoliul de business al Facebook, 75 de procente din numărul total al postărilor sunt imagini, iar dintre acestea 90 de procente nu au niciun fel de metadate sub formă de text. Oamenii aleg în mod conștient să își exprime gândurile prin imagini, iar acest lucru va avea un impact semnificativ al modului în care membrii comunităților aleg să relaționeze unul cu celălalt.

Din orice unghi ar putea fi privită această situație, nu se poate ignora realitatea că există miliarde de fișiere care trebuie analizate și interpretate. Nu numai din perspectiva relativ îngustă a marketingului și adaptării la specificurile piețelor, ci în direcții mult mai profunde care țin de evoluțiile macro ale societăților umane în general.

ÎNCOTRO

Modelele analitice ale viitorului par strâns legate de evoluția tehnologică, de modelele impuse, de produsele tot mai fiabile de inteligență artificială. Diversele stadii ale revoluției industriale de până acum au adus cu sine și noi tipuri de locuri de muncă, astfel încât în final au fost bine întâmpinate de oameni. Nimeni nu poate însă prezice care va fi de această dată impactul pe care formele tot mai subtile prin care AI se insinuează în viețile oamenilor și organizațiilor îl vor avea asupra designului actual al lumii.

Deja problemele legate de etică și viață privată preocupă straturi diverse ale societății. Stephen Hawking, cercetător britanic asociat Universității Cambridge, afirmă că *„Succesul în crearea AI ar putea fi evenimentul cel mai proeminent din istoria umanității. Din păcate, ar putea fi în egală măsură ultimul dacă nu aflăm cum să evităm riscurile."*

Dezvoltarea softurilor specializate, modelele tot mai sofisticate de deep learning, recunoaștere vocală și de imagine, utilizarea big data în ajustarea comportamentelor, toate vor avea un impact, mai mic sau mai mare asupra vieții. Analiza pe algoritmi cibernetici va fi tot mai prezentă în deciziile viitorului.

Și chiar în evoluția produselor informaționale ale serviciilor de *intelligence* din întreaga lume.

LATER EDIT. Pe 9 martie, supercomputerul Google l-a invins si pe campionul mondial Lee Se-dol, în primul meci din cele 5 programate. Pe Twitter, creatorii AlphaGo exclamau „We landed it on the Moon!"

ABSTRACT

Artificial Intelligence is no longer a science fiction reality. The development of technology makes obvious the fact that AI is possible, and the first steps in this direction have already been taken. Computers now have traits which had only been related to people. Defined as the ability to discover spontaneously, rationally, the meaning of a problem, intuition seemed until now an exclusively human attribute. Software programs like AlphaGo, Quakebot demonstrate that machines can learn and thus anticipate, just like people. All this while possessing enormous amounts of data which the human brain could never encompass. The path is open for creating applications useful in solving real-world problems. Treating cancer, identifying water resources in arid regions, social inequity can be addressed by intuitive analytical methods at an automated level. Specialized software development, increasingly sophisticated models of deep learning, speech recognition and imaging, the use of big data use in adjusting behaviors, all will have an impact on life. Cyber algorithms analysis will be increasingly present in future decision making processes. The questions of ethics and privacy, already concerns various layers of society. It was Stephen Hawking who said that "success in creating AI could be the most prominent event in human history. Unfortunately, it could equally be the last if we know how to avoid risks."

LOGISTICA SUCCESULUI
REFLECȚII LA PROIECTUL „CYBERINT“

de Iulian DOROBANȚU

Mă apropii cu obișnuința unui cunoscător al locului de bariera care limitează accesul în incinta unui complex de clădiri administrative situat pe malul râului Dâmbovița, în vecinătatea celui mai mare lac al municipiului București, Lacul Morii. Salutul de bun venit al personalului și promptitudinea ridicării barierei îmi aduc un zâmbet ușor, iar gândurile îmi fug la unul dintre proiectele derulate în ultimii ani. Pentru cei care au făcut parte din echipă, proiectul s-a intitulat simplu **Proiectul „Cyberint”**.

MARTIE 2014...

La șase kilometri distanță de Lacul Morii, într-un birou situat în centrul Bucureștiului, se definitiva actul normativ prin care se iniția investiția pentru realizarea unui sediu dedicat **Centrului Național Cyberint (CNC)**. Promovat pe circuitul de avizare în cursul lunii martie, actul se transpunea în Hotărârea Guvernului nr. 241/2014, pentru modificarea Hotărârii Guvernului nr. 233/1997 privind aprobarea indicatorilor tehnico-economici ai obiectivului de investiții „LG - 97” din municipiul București, adoptată în ședința din data de 2 aprilie 2014. Astfel, erau puse bazele derulării unei investiții pentru a cărei finanțare erau alocați circa **21,5 milioane lei**.

Rămânea să se răspundă la întrebarea „Este posibilă operaționalizarea sediului, atât execuția lucrărilor, cât și asigurarea dotărilor, într-o abordare integrată cu un alt proiect major inițiat în aceeași perioadă și în termenul de un an determinat de pierderea finanțării?”.

În fapt, inițierea investiției noului sediu se corela cu proiectul „Sistemului național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic”, al cărui contract de finanțare prin Fondul European de Dezvoltare Regională, în cadrul Programului Operațional Sectorial „Creșterea Competitivității Economice” fusese semnat în data de 2 decembrie 2013.

Obiectivele proiectului vizau implementarea unui sistem informatic destinat asigurării interoperabilității componentelor informatice de securitate, protecția sistemelor informatice și a informațiilor vehiculate de la nivelul autorităților publice, creșterea disponibilității și nivelului de încredere în serviciile publice specializate oferite, precum și eficientizarea și crearea premiselor pentru modernizarea serviciilor publice. Valoarea finanțării acordate proiectului era de **97 milioane lei**, iar termenul de implementare se înscria sub imperiul anului **2015**, în care înceta accesarea finanțării europene.

În condițiile stricte impuse de finanțare și de conexarea etapelor investiției și proiectului european, participarea la implementare a reprezentat pentru mulți oportunitatea de a se confrunta cu propriile aspirații. A fost momentul în care cei implicați reflectam, cu preocupare evidentă pentru un drum necunoscut pe deplin, la valoarea reunită a investiției și proiectului european, la volumul și dinamica previzionată a activităților, la riscurile asociate achizițiilor publice, la complexitatea tehnică a sistemului, dar și la necesitatea abordării corelate a etapelor și la imposibilitatea reluării acestora în cazul unor nereușite. Pe de altă parte, ne loveam de îndoielile receptate care îndemnau la renunțare. Tocmai acele îndoieli au dat și impulsul formării echipei care a condus la ceea ce avea să fie definit ulterior **un proiect integrat de succes**.

Echipa s-a constituit în jurul nucleului specialiștilor în securitate cibernetică, la care s-au adăugat alți specialiști din cadrul structurilor de planificare și achiziții publice, financiare și juridice, dar și de proiectare și inginerie în construcții, instalații și echipamente. Iar pe parcurs mulți dintre cei din jur ne-au venit în întâmpinare cu întrebarea „Cu ce putem ajuta?”.

Cu toate că echipa a suferit la capitolul numeric, lipsa resursei umane a fost compensată de entuziasmul dorinței de a reuși și de a dovedi că ceea ce păreau pentru mulți doar studii și documentații tehnico - economice puse în biblioraforturi puteau fi transpuse în realitate. Proiectul a adus în prim plan și provocarea parteneriatului cu alte patru instituții, reprezentate de Ministerul Comunicațiilor și pentru Societatea Informațională, Ministerul Apărării Naționale, Ministerul Afacerilor Interne și Serviciul de Telecomunicații Speciale, dar și a colaborării cu cele 54 de instituții și autorități beneficiare.

Privind statistica proiectului, observăm că au fost desfășurate 48 de achiziții publice, din care 16 prin licitații publice deschise, au fost recepționate 2.581 de bunuri și au fost organizate cursuri pentru 465 de specialiști.

Dincolo de statistică, de ceea ce poate reliefa parcurgerea celor peste 100.000 de file ale dosarelor, rămâne partea nescrisă a momentelor unice trăite de o echipă în încercarea reușită de a împlini un destin, a miilor de ore dedicate cu îndârjirea unor învingători, cu bucurii și tristeți deopotrivă, a căutării soluțiilor și răspunsurilor la situațiile neprevăzute, a înțelegerii și cunoașterii în domenii pentru mulți neexplorate, dar și a răspunsului la întrebarea inițială, „Da, este posibil!”.

MARTIE 2015...

După trecerea unui an, noul sediu al **CNC** începea să fie operaționalizat și pregătit în vederea primirii personalului. Cu o suprafață totală de **2.600 mp**, din care **370 mp destinați Centrului de Date**, sediul era pregătit pentru a-și întâmpina proprii specialiști și a găzdui tehnologia de ultimă generație. Sediul oferă spații de birouri pentru întruniri și dezbateri, de comandă și răspuns la situații specifice, laboratoare, zone tehnice și pentru suport, precum și Centrul de Date.

Noul sediu urma să fie inaugurat în **4 iunie 2015**, în prezența domnului **Klaus IOHANNIS**, președintele României, a domnului **Eduard HELLVIG**, directorul Serviciului Român de Informații, și a conducerii Serviciului.

97
MILIOANE DE LEI ESTE VALOAREA FINANȚĂRII PROIECTULUI

54
DE INSTITUȚII ȘI AUTORITĂȚI BENEFICIARE AU COLABORAT ÎN ACEST PROIECT

465
DE SPECIALIȘTI AU URMAT CURSURI DE PREGĂTIRE ÎN ACEST PROIECT

2.600
DE MP ESTE SUPRAFAȚA TOTALĂ A CYBERINT

În paralel, proiectul european prindea consistență la deținătorii de infrastructuri cibernetice de interes național, prin asigurarea interoperabilității pentru cele 54 de instituții beneficiare și instruirea personalului pentru utilizarea componentelor sistemului, generându-se astfel posibilitatea securizării sistemelor informatice, prin furnizarea permanentă a unor servicii de alertare, informare, evaluare de securitate, suport **CSIRT** (*Computer Security Incident Response Team*), consultanță în domeniul securității cibernetice, instruire și interoperabilitate în domeniul securității cibernetice prin managementul centralizat al evenimentelor de securitate la nivel național.

Proiectul contribuia la securitatea cibernetică națională prin securizarea rețelelor informatice din categoria infrastructurilor cibernetice de interes național și prin implementarea unui sistem de management centralizat a incidentelor de securitate la nivel național, fiind aplicate tehnici de securizare de tip prevenție, detecție, investigație și corecție.

Prin notificările și alertele oferite, era asigurată astfel funcționarea sistemului național de alertă cibernetică și stabilirea nivelului de alertă cibernetică, indicator al stării de securitate cibernetică la nivel național, determinând deopotrivă coordonarea reacției la atacurile cibernetice derulate împotriva unei infrastructuri sau unui grup de infrastructuri cibernetice de interes național.

Totodată, se reușea crearea unui poligon cibernetic, destinat simulării în mediul virtual a infrastructurilor cibernetice protejate și a unor categorii de atacuri cibernetice la adresa utilizatorilor acestora, a serviciilor oferite, precum și la nivelul sistemelor de comunicații.

Prin conjugarea eforturilor celor implicați, proiectul european a fost implementat în termen, conferința de finalizare având loc în data de **2 noiembrie 2015**, cu participarea partenerilor, instituțiilor și autorităților beneficiare, precum și a ministrului Fondurilor Europene, respectiv a reprezentanților structurilor direct interesate.

MARTIE 2016...

Mă îndrept spre sala de ședințe din sediul **CNC** pentru a participa la analiza asupra implementării unui proiect vizând înființarea unui centru de instruire în domeniul *cyber security*, finanțat prin Programul Național aferent Fondului pentru Securitate Internă. Privind la cei prezenți, regăsesc cu plăcere membri din echipa Proiectului „Cyberint” și observ că referirile la experiența proiectului finalizat se reflectă în discuțiile purtate. Iar dezbaterile din ședință îmi întăresc convingerea că proiectul a devenit un model adoptat, un *know-how* adus componentei investiționale, unul dintre obiectivele la care s-a reușit integrarea resurselor operaționale, tehnice, financiare și umane în mod eficient și cu eficacitate maximă.

Suntem din nou în acel moment de reflecție, de această dată analizând perspectiva implementării unui nou proiect cu încrederea conferită de cunoaștere și experiență. Este un nou început, o nouă provocare...

ABSTRACT

The Cyberint Project is designed to contribute to protecting our national cyber security by securing the computer networks of national interest cyber infrastructures of and by implementing a system of centralized management of national security incidents. The applied techniques have prevention, detection, investigation, and correction features. Now, the project has become an adopted model, a know-how applied to the investment component of the national security system. It has managed to successfully integrate the operational, technical, financial, and human resources in order to achieve maximum efficiency.

MĂRTURII ISTORICE PRIVIND DESFĂȘURAREA UNOR ACTIVITĂȚI DE INTELLIGENCE PRIN SERVICIILE POȘTALE

de Adrian POPESCU

Ipak, dau știre domniilor voastre... „[...] **gradul de civilizație al unui popor sau al unei** țări se măsoară după starea de perfecțiune a acestui supranatural organ de transmitere al ideilor, simțămintelor și al lucrurilor și [...] **acolo unde manifestările sunt regulate, sigure, repezi și puțin costisitoare, acolo este prosperitatea economică, activitatea comercială și viața inteligentă**”. **Acolo, de fapt, există securitate națională**!

În pragul unor nevoi sau pericole comune ori din dorința de a construi afaceri comerciale, popoarele au reușit să stabilească prin serviciile poștale **relații** (alianțe, învoieli, înlesniri) menite să le apere propriile interese și de cele mai multe ori acestea s-au dovedit a fi unica sau cea mai bună soluție. Din această perspectivă, este remarcabil **rolul civilizator de necontestat pe care serviciile poștale l-au jucat în soarta omenirii**, dat fiind faptul că timp de peste două milenii, mai precis **până la apariția altor posibilități de interacțiune umană (telegraf, telefon etc.), ele au constituit principalul canal de comunicare cu ramificații extinse bine stabilite**.

Iar dacă avem în vedere faptul că, de-a lungul timpului, prin serviciile poștale au călătorit, în ambele sensuri, oameni, informații (scrisori), valori și colete, se naște întrebarea: **Ce a fost mai întâi, serviciul de informații (spionajul) sau serviciul poștal (poșta)?** Încercarea de a alege între cele două servicii nu este o eroare; unii se vor grăbi să aleagă spionajul, aducând drept argument simpla curiozitate manifestată de către oamenii preistorici pândind din spațiul unor ascunzători, iar alții vor alege poșta, mizând pe satisfacerea unei nevoi umane primare, aceea de interacțiune prin comunicare.

De fapt, dificultatea de a alege corect este firească având în vedere faptul că atât în ceea ce privește spionajul, cât și poșta, începuturile sunt necunoscute, puținele izvoare istorice existente remarcând plasarea temporală a celor două sisteme de organizare în imediata apropiere a grupării oamenilor în familii, triburi și popoare. **Ambele servicii implică comunicarea umană, însă punctul de plecare este diferit**, fiind fundamentat de natura intenției. Nu întâmplător în dicționarul explicativ al limbii române avem astăzi în suma de explicații a cuvântului poștă și pe aceea pentru expresia „a duce poșta” - ”a colporta știri, aprecieri, păreri, zvonuri de la o persoană la alta”, „a umbla cu vorbe”, „a face intrigi”.

Tocmai de aceea, provocarea lansată prin formularea acestei întrebări nu vizează obținerea unui răspuns ferm, ci mai curând declanșarea interesului pentru receptarea unor elemente de cunoaștere istorică despre organizarea și funcționarea serviciilor poștale în forme din ce în ce mai dezvoltate și care au facilitat inițierea și aplicarea unor metode și tehnici de tip informativ care sunt utilizate și astăzi de către toate serviciile de informații. Atunci ca și acum acestea au servit, în principal, unor obiective statale, strategice, geopolitice etc.

Cuvântului „**poștă**” este o **formă prescurtată a lui *posita,*** participiul trecut feminin al verbului latin *ponere* („a pune”), prin care se indicau stațiile așezate din loc în loc, la distanțe egale, pe drumurile pe care treceau curierii statului roman (serviciul poștal roman, în ansamblul lui, se numea ***cursus publicus).*** În sensul unui drept de circulație, cuvântului **„poștă” este folosit pentru prima dată în evul mediu**, în timpul lui **Alfonso al X-lea**, regele Castiliei (1252-1284), și al Papei **Honorius al III-lea** (1216-1227), iar mai târziu îl găsim în memoriile cronicarului **Comines** și într-o ordonanță al lui **Carol al VIII-lea**, regele Franței, în anul 1487.

SERVICIILE POȘTALE ÎN LUME ÎNCEPUTURILE ORGANIZĂRII SERVICIILOR POȘTALE (ANTICHITATE)

Primele mărturii despre serviciile poștale datează **din perioada antică** și aparțin istoricilor vremii care atestă existența acestora în țări precum Egipt, Persia, China, Grecia, Statul Roman. În toate cazurile, organizarea lor presupunea stabilirea unor trasee de deplasare a curierilor (pe jos, cu animale sau mijloace de transport cu tracțiune animală) și a unor stații de odihnă și schimb al mijloacelor de transport (relee), serviciul poștal fiind susținut prin **efortul localnicilor**, deși nu servea intereselor directe ale acestora. Particularitățile țineau de gradul de rapiditate al deplasării curierilor și elementele de ordin geografic, politic și cultural, potrivit nivelului de dezvoltare statală.

Apreciind importanța cunoașterii situației operative interne și externe a ținuturilor aflate sub stăpânirea lor, șefii de stat desfășoară prin serviciile poștale o activitate regulată de culegere de informații care include și **transmiterea cifrată a mesajelor confidențiale**, numind pentru aceasta oameni cu calități native, instruiți, bine remunerați și cu posibilități de avansare pe scara ierarhică.

Într-o descriere a serviciului poștal **egipt**ean, istoricul grec **Diodor din Sicilia**, arată că „Trezit de dimineață regele primea singur scrisorile sosite din toate părțile regatului pentru a fi în măsura de a trata și rezolva afacerile cât de înțelept posibil, după ce lua la cunoștință exact despre tot ce se petrecea în statele sale.”, iar în ceea ce privește organizarea acestuia în **Persia**, în relatările istoricului **Xenophon**, găsim consemnat faptul că: „[...] se cunoștea încă o descoperire a lui **Cirus**, foarte folositoare pentru a asigura guvernarea întinsului său regat: este un mijloc de a ști, fără întârziere, tot ce se petrece în părțile cele mai îndepărtate. Socotind distanța pe care un cal poate să o străbată într-o zi fără a fi obosit, el făcu să se construiască pe drumuri grajduri despărțite între ele printr-o aceeași distanță. El așeză acolo cai și servitori însărcinați a-i îngriji. Însărcina în fiecare dintre ele un om deștept, pentru a-i primi scrisorile aduse de un curier, a le încredința altui curier, a avea grijă de voiajori și de caii care soseau obosiți și a-i înlocui prin alții.”.

Herodot amintește despre faptul că **Cirus**, în timpul expediției sale contra sciților (în anul 500 înainte de Hristos), înființase un **serviciu de curieri** pentru a fi cât mai repede pus la curent cu evoluția evenimentelor care se produceau în Persia, iar istoricul grec **Plutarch** arată că **Darius I**, fiul lui Histaspe, înainte de a urca pe tronul Persiei, fusese inspector general al releelor de poștă. În **Persia**, instituția poștelor purta denumirea de *angara* sau *corvadacare* și se traducea prin obligația locuitorilor țării de a-și da gratuit concursul cu oameni, vite, mijloace de transport la executarea unui serviciu care, deși era de interes general, nu era perceput ca pe un avantaj particular (termenul este utilizat și în zilele noastre într-un înțeles similar).

Descriind serviciul poștal organizat în **Grecia antică** (constituită din mici republici care dețineau curieri particulari numiți *anghelos* - „anunț”), **Herodot** oferă și o mărturie despre **transmiterea prin serviciul poștal a unor mesaje cifrate**: „eforii spartani care aveau putere mai mare decât regii și Senatul comunicau cu regii în campanie prin mijlocul Scytalei, baston înconjurat de o bandă de piele, pe care ei scriau ordinele. Această bandă desfășurată nu prezenta decât caractere fără șir, dar regele sau generalul citeau ordinul prin mijlocul unui alt baston la fel și pe care îl purtau cu sine.”.

Poșta califilor arabi, fondată de către înțeleptul calif **Moavia** în anul 630 după Hristos, era organizată **numai pentru necesitățile statului**, pe o suprafață extinsă și pe principii împrumutate de la perși și romani. **Personalul poștal** era condus de **directori** care mai aveau o misiune importantă: obligația de a observa și raporta despre îndeplinirea atribuțiilor funcționarilor financiari, politici, administrativi, despre situațiile agricole, baterea monedelor, plata soldelor, starea trupelor; rapoartele acestora erau adresate **director**ului **general al poștelor**, subordonat direct califului. **Cea mai sugestiv**ă apreciere a **importanței poștei ca administrație de guvernământ în stat și caracterul ei de veritabil serviciu de informații** a fost lansată de către califul **Mansur** când a afirmat: „Tronul meu se reazemă pe patru picioare, iar suveranitatea mea pe patru oameni, un cadiu (judecător) care să nu greșească, un prefect de poliție energic, un ministru de finanțe cinstit și un director de poștă credincios care să mă informeze în mod drept de tot ceea ce se petrece.”.

SERVICIUL POȘTAL ÎN IMPERIUL ROMAN - UN MODEL UNIVERSAL

Cea mai impresionantă organizare a unui serviciu poștal, din perspectiva similitudinilor cu organizarea actuală a poștei speciale, a fost realizată în **Imperiul Roman**.

Primele date despre înființarea serviciului poștal la romani sunt aduse de **Titus Liviu** și arată că acesta exista între anii 510-530 î.e.n., sub denumirea de ***Angaries,*** redenumit în perioada înfloritoare a Imperiului Roman ***cursus publicus***. Potrivit istoricului latin **Sueton**, în scopul de a cunoaște prin mijloacele cele mai rapide ceea ce se petrecea în provincii, **Augustus** a așezat pe drumurile militare, la distanțe scurte, oameni pe jos (ulterior curieri călare sau căruțe) care transmiteau din mână în mână scrisorile și le aduceau în cel mai scurt timpdin țările cele mai îndepărtate.

Cursus publicus funcționa pe drumurile militare și transporta poruncile imperiale, banii publici, pe funcționarii statului în misiune, ambasadorii și chiar pe împărații romani. Din loc în loc se aflau stații pentru adăpostirea curierilor, cailor și căruțelor, iar din punct de vedere al vitezei, serviciul poștal era împărțit în **poșta rapidă** / ***cursus celer*** sau ***velox,*** pentru care erau folosiți cai de rasă superioară și mijloace de transport ușoare în scopul transportului de valori, bani publici, arme, și **poșta grea de transport** / ***cursus clabularis,*** pentru care erau folosite trăsuri de capacitate mare în scopul transportului bagajelor, mărfurilor și al aprovizionării militare. Conducerea și supravegherea releelor era încredințată pe termen de cinci ani locuitorilor notabili ai orașelor, la retragerea lor din funcție fiindu-le decernate titluri onorifice.

Publicul nu profita de **serviciul poștal**, acesta fiind pus **doar la dispoziția împăratului, casei sale și a înalților funcționari ai Imperiului** care puteau folosi serviciul în baza unei autorizații speciale / ***diploma*** sau ***littaere evertionis***, care purta sigiliul și semnătura împăratului sau a prefectului pretoriului. Înstrăinarea diplomelor era interzisă, iar un birou înființat pe lângă prefectul pretoriului se ocupa de supravegherea acordării diplomelor și de constatarea și sancționarea nerespectării de către deținători a condițiilor consemnate pe ea: numele, demnitatea și misiunea posesorului, felul poștei și trăsurilor pe care putea să le utilizeze, durata valabilității diplomei, itinerariul, locul releelor, proviziile pe care putea să le solicite, precum și cantitatea și calitatea lor.

Împărații romani Adrian (117-138) și **Septimiu Sever** (193-211) trec **în sarcina statului toate cheltuielile** de organizare și funcționare a serviciului poștal, iar **Diocliția**n (284-306) îl reorganizează în **poștă militară**, **poștă publică** sau **fiscală** (rezervată transporturilor statului și aprovizionării generale) și **poștă particulară** (cu funcționare pe drumuri secundare și de mică importanță).

Corespondența dacilor se realiza **tot prin serviciul poștal roman** și era însemnată deoarece aceștia cunoșteau scrisul și cititul, judecând după mulțimea inscripțiilor făcute într-o limbă corectă și duioasă care s-au găsit de-a lungul timpului pe întreg teritoriul Daciei.

SERVICIILE POȘTALE ÎN EUROPA EVULUI MEDIU - ACTIVITĂȚI DE INTELLIGENCE

În **Franța**, regele **Ludovic al XI-lea** (1464) stabilește un serviciu poștal cu scopul declarat de a cunoaște permanent starea sănătății fiului său, însă autori ai timpului susțin că regele se afla în conflict cu vasalii săi și ducele Burgundiei, fapt pentru care, prin **serviciul poștal înființat (pe principiile poștei romane)** el avea să fie informat exact despre tot ceea ce se petrecea nu numai în statele sale, dar și în țările vecine în care avea informatori. **Personalul poștal** trebuia să fie **credincios** și să depună un jurământ de fidelitate regelui; anumiți funcționari erau însărcinați cu supravegherea efectuării serviciului. Astfel, serviciul era condus și supravegheat de către un **ofițer al Coroanei**, atașat pe lângă persoana regelui, care trebuia să asigure mai ales punctele de intrare în țară, având obligația de a veghea ca niciun curier sosit din țări străine să nu treacă în Franța pe căi ascunse, de a se informa asupra conținutului corespondenței transportate de către aceștia, de a elibera pașapoarte și de a asigura primirea/transmiterea corespondenței guvernului.

Începând cu domnia regelui **Ludovic al XIII-lea**, este semnalată funcționarea așa-zisului „**Cabinet negru**” care, în scop politic, se ocupa cu deschiderea scrisorilor adresate anumitor persoane spre a le afla conținutul, activitate care se extindea și perfecționa continuu. Funcționari speciali și bine plătiți desfăceau cu pricepere scrisorile anumitor persoane și extrăgeau părți din conținutul acestora pe care le comunicau celor în drept. Cabinetul negru este **desființat în anul 1775** de către regele **Ludovic al VI-lea**, fiind citată sub domnia sa anularea unei sentințe de condamnare dată pe baza unei scrisori interceptate.

În ceea ce privește funcționarea Cabinetului negru, la data de **27 iulie 1789** în cadrul unei reuniuni organizate la **Versailles** cu participarea reprezentanților nobilimii, clerului și ai Adunării naționale, între alte deziderate, este **garantat secretul corespondenței poștale**,

contele **Stanislas de Clermont - Tonnerre** afirmând în plen, la citirea raportului Adunării generale: „Adunarea se ridică cu indignare împotriva violării secretului poștei, una dintre cele mai absurde și infame invenții ale despotismului”. Principiul enunțat este legiferat abia în **septembrie 1791**, când Adunarea națională introduce în Codul penal dispoziții prin care se prevede **pedepsirea sustragerii și violării secretului corespondenței**, săvârșită atât de către particulari, cât și de către funcționarii statului.

Cu toate acestea istorici contemporani ai împăratului **Napoleon Bonaparte** consemnează despre ample activități ale Cabinetului negru. Însuși Napoleon mărturisește în perioada exilului său: „Este **o rea instituție** care face mai mult rău decât bine. Se întâmplă deseori suveranului să fie într-o dispoziție rea, obosit, influențat din cauze străine... și apoi francezii sunt atât de ușuratici, atât de neglijenți în corespondență ca și în vorbele lor! Am întrebuințat foarte des Cabinetul negru pentru a cunoaște corespondențele intime ale miniștrilor, șambelanilor și ale marilor mei ofițeri...”.

Austria deținea, la rândul ei, un cabinet negru în legătură cu care **Alfred MICHIELS** relatează faptul că directorul poliției austriece îi mituise pe curierii cabinetului prusac și că, pe drumul de la frontieră la Viena, în timp ce caii alergau în galop, ei desfăceau cu cea mai mare îndemânare corespondența, luau notă despre conținut, o resigilau și o aduceau ambasadorului Prusiei. Contele **Torre PALMA**, ambasador al Spaniei la Viena, reclamă la un moment dat faptul că trimiterile poștale adresate guvernului său nu-i parvin întotdeauna intacte, uneori fiind chiar sustrase și înlocuite cu variante scrise de către funcționarii germani.

În **Saxonia**, începând cu anul **1448**, se înființează la dispoziția prințului și a guvernului **curse de curieri speciali**.

Într-o scriere dedicată istoriei poștelor din **Italia**, **Adriano PALOMBI** arată că în anul **1445**, între **Milano** și **Genova**, existau **curse poștale înființate de ducele Francisc de SFORZA** care scria pe scrisorile adresate miniștrilor săi un avertisment pentru curieri: „Repede, repede, zburați zi și noapte că vă amenință pedeapsa furcilor!”.

ROLUL CIVILIZATOR AL SERVICIILOR POȘTALE

În scopul asigurării unui serviciu poștal regulat, **romanii** s-au îngrijit de construirea acelor renumite **drumuri** (care aveau partea din mijloc pavată cu mari blocuri de lavă bazaltică așezate pe un pat format din trei pături diferite suprapuse, cu înălțimea totală de 1 metru, fiecare parte a drumului fiind mărginită de un trotuar pe lungimea căruia erau plasate borduri de piatră care indicau distanța în mile) care conduceau **din centrul Romei** (de la templul lui Saturn de unde se măsurau distanțele) în diferite direcții către frontierele imperiului și ale căror urme se mai văd și astăzi în toate țările foste componente ale Imperiului Roman. Împăratul Traian (98-117) deschide un astfel de **drum până la Pontul Euxin** (Marea Neagră).

În **feudalismul timpuriu european** contextul dat de înființarea universităților și înavuțirea progresivă a mănăstirilor a impus **reorganizarea serviciilor poștale prin contribuția mesagerilor universitari** (pentru menținerea legăturii studenților sosiți la studii cu familiile lor) și a **curierilor mănăstirilor** (îndrituiți cu transmiterea ordinelor religioase). **Universitatea din Paris** a fost fondată în anul **1150**, era împărțită în **patru facultăți** (medicină, teologie, drept și arte) și strângea laolaltă studenți veniți din Anglia, Elveția, Prusia, Bavaria, Olanda, Polonia, Ungaria etc**. Mesagerii universitari** erau împărțiți în **mici mesageri**, aleși din rândul oamenilor săraci, dar cinstiți, și **mari mesageri**, care erau recrutați dintre persoanele notabile și bine situate în orașe și care beneficiau de avantajul protecției universității, de invitații pentru participarea la evenimente și de scutirea de la anumite taxe. Pe măsură ce și-au diversificat felul obiectelor transportate **mesagerii universitari** s-au transformat într-un **serviciu poștal semi-oficial**, care, la solicitarea unor lideri religioși (de exemplu, Papa Grigore al IX-lea și Nicolae al IV-lea), au primit din partea **regilor protecție și apărare în fața justiției**.

Menținut timp de câteva sute de ani, **rolul civilizator al serviciului poștal constituit de mesagerii universitari pe lângă sistemul organizat de stat este covârșitor în sfera transmiterii științelor către toate clasele sociale**.

Familiei **TAXIS** i se datorează **intensificarea relațiilor comerciale dintre** țările europene, prin organizarea pe o perioadă îndelungată, a unor servicii poștale menite să facă legătura între statele germanice și Italia, Olanda, Elveția, precum și intermedierea legăturilor poștale ale Țărilor de Jos cu Austria. **M. de Reust**, într-o scriere apărută în anul **1748**, afirma: „Lumea întreagă considera o astfel de întreprindere ca o afacere rea. [...] dar când comercianții germani băgară de seamă că prin mijlocul poștei, ei puteau să-și procure cursul bursei și să știe prețul tuturor mărfurilor în condiții facile, fără a fi obligați să meargă la Bruxelles sau Anvers, se îngrămădiră la tânăra poștă a lui **TAXIS** cu o cantitate așa de mare de scrisori...”.

În același context, regele **Friderich GUILLAUME** (1713-1740) explică importanța serviciului poștal în organizarea statului: „Poștele sunt absolut trebuincioase astfel încât comerțul să progreseze și ele îndeplinesc funcția untdelemnului în rulajul mașinii guvernamentale”. Sub domnia sa prin ordonanțe și regulamente se stabilește în cele mai mici detalii **itinerariul poștelor ordinare și extraordinare, al curierilor, ștafetelor**, dispunându-se ca prinții și funcționarii să-și trimită corespondențele prin ștafete și curieri, publicul prin poștele ordinare (cai și trăsuri), iar transportul călătorilor să se facă prin poștele cu trăsuri ordinare și extraordinare.

Serviciilor poștale li se datorează nașterea jurnalismului; în **Germania**, primele gazete periodice apar în anul **1600** sub formă de **note manuscrise** pe care le distribuia poșta, iar în unele orașe franceze jurnalele erau editate chiar de către funcționarii poștei care se ocupau apoi cu distribuirea lor.

(Partea a II-a a articolului, Serviciile poștale în spațiul românesc, în numărul următor al revistei)

ABSTRACT

The most impressive aspect of a documentation work in the history of postal services organized around the globe is that although they are built on similar principles which are still viable nowadays, their evolutionary stages are numerous and inextricably linked to the most important events throughout human history.

It is known that postal services represented a necessity at the highest organizational level, once people gathered together in communities, states or empires, as leaders needed to disseminate their orders in any circumstances to different directions on longer and longer distances and as soon as possible. Historical sources also speak about the leaders' concern to concurrently exploit another opportunity offered by the postal services, namely to collect information about everything that happened within the area of their state, as well as outside it, and to communicate through coded messages. The main historical source used for this article is the book „Istoria Poștelor Române” - a history of postal services - written by Constantin MINESCU and published in 1916.

26 ANI ÎN SERVICIUL CETĂȚENILOR

2016