SPAŢIUL CIBERNETIC – UN NOU MEDIU DE CONFRUNTARE

CYBERSPACE – A NEW ENVIRONMENT OF CONFRONTATION

Expert securitate națională Cătălin-Iulian BALOG*

Pe parcursul ultimilor 20 de ani, tehnologia informaţiei s-a dezvoltat rapid. De la un instrument administrativ pentru optimizarea proceselor de birou, aceasta reprezintă acum un instrument strategic în industrie, administraţie şi armată. Înainte de 11 septembrie 2001, subiectele referitoare la riscurile şi ameninţările din spaţiul cibernetic, precum şi cele despre confruntarea cibernetică, erau discutate doar în grupuri reduse de experţi. Însă, începând cu 11 septembrie, a devenit evident faptul că spaţiul cibernetic presupune nu doar existența unor vulnerabilităţi serioase, dar şi posibilitatea unor confruntări la nivelul întregii societăţi.

Over the past 20 years, information technology has developed greatly. From an administrative tool to optimize office processes, it is now a strategic instrument of industry, government or military. Before September 11, topics related to risks and threats in cyberspace, and those about cyber confrontation were discussed only by small groups of experts. But since September 11, it is obvious that cyberspace is not only about the serious vulnerabilities, but also about the possibility of confrontation at all levels of society.

Cuvinte-cheie: cyberspace; risks; threats; vulnerabilities; confrontation.
Keywords*: spaţiu cibernetic; riscuri; ameninţări; vulnerabilităţi; confruntare.*

De peste două decenii, oamenii încearcă să înţeleagă ameninţarea cibernetică, să evalueze riscurile specifice la adresa indivizilor şi a organizaţiilor (inclusiv a statelor-naţiune), precum şi răspunsurile adecvate. Deşi s-a investit semnificativ în asigurarea securităţii informaţiilor, majoritatea experţilor în securitate cibernetică apreciază că un adversar persistent, bine pregătit şi care dispune de resurse suficiente, va avea adesea succes în atacurile asupra sistemelor informatice, mai ales în situaţia în care sporirea capacităţii de apărare este singura formă de răspuns la un atac cibernetic. Din acest motiv, o atenţie sporită este acordată descurajării unor astfel de atacuri, în primă instanţă, în special la nivel guvernamental, acolo unde există atribuţiuni şi competenţe, precum şi o gamă largă de instrumente specifice pentru investigarea activităţilor care pot afecta siguranţa publică şi securitatea naţională.

Ministerul Apărării Naționale
e-mail: *catalin.balog@gmail.com*

Înţelegerea ameninţărilor în spaţiul cibernetic

Înțelegerea ameninţărilor cibernetice este o sarcină dificilă, atât în ceea ce privește evaluarea, cât şi diminuarea având în vedere următoarele argumente:

- Există mulţi actori care manifestă intenţii rele. Costurile reduse ale tehnologiei informaţiei şi comunicaţiilor, conectivitatea pe scară largă la Internet, precum şi uşurinţa de a crea sau de a obţine produse *software* de tip *malware* înseamnă că aproape oricine poate desfăşura activităţi de tip *malware*[1]. Într-adevăr, Internetul este un mediu ideal pentru a comite o infracţiune cibernetică, deoarece acesta oferă o serie de caracteristici specifice: conectivitate, anonimat, lipsa de trasabilitate, precum şi o mare diversitate de obiective. Actorii care manifestă intenţii rele includ persoane, grupuri de crimă organizată, grupuri teroriste şi chiar state-naţiune, iar acţiunile care ar putea descuraja un grup pot fi mai puţin eficace împotriva altuia.
- Există la fel de multe motive ca şi actori. Aceste motive pot avea legătură cu zonele tradiţionale de activitate infracţională (de exemplu,

fraude cibernetice sau pornografie infantilă), spionaj economic, spionaj militar sau chiar război cibernetic.

- Există o diversitate de vectori, mulţi utilizaţi în mod obişnuit ca vectori de atac. Lăsând la o parte lanţul de aprovizionare şi ameninţările din interior, care prezintă provocări proprii, agresorii din exterior ar putea profita de vulnerabilităţi ale unor produse, erori de configurare ale sistemelor informatice şi tehnici de inginerie socială. Deoarece actori diferiţi pot utiliza tehnici similare, este posibil ca natura atacului să nu ofere indicii suficiente referitoare la identitatea agresorului sau la motivele acestuia. Acest fapt, combinat cu anonimatul şi lipsa de trasabilitate, înseamnă că atribuirea atacurilor este foarte dificilă, iar încadrarea în gama activităţilor de tip *malware* este, de asemenea, foarte dificilă.
- Internetul este un domeniu comun şi integrat. Totodată, acesta este un mediu comun pentru cetăţeni, întreprinderi şi guverne, într-un mod în care este dificilă separarea unui grup de altul. Mai mult decât atât, libertatea de exprimare, tranzacţiile comerciale, activităţile de spionaj şi războiul cibernetic pot coexista în acest domeniu comun şi integrat, toate în acelaşi timp şi în acelaşi mediu. Cu o capacitate limitată de a analiză a actorilor şi a activităţilor este extrem de greu de găsit răspunsuri adecvate unor ameninţări specifice.
- Posibilele consecinţe ale unui atac sunt foarte greu de prezis. Anumite activităţi de tip *malware*, cum ar fi scanarea reţelei sau accesul neautorizat, pot fi un preludiu la furtul de informaţii, o încălcare a integrităţii datelor sau o întrerupere a unui serviciu. Mai mult decât atât, interdependenţele complexe dintre sistemele informatice sugerează că ar putea exista efecte în cascadă, neprevăzute, unele chiar mai severe decât cele anticipate. În cele din urmă, în timp ce unele atacuri pot fi evidente (de exemplu, un atac de tip *Denial of Service*[2] împotriva unei infrastructuri critice) şi generează un răspuns rapid, alte atacuri pot fi extrem de greu de detectat. În context, putem avea în vedere extragerea unor date din sisteme sensibile, iar un scenariu mai grav ar putea fi modificarea unor date critice într-un astfel de sistem. Nu numai că aceste atacuri sunt dificil de detectat, dar poate exista dificultatea de a discerne dacă datele au fost schimbate fără drept, făcând astfel dificilă revenirea într-o stare anterioară, bună.
- Cele mai rele scenarii sunt alarmante. În mass-media, în spaţiul politic şi în cel al experţilor în domeniu, aceste scenarii includ perturbarea serviciilor de infrastructură critică, împiedicând funcţii economice cheie sau chiar primejduirea siguranţei publice şi a securităţii naţionale (explicând astfel, trimiterile des repetate la un „Pearl Harbor electronic”). Complexitatea acestor scenarii, care rezultă în parte din interconectivitatea masivă şi dependenţele dintre sistemele care nu sunt întotdeauna bine înţelese, a făcut dificilă posibilitatea dezvoltării unui consens în ceea ce priveşte consecinţele probabile ale unui atac. O societate dependentă de sistemele informatice şi de datele pe care acestea le conţin poate fi deosebit de grav afectată în lipsa capacităţii de recuperare rapidă în urma unui astfel de atac.

Aşadar, într-un mediu în care există atât de mulţi actori cu atât de multe motive – şi aceşti actori şi activităţile lor sunt combinate cu activităţi inofensive şi chiar protejate constituţional – este de înţeles de ce persoanele şi instituţiile însărcinate cu elaborarea unor soluţii tactice şi strategice sunt în dificultate. Astfel, este uşor de înţeles de ce există o atât de mare îngrijorare pentru un mediu în care actorii şi motivele pot fi necunoscute şi în care consecinţele unor asemenea activităţi pot fi catastrofale.

În consecinţă, se poate afirma că, în funcţie de categoria de ameninţare, fiecare stat implementează diferite resurse şi fiecare resursă are propriul set de reguli. Acest model tradiţional funcţionează bine atunci când se poate identifica natura atacului; în mod special, „cine” şi „de ce” atacă. Însă, în era informaţională, acest model tradiţional eşuează pentru că atunci când sistemele informatice sunt supuse unui atac, „cine” şi „de ce” atacă sunt cel mai adesea necunoscute. În context, se poate aminti un lucru deja cunoscut: faptul că doar statele au acces la arme de război nu mai este o afirmaţie corectă, cel puţin nu în cazul unui război informaţional.

Regândirea ameninţărilor în spaţiul cibernetic

Într-o lume în care ameninţările şi acuzaţiile vizând activităţi de criminalitate cibernetică, spionaj economic, militar şi război cibernetic sunt în continuă creştere, este deosebit de important ca guvernele şi experţii în securitate cibernetică să analizeze cu toată seriozitatea activităţile de tip *malware* şi cele mai adecvate forme de

răspuns. Punctul de plecare este descurajarea şi oprirea acestui gen de activităţi, pe baza stabilirii identităţii agresorului (atribuirea) şi a motivaţiei atacului (categoria). În privinţa atribuirii, „cine” şi, prin deducţie, probabil, „de ce”, se poate stabili o atribuire puternică, o anumită probabilitate de atribuire (ridicat la scăzut) sau nicio atribuire. În privinţa categoriilor, se poate stabili o încadrare într-una dintre cele patru activităţi: criminalitate cibernetică, spionaj economic, spionaj militar şi război cibernetic. Fiecare nivel de atribuire şi fiecare categorie de atac ridică probleme unice în ceea ce priveşte răspunsul cel mai adecvat. Deşi măsurile defensive sunt întotdeauna adecvate şi nimic nu împiedică pe cineva să adopte măsuri puternice de securitate, precum adoptarea autentificării multi-factor, măsurile puternice de apărare nu sunt suficiente, chiar dacă ar putea descuraja agresorii care caută ţinte uşoare. Agresorii motivaţi, bine pregătiţi şi care dispun de resurse suficiente sunt, mai degrabă, stimulaţi de o apărare puternică.

Problema atribuirii

Punctul de plecare pentru orice nouă strategie de securitate cibernetică trebuie să se concentreze asupra problemei atribuirii pentru că, chiar dacă caracterul deschis şi anonimatul specific Internetului determină dificultatea atribuirii, existenţa unei idei referitoare la „cine” şi „ce” ar putea face – referitor la un eventual atac – este cu siguranţă de ajutor. Astăzi, atribuirea este extrem de dificilă, atât din motive tehnice, cât şi nontehnice. Informaţiile privind sursa pot lipsi total sau parţial, sau pot fi inexacte, iar posesorii unor informaţii relevante pot manifesta reticenţă în publicarea acestora; chiar şi guvernele care doresc să colaboreze întâmpină uneori anumite dificultăţi de natură juridică. Mai mult decât atât, de fiecare dată când se vorbeşte despre partajarea unor date, este aproape imposibil să se ajungă la un consens asupra a ceea ce înseamnă acestea. Pe de altă parte, problema atribuirii evidenţiază numeroasele provocări în acest domeniu. Cum se apreciază „gradul de probabilitate” şi care este gradul de toleranţă pentru „ceva rău”, cum se apreciază „asistenţa semnificativă” şi „asistenţa în timp util” şi care va fi modul de „răspuns proporţional”? Toate aceste întrebări dificile au fost abordate și în alte domenii, de exemplu, în domeniul proliferării nucleare, în domeniul dezvoltării armelor de distrugere în masă şi în domeniul sprijinului acordat teroriştilor.

Categorii de atacuri

Desigur, în unele cazuri, atribuirea – sau cel puţin o probabilitate mare de atribuire exactă – este posibilă, indiferent de categoria[3] în care se poate încadra un atac cibernetic. Odată ce acest lucru este fundamentat, devine clar cazul în care mecanismele actuale de intervenţie ale societăţii ar putea fi îmbunătăţite şi cazul în care trebuie să fie adoptate noi strategii.

Prima categorie se referă la infracţiuni cibernetice convenţionale[4]. Aceste infracţiuni includ cazurile în care calculatoarele sunt utilizate în scopuri criminale tradiţionale, cum ar fi frauda, sau folosite ca instrumente pentru a comite infracţiuni tradiţionale (de exemplu, distribuţia de pornografie infantilă). În această categorie, mecanismele existente de aplicare a legii oferă cadrul general pentru un răspuns adecvat, dar mai este mult de lucru pentru a actualiza şi armoniza regimurile juridice naţionale şi pentru a creşte semnificativ viteza de execuţie în aplicarea legii. Statele-naţiune ar trebui să fie încurajate să adopte o legislaţie a criminalităţii cibernetice acolo unde este nevoie, pentru a se putea dezvolta capacitatea şi capabilitatea de luptă împotriva criminalităţii cibernetice, precum şi de a se alătura eforturilor internaţionale în acest sens[5]. Eforturile de combatere a spălării banilor şi a altor infracţiuni transnaţionale pot constitui lecţii valoroase în acest domeniu.

A doua categorie se referă la cazurile de spionaj militar; mai precis, la afirmaţiile conform cărora unele state-naţiuni pătrund în sistemele unor agenţii guvernamentale şi/sau baze industriale militare şi extrag cantităţi mari de date sensibile, cu caracter militar. Fără a diminua gravitatea acestor afirmaţii, este important să se recunoască faptul că spionajul militar este o activitate care se desfăşoară din timpuri imemoriale şi că unele victime ale spionajului militar pot fi angajate în astfel de activităţi de spionaj, ele însele. Știind că este puţin probabil ca un astfel de comportament să fie eradicat, statele ar trebui să adopte un nivel de apărare cibernetică agresivă, graţie capacităţilor lor ofensive, și să folosească acele elemente tradiţionale ale puterii naţionale care sunt de obicei utilizate pentru a răspunde preocupărilor de spionaj.

A treia categorie se referă la cazurile de spionaj economic şi alte evenimente cibernetice în care guvernele au clar diferenţe filozofice asupra a ceea ce constituie un comportament acceptabil.

De exemplu, multe state cred că întreprinderile ar trebui să concureze pe un teren de egalitate şi că sistemele juridice ar trebui să protejeze dreptul celor care dezvoltă idei noi pentru a le valorifica. Prin contrast, alte state cred că securitatea naţională este dependentă de securitatea economică şi, pentru a obţine un avantaj economic, guvernului îi revine rolul de a sprijini industriile autohtone împotriva furtului de proprietate intelectuală creată în alte state (sau cel puţin de a închide ochii atunci când o firmă autohtonă sustrage informaţii de la concurenţii străini). Aceste state nu sunt descurajate de faptul că o astfel de abordare este în acelaşi timp imorală şi fără perspectivă. Este imorală, deoarece furtul de proprietate intelectuală este, pur şi simplu, furt, iar lipsa de perspective decurge din faptul că o ţară nu poate stabili o cultură a inovării şi nu poate obţine un avantaj economic adevărat în condiţiile în care drepturile de proprietate intelectuală nu sunt respectate. În cazul în care între state nu se manifestă astfel de diferenţe filozofice, diplomaţia internaţională ar trebui să se concentreze pe stabilirea normelor internaţionale adecvate şi pe reglementarea acestor norme în cadrul acordurilor internaţionale, aşa cum s-a procedat în alte domenii, amintite anterior.

Un alt domeniu de dispută filozofică, şi unul chiar mai dificil decât spionajul economic, se referă la libertatea de exprimare. În ceea ce priveşte spionajul economic, dezbaterea este una destul de simplă: este sau nu adecvat furtul de proprietate pentru obţinerea unor beneficii economice naţionale? În schimb, dreptul de liberă exprimare se bazează pe un *continuum*: unele state sunt mai restrictive decât altele. În astfel de cazuri pot apărea probleme în ceea ce priveşte măsura în care exprimarea este limitată (de exemplu, există o mare diferenţă între incriminarea unui discurs caracterizat de ură şi incriminarea unui discurs religios sau politic), precum şi dacă guvernul care restricţionează exprimarea a fost ales în mod democratic (astfel, indicând faptul că orice restricţii sunt sancţionate de către populaţie). Pentru a complica şi mai mult lucrurile, putem spune că atunci când statele negociază acorduri internaţionale şi stabilesc comportamentul normativ, este ceva obişnuit să existe anumite prevederi ale tratatului – în esenţă, limitate – care asigură guvernelor autoritatea de a lua măsurile necesare pentru protejarea siguranţei publice şi asigurarea securităţii naţionale, fără a aduce atingere altor dispoziţii ale tratatului. Deoarece statele nu vor renunţa la dreptul suveran de protejare a siguranţei publice şi de asigurare a securităţii naţionale – şi pentru că limitări ale exprimării sunt adesea justificate ca fiind necesare pentru menţinerea ordinii publice – este puţin probabil că astfel de negocieri vor produce cu uşurinţă noi comportamente normative. Totuşi, acordurile privind marjele pot fi încă realizabile. De exemplu, într-o epocă în care conţinutul creat de utilizatori este transmis prin intermediul sistemelor informatice la nivel mondial şi stocat în *cloud*[6], asigurarea unei protecţii pentru cei care oferă canale de transport sau servicii de *cloud computing* ar fi justificată, în special dacă aceştia sunt receptivi atunci când sunt invocate probleme de legalitate.

A patra categorie se referă la războiul cibernetic, un domeniu deosebit de dificil pentru că, aşa cum am menţionat anterior, Internetul este un domeniu comun şi integrat. În lumea fizică este mai uşor să faci distincţia dintre trupe şi spitale şi există chiar norme / reguli de război care stipulează răspunsurile permise atunci când trupele lansează atacuri de pe acoperişurile spitalelor. Internetul nu permite existenţa unor astfel de delimitări clare. Însă, astăzi există şi o altă problemă: societatea redefineşte războiul cibernetic. Să luăm, ca exemplu, cazul unui individ care a încercat să bombardeze, recent, un avion care se deplasa către Detroit, Michigan, şi în care, pe baza informaţiilor cunoscute, s-a sugerat faptul că acest individ a avut conexiuni cu un cunoscut grup terorist. În urma acestei încercări, a existat o dezbatere intensă referitoare la încadrarea juridică a autorului: această persoană reprezintă un criminal, căruia trebuie să-i fie citite drepturile constituţionale, sau un combatant inamic, căruia trebuie să i se asigure o custodie militară. Desigur, în viitor, întrun caz similar, un simpatizant al unei cauze extremiste s-ar putea să se angajeze să arunce în aer un avion, fără a avea nicio legătură oficială cu vreun grup terorist organizat; autorul ar putea fi, pur şi simplu, un simpatizant care acţionează singur. În cazul în care acest lucru se va întâmpla, un stat-naţiune s-ar putea găsi în stare de război cu un singur individ. Războiul asimetric are implicaţii semnificative pentru atacurile cibernetice, pentru că Internetul permite unui potenţial individ, anonim şi nedetectabil, care dispune de resurse reduse, să se angajeze într-un război cibernetic cu un stat-naţiune. Ca atare, este necesar să fie luate în considerare regulile unui astfel de război cibernetic, asimetric.

Chiar dacă războiul cibernetic a fost limitat la activitatea statului-națiune, riscul producerii unor accidente în domeniul infrastructurilor critice şi a bunurilor aparținând unor persoane cu statut *non-combatant* este unul semnificativ, mai ales atunci când se consideră că este greu de prezis care ar fi consecinţele nedorite ale unui atac cibernetic. La ora actuală, ținând seama de apariția serviciilor de *cloud computing* şi de dezvoltarea accentuată a Internetului, se manifestă o părere unanimă referitoare la creșterea importanței militare și la perfecționarea capacităților cibernetice militare, avându-se în vedere tot ceea ce poate constitui o activitate militară adecvată în acest domeniu comun şi integrat. Dacă, într-adevăr, temerile actuale se îndreaptă către un „Pearl Harbor electronic”, atunci, poate că o parte a unui răspuns adecvat ar putea fi reprezentat de o „Convenție de la Geneva electronică” [7], pentru a proteja drepturile celor necombatanți.

Cele patru categorii prezentate anterior sunt importante nu pentru că elimină cele mai dificile întrebări, ci pentru că pot ușura, în anumite situații, dezvoltarea unor strategii preventive şi reactive în cazurile în care există o atribuire. De asemenea, ele pot ajuta la reducerea paraliziei care poate să apară atunci când se încearcă proiectarea unei strategii unice pentru nenumărate alte ameninţări, similare doar prin înglobarea lor tehnologică.

Concluzii

Nu există îndoială că Internetul, caracterizat de conectivitatea sa la nivel global, anonimatul şi lipsa de trasabilitate, reprezintă cele mai serioase provocări pentru sectoarele public şi privat care au sarcina de a-l proteja. Amploarea activităţii infracţionale, numărul de actori şi motive, precum şi incertitudinea de atribuire au determinat improvizarea unor răspunsuri adecvate la atacuri dificile şi imposibilitatea standardizării acestor răspunsuri de natură cibernetică. Deşi nu există răspunsuri uşoare, o probabilitate sporită în atribuire şi reguli mai clare pentru a răspunde atât atacurilor atribuite şi nonatribuite ar permite dezvoltarea şi punerea în aplicare a unor strategii și tactici mai bune pentru a răspunde ameninţărilor cibernetice.

Dacă această analiză este corectă, cursul de acţiune viitor devine mai clar:

- trebuie să existe o inovaţie referitoare la atribuire. Aceasta include atât inovaţia tehnologică (pentru a permite surselor găsirea unui punct de vedere tehnic) şi inovaţii juridice / diplomatice (pentru a permite datelor partajarea rapidă, chiar şi la nivel transfrontalier).
- pentru a face faţă criminalităţii cibernetice, este important ca statele să adopte legi naţionale care să protejeze spaţiul cibernetic, să construiască capacitatea de aplicare a legii şi să sprijine eforturile internaţionale de combatere a criminalităţii informatice.
- pentru a aborda spionajul economic şi alte domenii în care există un dezacord filozofic, trebuie să existe, în prealabil, discuţii la nivel internaţional care să urmărească stabilirea unor norme care apoi să fie puse în aplicare prin intermediul politicilor naţionale şi a organizaţiilor internaţionale.
- pentru a aborda spionajul militar, statele-naţiune trebuie să-şi îmbunătăţească propria stare de securitate informatică, să-şi construiască cele mai adecvate capacităţi ofensive, după caz, şi să recurgă doar la mecanismele diplomatice şi politice existente pentru a aborda eventualele litigii.
- pentru a aborda problemele referitoare la războiul cibernetic, statele trebuie să-şi dezvolte, în primul rând, poziţiile interne care vor sta la baza normelor care vor stipula în ce va consta acest nou domeniu, având grijă să recunoască caracterul comun şi integrat al acestuia. Apoi, trebuie să existe un dialog internaţional, conceput pentru a crea normele internaţionale de comportament în spaţiul cibernetic. Crearea acestor norme va fi o sarcină extrem de dificilă, dar necesară şi, în cele din urmă, inevitabilă. Absența unui astfel de acord și, în mod implicit, existența unor acțiuni unilaterale şi potențial neprincipiale va determina apariția unor consecinţe care vor fi inacceptabile şi ulterior, regretabile.

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanțat prin Fondul Social European, în cadrul proiectului **POSDRU/159/1.5/S/138822**, cu titlul **„Rețea Transnațională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile „Ştiinţe Militare”, „Securitate şi Informaţii” şi „Ordine Publică şi Siguranţă Naţională” – Program de Formare Continuă a Cercetătorilor de Elită – „SmartSPODAS”.”**

NOTE:

1 *Software* rău intenționat (numit adesea ***malware***, construit din sintagma ***mal****icious* ***soft****ware*, „software răuvoitor”) – este un tip de *software* proiectat intenționat pentru deteriorarea unui calculator sau infiltrarea în el, sau/și deteriorarea ori infiltrarea în întregi rețele de calculatoare, fără consimțământul proprietarului respectiv. Noțiunea se utilizează generalizat de către specialiștii IT pentru a desemna orice formă ostilă, intruzivă sau supărătoare de *software* sau cod de program.

2 Un atac cibernetic de tip ***DoS*** (de la expresia engleză „**D**enial **o**f **S**ervice”, în traducere: refuzul, blocarea serviciului) sau ***DDoS*** („**D**istributed **D**enial **o**f **S**ervice”, blocarea distribuită a serviciului) este o încercare frauduloasă de a indisponibiliza sau bloca resursele unui calculator. Deși mijloacele și obiectivele de a efectua acest atac sunt foarte diverse, acest atac este, în general, efectul eforturilor intense ale unei (sau a mai multor) persoane de a împiedica un *website* sau și servicii Internet de a funcționa eficient, temporar sau nelimitat.

3 Aceste atacuri se încadrează în patru categorii diferite, prezentate în continuare.

4 Categoria criminalității cibernetice este de departe cea mai largă și cea care surprinde cel mai mare număr de actori (de la minori la recidiviști) și cel mai mare număr de motive / acțiuni (de la falsificarea notelor în catalogul electronic, la școală, la comiterea unor fraude complexe, cu provocarea unor pagube semnificative într-un sistem IT, într-un context non-război). În mod evident, răspunsurile guvernamentale internaționale vor trebui să fie flexibile și proporționale.

5 De exemplu, Convenția Consiliului Europei din 23/11/2001 privind Criminalitatea Informatică, publicată în Monitorul Oficial, Partea I nr. 343 din 20/04/2004, Seria Tratatelor Europene nr. 185, Budapesta, 23 noiembrie 2001.

6 *Cloud* sau *cloud computing* este un concept modern în domeniul IT, reprezentând un ansamblu distribuit de servicii de calcul, aplicații, acces la informații și stocare de date, fără ca utilizatorul să aibă nevoie să cunoască amplasarea și configurația fizică a sistemelor care furnizează aceste servicii.

7 *Convențiile de la Geneva* reprezintă ansamblul a patru tratate formulate la Geneva, Elveția, tratate care stabilesc standardele dreptului internațional în ceea ce privește problemele umanitare. Aceste tratate se referă în principal la tratamentul necombatanților și prizonierilor de război. Ele nu au nicio legătură cu problema folosirii armamentului în timp de război, care este acoperită de Convențiile de la Haga din 1899 și 1907 și de Protocolul de la Geneva din 1925 *(care privește folosirea armelor chimice și biologice)*. O Convenție de la Geneva electronică ar putea fi un document care se referă la strategia de securitate cibenetică a UE, clarificând roluri și responsabilități și stabilind acțiunile necesare, pe baza unei protecții și promovări solide și eficace a drepturilor cetățenilor, astfel încât mediul *online* să devină cel mai sigur din lume.

BIBLIOGRAFIE

Strategia de Securitate Cibernetică a României şi *Planul de acţiune la nivel naţional privind implementarea Sistemului Naţional de Securitate Cibernetică,* în M.O. nr. 296 din 23 mai 2013, H.G. nr. 271/2013)

Dunnigan James F., *Noua ameninţare mondială: cyberterorismul*, Editura Curtea Veche Publishing, Bucureşti, 2010.

McLuhan Marshall, *Mass-media sau mediul invizibil*, Editura Nemira, Bucureşti, 1997.

Lawrence A. Gordon, *Cybersecurity risk management: an economics perspective*, http://www.rhsmith.umd.edu/faculty/lgordon

FFIEC Handbook Definition of Reputation Risk, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-riskmanagement/reputation-risk.aspx

Governing for Enterprise Security, http://www.cert.org/governance/

Socializing Securely: Using Social Networking Services, http://www.us- cert.gov/reading_room/safe_social_networking.pdf

US-CERT's Protect Your Workplace Posters & Brochure, http://www.us- cert.gov/reading_room/distributable.html

What Businesses can do to help with cyber security, http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Bus inesses%20Can%20Do%202011%20Final_0.pdf

http://news.bbc.co.uk/2/hi/technology/6653119.stm

http://www.securitatea-informatiilor.ro

http://www.sri.ro