Identitatea cibernetică și viața socială în Cyberspace (cap. 4)

Lucasevici Iulia Daniela,
Cibernetica si economie cantitativa,
an II, grupa 1093

De la inventarea tiparului, nimic nu a mai revoluţionat la fel de mult domeniul comunicaţiilor precum calculatorul şi apariţia Internetului, care a făcut posibilă prin World Wide Web (unul dintre cele mai importante servicii şi aplicaţii informatice), conectarea la o reţea mondială de documente şi date, facilitând legături între persoane din colţuri diferite ale lumii, greu de întreţinut în alte condiţii şi cu un consum mult mai mare de energie, timp şi mijloace materiale. Una dintre cele mai răspândite inovaţii în domeniul tehnologiei şi comunicaţiilor, Internetul, a influenţat în mod iremediabil indicatorii comunicării între oameni, de la apariţia sa căpătând o amploare şi adăugând anual milioane de utilizatori, la un nivel neanticipat poate nici măcar de creatorii săi şi asigurându-şi, în scurt timp, supremaţia printre celelalte mijloace de comunicare şi informare, la concurenţă strânsă cu telefonia mobilă.

În ţara noastră, deşi conectarea la noile tehnologii informaţionale şi comunicaţionale s-a realizat mai târziu, în ultimii ani s-a redus mult decalajul faţă de ţările dezvoltate, calculatorul devenind o prezenţă constantă în viaţa de zi cu zi, informatizarea intensă a serviciilor, şcolilor, universităţilor, bibliotecilor ori instituţiilor fiind susţinută prin politici publice şi programe 3 guvernamentale. În paralel, aceeaşi politică agresivă s-a aplicat şi în ce priveşte dotarea elevilor şi accesul acestora la calculatoare. În pofida preocupărilor de informatizare a societăţii, la nivel internaţional accesul la Internet nu este globalizat, numeroase studii arătând că există state în care, din cauza sărăciei, accesul la un calculator şi la Internet nu reprezintă încă o „opţiune”.

Începând cu noul mileniu, economia mondială şi securitatea naţiunilor dezvoltate au devenit dependente complet de tehnologia informaţiei şi a infrastructurii de comunicaţii. Un număr impresionant de reţele de calculatoare şi sisteme de comunicaţii asigură în mod direct funcţionarea tuturor sectoarelor de activitate din sfera publică şi privată fie că este vorba despre sectorul energetic (energie electrică, petrol şi gaze), transport (feroviar, maritim şi aerian), financiar-

bancar, comunicaţii şi telecomunicaţii, servicii de urgenţă şi utilitate publică, apărare naţională etc. Prin intermediul acestora se controlează, de asemenea, obiecte fizice, cum ar fi, transformatoare electrice, sisteme de pompare, instalaţii chimice, sisteme de dirijare a traficului (terestru, maritim şi aerian), trenuri, vapoare, avioane şi sateliţi artificiali. Raza de acţiune a acestor reţele de calculatoare şi sisteme de comunicaţii care formează infrastructura critică de comunicaţii depăşeşte limitele spaţiului cibernetic, punându-şi amprenta asupra existenţei umane, în ansamblu.

În spaţiul cibernetic există o serie de indivizi sau entităţi rău intenţionate care pot iniţia atacuri împotriva infrastructurii critice de comunicaţii. În acest sens, o preocupare majoră a autorităţilor guvernamentale, precum şi a unor entităţi private, o reprezintă posibilitatea ca un atac cibernetic organizat să fie capabil să provoace daune majore infrastructurii critice de comunicaţii, economiei sau chiar să afecteze securitatea naţională a unui stat. Însă, cunoştinţele teoretice şi capacităţile tehnice necesare pentru a efectua un astfel de atac sunt deosebit de complexe – ceea ce ar putea explica parţial lipsa unui atac cu astfel de efecte, până în prezent. Pe lângă acestea există şi riscul exploatării unor vulnerabilităţi care să implice efecte încă ignorate sau chiar negândite.

În prezent, încă există incertitudini referitoare la intenţiile sau capacităţile distructive ale unora dintre atacurile înregistrate în spaţiul cibernetic, ştiut fiind faptul că efectul acestora nu este întotdeauna unul vădit. De aceea este necesară o analiză îmbunătăţită pentru a identifica vulnerabilităţile, tendinţele ameninţărilor şi evaluarea efectelor atacurilor cibernetice, pe termen lung. Ceea ce se ştie este faptul că metodologiile şi instrumentele de atac devin disponibile pe scară largă, iar cunoştinţele teoretice şi capacităţile tehnice ale utilizatorilor cu astfel de preocupări se îmbunătăţesc permanent. Din cauza perfecţionării metodologiilor şi instrumentelor de atac, un număr tot mai mare de indivizi sau entităţi sunt capabile să lanseze atacuri cibernetice semnificative la nivel naţional, iar frecvenţa acestora este în continuă creştere. În timp de pace, adversarii sau inamicii unei naţiuni pot desfăşura acţiuni de spionaj care vizează activitatea instituţiilor guvernamentale, centrelor de cercetare şi companiilor naţionale sau multinaţionale. De asemenea, pot să se pregătească pentru executarea unor atacuri cibernetice ulterioare prin cartografierea infrastructurilor critice naţionale, identificarea obiectivelor cheie, generând breşe de securitate controlate prin programe specializate (back doors) sau prin alte mijloace (infiltrarea de agenţi). În timp de criză sau război, aceştia pot încerca intimidarea liderilor politici şi a formatorilor de opinie prin atacarea infrastructurilor critice de comunicaţii şi alterarea funcţiilor economice

cheie sau prin erodarea încrederii populaţiei în sistemele de informare publică. Astfel de atacuri cibernetice pot avea consecinţe deosebit de grave, iar contracararea lor necesită dezvoltarea unor capacităţi de apărare extrem de rapide şi robuste. Doar astfel pot fi reduse vulnerabilităţile şi pot fi descurajaţi indivizii sau entităţile rău intenţionate. Spaţiul cibernetic permite un atac organizat asupra infrastructurii critice a unei naţiuni, de la distanţă. Iniţiatorii unui asemenea demers au nevoie doar de tehnologia adecvată care le va permite ascunderea identităţii, dispunerea fizică şi breşele de securitate. Nu numai că spaţiul cibernetic oferă posibilitatea de a exploata punctele slabe ale infrastructurilor critice, dar oferă, de asemenea, un sprijin semnificativ pentru executarea unor atacuri fizice, permiţând perturbarea comunicaţiilor, întârzierea unei intervenţii de urgenţă şi împiedicând un răspuns adecvat (defensiv sau ofensiv) – elemente esenţiale în urma unui atac fizic. Se poate aprecia că în trecut (secolul XX), izolarea geografică a constituit o piedică în calea unei invazii fizice directe a unor state, precum Statele Unite. În prezent, din perspectiva spaţiului cibernetic, graniţele naţionale nu mai au acelaşi sens, acestea diluându-se într-o foarte mare măsură. Chiar şi infrastructura – software şi hardware – care alcătuieşte spaţiul cibernetic devine globală, dacă avem în vedere proiectarea şi dezvoltarea sa. Din această cauză, a globalizării spaţiului cibernetic, orice potenţială vulnerabilitate poate fi exploatată de către oricine, oriunde s-ar afla, cu condiţia să dispună de suficiente cunoştinţe teoretice şi capacităţi tehnice pentru a o „valorifica", transformând-o într-o ameninţare reală.

Datorită numărului şi diversităţii utilizatorilor prezenţi în spaţiul cibernetic, gestionarea ameninţărilor şi reducerea vulnerabilităţilor în acest domeniu reprezintă o provocare extrem de complexă. De asemenea, având în vedere numărul calculatoarelor şi al sistemelor de comunicaţii existente în spaţiul cibernetic, asigurarea securităţii necesită acţiuni desfăşurate pe mai multe niveluri, de către grupuri diferite de utilizatori. Problema securităţii în spaţiul cibernetic poate fi cel mai bine abordată ca o problemă cu cinci niveluri.

• Nivelul 1, Home Users / Small Business

Deşi nu fac parte dintr-o infrastructură critică, calculatoarele utilizatorilor individuali şi întreprinderilor mici şi mijlocii pot deveni parte a reţelelor de calculatoare controlate de la distanţă, folosite ulterior pentru atacarea infrastructurilor critice. Calculatoarele lipsite de apărare ale utilizatorilor individuali şi întreprinderilor mici şi mijlocii, în special cele care folosesc conexiuni de tip DSL (Digital Subscriber Line) sau conexiuni prin cablu sunt vulnerabile la atacuri care pot angaja utilizarea acestora fără ştirea proprietarului. Grupuri astfel constituite de calculatoare

„zombie” pot fi apoi utilizate de către terţi actori pentru a lansa atacuri de tip DoS (Denial of Service) asupra nodurilor cheie de Internet, companiilor importante sau chiar asupra infrastructurilor critice.

• Nivelul 2, Large Enterprises

Întreprinderile mari (societăţi comerciale, agenţii guvernamentale şi universităţi) reprezintă obiective obişnuite ale atacurilor cibernetice. Multe dintre acestea sunt parte a infrastructurilor critice. Întreprinderile mari necesită în mod clar politici active şi articulate de securitate a informaţiilor şi programe de supraveghere, în conformitate cu cele mai bune practici în domeniu. Se poate aprecia că reţelele de calculatoare ale acestor întreprinderi se vor confrunta cu o creştere a atacurilor iniţiate de indivizi sau entităţi rău intenţionate, având în vedere datele şi informaţiile, dar şi puterea de calcul de care acestea dispun.

• Nivelul 3, Critical Sectors / Infrastructures

Atunci când organizaţii din sectorul economic, guvernamental sau academic îşi unesc eforturile pentru abordarea unor probleme comune de natură cibernetică, se pot reduce sarcinile individuale ale unei întreprinderi. De foarte multe ori, astfel de colaborări pot da naştere unor instituţii şi mecanisme comune, care prezintă, la rândul lor, anumite vulnerabilităţi a căror exploatare afectează în mod direct activitatea organizaţiilor partenere şi a sectorului, în ansamblu. Totodată, întreprinderile pot contribui la reducea riscurilor din spaţiul cibernetic prin participarea la grupuri de lucru care elaborează recomandări de specialitate, evaluări tehnologice, certificări de produse şi servicii şi distribuie informaţii. Ca şi în alte domenii, nevoia de a reacţiona rapid cu specialişti care înţeleg complexitatea unor astfel de ameninţări a dus la apariţia echipelor de răspuns la incidente de securitate informatică, cunoscute sub denumirea de echipe de tip CERT sau CSIRT2 . Acestea reprezintă, de asemenea, un instrument pentru schimbul de informaţii cu privire la tendinţele de atac, ameninţări şi vulnerabilităţi, precum şi cele mai bune practici în spaţiul cibernetic.

• Nivelul 4, National Issues and Vulnerabilities

Unele probleme din spaţiul cibernetic au implicaţii majore, la nivel naţional şi nu pot fi rezolvate de către o întreprindere sau un sector, în mod singular. Toate sectoarele de activitate la nivel naţional utilizează Internetul. În consecinţă, toate acestea sunt expuse aceluiaşi risc în cazul în care unele dispozitive, la nivel naţional, nu prezintă siguranţă. De asemenea, anumite deficienţe – software sau hardware – utilizate pe scară largă pot genera probleme, la nivel naţional, care

necesită activităţi coordonate pentru cercetarea şi dezvoltarea unor tehnologii îmbunătăţite. Totodată, şi numărul insuficient al profesioniştilor certificaţi în domeniul securităţii cibernetice reprezintă o problemă de nivel naţional.

• Nivelul 5, Global

Sistemul WWW (World Wide Web) este o reţea de informaţii globală. Existenţa standardelor comune la nivel internaţional permite interconectarea şi interoperabilitatea sistemelor de calculatoare şi comunicaţii din lumea întreagă. Acest fapt creează premisele extinderii unor probleme de pe un continent pe altul. Prin urmare, este esenţială cooperarea internaţională pentru distribuirea informaţiilor referitoare la problemele din spaţiul cibernetic, precum şi pentru urmărirea infractorilor cibernetici. În lipsa acestei forme de cooperare, capacitatea colectivă de a detecta, a descuraja şi a reduce efectele atacurilor din spaţiul cibernetic ar fi mult diminuată.

Totodată, dezvoltarea informaţională şi tehnologică a determinat schimbarea esenţială a stilului general de viaţă. Majoritatea, pentru a ne adapta evoluţiei şi progresului, alegem să tranzităm cea mai mare parte a activităţilor zilnice prin computerele personale sau de serviciu, acestea din urmă ajungând să ne monopolizeze progresiv timpul, cu riscul creării unei dependenţe de spaţiul virtual.

Era digitală a influenţat cel ami mult stilul de viaţă al copiilor şi adolescenţilor, generând întrebări cu privire la modul în care aceştia îşi construiesc identitatea într-o lume intens tehnologizată, din moment ce relaţiile interpersonale şi comunicarea sunt mediate într-o proporţie covârşitoare de prezenţa computerelor şi a telefoanelor mobile.

Pentru generaţia digitală, locurile de socializare s-au mutat din curtea şcolii sau a blocului pe site-urile de acest gen de pe Internet (Facebook, MySpace, Hi5, Twitter, YouTube ş.a.) sau pe blog-urile personale care le permit, spre deosebire de comunicarea faţă în faţă, o modelare, transformare şi adaptare permanentă a identităţii şi personalităţii, raportat la cerinţele şi preferinţele celorlalţi interlocutori şi prieteni cu care comunică în spaţiul virtual. Totodată, pot controla în mod direct propria imagine virtuală, prin modul de gestionare în acest spaţiu a informaţiilor personale, nivelul de divulgare a unor astfel de date ori de completare a profilurilor de prezentare cu aspecte reale sau inventate.

Indiferent dacă informaţiile personale încărcate în spaţiul virtual sunt sau nu reale, au fost realizate studii care au arătat că se înregistrează un echilibru între, pe de o parte, tendinţa tinerilor de a promova, virtual, o imagine proprie cât mai atractivă, prin exagerarea aspectelor pozitive, iar

pe de altă, conţinutul experienţelor pe care le aleg să le împărtăşească prin intermediul Internetului, care este preponderent pesimist (pierderi, eşecuri, suferinţe, dezamăgiri), în acest din urmă caz fiind vorba de o abordare emoţională a laturilor negative ale propriilor trăiri în moduri care să impresioneze sau să atragă atenţia. Unele studii au condus la concluzii potrivit cărora, activitatea virtuală a tinerilor este în strânsă legătură cu viaţa reală şi influenţată de aceasta în mod direct sau indirect, relaţiile pe care le creează în mediul Internet urmărind uneori tipare din realitate, în ambele ipostaze fiind animaţi prioritar de dorinţa de socializare şi de apartenenţă la un grup.

Prin intermediul reţelelor de socializare online (de tipul Facebook, Twitter, MySpace, Netlog, Dailymotion, Bebo ş.a.) sunt vehiculate mari cantităţi de date personale postate de tineri, potenţial a fi utilizate şi de persoane rău intenţionate, care urmăresc specularea vulnerabilităţilor din acest punct de vedere şi identificarea victimelor perfecte pentru satisfacerea unor interese reprobabile (de exemplu, în scopul exploatării sexuale ulterioare). Practici online precum grooming şi stalking sunt favorizate de faptul că, nu întotdeauna, noua identitate construită virtual de către adolescenţi are la bază şi date de identificare false, ci tendinţa preponderentă este cea de prezentare a reperelor reale din acest punct de vedere şi „fabricarea" doar a unor caracteristici personale noi, a unei personalităţi diferită de cea reală.