

Rețelele sociale online din perspectiva securității

Laurențiu MIHĂILESCU

Tudor RAȚ

Serviciul Român de Informații

e-mail: ani@sri.ro

Abstract

Social Networking Services provide both advantages and disadvantages for individual users and the Intelligence Community alike.

While individuals can develop vast networks of friends and acquaintances, they must be aware that these new means of communication bring along a threat to their security.

Social networks' ubiquity nowadays offers an impressive number of new domains of interest for intelligence agencies, but, as with any „uncharted territory”, they come with great security issues, digital espionage being just one of them.

Keywords: social network services, captive audience, web 3.0.

1. Expansiunea SNS

În ultimii ani rețelele sociale online („social networking services”, SNS) au devenit omniprezente. Au existat chiar voci care au afirmat că relaționarea prin intermediul site-urilor de socializare reprezintă modul în care s-a ajuns să se comunice predominant în secolul al XXI-lea.

Posibilitatea de a publica și a aduna informații (legate de interese, activități sau opinii ale apropiaților, cunoscuților) a reprezentat încă de la început un factor major în succesul Internetului, însă acesta a devenit abia în anul 2003 un spațiu activ de socializare pentru majoritatea utilizatorilor¹.

Rețele sociale online implică adesea organizarea în grupuri a unor indivizi sau organizații. În timp ce numeroase rețele sunt comunități legate de un interes comun principal (precum „Reno.ro”, „Animale.ro”), există și site-uri cu un orizont general de socializare, de genul „MySpace” sau

¹ Mika Peter „Flink: Semantic web technology for the extraction and analysis of social networks”, *Journal of Web Semantics*, vol. 3, pp. 211-223, octombrie 2005.

„Facebook”, care nu se concentrează pe un anumit interes, numite uneori „tradiționale” și care sunt deschise tuturor internauților.

Cele mai multe rețele sociale online solicită ca ambii utilizatori să confirme că sunt prieteni, înainte ca între ei să fie creată o legătură. Alte rețele au o secțiune, numită în general „Favorit”, „Fan” sau „Interesat” care nu necesită aprobarea celuilalt utilizator, însă unele SNS folosesc tot termenul de „Prieten”, ceea ce poate duce la confuzii, deoarece legătura nu înseamnă în mod neapărat prietenie în sensul clasic, iar motivele pentru care oamenii intră în contact pot fi foarte variate.

Dincolo de profiluri, prieteni, comentarii și mesaje private, rețelele sociale online variază foarte mult în funcție de aplicațiile pe care le utilizează și utilizatorii cărora li se adresează². Unele dintre ele permit „sharing”-ul de fotografii sau filmulețe, altele găzduiesc bloguri și tehnologii pentru transmiterea de mesaje instant. Multe rețele sociale online vizează persoane din anumite regiuni geografice sau anumite grupuri lingvistice, deși aceasta nu determină întotdeauna componența rețelei.

De exemplu, „Orkut” a fost lansat în SUA cu o interfață doar în limbă engleză, însă brazilienii vorbitori de portugheză au devenit repede grupul dominant de utilizatori³.

Avantaje

În condițiile în care relaționarea cu alte persoane avea loc în mod tradițional la locul de muncă, în instituții de învățământ sau în locuri foarte frecventate, comunicarea pe platformele de socializare este mult mai populară, milioane de oameni căutând să cunoască noi persoane, să adune și să împărtășească impresii, gânduri, informații pe diverse teme, să discute despre interese comune, să dezvolte alianțe personale și profesionale, să găsească locuri de muncă sau să stabilească eventuale contacte de afaceri.

Punctul central al site-urilor de socializare este reprezentat de profilurile personale ale utilizatorilor, un loc în care aceștia își exprimă sentimentele și gândurile, postează fotografii și se laudă cu rețeaua lor de prieteni. Cele mai populare rețele sociale pun un accent deosebit pe profilul

² Boyd Danah și Ellison Nicole „Social Network Sites: Definition, History, and Scholarship”, URL: <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>, 2007.

³ Kopytoff Verne „Google’s Orkut puzzles experts. San Francisco Chronicle” URL: www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/11/29/2004/BUGU9A0BH441.DTL, 2004.

personal, făcându-l ușor de folosit, dar capabil în același timp să reflecte personalitatea acestuia.

Dezavantaje

Deși rețelele sociale online au făcut să apară noi forme de interacțiune între utilizatori, problemele în materie de intimitate și securitate devin tot mai mediatizate, ajungând în atenția tuturor celor interesați de acest fenomen.

Implicațiile în materie de intimitate depind în general de gradul în care pot fi identificate informațiile postate de utilizator, de posibilități beneficiari și de modul în care pot fi folosite. Deși cele mai multe rețele sociale nu expun în mod deschis identitatea utilizatorilor, ele furnizează suficiente date pentru identificarea profilurilor. Acest lucru se poate realiza, de exemplu, prin recunoașterea fizionomiilor⁴ sau ca urmare a faptului că adesea utilizatorii folosesc aceeași fotografie sau unele similare pe site-uri diferite. De asemenea, identificarea profilurilor este posibilă cu ajutorul unor date demografice sau a unor caracteristici care se dovedesc unice sau rare. Un profil anonim sau pseudonim poate fi identificat fie pe baza unor cunoștințe anterioare despre caracteristicile și trăsăturile acestuia, fie prin deducerea unor necunoscute anterior.

Chiar și în aceste condiții, administratorii site-urilor de socializare încurajează împărtășirea publică a informațiilor personale și stochează date pe care apoi le vând unor terți interesați de publicitate. Nu e de mirare: aceste grupuri de oameni cu interese comune, profiluri psihologice similare și trăsături împărtășite constituie o resursă de marketing formidabilă.

Cele mai cunoscute pericole legate de relaționarea online sunt „prădătorii virtuali” (indivizi care pretind că sunt altceva decât sunt în realitate), furturile de date, virusii, în condițiile în care foarte multe persoane sunt dispuse să facă publice date cu caracter personal, iar, uneori, simple informații despre locul și data nașterii unei persoane pot fi exploatate în scopuri ilicite.

În ultimii ani, s-a remarcat un nou pericol: adicția psihologică pe care aceste rețele de socializare o pot genera. Programele software de tip jocuri (în special „Farmville”), chestionare și alte aplicații menite să facă

⁴ Gross R., „Re-identifying facial images. Tehnical Report”, URL: <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>, 2005.

din utilizatori un „public captiv” sunt omniprezente pe aceste site-uri. Este și ușor de înțeles de ce: conform unor statistici oferite de „Facebook”⁵, în fiecare zi, utilizatorii petrec cumulativ 3 miliarde de minute relaționând cu prietenii, comentând status-uri de activitate sau jucând diverse jocuri.

Un nivel și mai ridicat de dependență îl pot provoca noile tipuri de rețele sociale apărute, cu un grad înalt de imersiune, precum „Second Life”, „World of Warcraft” sau „eRepublik”. Aceste platforme care integrează rețele sociale, jocuri de tip multiplayer, blog-uri sau activități jurnalistice și chiar activități economice, reprezintă o nouă etapă a relaționării umane.

Țări precum Republica Maldive, Suedia, Serbia, Estonia, Columbia, Macedonia, Filipine, Israel și Albania și-au deschis ambasade și centre culturale sau organizații de promovare turistică în „Second Life”. Astfel, natura relațiilor diplomatice se schimbă profund, vechile și complexe reguli și uzanțe politice nemaigăsindu-și aplicabilitatea.

Nu doar diplomația capătă noi nuanțe în mediile virtuale, însăși relaționarea și agregarea umană se schimbă. Orașele din „Second Life” se construiesc în jurul ideilor și intereselor, nu în funcție de existența resurselor naturale (ape curgătoare, forme de relief, calitatea pământului arabil etc.). Putem găsi orașe ale muzicii rock gotice, orașe ale comunismului sau metropole religioase. Forme vechi de secole de devoțiune religioasă au căpătat un corespondent virtual, un exemplu elocvent în acest sens putând fi pelerinajul virtual la Mecca, la rândul lui, oraș virtual omonim cu cel saudit.

În mediul virtual, chiar și ordinea puterilor mondiale se realizează după alte coordonate. De exemplu, „eRepublik” le permite utilizatorilor săi să urmărească o carieră politică (se organizează alegeri de diferite forme), să devină soldați virtuali sub „drapelul” țărilor din care fac parte sau să participe la viața economică. „Statele” din „eRepublik” pot purta tratative diplomatice, pot declara război sau încheia alianțe.

Pe „eRepublik”, la 03.06.2010, România era angrenată, în războiul israeliano-turc, de partea Israelului. Deși se poate observa o paralelă a evenimentelor virtuale cu acțiuni care se întâmplă în timp real (forțele israeliene au capturat, la data de 31.05.2010, o flotilă cu scop umanitar care a plecat din Turcia cu destinația Fâșia Gaza), dinamica forțelor militare este mult schimbată din cauza sistemelor de alianțe virtuale. În „eRepublik”, țara noastră are alianțe încheiate cu țări de pe diferite continente, cum ar fi Spania, Israel, Australia, Japonia sau Peru. Rapiditatea cu care aceste

⁵ „Facebook” (site oficial), URL: <http://www.facebook.com/press/info.php?statistics>.

configurații de putere se schimbă este impresionantă: alianțele nu se încheie pe ani, ci pe săptămâni sau zile, războaie „mondiale” putând începe și încheia într-o lună.

Un alt aspect demn de menționat este creșterea influenței și puterii financiare a administratorilor acestor site-urilor de socializare: revista „Forbes” a estimat valoarea de piață a „Facebook” la 6,5 miliarde de dolari americani⁶, mai mult decât Produsul Intern Brut al multor state africane (Togo, Sierra Leone, Rwanda etc.), iar „Google”, administratorul platformei de socializare „Orkut”, a avut în anul 2009 un profit similar valorii de piață a „Facebook”, aproximativ 6,520 miliarde de dolari⁷.

Puterea de care se bucură acești giganți corporatiști are capacitatea de a influența politici de securitate ale unor mari puteri mondiale. Exemplul Chinei, care a pierdut temporar controlul asupra conținutului accesibil internauților săi, este relevant în acest sens. La 23.03.2010, „Google” a anunțat că-și va redirecționa serviciile prin filiera Hong Kong⁸, după ce în urmă cu 4 ani încheiasă un acord cu China prin care se angaja să cenzureze anumite referințe la evenimente sau topicuri de discuție pe care guvernul chinez le consideră sensibile (protestele din Piața Tiananmen, situația uigurilor, Tibet).

Prin această mișcare, pe care multe voci au considerat-o curajoasă, utilizatorii chinezi au putut ocoli restricția impusă de autoritățile chineze, având acces, cel puțin temporar, la întregul conținut disponibil pe *world wide web*.

Acest fenomen este cu atât mai îngrijorător cu cât autoritățile anumitor state, cum ar fi cazul Statelor Unite ale Americii, depind de serviciile „Google” pentru desfășurarea activităților zilnice. Peste 60% din agențiile guvernamentale ale Statelor Unite folosesc aplicații „Google”, în special stocarea datelor pe servere deținute de această companie⁹. Cu alte cuvinte, date deținute de drept de autoritățile americane sunt stocate în locații ce aparțin „Google”, sunt depozitate pe soluții hardware asupra cărora „Google” are drept

⁶ „Forbes” (site-ul revistei) URL: <http://www.forbes.com/forbes/2010/0118/outfront-facebook-shares-internet-friends-like-these.html>.

⁷ „Google investor relations” (tabel cu venituri realizate) URL: <http://investor.google.com/financial/tables.html>.

⁸ „The Guardian” (publicație, UK) URL: <http://www.guardian.co.uk/technology/2010/mar/23/google-china-censorship-hong-kong>.

⁹ „Philosecurity.org” (blog IT) URL: <http://philosecurity.org/2009/12/24/our-google-government>.

de proprietate, iar angajați „Google” au acces fizic în spațiile de depozitare a serverelor. Mai mult, „Google” are încheiate parteneriate similare cu alte state, unele cu interese divergente față de cele americane. Exemplul Chinei, cu care „Google” a colaborat timp de 4 ani, acceptând termenii cenzurii și făcând excepții semnificative de la politica de operare și codul etic corporatist care definesc compania, face necesară nuanțarea politicii de colaborare cu această companie din ce în ce mai influentă.

Ținând cont de aceste tendințe, se poate afirma că mediile de socializare virtuale se îndreaptă spre disoluția barierei public-privat, majoritatea utilizatorilor găsind acest mod de a interacționa cu firme și agenții de publicitate mai eficient, deoarece se elimină mesajele nedorite sau în neconcordanță cu interesele fiecăruia. Chiar și așa, grupuri de indivizi conduc campanii de conștientizare tot mai vocale cu privire la aspectele etice ale practicilor de încurajare și uneori chiar de „păcălire” a utilizatorilor prin folosirea unui limbaj ambivalent sau a unor clauze care lasă loc de echivoc.

2. Interesul serviciilor de informații

Rețelele sociale online devin din ce în ce mai interesante din perspectiva serviciilor de informații, fapt dovedit de programul „Total Information Awareness” al Agenției pentru Proiecte de Cercetare Avansată în domeniul Apărării (DARPA) din SUA care efectua cercetări aprofundate în domeniul strategiilor pentru analiza rețelelor sociale pentru a stabili dacă cetățeni americani prezintă amenințări asimetrice pentru securitatea națională. În cadrul acestui program, proiectul „Scalable Social Network Analysis” viza, între altele, dezvoltarea unor tehnici bazate pe analiza rețelelor sociale pentru a stabili caracteristicile unui grup terorist și pentru a diferenția aceste grupări de alte tipuri de grupuri sociale¹⁰.

În urma criticilor legate de faptul că dezvoltarea și desfășurarea de tehnologii specifice ar putea duce la un sistem de supraveghere în masă, unele proiecte nu au mai primit fonduri, însă altele au continuat să existe sub nume diferite¹¹.

¹⁰ Ethier Jason, „Current research in social network theory” URL: <http://www.ccs.neu.edu/home/perrolle/archive/Ethier-SocialNetworks.html>, 15.03.2009.

¹¹ „Electronic Frontier Foundation” (site oficial) URL: http://w2.eff.org/Privacy/TIA/20031003_comments.php; Harris, Shane „National Journal” (site oficial) URL: <http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm>.

La nivel internațional, serviciile de informații desfășoară o serie de activități în domeniul SNS, printre care cele de recrutare, de monitorizare și de avertizare.

Promovarea imaginii serviciilor de intelligence

Caracteristicile rețelelor de socializare online, în special ușurința diseminării informației, accesul la un grup de indivizi interesați de problematica pe care respectivul serviciu dorește să o comunice și interacțiunea lipsită de rigori formale, fac din acestea un mijloc de comunicare extrem de valoros. Informarea publicului devine astfel un proces de dialogare în beneficiul serviciului de informație care folosește acest instrument, informația ajungând la receptori netrunchiată, imediat și într-un mod controlat de emițător.

Deoarece milioane de utilizatori petrec tot mai mult timp pe rețelele sociale, ele par să fi devenit chiar și parte componentă a strategiilor operaționale ale serviciilor de informații, prin cooptarea internauților în soluționarea unor cazuri de dispariții de persoane, cum este cazul Biroului Federal de Investigații (FBI).

Agenția Centrală de Informații (CIA), Serviciul britanic de informații externe (MI6) sau Serviciul de Informații și Securitate Australian (ASIO) și-au creat pagini proprii pe „Facebook”, unde au publicat informații privind oportunitățile de angajare¹² sau au demarat diferite acțiuni de promovare în cadrul strategiilor de relaționare cu publicul. Astfel, membrii rețelei sunt invitați să se înregistreze, să citească informațiile privind oportunitățile de angajare, iar serviciile de informații, în calitate de angajatori, pot căuta date despre actualii sau potențialii angajați, formându-și o imagine despre valorile și profilul moral al acestora, după modelul unor companii private¹³.

Demonstrându-și racordarea la noile realități ale comunicării publice, Ministerul israelian al Afacerilor Externe a anunțat, la 03.06.2010, organizarea unei conferințe pe site-ul „Facebook”, pentru a expune punctul de vedere israelian cu privire la evenimentele din 31.05.2010, când forțele speciale israeliene conduse de „Shayetet 13” (Forțele Speciale Navale) au

¹² „US News” (portal de știri, SUA) URL: <http://www.usnews.com/news/national/articles/2009/02/05/the-cia-and-nsa-want-you-to-be-their-friend-on-facebook.html>.

¹³ „Sophos” (site-ul oficial al companiei internaționale omonime) URL: <http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf>.

preluat controlul flotilei care se îndrepta spre Gaza cu scopul declarat de a transporta ajutoare umanitare¹⁴.

Yigal Palmor, purtător de cuvânt al MAE israelian, a precizat că această conferință va fi organizată prin conectarea la grupul virtual „Gaza Flotilla – the world should know the truth” (Flotila pentru Gaza – lumea ar trebui să știe adevărul). Acest grup, înființat după data de 31.05.2010, a strâns, în mai puțin de 3 zile, 115.000 de membri din întreaga lume.

Un risc demn de luat în calcul cu privire la aceste două conturi menționate este posibilitatea inducerii în eroare a utilizatorilor conectați la acestea de către cei care le administrează. Fotografiile cu siglele instituțiilor, trimerile la site-uri oficiale și postarea datelor de contact (adrese, numere de telefon) conferă un aspect „oficial” acestor două conturi.

Monitorizare și avertizare

În prezent, anumite servicii de informații supraveghează rețelele media de socializare, precum „Facebook”, „YouTube”, blogurile și camerele de discuție online, în condițiile în care s-a constatat o proliferare a instrumentelor, tehnologiilor și metodelor utilizate în desfășurarea unor activități ilegale online, precum: fraudă, furt de identitate, trafic de ființe umane, comunicații teroriste, atacuri asupra site-urilor guvernamentale etc..

Dacă în urmă cu un deceniu agenții federali americani monitorizau camerele de discuții de pe „AOL” și „MSN” în vederea identificării persoanelor suspectate de abuzuri sexuale sau comiterea de infracțiuni diverse, în 2009, CIA a decis să preia în observare și cercetare toate rețelele de socializare, semnând, prin intermediul diviziei sale de investiții, „In-Q-Tel”, un „parteneriat strategic” cu compania Visible Technologies, „furnizor de analize social-media și soluții de interacțiune cu consumatorii”¹⁵. CIA nu este singurul serviciu de informații care supraveghează rețelele de socializare, alte exemple fiind FBI, NSA, Shin Bet și Mukhabarat.

Potrivit unui document intern al Departamentului american de Justiție, datat martie 2010, agențiile guvernamentale americane recurg la identități și profiluri false pe site-urile de socializare pentru a comunica

¹⁴ Site-ul oficial al Ministerului israelian de Externe URL: <http://www.mfa.gov.il/MFA/About+the+Ministry/MFA+Spokesman/2010/MFA-web-conference-with-FACEBOOK-group-3-Jun-2010.htm>.

¹⁵ „News.ro” (portal de știri, România) URL: <http://www.news.ro/stire/94178/cia-vede-tot-ce-faceti.html>.

cu diverși suspecți. Spre exemplificare, FBI, alături de alte servicii de informații, a folosit conturi false pe platforma „Facebook” pentru a culege informații despre persoane de interes¹⁶.

Acest document, obținut în urma unui proces privind dreptul la informare, indică faptul că agenții americani folosesc logarea clandestină pentru a interacționa cu suspecții, pentru a le stabili cercul relațional și pentru a consulta informații private, cum ar fi postări, fotografii și filmulețe personale¹⁷. Totodată, agenții de investigații pot să verifice alibiurile suspecților, comparând declarațiile date Poliției cu mesajele trimise din perioada respectivă privind locul unde se aflau.

Totuși, pentru a accesa date despre persoane de interes, nu este obligatorie asumarea unei identități false sau crearea unui cont, informațiile postate pe rețelele de socializare putând fi consultate de persoane interesate. Fotografiile postate pe rețele sociale reprezentând persoane pozând cu arme, bijuterii sau mașini de lux, pot constitui indicii pentru agenții de investigații în legătură cu desfășurarea unor activități ilegale. În ultima perioadă, a crescut numărul referirilor mediatice în presa occidentală la cazuri de persoane arestate după ce au publicat, în special pe „Facebook”, fotografii în care se afișau purtând arme¹⁸.

Un alt exemplu este cel al lui Pasquale Manfredi, persoană importantă în ierarhia Mafiei italiene și urmărit general în Peninsula, care a fost capturat datorită faptului că a divulgat informații privind locația sa pe „Facebook”¹⁹.

Serviciile de informații acordă atenție și campaniilor de avertizare privind pericolul reprezentat de spionajul digital. Shin Bet²⁰ le-a solicitat israelienilor să acorde o atenție deosebită corespondenței pe această rețea socială online, explicând că au existat tentative din partea unor grupări

¹⁶ „USA Today” (publicație, SUA) URL: <http://content.usatoday.com/communities/ondeadline/post/2010/03/fbi-uses-phony-profiles-on-social-networks-to-gather-information-on-suspects/1>.

¹⁷ „On Dead Line” (portal de știri și informații, SUA) URL: <http://content.usatoday.com/communities/ondeadline/post/2010/03/fbi-uses-phony-profiles-on-social-networks-to-gather-information-on-suspects/1>.

¹⁸ „The Sun” (site-ul publicației omonime, UK). URL: [//www.thesun.co.uk/sol/.../Facebook-gun-pics-catch-Crew.html](http://www.thesun.co.uk/sol/.../Facebook-gun-pics-catch-Crew.html).

¹⁹ „USA Today” (publicație, SUA) URL: <http://content.usatoday.com/communities/ondeadline/post/2010/03/italian-police-track-down-most-wanted-suspect-via-facebook-/1>.

²⁰ „Taragana” (blogul companiei IT, SUA) URL: <http://blog.taragana.com/index.php/archive/israel-says-arabs-are-hiring-spies-through-facebook/>.

violente de a atrage cetățeni israelieni să se întâlnească față-n față cu membri ai organizațiilor teroriste, „pentru a-i răpi, ucide sau recruta ca spioni”²¹.

La rândul lor, Serviciul General de Informații și Securitate (AIVD)²² și Serviciul de Informații Militare și Securitate (MIVD) din Olanda au demarat o campanie de informare destinată persoanelor care lucrează cu informații clasificate, explicând că oamenii pot fi urmăriți ușor pe Internet, prin intermediul unor rețele precum „Facebook”.

Eradicarea scurgerilor de informații

Un alt aspect care prezintă interes pentru serviciile de informații este reprezentat de datele personale postate pe profilurile de pe rețelele sociale online de indivizi care activează în domenii sensibile.

Un exemplu este cazul unui șef al serviciului MI6, John Sawers, a cărui soție a publicat pe „Facebook” fotografii și date personale despre membrii familiei, precum și adresa locuinței cuplului²³.

Totodată, armata SUA²⁴ și cea israeliană (Tahal)²⁵ au impus restricții legate de accesarea acestui gen de rețele de către soldați sau de conținutul postat de militari la profilurile lor în urma unor cazuri în care informații sensibile au ajuns la inamici prin intermediul rețelelor sociale.

Mai mult, Tahal a anunțat înființarea în cadrul serviciilor proprii de securitate, a unei divizii noi cu responsabilități în eradicarea scurgerilor de informații secrete în media, acordând o atenție sporită rețelelor de socializare²⁶.

Oportunități de culegere de informații pe probleme de securitate

SNS oferă multiple facilități (acces instantaneu la informații și la un grup de beneficiari extins din arii geografice diferite, schimb rapid de

²¹ „Haaretz” (ediția electronică, Israel) URL: <http://www.haaretz.com/hasen/spages/1086343.html>.

²² „Radio Netherlands Worldwide” (site-ul oficial al postului de radio, Olanda) URL: <http://www.rnw.nl/english/article/digital-spying-rife-dutch-agency-warns>.

²³ „CBS News” (site-ul oficial, SUA) URL: <http://cbsnews.com/stories/2009/07/05/tech/main5135008.shtml>.

²⁴ „Wired” (ediția electronică, SUA) URL: <http://www.wired.com/dangerroom/2009/06/army-orders-bases-stop-blocking-twitter-facebook-flickr/>.

²⁵ „BBC News” (site-ul oficial, UK) URL: <http://news.bbc.co.uk/2/hi/7343238.stm>.

²⁶ „Anima News” (site-ul oficial al agenției de știri, Israel) URL: <http://www.animanews.com/eveniment/tiri/691-armata-israelian-i-a-fcut-divizie-de-facebook.html>.

informații și posibilitate de coordonare, anonimizare, mobilitate, promovare cu costuri reduse) care pot fi, și în multe cazuri sunt, exploatate de către indivizi sau structuri interesate și implicate în activități ce intră în contradicție cu interesele de securitate ale unui stat sau ale comunității în ansamblul său. Arhitectura rețelelor sociale și tipul de comunicare pe care acestea îl presupun sunt compatibile cu noile forme de amenințări asimetrice conștientizate pe scară largă după evenimentele din 11 septembrie 2001.

O platformă de socializare se poate dovedi vehiculul ideal de comunicare între membrii rețelelor teroriste, mesaje criptate sau steganografiate²⁷ putând fi schimbate între membri fără nicio legătură fizică. Lipsa necesității de a declina identitatea reală în mediul virtual poate conferi un nou nivel de anonimizare a comunicării, în spatele unor conturi cu nume fictive putându-se ascunde indivizi cu intenții teroriste sau împotriva securității unor state.

Cenzură

Forumurile de discuții, rețelele precum „Twitter” sau blogurile pot fi utilizate în coordonarea unor proteste, a unor acțiuni de stradă, pentru diseminarea unor informații care să influențeze percepția opiniei publice în legătură cu anumite evenimente sau instituții sau pentru argumentarea ori criticarea unor decizii socio-politice.

Intitulată „prima revoluție web 2.0”²⁸, mișcarea de protest a tinerilor din Chișinău din aprilie 2009 s-a bazat pe platforme precum „Twitter” și „Facebook” pentru a oferi informații în timp real despre evenimentele din capitala Republicii Moldova în condițiile în care guvernul moldovean impusese o restricție mediatică pe canalele clasice (radio, televiziune, presă) cu privire la mișcările de protest.

În iunie 2009, Iranul a blocat accesul protestatarilor iranieni la rețelele online de socializare „Twitter”, „Facebook”, „Flickr” și „YouTube”, folosind un sistem performant de telecomunicații²⁹.

²⁷ Obiectivul steganografiei este de a transmite neobservat un mesaj într-un alt mesaj și nu de a face neinteligibil conținutul acestuia altcuiva.

²⁸ „9am News” (publicație online) URL: <http://www.9am.ro/stiri-revista-presei/International/126977/Prima-revolutie-web-2-0-Protestele-de-la-Chisinau-LIVE-pe-internet.html>.

²⁹ Idem 19.

Grație acestui sistem, serviciile de informații din Iran au putut controla, cenzura și chiar modifica mesajele de telefonie mobilă și mesajele online ale protestatarilor.

Cu ajutorul unei bănci de date a disidenților, serviciile de informații au preluat controlul asupra computerelor și telefoanelor mobile ale acestora, fiind transmise mesaje false pentru a-i induce în eroare pe cei care comunicau cu disidenții.

3. Web 3.0

Următoarea schimbare de paradigmă în ceea ce privește rețelele sociale online este un subiect de interes pentru investitori, utilizatori și persoane interesate de acest mod de interacțiune umană.

Viitoarele rețele de socializare, versiunea „3.0” a celor existente acum, nu au căpătat o formă, nici măcar la nivel de concept, unanim acceptată. Întrebarea „Cum va arăta SNS 3.0?” este una legitimă, cu atât mai mult cu cât platforme cum ar fi „Facebook” sau „LiveJournal” au integrate o multitudine de aplicații oferite de terți (bloguri, jocuri, materiale video).

Manoj Sharma, consultant pe probleme de strategie organizațională din India, este de părere că rețelele sociale se îndreaptă spre imersiunea totală a utilizatorului în mediul virtual, acesta fiind conectat „cradle-to-grave”³⁰.

Cu mult înaintea vremii lui, Isaac Asimov a descris, în cel de-al doilea roman al său, „Soarele Gol” (1957), o societate în care oamenii trăiau izolați, la mari distanțe geografice, iar singura lor formă de comunicare se realiza prin intermediul unei interfețe electronice. La nivel psihologic, acele personaje dezvoltaseră fobii cu privire la contactul uman, evitând cu orice preț expunerea în fața altui om în carne și oase.

Se pare că intuiția autorului de origine rusă s-a apropiat de anumite aspecte ale realității contemporane într-o măsură semnificativă. Un articol scris de Robin-Marie Shepherd și Robert J. Edelman indică faptul că ar putea să existe o legătură între folosirea Internetului pentru socializare și anxietatea socială, anxietatea în general și depresia utilizatorilor³¹.

³⁰ Manoj Sharma (site personal) URL: <http://www.manojsharma.com/keynotes/the-brave-new-world-of-web-3-0-the-next-big-thing-its-integrative-impact-on-the-world-governments-businesses-society-you/>.

³¹ „Science Direct” (site-ul oficial al revistei) URL: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V9F-4G94HHC-2&_user=9292790.

4. Concluzii

Deși există indicii conform cărora rețelele sociale pot avea efecte negative, variind de la aspectele personale până la cele de siguranță a statului, nu trebuie pierdute din vedere numeroasele oportunități pe care acestea le oferă în toate aceste domenii.

Cert este că rețelele sociale online se dovedesc a fi un mediu extrem de interesant, în special din perspectiva securității, oferind noi oportunități de analiză, dar prezentând și pericole de natură să vulnerabilizeze entități oficiale ale oricărui stat.

Bibliografie

1. Albrechtslund, Anders. „Online Social Networking as Participatory Surveillance”, 2008.
2. Backstrom, Lars, Dwork, C. și Kleinberg, Jon. „Wherefore art thou r3579x? Anonymized social networks, hidden patterns, and structural steganography”, 2007.
3. Boyd, Danah și Ellison, Nicole. „Social Network Sites: Definition, History, and Scholarship”, 2007.
4. Ethier, Jason. „Current research in social network theory”, 2009.
5. Gross R., „Re-identifying facial images. Tehnical Report”, 2005.
6. Mika, Peter. „Flink: Semantic web technology for the extraction and analysis of social networks”, Journal of Web Semantics, vol. 3, 2005.
7. Ploderer, Bernd, Howard, Steve și Thomas, Peter. „Being online, living offline: The influence of social ties over the appropriation of social network sites”, 2008.