Riscuri organizaționale asociate instrumentelor *new media*

drd. Mihaela STOICA
Academia Națională de Informații *„Mihai Viteazul”*
stoicamihaela11@yahoo.com

Abstract

In a global competitive environment, facilitated by new media instruments, the organizations can and do take the advantages of technology. However, all those advantages have a lot of other disadvantages, which make the goal achievement more and more difficult. In front of those risks, governments and organizations are taking measures for protecting the infrastructure and to make cyber infrastructure more resilient.

Keywords: new media, social media, management, security strategy.

În 1950, Petre Drucker, în lucrarea sa, *The new society*, a adus în prim plan schimbările care se vor prefigura mai târziu în societatea modernă. În lucrarea sa, Drucker prezintă ideea de *knowledge worker* (lucrătorul al cărui singur capital este cunoaşterea, oameni care gândesc pentru a trăi), un concept care revoluționează știința managementului, prin faptul că aduce în prim plan omul ca factor principal al schimbării în organizație.

Ceva mai târziu, în 1968, Doug Engelbert, cercetător la Stanford Research Institute, preia ideea şi o dezvoltă. Activitatea de cercetare a lui Engelbert duce la crearea unei noi discipline în 1962, „Augmenting Human Intellect: A Conceptual Framework,” în cadrul unui contract cu şeful Information Sciences of the U.S. Air Force Office of Scientific Research.

Concepte precum creşterea potențialului intelectului uman, îmbunătățirea infrastructurii, evoluția artifactelor, practica social culturală a limbajelor, au dus la conceptul de *IQ colectiv*[1]. Acesta spune că IQ-ul colectiv este o măsură a cât de bine pot munci oamenii în probleme importante şi profita de oportunități în mod *colectiv* – cât de repede şi inteligent pot anticipa

[1] http://www.dougengelbart.org/about/collective-iq.html; A Research Center for Augmenting Human Intellect. Douglas C. Engelbart and William K. English, *AFIPS Conference Proceedings of the December 1968 Fall Joint Computer Conference*, San Francisco, CA, Vol.33, pp. 395-410.

sau răspunde la o situație, valorificând percepția, înţelegerea, planificarea, raţionamentul, previziunea, cunoştinţele şi experienţa în valoare colectivă. IQ-ul colectiv este o măsură a eficienței. Este, de asemenea, o măsură a cât de eficient poți combate problemele urgente şi complexe şi cum să ridici IQ-ul colectiv la cel mai înalt potențial, astfel fiind mult mai eficienți în rezolvarea problemelor urgente şi complexe.

Motivația acestui tip de discurs vine din presupunerea că urgența şi complexitatea problemelor vor creşte exponențial iar combinația dintre cele două vor crea adevărate provocări pentru organizație, fie ea publică sau privată.

O primă descriere a interacțiunii sociale care poate fi realizată prin intermediul unei rețele, definită prin conceptul de „galactic network", a fost publicată într-o serie de memo-uri de către J.C.R. Licklider, conducătorul unui program de cercetare la DARPA[2]. El a imaginat o interconectare globală printr-un set de computere prin care fiecare poate accesa date şi programe din orice loc.

Toate aceste teorii au culminat în 1989 când, din dorința de a asigura un management al informațiilor, Berners-Lee a propus pentru prima dată (martie 1989) un sistem de management al informatiilor, care la scurt timp, cu ajutorul lui Robert Cailliau a implementat cu succes prima comunicare HTTP între un client si un server „via Internet".

De la invenția lui Sir Tim Berners-Lee[3] în 1989 şi creşterea sa spectaculoasă, World Wide Web are un profund impact asupra umanității. Acest impact evoluează în mod continuu prin crearea de noi conținuturi, softuri de conectare şi infrastructură[4]. Astfel, acum, nu suntem numai dependenți de drumuri, cabluri de electricitate, conducte de gaze sau de apă, ci şi de rețelele de calculatoare, numite Internet.[5]

„Internetul este în primul rând o capabilitate de transmisiune globală, un mecanism pentru diseminarea informațiilor şi un mediu pentru colaborare şi interacțiune între indivizi şi computerele lor fără constrângeri legate de locația geografică"[6].

---

[2] The Advanced Research Projects Agency (ARPA) şi-a schimbat numele în Defense Advanced Research Projects Agency (DARPA) în 1971, apoi iar în ARPA în 1993, şi iar în DARPA in 1996.

[3] Sir Timothy John (Tim) Berners-Lee (n. 8 iunie 1955) este un programator englez, inventator al World Wide Web-ului. Este actualmente director al World Wide Web Consortium (W3C), organizația ce tutelează standardele Web-ului.

[4] Webindex, Web Foundation's Website: www.webfoundation.org, 2012.

[5] A. G. M. VAN DIJK, 2006, The network society – social aspects of New Media, Second Edition, SAGE Publications, London.

[6] http://www.internetsociety.org/internet/what-internet

Internetul operaționalizează astfel conceptul de IQ colectiv, deschiderea şi interconectarea indivizilor din orice parte a globului făcând ca lucrul colaborativ, cunoştinţele şi experienţa în valoare colectivă să aibă un impact nemaiîntâlnit în istorie. Trebuie avut însă în vedere şi faptul că această colaborare globală nu este întotdeauna în favoarea organizației, ci poate aduce, de multe ori, prejudicii grave, atât financiare, cât şi de imagine.

Riscuri organizaționale asociate instrumentelor New Media

Procesele complexe din cadrul organizației sunt în mod constant favorizate de canalele de informare şi comunicare denumite *new media*. Organizațiile au integrat rapid instrumentele *new media* în diversele departamente. Astfel, acestea pot fi utilizate cu succes în multe din departamentele din cadrul unei organizații, acestea ajutând la scăderea costurilor asociate serviciilor de marketing, e-comerț, intelligence competitiv, relații cu clienții, resurse umane etc.

În ultimele decenii, aceste tehnologii au început să joace un rol tot mai important în acest proces. Organizațiile au devenit atât de dependente de aceste canale încât ele încetează să funcționeze atunci când computerele cedează și rețeaua nu funcționează.[7]

Comerțul online este un segment în continuă creştere. O prognoză privind proiectele de vânzări online în Statele Unite ale Americii arată o creştere de 7 spre 8 procente pe an, ajungând la $250 billioane până în 2014. Vânzările online permit antreprenorilor să facă afaceri repede, cu costuri mici şi cu acces la milioane de potențiali clienți, aceasta încurajând inovația și crearea de noi locuri de muncă.[8]

Conform datelor furnizate de Uniunea Europeană, sunt estimați 150,000 viruși informatici în circulație în fiecare zi şi 148,000 de computere compromise în fiecare zi.[9]

World Economic Forum estimează ca 10% din infrastructura critică de informații să fie în colaps în următoarea decadă, ceea ce ar cauza pierderi de 250 billioane de dolari.

---

[7] Harry BOUWMAN, Bart VAN DEN HOOFF, Lidwien VAN DE WIJNGAERT, Jan VAN DIJK, 2005, *Information &Communication Technology in Organizations Adoption, Implementation, Use and Effects*, First Published In Holland With The Title *Ict In Organisaties. Adoptie, Implementatie, Gebruik En Effect.*Amsterdam, Boom Uitgeverij, 2002, Sage Publications, London · Thousand Oaks · New Delhi, p. 41.

[8] http://www.nist.gov/nstic/business.html

[9] http://europa.eu/rapid/press-release_IP-13-94_en.htm

Criminalitatea informatică cauzează incidente de securitate cibernetică. Symantec estimează că victimele criminalității informatice în lume pierd 290 bilioane de euro în fiecare an, în timp ce un studiu realizat de McAfee estimează profiturile din criminalitatea informatică la 750 de bilioane de euro în fiecare an.[10]

Într-un studiu coordonat de Comisia Europeană, numit Eurobarometrul 390[11], privind securitatea cibernetică, se menționează faptul că 38% din utilizatorii de Internet şi-au schimbat comportamentul online din cauza îngrijorării privind securitatea cibernetică: 18% spun că este puțin probabil să mai facă cumpărături online iar 15% spun că este puțin probabil să folosească online banking. De asemenea, 74% din respondenți sunt de părere că riscul de a deveni o victimă a crescut, 12% deja au experimentat fraudele online şi 80% evită să dezvăluie informații personale.

Cu toate acestea, cifrele Eurostat arată că în ianuarie 2012 doar 26% din întreprinderile din Uniunea Europeană şi-au definit o politică de securitate a infrastructurii de tehnologie şi comunicații.

Creşterea tranzacțiilor online face accesul criminalilor cibernetici mult mai facil ca înainte, existând astfel riscuri majore în ceea ce priveşte furtul de identitate, furtul de proprietate intelectuală şi altele. Impactul amenințărilor de securitate cibernetică poate fi ierarhizat în trei componente majore:

- *Impactul politic, economic şi social*
- *Impactul asupra infrastructurii şi comunicațiilor instituționale*
- *Impactul asupra vieții şi securității personale.*

Strategii organizaționale de gestionare a riscurilor cibernetice

În acest context fragil al piețelor influențate de numeroase atacuri atât la nivel guvernamental, cât şi la nivelul organizațional favorizate de infrastructura cibernetică, organizațiile trebuie să ia propriile măsuri de protecție. Precizăm aici două moduri în care organizațiile pot gestiona riscurile asociate new media.

➢ ***Adoptarea politicilor de utilizare a social media***

În ultimii ani printr-o reţea socială se înţelege deseori şi o reţea (informaţională) de utilizatori Internet, bazată pe anumite site-uri web la care utilizatorii se pot înscrie şi interacţiona cu alţi utilizatori, deja înscrişi.

[10] http://europa.eu/rapid/press-release_IP-13-94_en.htm

[11] Special Eurobarometer 390 / Wave EB77.2 – TNS Opinion & Social, Survey co-ordinated by the European Commission, Directorate-General for Communication, (DG COMM "Research and Speechwriting" Unit), European Comission, 2012, p. 4.

Aceste reţele sociale fac parte din fenomenul relativ nou, global, numit Web 2.0. Astfel, membrii unei reţele sociale sunt legaţi între ei în mod informal, fără obligaţii, dar de obicei contribuie activ la colectarea şi răspândirea informaţiilor pe întregul glob prin intermediul web-ului. Eventual denumirea unei astfel de reţele (informaţionale) de utilizatori s-ar putea echivala cu „reţea internautică de utilizatori".

Pe lângă avantajele acestor reţele, care facilitează de exemplu întrajutorarea membrilor, formarea de noi cunoştinţe şi prieteni, răspândirea rapidă a ştirilor şi zvonurilor („bârfelor"), aceste reţele ascund şi pericole, deoarece de obicei nu se declară explicit care e sursa informaţiilor, cine este furnizorul de servicii, şi nici dacă acesta intenţionează să utilizeze informaţiile şi în alte scopuri.

Lipsa de reglementări clare deschide poarta pentru abuzuri grave asupra datelor private sau chiar secrete ale utilizatorilor, fie ale individului sau ale organizației.

În ultimii ani comunicarea prin reţelele sociale are consecinţe din ce în ce mai vizibile, chiar şi pe plan mondial, consecințe care se reflectă în mod indubitabil şi asupra mediului economic. Analiştii sunt de părere că fără reţele sociale evenimentele s-ar fi desfăşurat altfel. Câteva exemple de evenimente (2011) influenţate puternic de comunicaţia prin reţele sociale:

- Protestele din Egipt care au dus la demisia lui Hosni Mubarak, preşedintele statului.
- Revolta populară din Tunisia care a dus la răsturnarea preşedintelui Zine El Abidine Ben Ali.
- Dovedirea de plagiate, ca de ex. lucrarea de doctorat a fostului ministru al apărării din Germania, graful Karl-Theodor zu Guttenberg.
- Convocarea publicului la diverse întruniri sau chiar demonstraţii poate fi uşurată; de exemplu s-au înmulţit aşa-numitele *facebook parties* (singular: *facebook party*).
- Alegerile din Moldova, influențate puternic de comunicarea pe Twitter, căpătând chiar denumirea de „revoluția Twitter".
- Influența tot mai mare a consumatorului asupra produselor organizației, ceea ce poate duce foarte uşor la o criză a organizației care se poate solda o criză de imagine şi în final cu pierderi materiale.

În aceste condiții, organizațiile trebuie să aibă în vedere faptul că Internetul creează o expunere fără precedent şi că trebuie luate măsuri prin care această expunere trebuie să fie gestionată în aşa manieră încât să aducă beneficii organizației.

Datorită influenței în creştere pe care *social media* o are în asigurarea securității informațiilor organizațiilor, tot mai multe organizații au simțit nevoia de a crea un cadru formal de utilizare a *social media* în organizație, dar şi în afara acesteia.

Astfel, companiile au început implementarea unor politici de utilizarea a platformelor *social media*, pentru a se proteja de expunerea informațiilor confidențiale pe acestea. Spre exemplu, Dell[12] avertizează angajații în legătură cu faptul că nerespectarea principiilor de utilizarea a *social media* de către un angajat al companiei poate avea consecințe serioase care pot duce la terminarea contractului în acord cu legile din țara unde este angajatul. Câteva din aceste principii ar fi: protejarea informațiilor, respectarea legilor şi a codului de conduită, asumarea răspunderii.

În Online Social Media Principles ale Coca Cola Company[13], se admite importanța participării la conversațiile online şi se prevede faptul că aceste conversații trebuie să aibă loc în mod corect. Astfel, principiile au fost dezvoltate pentru a ajuta asociații de a participa la această nouă frontieră de marketing si comunicare, care reprezintă firma şi partaja spiritele optimiste şi pozitive ale mărcilor sale.

- ***Implementarea standardelor de management al informațiilor***

În condițiile creşterii numărului de tranzacții online, organizațiile trebuie să implementeze standarde de securitate a informațiilor, pentru a conferi o credibilitate crescută beneficiarilor.

Implementarea standardelor de securitate a informațiilor poate avea câteva avantaje, cum ar fi: [14]

- credibilitatea, integritatea si încrederea conferită clienților, angajaților, partenerilor contractuali şi proprietarilor ca informațiile şi sistemele informatice ale companiei sunt protejate;
- conferirea dovezii pentru autorități că sunt respectate legile si reglementările în vigoare;
- asigurarea unui plan de continuitate al afacerii şi de recuperare din dezastru, adecvat organizației;
- creşterea productivității prin reducerea riscurilor operaționale şi o mai mare disponibilitate în exploatarea sistemelor informatice;

[12] http://www.dell.com/Learn/us/en/uscorp1/corp-comm/social-media-policy?c=us&l=en&s=corp&delphi:gr=true

[13] http://www.coca-colacompany.com/stories/online-social-media-principles

[14] http://srac.ro/srac.php?id=162&meniu=1

- diferențierea față de alți competitori în cadrul licitațiilor organizate în cadrul sectorului public sau la încheierea unor contracte comerciale, care implică accesul la informații sau chiar secrete de stat.

Strategii internaționale de gestionare a riscurilor cibernetice

În condițiile în care mediul economic este profund afectat de schimbările rapide şi dependența de mediul online, guvernele au trebuit să stabilească măsuri pentru reglementarea acestuia.

Revelatoare din acest punct de vedere este *Strategia americană de securitate*, în care se specifică faptul că „Amenințările cibernetice asupra securității statului reprezintă una dintre cele mai serioase amenințări asupra securității naționale, a siguranței publice şi a provocărilor economice pe care le facem față ca națiune. Tehnologiile variate care ne împuternicesc pe noi să conducem şi să creăm, de asemenea împuternicesc pe cei care vor să disturbe şi să distrugă… Internetul şi comerțul electronic sunt chei ale competitivității noastre economice, dar criminalii cibernetici costă companiile şi consumatorii milioane de dolari şi o valoroasă proprietate intelectuală”[15].

În decembrie 2012, a fost actualizată poziția SUA privitor la amenințările cibernetice, ea fiind considerată cea mai mare amenințare, fiind pe locul întâi în ceea ce priveşte securitatea țării, surclasând şi terorismul internațional.

Astfel, SUA decide să acționeze în două direcții majore pentru crearea de rețele sigure, de încredere şi reziliente:

- ***Investițiile în oameni şi tehnologie***: pentru a avansa acest obiectiv se lucrează în cadrul guvernului şi cu sectorul privat pentru a proiecta tehnologii mai sigure care să dea abilitatea de a proteja mai bine şi de a îmbunătății reziliența sistemelor şi rețelelor critice ale guvernului şi a industriei. Astfel se urmăreşte intensificarea investițiilor în elementele active de cercetare şi dezvoltare necesare pentru inovare şi dezvoltare de care este nevoie pentru preîntâmpinarea aceste provocări şi se lansează o campanie națională de promovare cuprinzătoare pentru conştientizarea problemelor de securitate cibernetică şi de instruire de la nivelul conducerii până la nivelul sălilor de clasă şi de construire a forței de muncă digitale pentru secolul XXI.
- ***Parteneriate puternice***: extinderea parteneriatelor internaționale la mai multe categorii de probleme, incluzând dezvoltarea unor norme

[15] National Security Strategy, pag. 27-28, The White House, Washington, SUA, May 2010.

de conduită acceptabilă în cyberspațiu; legi care privesc criminalitatea cibernetică; protejarea datelor, protecția şi zona privată; şi abordări privind apărarea rețelelor şi răspunsul la atacurile cibernetice; colaborarea cu toți actorii cheie – incluzând toate nivelurile sectoarelor guvernamental şi privat, naționale şi internaționale – pentru a investiga intruziunile cibernetice şi de a asigura un răspuns organizat şi unitar pentru incidentele cibernetice. Planurile şi resursele alocate vor trebui făcute anticipat în acelaşi mod în care se operează pentru dezastrele naturale.[16]

În concordanță cu Strategia Casei Albe de promovare a culturii de securitate cibernetică a fost creat *National Strategy for Trusted Identities in Cyberspace (NSTIC),* o inițiativă a Casei Albe de lucru colaborativ cu sectorul privat, cu grupurile de susținere, agențiile sectorului public şi alte organizații pentru îmbunătățirea securității, secretelor şi utilității tranzacțiilor online.

Această Strategie conduce spre dezvoltarea standardelor şi politicilor de interoperabilitate a tehnologiilor, numit "Identity Ecosystem", în care indivizii, organizațiile şi infrastructura aferentă – cum ar fi ruterele şi serverele - să fie în mod automat autentificate. Scopul acestei Strategii este acela de a proteja indivizii, afacerile şi agențiile publice de costurile ridicate asociate cybercrimei, cum ar fi furtul de identitate şi fraudele, ajutând în acelaşi timp ca Internetul să fie un suport pentru inovare şi piață înfloritoare pentru produse şi idei. [17].

Uniunea Europeană se aliniază şi ea eforturilor de prevenire a riscurilor. Astfel, în 07/02/2013, a fost elaborată şi strategia Uniunii Europene de protecție a libertăților şi oportunităților Internetului (EU Cybersecurity plan to protect open internet and online freedom and opportunity)[18]. Strategia europeană concretizează viziunea Europei asupra securității cibernetice în termen de cinci priorități:

- Realizarea rezilienței cibernetice.
- Reducerea drastică a criminalității informatice.
- Dezvoltarea politicilor de apărare şi a capacităților legate de politica de securitate şi apărare comună asupra amenințărilor cibernetice (PSAC) – Common Security and Defence Policy (CSDP).
- Dezvoltarea resurselor industriale şi tehnologice pentru securitatea cibernetică.

[16] National Security Strategy, pag. 27-28, The White House, Washington, SUA, May 2010.
[17] http://www.nist.gov/nstic/about-nstic.html
[18] http://europa.eu/rapid/press-release_IP-13-94_en.htm, accesat aprilie 2013

- Stabilirea unei politici internaționale coerente pentru Uniunea Europeană şi pentru promovarea valorilor acesteia.

În conformitate cu aceste principii, Uniunea Europeană a stabilit un Centru pentru Cybercriminalitatea în Europa (European Cybercrime Centre)[19], deschis la 11 ianuarie 2013 cu sediul la Haga, şi a propus legislație privind atacurile împotriva sistemelor informatice.

România s-a aliniat acestei politici de asigurare a securității cibernetice, urmare a politicilor internaționale în acest sens. Astfel, în februarie 2013, într-un anunț de presă postat pe site-ul preşedenției României a fost anunțat faptul că Consiliul Suprem de Apărare a Țării a aprobat Strategia de Securitate Cibernetică „care vizează implementarea unor măsuri de securitate care să conducă la creşterea nivelului de protecție a infrastructurilor cibernetice în concordanță cu noile concepte şi politici din domeniul apărării cibernetice elaborate si adoptate la nivelul NATO şi al Uniunii Europene”[20] . Ulterior, aceasta a fost publicată într-o hotărâre de guvern, HG 271 din 23 mai 2013.

Concluzii

Într-un mediu competițional global, favorizat de apariția şi dezvoltarea fără precedent a instrumentelor *new media*, fapt care duce spre o globalizare a comerțului şi serviciilor, guvernele, organizațiile şi indivizii se confruntă şi cu numeroase riscuri pe care trebuie să le gestioneze.

Implementarea politicilor guvernamentale, influențate de procesele birocratice, nu pot ține pasul cu dezvoltarea fără precedent a acestor tehnologii. Aşa cum sublinia Alvin Toffler, „Guvernele şi instituțiile parlamentare ale celui de-Al Doilea Val au fost concepute pentru adoptarea deciziilor fără grabă, în pas cu o lume în care era nevoie de o săptămână pentru ca un mesaj să ajungă de la Boston sau New York la Philadelphia. Astăzi, însă, dacă un ayatollah reține ostateci la Teheran sau strănută la Qom, conducătorii de la Washington, Moscova, Paris sau Londra trebuie uneori să reacționeze cu decizii în câteva minute”[21].

Astfel, organizațiile trebuie să îşi dezvolte propriile sisteme de rezistență şi reziliență la riscurile asociate acestora, implementând sisteme şi politici care să le protejeze.

[19] http://europa.eu/rapid/press-release_IP-13-13_en.htm, accesat aprilie 2013
[20] http://www.presidency.ro/?_RID=det&tb=date&id=14152&_PRID=search
[21] TOFFLER, Alvin, 1980, Al treilea val, Antet XXpress şi Lucman, Grupul drago print, Bucureşti.

Bibliografie

1. A. G. M. van Dijk, *The network society –social aspects of New Media*, Second Edition, SAGE Publications, London, 2006.

2. Harry Bouwman, Bart Van Den Hooff, Lidwien Van De Wijngaert, Jan Van Dijk, 2005, *Information &Communication Technology in Organizations Adoption, Implementation, Use and Effects*, First Published In Holland With The Title *Ict In Organisaties. Adoptie, Implementatie, Gebruik En Effect.*Amsterdam, Boom Uitgeverij, 2002, Sage Publications, London · Thousand Oaks · New Delhi, p. 41.

3. http://europa.eu/rapid/press-release_IP-13-13_en.htm
4. http://europa.eu/rapid/press-release_IP-13-94_en.htm
5. http://europa.eu/rapid/press-release_IP-13-94_en.htm
6. http://europa.eu/rapid/press-release_IP-13-94_en.htm
7. http://srac.ro/srac
8. http://www.coca-colacompany.com/stories/online-social-media-principles
9. http://www.dell.com/Learn/us/en/uscorp1/corp-comm/social-media-policy
10. http://www.dougengelbart.org/about/collective-iq.html; A Research Center for Augmenting Human Intellect. Douglas C. Engelbart and William K. English, *AFIPS Conference Proceedings of the December 1968 Fall Joint Computer Conference*, San Francisco, CA, Vol.33, pp. 395-410.
11. http://www.internetsociety.org/internet/what-internet
12. http://www.nist.gov/nstic/about-nstic.html
13. http://www.nist.gov/nstic/business.html
14. http://www.presidency.ro/
15. National Security Strategy, pag. 27-28, The White House, Washington, SUA, May 2010.
16. Special Eurobarometer 390 / Wave EB77.2 – TNS Opinion & Social, Survey co-ordinated by the European Commission, Directorate-General for Communication, (DG COMM "Research and Speechwriting" Unit), European Comission, 2012, p. 4.
17. Toffler, Alvin, *Al treilea val*, Editura Antet XXpress şi Lucman, Grupul Drago Print, Bucureşti, 1980.
18. Webindex, Web Foundation's Website: www.webfoundation.org, 2012.