SOCIALNA OMREŽJA Z VIDIKA VARNOSTI IN ZASEBNOSTI

Social networks from security and privacy point of view

mag. Marko Potokar
Predsednik sveta, IVK inštitut za varnostno kulturo
marko.potokar@instiut-ivk.si

Povzetek

V članku so na kratko predstavljena spletna družbena omrežja in mreženje ter internet in svetovni splet, kot platformi, ki sta te pojave omogočili. Po predstavitvi kratke zgodovine in delovanja interneta ter svetovnega spleta, se članek osredotoči na družbeno mreženje in njegove vplive v sodobni družbi. V zadnjem delu članka obravnavamo vprašanja varnosti in nadzora omenjenih pojavov.

Ključne besede: *socialna omrežja, internet, splet, varnost, zasebnost.*

Abstract

The article represents the online social networks and issues regarding security and privacy when using them for communication between individuals and groups. After the basis of the Internet and the World Wide Web, as a platforms that made these phenomena possible are presented., the article refers to social networking and its influence in modern society. In the last part of the article security and privacy issues of mentioned phenomena are discussed.

Keywords: *Social network, Internet, World Wide Web, Security, Privacy.*

Uvod

Živimo v svetu tehnologije in informacij. V zadnjih desetletjih so informacijske tehnologije prodrle na vsa področja našega življenja in močno vplivale na številne vidike, ki prej niso bili tako pomembni. Države, organizacije in ljudje smo tesno povezani z informacijsko tehnologijo in mnogo ključnih procesov in infrastruktur je odvisnih od informacijskih sistemov, ki temeljijo na visoko razvitih tehnologijah. S širjenjem informacijskih tehnologij

imajo ljudje priložnost, da proizvajajo in dostopajo do ogromne količine informacij, delijo znanje in zamisli hitreje kot kadarkoli prej, se povezujejo na različnih družbenih omrežjih. Internet in Web 2.0 sta pojava, ki ponujata možnost osvobajanja. Skupaj s televizijo, sateliti in mobilnimi telefoni so računalniki, povezani v mrežo, igrali pomembno vlogo pri globalizaciji informacijskih sistemov. Toda globalna povezanost omrežij in informacijskih sistemov je močno vplivala na področje varnosti in zasebnosti informacijskih sistemov. Z vsakim korakom, ki ga naredimo na svetovnem spletu, za seboj pustimo digitalno sled. Vsakokrat, ko uporabljamo internetne storitve, npr. Google search, vsakokrat, ko uporabljamo kreditne kartice ali pošiljamo elektronsko pošto, je lahko na preži predator, ki želi zlorabiti informacije, poslane prek interneta. Možnosti za pobiranje informacij in njihova uporaba za nadzor urejanja in organiziranja ljudi in krajev so nepredstavljive. Nadzor je postal skrit, neviden in skoraj neizsledljiv.

1. Internet in svetovni splet

Družbeno mreženje je postalo tako široko razširjen pojav zaradi razvoja tehnologije. Kritična točka je bila presežena z razvojem novih komunikacijskih tehnologij, danes poznanih kot informacijske tehnologije (IT). Po drugi svetovni vojni so se v svetu telekomunikacij spremenile tri stvari: telefonske tehnologije same po sebi (uporaba mobilnih telefonov, optičnih vlaken in brezžične komunikacije), kombinacija telekomunikacij in računalniškega hranjenja in obdelave ter prehod k zasebnim telekomunikacijskim podjetjem. Te spremembe pomenijo naraščanje konvergence tehnologij in interoperabilnost. In z razvojem tehnologije je prišel internet.

1.1. Internet

Internet je več medsebojno povezanih računalnikov. To je omrežje manjših omrežij in spletnih strani, ki vsebuje mnogo različnih informacij. To je omrežje omrežij. Obstajata dve sočasni zgodbi o tem, kako in zakaj je nastal internet.

Ena je s civilnega področja: Znanstveniki so imeli potrebo po hitrejši izmenjavi svojih novih odkritij, zato so zasnovali omrežje za standardizirano komunikacijo med računalniki. Prvo sporočilo je bilo poslano prek ARPANET-a med Univerzo Kalifornija, Los Angeles (UCLA) in Raziskovalnim institutom Stanford. Druga zgodba je manj romantična: Internet je leta 1969 ustanovila Agencija za višje raziskovalne projekte ameriškega obrambnega ministrsta,

poznana kot DARPA. Projekt je nastal iz strahu pred jedrsko vojno; ministrstvo za obrambo je želelo ustvariti telekomunikacijski sistem, ki bi preživel morebitni jedrski napad.

Na začetku je bil namen interneta izmenjava datotek med računalniki. Računalniki komunicirajo z izmenjavo sporočil prek mehanizma, imenovanega protokoli. Protokoli so algoritmi, podrobna pravila, ki natančno pojasnujejo, kako izmenjati določen niz sporočil. Ker je komunikacija med računalniki in drugimi omrežnimi napravami izredno zapletena dejavnost, ne preseneča, da je bilo za uporabo osnovnega interneta potrebno veliko tehničnega znanja. Uporaba interneta je narasla z razvojem računalniških programov, imenovanih spletni brskljalniki. Spletni brskljalniki so uporabniški vmesniki (programske aplikacije), ki uporabniku omogočajo, da dostopa, pridobiva in gleda dokumente ter druge vire in storitve na internetu skoraj brez računalniškega znanja. Prvi brskljalnik so izumili leta 1990 in ga poimenovali WorldWideWeb (pozneje preimenovan v Nexus). Leta 1993 so program brskljalnika prenovili z izdajo Mosaica (pozneje Netscape), prvega poljudnega brskljalnika, s katerim je World Wide Web postal bolj dostopen in enostaven za uporabo povprečnemu uporabniku interneta. Za javnost so ga izdali leta 1995. Najbolj znani spletni brskljalniki so Internet Explorer, Firefox, Chrome, Safari, Opera itd.

Internet se uporablja za različne stvari, ki se imenujejo storitve: prenos datotek, elektronska pošta, takojšnje sporočanje, spletno klepetanje, dostopanje do dokumentov in spletnih strani World Wide Weba, imenovanega tudi Web. Web je najbolj uporabljana storitev interneta. Vsebuje bloge, wiki-je (kot je Wikipedia) in druge spletne strani.

Danes je internet postal ogromen sistem sprotnih informacij, zabave, trgovine in družbenih omrežij.

1.2. World Wide Web

Termin World Wide Web ponavadi napačno uporabljamo za internet. World Wide Web je samo ena od storitev, ki jih zagotavlja internet, vendar ena najbolj uporabljanih. Ustvarili so ga leta 1990, leta 1993 so ga izdali za javnost. Decembra 1990 je bila na WWW ena spletna stran, decembra 2000 jih je bilo 25.675.581, novembra 2006 101.435.253, novembra 2011 že skoraj 600.000.000 (Robert Zakon, Internetna časovnica, http://www.zakon.org/robert/internet/timeline/#Growth). V preteklih letih se je internet preoblikoval iz sistema za deljenje in zagotavljanje informacij v komunikacijski medij, ki gradi skupnost, imenovan »družbeni medij«. World Wide Web je postal družbena programska oprema, poznana kot »web 2.0« ali »družbeni splet«, s storitvami kot so deljenje datotek,

wiki-ji, blogi, spletne strani, spletne strani z določeno vsebino, ki jih ustvarijo uporabniki, in strani družbenega mreženja, kot npr. Twitter, MySpace in Facebook. Z web 2.0 ljudje oblikujejo svoja lastna omrežja medsebojne komunikacije, povečali so možnost medsebojnega sodelovanja in skupnega delovanja. Termin »web 2.0« ne pomeni, da imamo opravka s popolnoma novim internetom. Najbolj priljubljene dejavnosti na internetu so še vedno elektronska pošta in iskanje informacij o izdelkih in storitvah. Na internetu je še vedno veliko 'starih' dejavnosti in platform, npr. spletno bančništvo, spletno nakupovanje, spletni časopisi, iskalniki itd. Nove dimenzije na internetu so današnje World Wide Web platforme, kot npr. YouTube, Wikipedia, Facebook, Twitter in Blogger, ki so med desetimi najbolj obiskanimi spletnimi stranmi na svetu. Razmeroma nove dejavnosti na web 2.0 soustvarjajo znanje z drugimi, npr. Wikipedio, delijo avdio in video vsebine z drugimi, pišejo bloge (spletne dnevnike), vzdržujejo stik s prijatelji in mikroblogajo (delijo kratka sporočila na spletu). S terminoma »družbeni mediji« in »web 2.0« mislimo na določene družbene značilnosti, kot sta spletno sodelovanje in objavljanje, ki sta se pojavila in ju podpira World Wide Web.

Platforme web 2.0 se imenujejo platafrme družbenih medijev. Te platforme temeljijo na spletu in podpirajo spletno izgradnjo in vzdrževanje skupnosti, skupno proizvajanje informacij, družbeno mreženje in proizvajanje vsebin s strani uporabnikov. Značilne platforme družbenih medijev so Google, Wikipedia, Facebook, LinkedIn, MySpace, YouTube (deljenje videoposnetkov), Flickr (deljenje fotografij), Blogger, Rapidshare, Wordpress, Skyrock, Friendster, YouPorn, PornHub, Youku, Photobucket, Twitter, Megavideo, Tagged, Tube8, Mediafire, Megaupload, Mixi, Metacafe, Digg, Livejournal, Netlog, ThePirateBay, Orkut, XVideos, StudiVZ, Adultfriendfinder, Orkut, Redtube, če jih imenujemo samo nekaj.

Kot skoraj vsi drugi tehnološko-družbeni sistemi, je tudi web 2.0 protisloven pojav. Družbeno mreženje nima enodimenzionalnega učinka, ampak zapletene medsebojno povezane vplive. Web 2.0 temelji na zbiranju in shranjevanju, uporabi in analizi ogromne količine informacij in osebnih podatkov. Analiziranje varnostnih vprašanj na spletu je postalo ključnega pomena. Razprava o zasebnosti in nadzoru spleta ter gospodarskem, kulturnem in političnem vplivu komunikacije in sodelovanja prek družbenih omrežij na web 2.0 je postala pomembna stvar.

2. Pojav družbenih omrežij

Družbena skupina je definirana kot dva ali več ljudi, ki drug z drugim komunicirajo, imajo podobne značilnosti in občutek enotnosti (Wikipedia.org). Družbene skupine lahko obstajajo

kot osebne in neposredne družbene vezi, ki povezujejo posameznike z enakimi vrednotami in prepričanji, ali kot neosebne (anonimne), formalne in instrumentalne družbene vezi.

Termin "družbeno omrežje" se uporablja za opis družbene strukture, ki jo določajo odnosi med posamezniki, skupinami, organizacijami ali celo celotnimi družbami. Družbena omrežja se sama organizirajo in so zapletena. Obstaja veliko različnih vrst povezav, posameznih ali v kombinaciji. Pristop družbenega omrežja k razumevanju družbene interakcije se dojema in raziskuje prek lastnosti odnosov med skupinami in znotraj njih.

Ločimo tri ravni omrežij: mikro, mezo in makro. Omrežja na mikro ravni so sestavljena iz nekaj posameznikov. Družbeno razmerje med dvema posameznikoma se imenuje diada. Lastnosti diad so struktura razmerja, družbena enakost in težnje po recipročnosti oz. vzajemnosti. Triada je družbena skupina, ki povezuje tri posameznike. V triadi analiziramo dejavnike ravnovesja in prehodnosti. Mezo raven označuje velikost populacije, ki se umešča med mikro in makro raven. Na makro ravni analiziramo rezultate interakcij gospodarskega in drugih prenosov na veliki populaciji.

Ko se je internet iz sistema za deljenje in iskanje informacij preoblikoval v sistem, ki je bolj usmerjen v komunikacijo in izgradnjo skupnosti, so se pojavili pojmi »strani družbenih omrežij« in »spletne skupnosti«. Termin »skupnost« definira določeno družbeno skupino, ki ima skupne vrednote. Pri vezeh skupnosti gre za to, kdo je s kom govoril, trgoval ali bil z njim povezan. Spletna skupnost (spletno družbeno omrežje) je razširjena skupnost, ki se je razvila prek telekomunikacijskih naprav in storitev družbenega omrežja.

Termin »spletno družbeno mreženje« lahko opišemo kot način, da se ena oseba dobi(va) z drugimi osebami na internetu. Ljudje uporabljajo spletne strani za spoznavanje novih prijateljev, komuniciranje z ljudmi, ki imajo enaka zanimanja ali enake težave. Družbena omrežja se uporabljajo za iskanje novih priložnosti v karieri, novih služb, uporabljajo jih politični aktivisti in teroristi. Storitve spletnega družbenega mreženja omogočajo, da se med seboj povežejo ljudje, ki si delijo enaka zanimanja in dejavnosti, preko političnih, gospodarskih in geografskih meja.

Strani družbenega mreženja so pokazale vrednost v družbenih in političnih gibanjih. Na primer Facebook, Twitter in nekatere druge spletne strani družbenega mreženja so igrale osrednjo vlogo pri povezovanju ljudi v upor v egipčanski revoluciji. Egipčanski aktivisti so uporabljali družbena omrežja ko platformo za načrtovanje protesta in sporočanje novic s trga Tahrir v realnem času. Družbeno omrežje je predstavljalo platformo tisočim ljudem, da so

sočasno delili videoposnetke glavnih dogodkov egipčanskega upora, ki so prikazovali krutost in nasilje. Očitno je, da se družbeno mreženje lahko uporablja kot ključno orodje/pripomoček v revolucijah in drugih množičnih (človeških) dogodkih.

3. Vprašanje varnosti na internetu

S pojavom družbenih omrežij in razvojem različnih spletnih družbeno-omrežnih storitev pride do množične zagotovitve in shranjevanja osebnih podatkov. Ti podatki se sistematično zbirajo, analizirajo, vrednotijo, tržijo in uporabljajo za ciljanje na uporabnike. V svetu globalne gospodarske krize in strahu pred terorizmom imajo tako korporacije kot državne ustanove velikanski interes za dostopanje do teh osebnih podatkov. Gre za vprašanje varnosti in zasebnosti v zvezi s komercialnim zbiranjem podatkov s pomočjo oglaševanja, spletnih strani za potrošnike in interaktivnih medijev, samorazkritjem na družbenem omrežju, nadzorom tistih, ki delijo datoteke, nadzorom državljanske straže na družbenih omrežjih in interaktivnim nadzorom v meddržavnem prostoru. Napredek digitalnih komunikacijskih tehnologij je posameznikom in skupinam ponudil sodobno in močno orodje, ki podpira različne družbene dejavnosti, legalne in nelegalne, dobre in slabe. S tehnologijami Web 2.0, ki so zasnovane z namenom, da bi stopnjevale širjenje informacij in sodelovanje med uporabniki interneta, je prišlo do razvoja spletnih skupnosti, kot so spletna omrežja MySpace in Facebook, YouTube in priljubljene strani z blogi.

Akdeniz (2009, 14-15) navaja, da so maja 2008 v poročilu Centra Simona Wiesenthala z naslovom "Online Terror and Hate: The First Decade" (Spletno nasilje in sovraštvo: Prvo desetletje) opozorili, da "ekstremisti uporabljajo tehnologije 2.0, s pomočjo katerih dinamično ciljajo na mlade ljudi prek digitalnih iger, scenarijev Second Life, blogov in celo videoposnetkov v slogu YouTubea in Facebooka, ki prikazujejo rasistično nasilje in terorizem". Aprila 2008 je članek v New York Timesu razkril, da "je med milijoni klipov na spletni strani za deljenje videoposnetkov YouTube 11 rasno žaljivih risank Warner Brothers, ki od leta 1968 niso bile prikazane v avtorizirani izdaji". Rasistične ideje in sovražni govor so prisotni na socialnih omrežjih Facebook in MySpace. Internetne igre kot npr. Second Life in World of Warcraft se uporabljajo za širjenje rasističnih vsebin. Lahko rečemo, da rasistične in teroristične skupine uporabljajo internet kot medij za propagando, novačenje, urjenje in komuniciranje.

Mednarodne organizacije in nadzorniki na državni ravni se soočajo s pomembnim vprašanjem, kako nadzorovati tok sovražnega govora, rasističnih in terorističnih vsebin na internetu. Dejstvo, da v različnih državah obstajajo različne moralne, kulturne, politične in

ustavne vrednote, samo poveča napore v iskanju ravnotežja med pravicami do svobode mnenja in izražanja ter prepovedjo govora, ki spodbuja nelegalne dejavnosti, kot sta rasizem in nasilje. Kot pravi Čaleta (2012, 5), določene družbene skupine in posamezniki izražajo svoja mnenja na popolnoma neciviliziran način – s terorističnimi dejanji, žrtve teh dejanj pa so v večini primerov nedolžni ljudje. Dolžnost vlade je, da uporabi vsa zakonita sredstva za varno in normalno delovanje države. In eden od teh ukrepov so nadzorni sistemi.

4. Nadzor na internetu

V prejšnjih poglavjih smo videli, da so se s preobrazbo interneta iz sistema za deljenje datotek in iskanje informacij v ogromen sistem spletnih informacij, zabave, trgovine in družbenih omrežij pojavile nove storitve, imenovane družbena spletna aplikacija. Z Web 2.0 je internet postal svet, ki povezuje posameznike bolj kot kateri koli drug medij v zgodovini. Internet je postal nov medij za informacije in komunikacijo. Toda med dobrimi in plemenitimi stvarmi, ki jih je internet nedvomno omogočil, je nekaj manj prijetnih ali celo nevarnih zadev, ki se dogajajo na področju tega medmrežja: otroška pornografija, sovražni govor in teroristična propaganda so zagotovo med njimi. Obstaja pa še en pojav, ki predstavlja varnostno vprašanje in je prepogosto neopažen. Imenuje se nadzor.

Nadzor je ena glavnih težav na internetu. Ne, da ga prej ne bi imeli. Nadzor imamo, odkar se je človeška vrsta začela združevati v skupine. Razlika je v tem, da je zdaj nadzor skrit, neopažen in neizsledljiv. Istočasno puščamo za seboj elektronske sledi z vsako transakcijo, ki jo opravimo na internetu: klepetamo s prijateljem, pošiljamo pozdrave kolegom po elektronski pošti, napišemo komentar na blogu, kliknemo na gumb 'všeč mi je' na Facebooku, naročimo knjigo, plačamo izdelek v spletni trgovini, uporabljamo Skype za pogovor z ljubljenimi osebami itd. Nadzor sam po sebi ni slaba stvar. Prepreči lahko slabe stvari, pomaga policiji, da ulovijo zlikovce, prepreči teroristom, da bi dosegli svoj cilj, lahko nam reši življenja. Težava nastane, ko vladne, varnostne in policijske organizacije nadzor zlorabijo. Procesi korporativnega in političnega nadzora na internetu lahko delujejo kot sistemi za utišanje ljudi. Neopazen, nezaznaven nadzor posameznikov, skupin in velikih populacij lahko utiša nasprotovanje. Internet lahko vidimo kot velik Panoptikon. Toda po drugi strani obstaja nevarnost, da tisti, ki so običajno tarča nadzora – 'zlikovci' – lahko obrnejo oči in ušesa nadzornega stroja v obratno smer, v internetni protinadzor. Z Web 2.0 in nadzorom na internetu je prišlo še do enega pojava. Internetni protest je izraz civilne družbe in aktivizem družbenega gibanja. Nadzor kot politični pojav je bil vedno povezan z vzponom in dejavnostmi državljanskih skupin. Internet na splošno in zlasti web 2.0 povzročata

določene okoliščine za dejavnosti družbenega gibanja, ki so povezane s politično temo nadzora.

Nadzor v virtualnem svetu lahko razdelimo na tri glavne oblike: nadzor, ki je povezan z zaposlitvijo, nadzor, povezan s trženjem in nadzor, povezan z varnostjo. Zgodovinsko je (bil) nadzor delovnih mest in zaposlenih osrednji vidik gospodarskega nadzora. Medtem ko nadzor s strani delodajalcev, npr. nameščanje sledilnih naprav v službena vozila, pri zaposlenih lahko vzbudi občutek, da jim delodajalci ne zaupajo, lahko nadzor, ki se uporablja v trženjske namene, dojemamo kot manj škodljiv, morda le nadležen. Toda ali je res tako? Kaj, če nekdo da (proda) osebne podatke, pridobljene iz zgodovine naših nakupov, neznanemu posamezniku, ali če nekdo naše osebne podatke nenamerno da na internet? Se bomo še vedno počutili v redu, ko bodo policisti potrkali na naša vrata in nam odvzeli prostost zaradi kaznivega dejanja, ki ga je storil nekdo, ki nam je ukradel identiteto? Dvomim. Tehnologije kot npr. podatkovno rudarjenje, skupno filtriranje, ambientalna obveščevalna dejavnost itd. omogočajo povečanje nadzora potrošnikov s pomočjo interneta.

Tretja vrsta nadzora je državni nadzor. V kazenskem pravosodju tveganje (po novem) zaseda pomembno mesto, zato se mora policija v svojih strategijah dodatno osredotočiti na dosledno uporabo nadzornih strategij in tehnologij ne le v prizadevanju, da zajezijo zločin na splošno, ampak da izrecno prepoznajo tiste, ki so nagnjeni h kaznivemu vedenju; da se proaktivno usmerijo/osredotočijo na samo jedro trdovratnih prestopnikov, za katere vlada verjame, da so najbolj odgovorni za težave z zločinom (Wood, 12-13). Težka naloga je, kako najti ravnovesje med državnim nadzorom in pravico do zasebnosti posameznih državljanov.

V sodobni družbi z močno informacijsko tehnologijo je nadzor samodejen, neviden in praktično neizsledljiv. Zbliževanje tehnologij in računalniških podatkovnih baz je osnova za tako veliko moč nadzora. Osebne in druge podatke je zdaj mogoče zbirati, analizirati in urejati po kazalkah hitreje kot kadarkoli prej. Različne skupine podatkov je mogoče primerjati med seboj in odkriti sumljive vzorce posameznikove dejavnosti. Podatki se analizirajo s pomočjo naprednih tehnologij, ki prepoznajo vzorce, ki morda zahtevajo dodatno preiskavo. Z novo tehnologijo lahko shranjujemo velikanske količine podatkov, ali pa jih 'izkopavamo' z algoritmi za podatkovno rudarjenje. Spletna družbena omrežja, kot npr. Facebook, Twitter in LinkedIn, so postala predmet intenzivnih raziskav v računalništvu, razvili so različne metode in algoritme za odkrivanje spletnih skupnosti v času delovanja. Obstajajo močna orodja za napovedovanje prihodnjega vedenja ciljnega uporabnika, npr. matematični modeli in programi umetne inteligence. Omejitve današnjega interneta pri podpori vsebinsko

usmerjenih storitev že rešujejo s konceptom informacijsko-centričnega mreženja. Seveda obstaja še veliko več nadzornih tehnik in sistemov, npr. videonadzorni sistemi, biometrični sistemi, inteligentni nadzorni sistemi, iskalni in sledilni sistemi itd. Predvidevamo lahko, da bodo z razvojem družbe in tehnologije ti sistemi postajali vedno bolj izpopolnjeni.

Zaključek

Kot smo videli, družbo poganja zapletena tehnologija. Informacije in informacijska tehnologija so postali najmočnejše orodje v bitki za prevlado. Toda bati se nam ni treba ne informacijske tehnologije ne nadzornih sistemov, podprtih z informacijsko tehnologijo. 'Roka, ki ziblje zibko' je tista, ki odloča, ali nam bo tehnologija prinesla blagostanje, ali bo pomenila konec za človeško raso. Internet in Web 2.0 sta orodji, ki ju uporabljajo različne spletne (in druge) družbene skupine, ki skušajo z njuno uporabo podpirati nadzor in prevlado nad drugimi skupinami. Po drugi strani je internet tudi orodje, ki ga je mogoče uporabljati kot upor proti prevladi. Očitno je, da tehnologije in platforme, kot so družbena omrežja, blogi, video- in druge platforme za deljenje vsebin, igrajo pomembno vlogo pri uveljavljanju upora proti prevladi. Uporabniki Facebooka, najbolj priljubljenega družbenega omrežja, nenehno nasprotujejo spremembam varnostne politike in pogojev uporabe, ki naj bi po njihovo povzročile ogrožanje zasebnosti in povečan nadzor. Nasprotovanje civilne družbe proti terorju in diktaturi v državah Srednjega vzhoda so podprli z družbenim aktivizmom na internetu, proteste proti kaznivim dejanjem nekaterih vlad organizirajo in podpirajo na Web 2.0. Takšni protesti kažejo na zmožnost spletnih družbenih skupin ter interneta in Web 2.0 kot globalne platforme za globalno povezan začetek, koordinacijo in podporo protestov.

Viri

- Akdeniz, Yamal, 2009. Racism on the Internet. Council of Europe.
- Bernik, I., Prislan, K., 2012. Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem. Ljubljana: Fakulteta za varnostne vede.
- Čaleta, D., Shemella, P., 2012. Managing the Consequences of Terrorist Acts – Efficiency and Coordination Challenges. Ljubljana, November 2012.
- Čaleta, D., Shemella, P., 2011. Counter terrorism challenges regarding the process of critical infrastructure protection. Ljubljana, September 2011.
- Kluwer, J., Kluwer, C., 2012. 11th International IFIP TC 6 Networking Conference, Prague, Czech Republic, May 21-25, 2012, Proceedings, Part I.
- Kluwer, J., Kluwer, C., 2011. Social understanding. Springer.

- Peltier, Thomas R., 2002. Information Security, Policies, Procedures and Standards: Guidelines for Effective Information Security Management. CRC Press LLC.
- Trček, Denis, 2006. Managing Information Systems Security and Privacy. Springer-Verlag Berlin Heidelberg.
- Vidmar, Tone, 2011. Računalništvo v oblaku 1. Del: Teorija distribuiranih sistemov. Pasadena: Ljubljana.
- Wood, D. M., 2006. A Report on the Surveillance Society. Surveillance Study Network.
- http://www.zakon.org/robert/internet/timeline/#Growth
- http://www.theguardian.com/world/video/2013/feb/10/raytheon-software-tracks-online-video (RIOT).