

Znanjem protiv zloupotrebe znanja

prof. dr Slobodan R. Petrović

mail: sp.ziteh@gmail.com

Sažetak: U radu se razmatra mesto, uloga i značaj znanja u zloupotrebi informacione tehnologije, kao i u suprotstavljanju toj zloupotrebi znanjem.

Ključne reči: zloupotreba IT, kiber-kriminal, kiber-terorizam, kiber-špijunaža (obaveštajno delovanje), kiber-ratovanje (informaciono ratovanje)

1. UVOD

Informaciona tehnologija, u najširem smislu, postala je esencijalni resurs za sve ekonomske i socijalne promene koje se u manjoj ili većoj meri kontinuirano odvijaju u svim segmentima društvene zajednice i na svim lokalitetima širom planete. Danas je teško čak i zamisliti, a još teže uspešno i kvalitetno odraditi i trivijalne poslove bez upotrebe informacione tehnologije. Ona je ušla u sve pore ljudskog bitisanja u toj meri da je čovekova zavisnost od ove tehnologije postala vrlo visoka, čak bi se, bez preterivanja, moglo reći da je ta zavisnost postala alarmantna. Iako ova eksplicitna i pomalo paranoična konstatacija može ličiti na neumesno preuveličavanje – ona to sigurno nije, jer svaka zavisnost po definiciji čini zavisnika osetljivim i ranjivim. Shodno tome, visoka čovekova zavisnost od informacione tehnologije čini savremeno društvo ekstremno osetljivim na negativne uticaje, odnosno poremećaje kojima zajednica može na mikro, makro i globalnom planu biti izložena zbog nepravilnog ili ilegalnog korišćenja ove tehnologije, sa posledicama koje su u lepezi od trivijalnih do katastrofalnih. Pojednostavljeno rečeno, informaciona tehnologija postaje "Ahilova peta" informacionog društva.

Ovo nameće imperativnu potrebu preduzimanja adekvatnih mera i akcija kako bi čovek sebe i informaciona dobra, sa kojima raspolaže, zaštitio od bilo kakvih slučajnih ili namerno izazvanih incidentnih situacija sa naželenim posledicama.

Iz tih razloga, za donosiocje odluka u svim oblastima i na svim nivoima, a posebno za one koji su na nacionalnom nivou odgovorni za stanje u ovoj oblasti, informaciona bezbednost postaje jedno od strateških pitanja čije uspešno razrešavanje obezbeđuje stabilno i perspektivno funkcionisanje delova i društvene zajednice u celini. Imajući tu činjenicu u vidu jasna je potreba da se ovo pitanje razrešava osmišljeno, kvalitetno i celovito. Navedene konstatacije su i jasne i obavezujuće, ali kada je reč o konkretizaciji ostaje i dalje otvoreno pitanje KAKO? Odgovori na ovo pitanje, posebno kada je reč o praksi, veoma su raznoliki, često nelogični, nerazumljivi, kontradiktorni, nerealni, neprimenljivi, a ulog je velik, čak kritično velik.

2. ISTORIJSKI OSVRT

Da bi se u celosti shvatili i razumeli procesi, koji se pod uticajem informacione tehnologije odvijaju u globalnoj društvenoj zajednici, korisno je osvrnuti se malo u ne tako davnu prošlost. Prvi komercijalni računari u odnosu na današnje dimenzionalno su bili ogromni, ekstremno skupi, skromnih mogućnosti i bili su namenjeni vrlo maloj grupi korisnika. Oni su jednostavno na kraju radnog vremena morali da brišu računarsku

memoriju, prikupe korišćene magnetne trake i bušene kartice, smeste ih u za to namenjen skladišni prostor, zaključaju kancelarije i na taj način su se štitili od upada provalnika. Dakle, korisnik je imao potpunu kontrolu operativnog ambijenta. Bezbednost računara bila je deo plana fizičke bezbednosti organizacionog entiteta, čiji je fokus bio na sprečavanju fizičkog upada, krađe aktuelne računarske opreme, računarskih diskova, koturova magnetnih traka ili bušenih kartica.

Pre 1980-ih godina bojazan od insajdera bila je malo verovatna za većinu organizacija. Vrlo malo ljudi imalo je korisničko obrazovanje, a od njih se izdvajao manji broj onih koji su stvarno radili na računarima. Oni su bili smešteni na lokacijama koje su bile fizičko-tehničkim merama zaštićene. Mnogi korisnici nikada nisu videli računarski sistem koji je izvršavao njihove svakodnevne zadatke. Oni su bili potčinjeni *batch* obradi i pregledanju rezultata. Protokom vremena računarska tehnologija se neprekidno razvijala, pa korisnici počinju da interaktuju sa računarima češće i da zahtevaju bolje korišćenje računarskih resura. Računarski ambijent počinje da se preobraća od centralizovane kontrole ka decentralizovanoj obradi. Ova promena u paradigmatima obrade snabdela je korisnike sa mogućnostima obimnije kontrole nad njihovim računarskim resursima, ali je i otvorila vrata za nove mogućnosti zloupotrebe računara.

Mogućnost pristupa računarima sa udaljenih lokacija revolucionisala je računarsku eru. Širenjem telekomunikacija, računarske mreže su se uvećavale u veličini i kompleksnosti. Mnoge velike firme počinju da automatizuju i skladište informacije o svojim klijentima, snabdevačima i komercijalnim transakcijama. Mrežno-baziran računarski pristup dramatično je uticao na edukaciju. Obrazovne ustanove otkrile su mogućnost da se povežu na velike računarske mreže i da centralizuju računarske baze podataka. Eksplozija u računarskoj dostupnosti snabdela je studente mogućnostima da eksperimentišu i rade sa računarima. Ovo je kreiralo efekat "snežne grudve" koji je doveo do ogromnog povećanja ukupnog broja ljudi koji koriste računar.

Uvođenje personalnih računara tokom 80-ih godina omogućilo je pristup još većeg broja korisnika. Ovi se računari pojavljuju na stolovima i u kancelarijama i domovima. Kako je cena računara počela da opada mnoge male firme videle su ovo kao mogućnost da automatizuju svoje operacije kako bi ostale konkurentne sa većim kompanijama. Pojava i raspoloživost personalnih računara prezentirala je drugi izazov za informacionu bezbednost. Ljudi su sada mogli da kod kuće kreiraju programe da bi krali informacije ili narušavaju operacije. Šta više, podaci, koji su sada trebali biti transferisani između sistema, bili su skladišteni na disketama i mogli su lako biti preuzeti ili ukradeni.

Krajem 80-ih i početkom 90-ih godina korišćenje računara se uvećavalo po eksponencijalnoj stopi. Kako se ovo korišćenje uvećavalo, tako se uvećavalo korišćenje mreže, elektronske pošte i BBS-ova (Bulletin Board Systems). Ovi novi razvoji u računarstvu uvećali su mogućnost korisnika da komuniciraju jedni sa drugima i sa drugim računarskim sistemima. Nova sloboda u računarskom ambijentu otvorila je jedno potpuno novo "igralište" za hakere. Pre opsežnog širenja korišćenja hakeri su mogli da prodru u samo jedan jedini sistem u isto vreme i to preko modema. Sada, potencijalni haker ima potencijal da pristupi mnogim sistemima sa jednim jednim upadom (break-in) i ima mogućnost da poremeti računarske sisteme po celom svetu.

1990-te godine videle su nastajanje otvorenih sistema i uvećavanje zavisnosti od mreža i potrebe deljenja podataka, aplikacija i hardverskih resursa. U prošlosti, bezbednost nije predstavljala glavnu brigu, ali pojavom Interneta, mogućnost da se dosegne bilo koja mreža – postala je globalna.

3. EFEKTI INFORMACIONE TEHNOLOGIJE

Računari i Internet čoveku su doneli bezbroj prilika i mogućnosti da svoj život učini lepšim, lakšim i lagodnijim. Oni su preinačili načine na koje ljudi komuniciraju, rade, uče i

zabavljaju se. Najkraće rečeno: Informaciona tehnologija ispunjava i nade i očekivanja onima koji su na vreme shvatili i prihvatili prilike i mogućnosti koje su im pružene.

U poslednjih nekoliko dekada mogućnosti informacione tehnologije da pojednostave, ubrzaju i olakšaju aktivnosti i poslovne procese organizacionih entiteta (preduzeća, ustanova, institucija) dramatično su se uvećale. Od "elektrifikacije" regularnih kancelarijskih zadataka, kao što je korespondencija, pa do najnovije pojave servisno orijentisane arhitekture (SOA), radni i poslovni rezultati postaju sve zavisniji od informacione tehnologije. Iz tih razloga za svaku organizaciju postaje kritično da implementira ovu tehnologiju na način koji minimizira vreme i troškove, a maksimizira kvalitet.

Tako, primera radi, dobro dizajniran i implementiran sistem elektronske trgovine može smanjiti troškove transakcija, smanjiti neefikasnost, promovisati bolji protok informacija i podsticati bolju saradnju između kupaca i prodavaca. U današnjem brzom menjaču sveta elektronske trgovine, gotovo sve može da se kupi preko Interneta i da se dostavi pravo na svačija ulazna vrata. Prevazilaženjem međunarodnih granica, Internet i World Wide Web omogućavaju kompanijama da na efikasan i ekonomičan način elektronskim putem, prodaju i isporučuju proizvode i usluge korisnicima lociranim u ciljnim zemljama, često udaljenim hiljadama kilometara. Sa nešto više od klika mišem, preduzeća mogu da komuniciraju, da se angažuju u trgovini i prošire svoje poslovne mogućnosti. S druge strane, za potrošače, ideja o on-line kupovini postala je privlačna iz nekoliko razloga. Naime, kupovina na Internetu nudi veći izbor, bolje karakteristike sa konkurentnijim cenama, brže isporuke, kao i više informacija za donošenje odluka.

Ono što u ovom kontekstu posebno treba naglasiti, a što obilje dokaza pokazuje, jeste da digitalna ekonomija može značajno olakšati i ubrzati izlazak iz tekuće ekonomske krize, jer je informaciona tehnologija značajan izvor produktivnosti, inovacija i društvenog rasta i napretka. Ona pomaže da se uveća konkurentnost, kreiraju poslovi i sprovodi globalizacija. U isto vreme ona obezbeđuje nove instrumente koji olakšavaju hvatanje u koštac sa velikim brojem velikih izazova, kao što su klimatske promene, energetska efikasnost i sl. Informaciona tehnologija je u samom srcu strategije za rast i zaposlenost i od suštinskog značaja je za uspešnu realizaciju takve strategije.¹

Upravo zbog toga u vreme ekonomske krize ova ključna uloga informacione tehnologije trebalo bi da bude pojačana, jer značajno pomaže da se iz krize izađe brže i uspešnije. Investiranje u nju je "pametna" investicija. Na kratak rok ova investicija podržava zapošljavanje u sektorima povezanim sa informacionom tehnologijom, dok na duži rok, ona povećava efikasnost, dovodi do inovacija i celu ekonomiju čini konkurentnijom.

Ako ne želimo da živimo od danas do sutra, već da ostvarujemo ambiciju na znanju zasnovanog društva, morali bi što više investirati u budućnost informacione tehnologije i posebno informacionih super-autostrada. Jer, informaciona tehnologija i inovacije su osnova za izlazak iz krize i ekonomski oporavak.²

4. IMPLIKACIJE I REPERKUSIJE

Uvođenje Interneta za globalnu zajednicu ubrzo je razotkrilo nespornu činjenicu da je on krcat rizicima koji su povezani sa nepoželjnim elementima žudnim, željnim, spremnim i sposobnim da zloupotrebe njegove mogućnosti. Pored stvaranja ogromnih socijalnih i ekonomskih mogućnosti, bezgranični i anonimni karakter Interneta predstavlja

¹ Post-i2010: priorities for new strategy for European information society (2010-2015), http://ec.europa.eu/information_society/eeurope/i2010/docs/post_i2010/090804_ipm_content.pdf

² Post-i2010: priorities for new strategy for European information society (2010-2015), http://ec.europa.eu/information_society/eeurope/i2010/docs/post_i2010/090804_ipm_content.pdf

ogroman izazov. Informaciona tehnologija čini ga idealnom platformom za prodiranje u tuđe računarske sisteme, uz mogućnost izvršavanja raznovrsnih kriminalnih aktivnosti. Kriminalci eksploatišu tu istu tehnologiju da izvršavaju kriminalne radnje i narušavaju bezbednost i privatnost korisnika IT. U rukama osoba koje deluju nečasno, zlonamerno ili bezobzirno, ova tehnologija postaje alat za aktivnosti koje ugrožavaju živote, imovinu, dostojanstvo pojedinaca i nanose štetu javnom interesu. Zaista, što više ljudi ide na mrežu, više kriminalaca shvata da on-line kriminal može biti veoma unosan, posebno imajući u vidu količinu vrednih komercijalnih i ličnih informacija sada smeštenih u elektronskom obliku.³

Državna administracija, organizacije i celokupno društvo u visokom stepenu zavise od efikasnosti i bezbednosti savremene informacione tehnologije. Međunarodne računarske mreže su nervi privrede, javnog sektora i društva u celini. Informaciona infrastruktura postala je kritičan deo kičme ekonomije. Bezbednost ovih računarskih i komunikacionih sistema i njihova zaštita od zloupotreba su stoga od suštinske važnosti. Širenja informacione tehnologije u gotovo svim oblastima života, kao i povezivanje računara sa međunarodnim računarskim mrežama doprineli su da kriminalne aktivnosti postanu raznovrsnije, opasnije i međunarodno prisutne.

Tokom proteklih godina brojni faktori nagoveštavali su mnoštvo pretnji stabilnosti informacionih sistema kroz kompromitaciju njihove bezbednosti. Krađa poslovnih tajni i zloupotreba zaštićenih podataka su dva primera kritične štete koja može biti naneta vlasnicima informacionih sistema kada se naruši njihova bezbednost. To što su mnoge kompanije interkonektovane sa geografski udaljenim sajtovima kao i sa partnerskim firmama i dozvoljavaju svojim zaposlenima da pristupaju internim sistemima sa mobilnih uređaja, kao što su lap-topovi ili personalni digitalni asistenti (PDA – *Personal Digital Assistants*), generisalo je mnoštvo novih potencijalnih ciljeva za napadače.

Rastući broj pretnji i njihove raznolikosti počeo je da osetno usložnjava problem njihovog identifikovanja, praćenja, analiziranja i odbrane. Iz takvog stanja proistekla je potreba "uvođenja reda" na osnovu odabranih kriterijuma. Međutim, zbog velikog broja postojećih i takoreći "svakodnevnog" pojavljivanja novih oblika zloupotrebe, vrlo je nezahvalno, a često i nemoguće, na osnovu izabranog kriterijuma vršiti preciznu identifikaciju, klasifikaciju i grupisanje. Njihova raznolikost i brojčano rastuća promenljivost predstavljaju značajan težinski koeficijent. Za potrebe ovog rada kao kriterijum koristiće se krupno-zrnasti pristup, bez ulaženja u detalje i finese, ako postoje. U tom smislu, svi poznati oblici zloupotrebe informacione tehnologije bi se u zavisnosti od cilja koji pred sobom imaju, mogli razvrstati u četiri osnovne grupe:

- kiber-kriminal;
- kiber-terorizam;
- kiber-špijunaža;
- kiber-ratovanje.

Prefiks kiber, koji je pozajmljen od naziva naučne discipline koja je svojim nastankom sredinom prošlog veka i najavila početak informacione revolucije – *kibernetika*, u ovom kontekstu bi trebalo da ukaže na tehnološku zavisnost i slabosti koje se sve snažnije formiraju i šire u novom još uvek neuređenom informacionom svetu u kojem je zloupotreba dobila nove mogućnosti delovanja, nove alate i mnoštvo novih atraktivnih ciljeva.

Osnovni kriterijum za ovu podelu je **motiv** izvršilaca, a osnovni cilj je klasifikacija ovih pretnji prema **stepenu društvene opasnosti**.

³ Crime online: Cybercrime and illegal innovation, Research report: July 2009, http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf

Kiber-kriminal. Obuhvata skoro sve oblike **klasičnog** kriminala koji se sada izvršava na novi način (pretnje, dečija pornografija, krađe (opreme, podataka i intelektualnih dobara), prevare, pronevere, iznude, falsifikovanja, nepoželjne poruke, on-line kockanje, govor mržnje, špijuniranje i dr), kao i novi oblici specifični samo za informacioni ambijent (haking, distribucija kontaminiranih računarskih virusa, ometanje i uskraćivanje računarskih usluga ovlašćenim korisnicima, obaranje računara sa poplavom neželjenih informacija i uzimanje, kopiranje, menjanje, brisanje ili uništenje računarskih podatke, softvera ili programa). Za motiv prvenstveno imaju materijalnu ili neku drugu korist.⁴

Kiber-terorizam. Oblici ove kategorije podrazumevaju atake na nacionalnu informacionu infrastrukturu sa ciljem da se poremete informacioni tokovi, uskrate raspoloživi servisi i uništi ili oštetiti informacioni sadržaj. Potencijalne mete na koje se fokusiraju su kontrolni sistemi kako bi se onemogućila fizička infrastruktura ili da bi se sa njom manipulisalo. To mogu biti, primera radi, sistemi za kontrolu snabdevanja električnom energijom, železničkog i vazdušnog saobraćaja ili za snabdevanje vodom. Motivi ovih napada su socijalni, ideološki, religiozni, politički ili slični ciljevi. U ovom kontekstu pomenimo izjavu iz 2008. godine, u kojoj je šef NATO-a za kiber-odbranu, Sulejman Anil, upozorio da terorizam baziran na računarima predstavlja istu pretnju nacionalnoj bezbednosti kao i raketni napad.⁵

Kiber-špijunaža. Aktivnosti u kiber-prostoru usmerene na sticanje tuđih poverljivih podataka i informacija različitih vrsta tajnosti i stepena poverljivosti, a bez dozvole njihovih vlasnika. Motiv je otkrivanje tuđih tajni pojedinaca, konkurenata, rivala, grupa i prijateljskih ili neprijateljskih vlada radi sticanja personalne, ekonomske, političke ili vojne prednosti.⁶

Kiber-ratovanje. Kombinovan skup kontinuiranih tajnih napadačkih aktivnosti na informaciona dobra protivničke strane. Motiv je sticanje informacione prednosti nad protivnikom.

Sa aspekta stepena društvene opasnosti najveću opasnost svakako predstavlja kiber-ratovanje, posebno ako ga preduzima jedna država protiv druge ili drugih država. Napadač u toj situaciji koristi sve svoje naučne, stručne, finansijske i materijalne potencijale da postigne željeni cilj, a napadnuta država čak nije ni svesna da se na nju vrši snažna i obimna agresija. U tom slučaju ostale tri kategorije (kiber-kriminal, kiber-terorizam i kiber-špijunaža) mogu se koristiti samo kao jedan od elemenata napada. Ozbiljnost i značaj ove kategorije zloupotrebe najbolje će ilustrovati podatak objavljen 2007. godine da najmanje 120 zemalja sveta u tajnosti razvija oružje kiber-ratovanja.⁷ To je informacija koju treba shvatiti vrlo ozbiljno i vrlo odgovorno.

Navedene kategorije sa svojim komponentama su veoma obimne i složene teme, čiju ozbiljnost i značaj nije lako uprošćeno izložiti, a istovremeno ne devalvirati njihovu suštinu.

Ono što treba posebno uočiti jeste da se svi navedeni oblici zloupotrebe informacione tehnologije izvršavaju u informacionom ambijentu. Sama činjenica da se izvršavaju u informacionom ambijentu ukazuje da se oni u odnosu na klasičnu situaciju

⁴ Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model, CERT Program, 2009, http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf; Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations, CERT, June 2009, <http://www.cert.org/archive/pdf/CyLabForeignTheftIP.pdf>; Crime online: Cybercrime and illegal innovation, Research report: July 2009, http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf; Petrović R. S., *KOMPIJUTERSKI KRIMINAL*, Vojnoizdavački zavod, Beograd, 2004, 564 st. III izdanje

⁵ Nato: Cyber-terrorism danger equal to missile attack, ZDNet UK, 10 Mar 2008, <http://news.zdnet.co.uk/security/0,1000000189,39364674,00.htm>

⁶ E-espionage: What risks does your organisation face from cyber-attacks? http://www.pwc.co.uk/pdf/e_espionage.pdf

⁷ Cyberwarfare, From Wikipedia, <http://en.wikipedia.org/wiki/Cyberwarfare>

izvršavaju bez velikih investicija (minimalni troškovi), sa neograničenim dosegom, brže, lakše, obimnije i, što je za izvršioce naročito bitno, anonimnije, a to znači i bezbednije.

5. MESTO I ULOGA ZNANJA

Ekspanzija informacione tehnologije i automatizacija poslovnih aktivnosti i procesa predstavljaju istinski fenomen današnjice – fenomen koji polako, ali sigurno, kreira novo informaciono društvo – društvo ekstremno zavisno od znanja. Ovo društvo, ka kojem se i mi ubrzano krećemo, je društvo u kojem je stvaranje, distribucija, difuzija, korišćenje, integracija i manipulacija informacijama značajna privredna, politička i kulturna aktivnost. Ključne funkcije u tom i takvom društvu postaju produkcija i distribucija znanja, a nosioci razvoja jesu i biće radnici znanja – pojedinci koji se vrednuju po njihovoj sposobnosti da interpretiraju informacije u okviru određenih tematskih oblasti. Oni koriste istraživačke veštine da kroz fokusiranu analizu definišu probleme i da identifikuju alternative. Podstaknuti svojom stručnošću i sagledavanjem, oni rade na rešavanju problema, u pokušaju da utiču na odluke, prioritete i strategije.⁸ Kako je društvo povećalo svoju zavisnost od informacione tehnologije, broj polja u kojima radnici znanja moraju da rade se dramatično proširio.⁹

Nesporno je da je znanje priznato kao značajan resurs, ali resurs koji se može zloupotребiti. Sa tog aspekta Stjuart T. A. u svojoj knjizi o intelektualnom kapitalu,¹⁰ spominje *"znanje kao termonuklearno oružje"*. Bez sumnje, ono je postalo takvo u informacionoj eri i ta činjenica se ne bi smela gubiti iz vida. Kao što su događaji od 11. septembra 2001. pokazali, efikasnije od bilo koje bombe je znanje koje uključuje veštine (kao što je letenje) i kompetencije, originalno i kreativno razmišljanje, razumevanje inženjeringa, učenje i integraciju mnogih kontekstnih procena, kao što su uticaj na komunikacije i ekonomiju.¹¹

S tim u vezi treba ukazati da izvršioци kriminalnih radnji u kiber-prostoru, bez obzira na njihovu vrstu i kategoriju, zahvaljujući informacionoj tehnologiji prolaze kroz fundamentalne promene. Mnoge od ovih promena su izvedene upravo iz implementacije i upravljanja znanjem i inovacijama. Razumevanje ove činjenice je ključ da im se suprotstavimo, jer zloupotreba je socijalni fenomen, i kao takav je usko integrisan sa promenama u našem društvu znanja. Pri tome treba imati u vidu da su i sami kriminalci radnici znanja, sa veštinama i sposobnostima da usmere informacionu tehnologiju prema sopstvenim ciljevima. Uz to, kiber-prostor i informaciona tehnologija pružaju kriminalcima iste mogućnosti i prednosti koje postindustrijsko informaciono doba omogućava bilo kom drugom pojedincu, grupi, organizaciji, naciji ili društvu u celini. Oni uživaju u globalnoj infrastrukturi Interneta zbog mogućnosti bezbedne razmene znanja, koje upijaju kao sunder, nezavisno od geografske lokacije, goreći od želje da ga što pre praktično iskoriste za lične potrebe.

⁸ Knowledge worker, From Wikipedia, http://en.wikipedia.org/wiki/Knowledge_workers

⁹ Firestone M. J., Doing Knowledge Management, http://www.kmci.org/media/Doing_KM.pdf; Information and Knowledge Management, 2009-2010, http://info.emeraldinsight.com/products/books/info/download/information_and_knowledge_management.pdf; Stages of knowledge management systems in police investigations, <http://learners.in.th/file/fatriya/Stages%20of%20knowledge%20management%20systems%20in%20police%20investigations.pdf>; Knowledge management processes, tools and techniques for counterterrorism, dec. 2009, <http://www.mip.sdu.dk/~ukwiil/ifvt-sud2/wiil.pdf>

¹⁰ Stewart, T. A., *Intellectual capital: The new wealth of organizations*. New York: Doubleday/Currency, 1997, str. IX).

¹¹ Gil Ariely, Knowledge - The thermonuclear weapon for terrorists in the information age, <http://www.ict.org.il/Articles/tabid/66/Articlesid/97/currentpage/11/Default.aspx>; Hoffman Bruce, The Leadership Secrets of Osama bin Laden, SECURITY APRIL 2003 ATLANTIC, <http://www.theatlantic.com/doc/200304/hoffman>

Sada, oni mogu preko Weba otvoreno ili tajno (što je češće) da komuniciraju, drže obuku iz tema koje smatraju značajnim i da razmenjuju znanja sa kojima raspolažu (uključujući i znanja kako sprovoditi napade na računare, praviti bombe, distribuirati viruse i dr.). Uporan "kiber-učenik", može čak da pronađe obimna on-line znanja na mreži povezana sa oružjem za masovnu destrukciju.¹²

Znanje i informacije su, kao što je poznato, nematerijalni (neopipljivi) i za njih su informaciona tehnologija i kiber-arena prirodno stanište. Krijumčarenje materijalnog (opipljivog), kao što je bomba ili eksploziv, mnogo je teže nego slanje instrukcija preko Weba ili postavljanje lekcija na mreži. Pretraživanje preko Google, ilustracije radi, za tekst koji u naslovu ima *"make a bomb"*, rezultiralo je sa 47.500 naslova. Takođe je nađeno i 317 video klipova sa ovim iskazom. Zaista bogata literatura za samo jednu, ali vrlo opasnu temu.

Thomas Timothy ukazuje na različite primene Interneta koji se mogu koristiti za terorizam, od kojih privlači pažnju sledeće:¹³ *... u ratu, kao i u biznisu, informaciona tehnologija je veliki ekvilajzer (izjednačivač). Njena niska finansijska barijera omogućava čak i najsiriromašnijim organizacijama IT efikasnost koja je jednaka (ili gotovo jednaka) velikim korporacijama.*

6. SLIKA STANJA

Koliko je ovo zaista ozbiljno? Odgovor je najlakše potražiti u konkretnim pokazateljima. Na početku navodimo neke opšte podatke:

*Broj korisnika Interneta:*¹⁴

Populacija (2009 proc.)	Internet users 31. dec, 2000	Internet users Poslednji podaci	Obuhvaćeno (% Population)	Rast 2000-2009
6.767.805.208	360.985.492	1.733.993.741	25,6 %	380,3 %

Srbija:

Populacija (2009 proc.)	Internet Users sept. 2009	Obuhvaćeno (% Population)	Rast 2000-2009
7.379.339	3.300.000	44,7 %	725,0 %

*Statistika pretraživača:*¹⁵

godina	IE8	IE7	IE6	Firefox	Chrome	Safari	Opera
2010. jan.	14,3%	11,7%	10,2%	46,3%	10,8%	3,7%	2,2%
2009. jan.	0,6%	25,7%	18,5%	45,5%	3,9%	3,0%	2,3%

*Broj hostova:*¹⁶

¹² Gil Ariely, Knowledge - The thermonuclear weapon for terrorists in the information age, <http://www.ict.org.il/Articles/tabid/66/Articleid/97/currentpage/11/Default.aspx>

¹³ Thomas L. Timothy, Al Qaeda and the Internet: The Danger of Cyberplanning, *Parameters*, Spring 2003, pp. 112-123, <http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf>

¹⁴ Internet World Stats, World Internet Users and Population Stats, <http://www.internetworldstats.com/stats.htm>

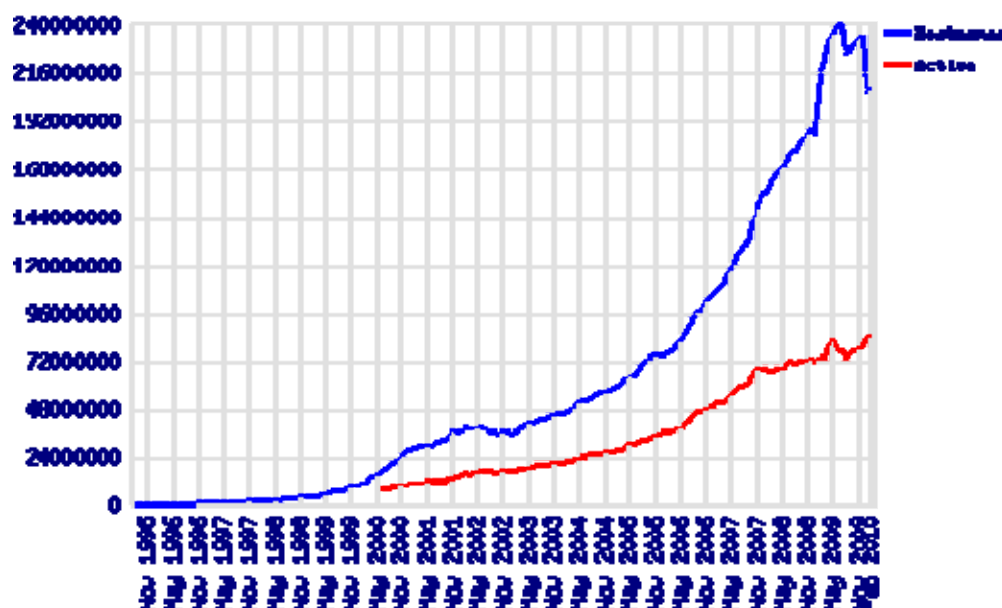
¹⁵ Browser Statistics, http://www.w3schools.com/browsers/browsers_stats.asp

¹⁶ Internet Systems Consortium, Internet host count history, <https://www.isc.org/solutions/survey/history>

1981.	213	2006.	394.991.609
1982.	235	2007.	433.193.199
1983.	562	2008.	541.677.360
1984.	1.024	2009.	681.064.561
1985.	1.961	2010.	732.740.444

Broj Web sajtova u februaru 2010. godine iznosio je 207.316.960.¹⁷

Pregled broja sajtova u svim domenima za period Avgust 1995. – Februar 2010: ¹⁸



Šema 01

Izneti opšti podaci, koji čine osnovu platforme za sve vrste zloupotreba, jasno ukazuju na ogroman potencijal raspoloživ za zloupotrebu i dinamiku promena koje se odigravaju na našem putu ka informacionom društvu.

Svake godine Institut za bezbednost računara (Computer Security Institute) razmatra velike i male organizacije u širokom industrijskom spektru u vezi sa njihovim bezbednosnim incidentima i alate i tehnike koje oni razvijaju da bi se oporavili od svojih bezbednosnih nevolja. Oni su publikovani u 14. godišnjem pregledu. Rezultati su bazirani na odgovoru 443 profesionalca informacione bezbednosti i informacione tehnologije u korporacijama, vladinim agencijama, obrazovnim institucijama, medicinskim institucijama i drugim organizacijama. Njihovi odgovori pokrivaju period od jula 2008. do juna 2009.¹⁹

- Anketirani su prijavili velike skokove u opsegu "njuškanja" lozinki (password sniffing: 17.3% u odnosu na 9% prethodne godine), finansijskih prevara (19.5% u odnosu na 12 % prethodne godine), infekcija zlonamernim softverom (64.3% u odnosu na 50% prethodne godine), uskraćivanja servisa (DoS: 29.2% u odnosu na 21% prethodne godine) i nagrdivanje (unakažavanje) Web sajtova (13.5% u odnosu na 6% prethodne godine);

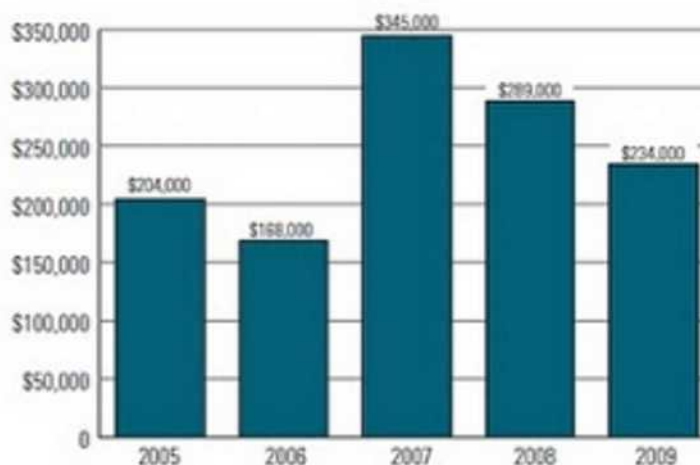
¹⁷ The Netcraft Web Server Survey, February 2010 Web Server Survey, http://news.netcraft.com/archives/2010/02/03/february_2010_web_server_survey.html

¹⁸ The Netcraft Web Server Survey, February 2010 Web Server Survey, http://news.netcraft.com/archives/2010/02/03/february_2010_web_server_survey.html

¹⁹ 2009 CSI Computer Crime and Security Survey, <http://pindebit.blogspot.com/2010/01/2009-csi-computer-crime-and-security.html>, CSI Computer Crime and Security Survey 2009, <http://v2.gocsi.com/2009survey/>

- Jedna trećina anketiranih organizacija bila je lažno predstavljena kao pošiljalac "phishing" poruka;
- Prosečan gubitak zbog bezbednosnih incidenata je opao sa 289.000 \$ u 2008. na 234.244\$ u 2009, mada su oba i dalje iznad proseka iz 2006. godine.
- Krađa personalnih identifikacionih informacija i zaštićenih zdravstvenih informacija u proseku po incidentu iznosi 710.000\$, a finansijske prevare su u proseku 450.000\$;
- Dvadeset i pet odsto ispitanika smatra da je preko 60 odsto njihovih finansijskih gubitaka pripisivo nezlonamernim akcijama insajdera.
- Ispitanici su bili zadovoljni, mada ne i presrećni, sa svim bezbednosnim tehnologijama.
- Većina anketiranih smatra da je njihovo investiranje u obuku krajnjih korisnika radi podizanja bezbednosne svesti bilo neadekvatno, ali većina smatra da su njihova ulaganja u ostale komponente njihovog bezbednosnog programa bila adekvatna.
- Na pitanje kakve akcije su bile preduzete u odnosu na bezbednosne incidente, 22 odsto ispitanika izjavilo je da su obavešteni pojedinci čiji su lični podaci bili kompromitovani, a 17 odsto je izjavilo da obezbeđuju nove bezbednosne usluge korisnicima i klijentima.
- Na pitanje koja bezbednosna rešenja najviše rangiraju na listi želja, mnogi od anketiranih su imenovali alate koji će poboljšati vidljivost – bolje upravljanje evidencijama (dnevnicima), upravljanje bezbednosnim informacijama i događajima, vizuelizacija bezbednosnih podataka, bezbednosne table i slično;

PROSEČAN GUBITAK PO ISPITANIKU



Šema 02

Korporacija Ernst & Young, koja obuhvata 140 pridruženih firmi i ima 144.000 ljudi, uradila je svoj 12. globalni pregled informacione bezbednostii. Pregled je urađen juna i augusta 2009. godine i obuhvatio je 1.900 organizacija širom sveta.²⁰

Od 1.900 učesnika ankete, 75% je izrazilo zabrinutost zbog moguće odmazde nedavno odstranjenih bivših radnika. Istraživanje pokazuje i sledeće:

- 41% je prijavilo porast eksternih napada;
- 25% potvrdilo je porast internih napada;

²⁰ Ernst & Young's 12th annual global information security survey,
[http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/\\$FILE/12th_annual_GISS.pdf](http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf)

- 30% se suočilo sa povećanjem interno izvršenih krađa.

Sedmi godišnji pregled globalnog stanja informacione bezbednosti, studija koju su uradili *CIO*, *CSO* i *PriceWaterhouseCoopers* u periodu april-juni 2009. godine zasnovana je na odgovorima 7.276 profesionalaca iz oblasti zaštite i informacione tehnologije iz više od 100 zemalja. Trideset i dva procenata učesnika bilo je iz Severne Amerike, praćeni sa dvadeset i sedam procenata iz Azije, dvadeset i šest procenata iz Evrope, četrnaest procenata iz Južne Amerike i dva procenta sa Srednjeg istoka i Severne Afrike. Granična greška za pregled je +/- 1%.²¹

Više kompanija uvećava trošenje na zaštitu nego što ga smanjuje. Smer trošenja je:

▪ uvećanje	38%
▪ ostalo isto	25%
▪ smanjenje	12%
▪ nije poznato	24%

Ugrožavanje podataka se uvećalo brže nego bilo koja druga bezbednosna upotreba. Glavni cilj napada su: baze podataka. Kako napadači dolaze do podataka? Preko:

▪ Baza podataka	57%
▪ File-sharing aplikacija	46%
▪ Lap-topova	39%
▪ Izmenljivih medija	23%
▪ Back-up traka	16%

Koliko košta kiber-kriminal? Gubici od incidenata u proseku iznose 833.000 \$.

▪ Finansijski gubitak	42%
▪ Kompromitacija brenda ili reputacije	30%
▪ Krađa intelektualnih dobara	29%
▪ Izmena ili naruživanje home page-a	20%
▪ Krađa	17%

M86 Security Labs je grupa bezbednosnih analitičara specijalizovanih za pretnje elektronskoj pošti i Webu, od spama do zlonamernih kodova.²²

Ključne tačke pregleda:

- obim spam-poruka uvećao se dramatično u 2009. godini, do preko **200 milijardi** dnevno sa ogromnim brojem distribuiranih kroz inficirane računare;
- zlonamerne spam-poruke dramatično su se uvećale u volumenu, dostižući **3 milijarde** poruka na dan, u odnosu na 600 miliona poruka na dan u prvoj polovini 2009. godine;

Tokom 2009. godine rastući trend bio je u korišćenju tehnike *Optimizacije pretraživača* (*Search Engine Optimization (SEO)*) da privuku korisnike do Web stranica na kojima su smešteni zlonamerni kodovi. Takođe poznata kao CEO trovač, ova tehnika cilja da uzdigne zlonamerno upecane stranice do bodovanja rezultata pretraživača, čime se obezbeđuje stalno snabdevanje žrtava. CEO trovač je posebno podmukao budući da korisnici implicitno veruju rezultatima pretraživača.

NetWitness, svetski lider u naprednom otkrivanju pretnji i forenzici mreže u realnom vremenu, objavio je 18. februara 2010. godine da su njegovi analitičari otkrili jedan

²¹ The Global State of Information Security, 2010, http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_cio_reprint.pdf

²² Security Labs Report Jul 2009-Dec 2009 Recap, http://www.m86security.com/newsimages/trace/M86_Labs_Report_Jan2010.pdf

opasan nov Zeus botnet (Trojanac koji krađe bankarske informacije) koji je napao 75.000 sistema u 2.500 organizacija širom sveta.²³

U jednoj studiji o ugrožavanju podataka (*2009 Data Breach Investigations Report*²⁴) navodi se da je tokom 2008. godine 285 miliona podataka bilo kompromitovano.

Izveštaj *Identity thefts*²⁵ upozorava da će se broj ljudi u Britaniji, čiji je kreditni rejting narušen krađom identiteta, duplirati u toku narednih pet godina. Krađa identiteta se svake godine od 2000. godine uvećava za trećinu.

Broj slučajeva se uvećava za oko trećinu svake godine tokom poslednjih osam godina, a očekuje se da će broj žrtava nastaviti da raste i zbog ekonomske recesije. Istraživanje je utvrdilo da su prosečni troškovi po osobi koja je žrtva krađe identiteta 2.100£ za korekciju nastale štete.

Izveštaji o krađi identiteta:

- Krađa identiteta pogodila je 27,3 miliona Amerikanaca u poslednjih pet godina (1998-2002), a skoro 10 miliona samo u 2002;²⁶
- Krađa identiteta pogodila je 1 od svakih 8 Amerikanaca u poslednjih pet godina (12,7%).²⁷
- Ukupan broj žrtava u 2005. iznosio je 8,3 miliona osoba (3,7%);²⁸
- S obzirom na procenat rasta, stvarnost je da će većina od nas postati žrtva krađe identiteta tokom života, ako ne i više puta.²⁹
- Krađa identiteta je najbrže rastući kriminal u Sjedinjenim Državama.³⁰

Prosečan iznos ukraden od žrtava Internet prevare je 463£.³¹

Rezultati izveštaja o kriminalu na Internetu³² prikazani su na sledećoj šemi:

²³ "Kneber Botnet" Targets Corporate Networks and Credentials, February 18, 2010, <http://www.netwitness.com/resources/pressreleases/feb182010.aspx>

²⁴ 2009 Data Breach Investigations Report, A study conducted by the Verizon Business RISK Team, <http://www.scribd.com/doc/24861153/0100010101010100110010101000101100001001001010001110101100101001001010101110101001110010001010-100100001000101010010010100010101000>

²⁵ *Identity thefts are 'set to double', April 28, 2009*, <http://www.thisissouthwales.co.uk/news/Identity-thefts-set-double/article-942501-detail/article.html>

²⁶ Federal Trade Commission – Identity Theft Survey Report, <http://www.ftc.gov/os/2003/09/synovatereport.pdf>

²⁷ Federal Trade Commission – Identity Theft Survey Report, <http://www.ftc.gov/os/2003/09/synovatereport.pdf>

²⁸ Federal Trade Commission – 2006 Identity Theft Survey Report, <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>

²⁹ Identity Theft, February 5, 2010, <http://mycreditreportherp.blogspot.com/2010/02/identity-theft.html>

³⁰ Identity Theft, February 5, 2010, <http://mycreditreportherp.blogspot.com/2010/02/identity-theft.html>

³¹ The Anonymous Attacker: a Special Report on Identity Fraud and Account Takeover, <http://www.stop-idfraud.co.uk/resources/the-anonymous-attacker-CIFAS-special-report.pdf>

³² 2008 Internet Crime Report, http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf



Šema 3

7. ŠTA ČINITI

Postojeće i novonastajuće pretnje u informacionom ambijentu postaju veće i opasnije sa svakim danom koji prođe, jer su kriminalci, teroristi, obaveštajne službe i vojne strukture mnogih zemalja uveliko postale svesne moći informacionih alata i informacionog oružja. Sukob, koji je već počeo i uveliko traje, nije bilo moguće izbeći, a ta činjenica nalaže svima da bezrezervno participiraju u merama i akcijama koje se preduzimaju ili ih treba preduzeti da bi se uspešno suprotstavili ovoj velikoj pošasti dvadesetprvog veka.

S tim u vezi, izuzetno je poučna i korisna konstatacija da se treba učiti na tuđim iskustvima, ali se ona ne ograničava samo na pozitivnim. Nekada, tuđa negativna iskustva su znatno vrednija od njihovih pozitivnih iskustava. Cilj prvih (pozitivnih) je da se ostvari dobit koje vrste, a cilj drugih (negativnih) je da se spreči šteta bilo koje vrste.

Korišćenjem, u razmatranom kontekstu, obe vrste tuđih i sopstvenih iskustava i znanja iz ove problematike, autor je slobodan da, za suprotstavljanje pretnjama zloupotrebe informacione tehnologije i njihovo stavljanje pod dugoročnu društvenu kontrolu, ukaže na imperativne preduslove koji se moraju ispuniti:

- Bezbednosna kultura;
- Svest o potrebi zaštite informacionog ambijenta;
- Znanje da se zloupotreba:
 - o spreči,
 - o otkrije,
 - o dokaže,
 - o sankcioniše.

Sva tri navedena preduslova se u suštini oslanjaju na znanje. Dakle, upravljanje znanjem je u žiži konfrontacije. Programi upravljanja znanjem povezuju znanja generisana iz nauke, sinteze i učenja sa njegovim korišćenjem. S obzirom da je znanje glavni resurs za izvršavanje zloupotrebe informacione tehnologije, ali i za suprotstavljanje zloupotrebi, upravljanje znanjem kao resursom u okviru borbe protiv zloupotrebe je od suštinskog značaja, kao što je značajno i uskraćivanje tog resursa kriminalcima gde god je to moguće.

Upravo zbog toga, saznanje izvedeno iz našeg dubokog razumevanja uloge znanja nameće potrebu *da se analiziraju razni aspekti znanja kao resursa za zloupotrebu i permanentno procenjuju operative mogućnosti protivnika da koristi znanje i naših potreba da u konkretnim situacijama sučeljavanja sa njima odgovorimo znanjem.*

Upravljanje znanjem kroz opsežni transfer znanja na široku javnost, čime će se njihova bezbednosna kultura i svest o potrebi zaštite uzdići do željenog nivoa, je ključno u suprotstavljanju svakoj vrsti zloupotrebe, pa i ovoj. Takvi programi obrazovanja javnosti su neprocenjivi. Implementiranje upravljanja znanjem na najširoj mogućoj skali trebalo bi da maksimalno doprinese izgradnji javne otpornosti na pretnje koje potiču od zloupotrebe informacione tehnologije.

Ako već cenimo i prihvatamo tuđa iskustva i znanja, onda nema razloga da ne prihvatimo i stav da je u dolazećem informacionom dobu svakome potrebna bazična obuka o konceptima i procedurama zaštite kiber-prostora. Ono čega moramo biti svesni jeste da taj opšti zahvat i potreban nivo nije lako ostvarti.

Kada je reč o specijalizovanom znanju ono što nam daje nadu i uliva poverenje to je naš podmladak, željan znanja, voljan i spreman da se uhvati sa svakim problemom u koštac. O njima najbolje govore brojne medalje i nagrade osvojene širom sveta. Ovim biserima nacije treba samo pružiti pravu šansu, usmeriti ih i stvoriti im adekvatne uslove. Oni će nam se za to višestruko odužiti. Ovo bi bio veliki podsticaj i snažan iskorak ka kreiranju kulta znanja i stručnosti. A to nam je potrebno kao vazduh koji udišemo.

8. ZAKLJUČAK

I površna analiza stanja napred navedenih preduslova u našem informacionom prostoru sigurno bi rezultirala razočaravajućim zaključcima. Jedan od pokazatelja ovakvog stanja svakako je i činjenica da se na ovakvim i sličnim skupovima koji su posvećeni informacionoj bezbednosti uglavnom okupljaju informatičari i skoro zanemarljiv broj donosilaca odluka i odgovornih za stanje u ovoj oblasti, bilo na mikro, makro ili nacionalnom planu. Dok se ta proporcija ne obrne, i odgovorni ne postanu svesni svoje odgovornosti, situacija se neće poboljšati. Kakvu će štetu društvo do tada prepeti ostaće tajna, a ono što se bez i najmanje rezerve može tvrditi, ta šteta će biti ogromna, jer ovde je pre svega i iznad svega reč o nacionalnom interesu. Ovo nije bombasta konstatacija koja se olako iznosi da bi se samo ostavio utisak. To je činjenica koju je lako dokazati i koju autor već dugo vremena ponavlja kao papagaj: Tri od četiri gore navedene kategorije zloupotrebe informacione tehnologije (kiber-terorizam, kiber-špijunaža i kiber-ratovanje) za primarni cilj svog delovanja imaju tuđe nacionalne interese, a četvrta kategorija (kiber-kriminal) po potrebi im služi često kao ispomoć.

Da bi se učinio osetan i vidljiv pomak u uspešnom razrešavanju obimnog, ozbiljnog i ekstremno složenog problema zloupotrebe informacione tehnologije, čije dimenzije po svim kriterijumima dosežu ne samo nacionalni, već i međunarodni nivo, prvi korak bi svakako bio pokretanje inicijative izrade **Nacionalne strategije zaštite kiber-prostora**, kao najvažnijeg i najsnažnijeg pokretačkog i usmeravačkog instrumenta za sve ostale aktivnosti i akcije. Nosilac ove ključne aktivnosti bi morala da bude vlada, kao državni entitet najodgovorniji za opšte stanje u naciji, koji istovremeno ima i najviši autoritet i najveći kapacitet koji su neophodni za realizaciju takvog značajnog zadatka.³³

Da nepotrebno ne gubimo dragoceno vreme, paralelno sa izradom Strategije trebalo bi pokrenuti akciju donošenja i usvajanja programa razvijanja bezbednosne kulture i podizanja svesti o neophodnosti zaštite kiber-prostora. Ovaj program bi trebalo da pokrije, pre svega, vojsku, policiju, tužilaštvo i sudstvo, ključne stubove svake države, ali i celu naciju, sve pojedince koji na bilo koji način učestvuju ili će učestvovati u informacionim procesima, jer *informaciona bezbednost je posao svih*.

³³ Petrović R. S., *Bezbednosna svest, obuka i edukacija – kritične komponente zaštite kiber-prostora*, Savetovanje *Zloupotrebe informacionih tehnologija* (ZITEH), Zbornik radova (CD-ROM), ISBN 86-909511-0-5, COBISS SR-ID 135535372, Tara, 31. maj – 03. juni 2006.

I najzad, treća značajna akcija za paralelno izvođenje je program obuke i edukacije. Kako se elementarne osnove informaciono-bezbednosne pismenosti (bezbednosni termini, koncepti, osetljivosti, pretnje, posledice) stižu kroz podizanje svesti o potrebi zaštite, a nadogradnja se realizuje kroz obuku, tako bi trebalo da se tranzicija od svesti ka obuci odvija osmišljeno na planiran i očekivan način.

Edukacija je jasno identifikovana kao separatan nivo učenja namenjen profesionalcima i specijalistima za zaštitu. Obezbeđivanje formalne edukacije i specifičnih kriterijuma edukacionog nivoa za ovu grupu je u nadležnosti programa koje bi trebalo da realizuju akademske ustanove. Smatra se da su edukacija, koja se razlikuje od obuke, i iskustvo povezano sa poslom esencijalni za profesionalce i specijaliste informacione zaštite da bi bili u stanju da odigraju svoje uloge na efikasan način, a to znači da:

- spreče,
- otkriju,
- dokažu,
- sankcionišu.

Ovakav pristup u rešavanju problema zloupotrebe bi stvorio veru i pružio nadu da ćemo pod permanentnom kontrolom imati ovaj ekstremno značajan problem, kako mi ne bi bili sledeća žrtva.

9. LITERATURA

1. Post-i2010: priorities for new strategy for European information society (2010-2015), http://ec.europa.eu/information_society/eeurope/i2010/docs/post_i2010/090804_ipm_content.pdf
2. Nato: Cyber-terrorism danger equal to missile attack, ZDNet UK, 10 Mar 2008, <http://news.zdnet.co.uk/security/0,1000000189,39364674,00.htm>
3. Cyberwarfare, From Wikipedia, <http://en.wikipedia.org/wiki/Cyberwarfare>
4. Knowledge worker, From Wikipedia, http://en.wikipedia.org/wiki/Knowledge_workers
5. Stewart, T. A., *Intellectual capital: The new wealth of organizations*. New York: Doubleday/Currency, 1997, str. IX).
6. Hoffman Bruce, The Leadership Secrets of Osama bin Laden, SECURITY APRIL 2003 ATLANTIC, <http://www.theatlantic.com/doc/200304/hoffman>
7. Gil Ariely, Knowledge – The thermonuclear weapon for terrorists in the information age, <http://www.ict.org.il/Articles/tabid/66/Articlsid/97/currentpage/11/Default.aspx>
8. Thomas L. Timothy, Al Qaeda and the Internet: The Danger of Cyberplanning, *Parameters*, Spring 2003, pp. 112-123, <http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf>
9. Internet World Stats, World Internet Users and Population Stats, <http://www.internetworldstats.com/stats.htm>
10. Browser Statistics, http://www.w3schools.com/browsers/browsers_stats.asp
11. Internet Systems Consortium, Internet host count history, <https://www.isc.org/solutions/survey/history>
12. The Netcraft Web Server Survey, February 2010 Web Server Survey, http://news.netcraft.com/archives/2010/02/03/february_2010_web_server_survey.html
13. 2009 CSI Computer Crime and Security Survey, <http://pindebit.blogspot.com/2010/01/2009-csi-computer-crime-and-security.html>
14. CSI Computer Crime and Security Survey 2009, <http://v2.gocsi.com/2009survey/>
15. Ernst & Young's 12th annual global information security survey, [http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/\\$FILE/12th_annual_GISS.pdf](http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf)

16. The Global State of Information Security, 2010,
http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_cio_reprint.pdf
17. Security Labs Report Jul 2009-Dec 2009 Recap,
http://www.m86security.com/newsimages/trace/M86_Labs_Report_Jan2010.pdf
18. "Kneber Botnet" Targets Corporate Networks and Credentials, February 18, 2010,
<http://www.netwitness.com/resources/pressreleases/feb182010.aspx>
19. 2009 Data Breach Investigations Report, A study conducted by the Verizon Business RISK Team,
<http://www.scribd.com/doc/24861153/0100010101010110010011100101010001011000100100011101011001010010010011010101110101001101001110010001010-100100001000101010010010100010101000>
20. Identity thefts are 'set to double', April 28, 2009,
<http://www.thisissouthwales.co.uk/news/Identity-thefts-set-double/article-942501-detail/article.html>
21. Federal Trade Commission – Identity Theft Survey Report,
<http://www.ftc.gov/os/2003/09/synovatoreport.pdf>
22. Federal Trade Commission – 2006 Identity Theft Survey Report,
<http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>
23. Identity Theft, February 5, 2010,
<http://mycreditreporthelper.blogspot.com/2010/02/identity-theft.html>
24. The Anonymous Attacker: a Special Report on Identity Fraud and Account Takeover,
<http://www.stop-idfraud.co.uk/resources/the-anonymous-attacker-CIFAS-special-report.pdf>
25. 2008 Internet Crime Report,
http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf
26. Petrović R. S., *Bezbednosna svest, obuka i edukacija – kritične komponente zaštite kiber-prostora*, Savetovanje Zloupotrebe informacionih tehnologija (ZITEH), Zbornik radova (CD-ROM), ISBN 86-909511-0-5, COBISS SR-ID 135535372, Tara, 31. maj – 03. juni 2006.
27. Petrović R. S., *Kiber-prostor – izvorište novih pretnji nacionalnoj bezbednosti*, Međunarodni naučno-stručni skup Informaciona bezbednost 2009, Beograd, februara 2009.
28. Petrović R. S., *Kiber prostor – peta dimenzija ratovanja*, Vojni informator, br. 4, jul-avgust 2001, str. 29-50.
29. Petrović R. S., *Kiberterorizam*, Vojno delo, god. LIII, br. 2/2001, str. 100-122.
30. Petrović R. S., *KOMPJUTERSKI KRIMINAL*, Vojnoizdavački zavod, Beograd, 2004, 564 st. III izdanje
31. Petrović R. S., *Nacionalna bezbednost u raljama informacione tehnologije*, *Info m*, Fakultet organizacionih nauka, Beograd, god 8, sv. 30, 2009.
32. Petrović R. S., *Neki aspekti nacionalne bezbednosti u informacionom dobu*, Nauka, Tehnika, Bezbednost, (NTB), Rad po pozivu, UDC: 681.324; 65.012.8, Godina XI, Broj 1, Septembar 2001, str. 7-27.
33. Petrović R. S., *O informacionoj revoluciji u kontekstu zloupotrebe informacione tehnologije*, Savetovanje Zloupotrebe informacionih tehnologija (ZITEH), Zbornik radova (CD-ROM), Tara, 31. maj – 03. juni 2004.
34. Petrović R. S., *O neophodnosti nacionalne strategije zaštite kiber-prostora*, Nauka Bezbednost Policija (NTB), Beograd, vol. XI, no. 2, 2006, str. 3-28.
35. E-espionage: What risks does your organisation face from cyber-attacks?
http://www.pwc.co.uk/pdf/e_espionage.pdf
36. Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model, CERT Program, 2009,
http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf

37. Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations, CERT, June 2009, <http://www.cert.org/archive/pdf/CyLabForeignTheftIP.pdf>
38. Crime online: Cybercrime and illegal innovation, Research report: July 2009, http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf
39. Firestone M. J., Doing Knowledge Management, http://www.kmci.org/media/Doing_KM.pdf; Information and Knowledge Management, 2009-2010, http://info.emeraldinsight.com/products/books/info/download/information_and_knowledge_management.pdf
40. Stages of knowledge management systems in police investigations, <http://learners.in.th/file/fatriya/Stages%20of%20knowledge%20management%20systems%20in%20police%20investigations.pdf>
41. Knowledge management processes, tools and techniques for counterterrorism, dec. 2009, <http://www.mip.sdu.dk/~ukwiil/ifvt-sud2/wiil.pdf>
42. Gottschalk Petter, Knowledge Management in Policing: Enforcing Law on Criminal Business Enterprises, SBN 978-977-454-078-3, Hindawi Publishing Corporation, 12008.

KNOWLEDGE AGAINST MISUSE OF KNOWLEDGE

prof. dr Slobodan R. Petrović

mail: sp.ziteh@gmail.com

Abstract: In this piece of paper a place and role and importance of knowledge in information technology missuse, as well as in countermeasure to this missuse by knowladge are considered.

Key words: *misuse of IT, cyber-crime, cyber-terrorism, cyber-espionage, cyber-warfare*