UDC: **351.746:004** INFO M: str. 4-13

NACIONALNA BEZBEDNOST U RALJAMA INFORMACIONE TEHNOLOGIJE
NATIONAL SECURITY IN THE JAWS OF INFORMATION TECHNOLOGY

Slobodan R. Petrović

REZIME: Polazeći od činjenice da informaciona tehnologija vrši izuzetno snažan uticaj na društvenu zajednicu nudeći joj, sa jedne strane, obilne pogodnosti i brojne mogućnosti, a sa druge strane, čineći je ekstremno zavisnom i enormno osetljivom na poremećaje izazvane zloupotrebom ove tehnologije, u radu se razmatraju implikacije ove tehnologije na nacionalnu bezbednost.
KLJUČNE REČI: informaciono doba, informaciona revolucija, nacionalna bezbednost, kompjuterski kriminal, kiber-terorizam, obaveštajno delovanje, informaciono ratovanje.
ABSTRACT: Starting from the fact that information technology makes a very strong impact on the community by offering it on one hand, the abundant benefits and numerous opportunities, and on the other hand, making it extremely dependent and enormously sensitive to the disruptions caused by the misuse of this technology, the paper considers the implications of this technology to national security.
KEY WORDS: information era, information revolution, national security, computer crime, cyber-terrorism, intelligence activities, information warfare.

1. UVOD

Živimo u vremenu u kojem su pokrenute i odvijaju se duboke društvene promene izazvane rapidnim širenjem i upotrebom informacine tehnologije. Jedno od obeležja ovog procesa u istorijskom kontekstu je i imenovanje sadašnjice kao Informacionog doba – vremenskog segmenta koji je tek počeo, a već je veoma snažno obeležio razvoj ljudske civilizacije. Pronalazak sistema baziranih na računarskoj tehnologiji i njihovo integrisanje sa sistemima zasnovanim na komunikacionoj tehnologiji rezultiralo je novom, vrlo snažnom multidimenzionalnom i multifunkcionalnom – informacionom tehnologijom, koja čini osnovu ovog novog doba. Promene koje je ova tehnologija sa sobom donela i još uvek donosi toliko su snažne i sveobuhvatne da je ceo proces dobio i drugo prepoznatljivo obeležje – Informaciona revolucija. Najzad, kao rezultat ovih revolucionarnih procesa nastao je i Internet, koji je od svoje inicijalne forme, kao bezbedni, nuklearnootporni komunikacioni sistem za vojne potrebe, prerastao u istinski globalni komunikacioni medij, koji danas predstavlja treće ključno obeležje i najupečatljiviji simbol novog doba. Njegove poznate procenjene dimenzije su: broj hostova 439,286,364 (juli 2006. god.),[1] broj sajtova 101,435,253 (novembar 2006. god.) i broj korisnika [2] 1,596,270,108 (31. mart 2009. godine).

Reč je o jednoj svetski rasprostranjenoj mogućnosti, mehanizmu za diseminaciju informacija i medijumu za saradnju i interakciju na pojedinačnoj i grupnoj osnovi, bez obzira na geografsku lokaciju učesnika. Ključni koncept *Interneta* je da on nije bio dizajniran za samo jednu aplikaciju, već kao generalna infrastruktura na kojoj se mogu razvijati nove međusobno nezavisne aplikacije. Ovo je u najvećoj meri omogućila opšta priroda servisa koju pruža familija protokola *TCP* i *IP*. Za razliku od drugih računarskih mreža, Internet je suma mnogih delova i sastoji se ne samo od jednog već od višestrukih sistema podataka koji su razvijeni nezavisno.

Ono što ga, pored njegove veličine i rasprostranjenosti, čini toliko poznatim, značajnim i iznad svega privlačnim su svakako njegove specifične karakteristike i brojni servisi koje širom sveta nudi svojim korisnicima.

Od specifičnih karakteristika Interneta svakako treba pomenuti sledeće:

– *Laka pristupačnost;*
– *Elastičnost u ne-kritičnim situacijama;*
– *Niski troškovi.*

Laka pristupačnost. Pristup Internetu, uz minimalne tehničke uslove, sa bilo koje fizičke lokacije (kancelarija, radna, hotelska ili spavaća soba) je jednostavan i lako ostvarljiv. Ako se tome doda i mogućnost pristupa sa mobilnih platformi, koje u sve većoj meri postaju i komercijalno raspoložive, onda se zaista može konstatovati da pristupanje Internetu maltene i nema ograničenja.

Elastičnost u ne-kritičnim situacijama. Dosadašnja iskustva pokazuju da Internet obezbeđuje adekvatnu raspoloživost i pouzdanost za rutinsko korišćenje. Uprkos široko publikovanim prognozama predstojećeg "Internet kolapsa" i znatnog porasta njegovog korišćenja, dugi prekidi nisu zapaženi, a prekidi koji su se javili generalno su bili razrešeni prilično brzo. Ono što svakako nije teško predvideti je da će porast komercijalnog korišćenja Interneta stimulisati rast njegovih sposobnosti i poboljšanje njegove raspoloživosti i pouzdanosti.

Niski troškovi. U poređenju sa alternativnim telekomunikacionim mogućnostima, Internet komunikacija se može oceniti kao jeftina. Mada će se neke zemlje suočiti i sa višim troškovima, razumne procene troškova alternativnih komu-

[1] Robert H'obbes' Zakon, Hobbes' Internet Timeline v8.2, http://www.zakon.org/robert/internet/timeline/
[2] Internet Hits 1,596 Million, http://www.internetworldstats.com/pr/edi040.htm#3

nikacija na kraju ipak favorizuju Internet. Iz tog razloga, korišćenje Interneta je atraktivan put za mnoge organizacije, grupe i pojedince.

Ključni servisi su:

– *Elektronska pošta (e-mail);*
– *World Wide Web;*
– *Usenet;*
–*Video konferencijski sistemi.*

Ovi i mnogi drugi servisi Interneta pružaju svim korisnicima globalne mreže brojne i raznolike usluge i mogućnosti utičući direktno ili indirektno na način odvijanja najraznovrsnijih aktivnosti i poslova u lepezi od trivijalnih do najobimnijih i najsloženijih. Informaciona revolucija je u toj meri zahvatila društvenu zajednicu da ni jedan, čak ni najsitniji, društveni segment nije ostavljen po strani. To drastično i dramatično redefiniše načine kako pojedinci, grupe, organizacije i nacije komuniciraju, uče i rade.[3]

Zašto informaciona tehnologija osvaja svet brzinom i na način koji su bez presedana u istoriji ljudskog razvoja? Sažet odgovor bi mogao da glasi: sa informacionom tehnologijom sve se može raditi *bolje, brže, lakše, obimnije* i *jeftinije*, a to su sasvim dovoljni razlozi za svakog ko racionalno razmišlja i odgovorno se ponaša da bez rezerve prihvati ovu tehnologiju. Dokazi ispravnosti ovakvog stava su u činjenici da najrazvijenije zemlje sveta za dostignuti nivo razvoja u najvećoj meri duguju obimnom korišćenju informacione tehnologije. Takođe ne treba zanemariti i činjenicu da je za izlaz iz globalne ekonomske krize, koja je trenutno zahvatila ceo svet, jedno od najsnažnijih i najefikasnijih sredstava upravo informaciona tehnologija. Zbog toga nezadrživo i sveobuhvatno širenje informacione tehnologije ne bi trebalo ni da čudi ni da iznenađuje.

Na veliku žalost, iz globalnih uticaja informacione tehnologije ne proizilaze samo društveno prihvatljive i poželjne mogućnosti i pogodnosti, dostupne savremenom čoveku, već i vrlo ozbiljne implikacije: velika zavisnost društvene zajednice od informacione tehnologije, pa samim tim i njena visoka osetljivost (ranjivost) na slučajne ili namerne poremećaje, sa posledicama koje mogu da dosegnu čak i do ugrožavanja nacionalne bezbednosti.

S tim u vezi značajno je ukazati da termin *nacionalna bezbednost*, oko čije definicije, zbog ekstenzivno menjajućih karakteristika bezbednosnog ambijenta, ne postoji opšta saglasnost, na najvišem nivou opštosti podrazumeva obezbeđivanje zaštite pojedinaca, društva i države od rizika izazvanih internim ili eksternim uticajima političke, ekonomske, socijalne, vojne, ekološke, informacione i druge prirode.

Dakle, transformacija koja se na buran način odvija pred našim očima praćena je, s jedne strane, efektima koji ukazuju na njen ogroman potencijal iskazan prilikama i mogućnostima dostupnim savremenom čoveku, a sa druge strane implikacijama koje označavaju svu ozbiljnost i složenost brojnih rizika čije su glavne odrednice razne vrste poremećaja koji iz toga mogu da proizađu.

2. EFEKTI INFORMACIONE TEHNOLOGIJE

Tranzicija iz Industrijskog u Informaciono (post-industrijsko) društvo odvija se uz pomeranje fokusa od proizvodnje materijalnih dobara ka pružanju usluga, kreirajući istovremeno i novi ambijent u kojem ključni društveni resursi industrijskog doba (pre svega materijal i energija) na skali društvenih vrednosti ustupaju mesta informacijama, odnosno znanju, koji u novom informacionom dobu postaju najviše društvene vrednosti. U takvom ambijentu, sa novanastalim društvenim vrednostima, rađa se i novo učeno društvo bazirano na znanju, a njegove vodeće socijalne grupe postaju radnici sa znanjem kojima će informaciona tehnologija predstavljati pokretačku snagu za snažno reoblikovanje svakog aspekta socijalnog, političkog, kulturnog i ekonomskog života.

Transformacija je zahvatila sve segmente društvene zajednice, a njeni efekti su brojni, obimni i dalekosežni. Korporacije i vlade se reorganizuju da bi povećale produktivnost, poboljšale kvalitet proizvoda i usluga i kontrolisale troškove. Cele industrije bivaju restrukturirane da bi se prilagodile zahtevima digitalnog doba. Institucije svih vrsta se hvataju u koštac da na nove izazove odgovore adaptiranjem svojih strategija i aktivnosti. Dakle, bukvalno niko ne ostaje po strani.

Ilustracije radi pomenimo samo tipične promene u oblastima koje su ključne za funkcionisanje svakog društva i u kojima primena informacione tehnologije može imati impresivne ekonomske i socijalne efekte: [4]

– *Socijalni domen;*
– *Državna uprava;*
– *Poslovanje;*
– *Naučno-istraživački rad;*
– *Edukacija;*
– *Zdravstvena zaštita.*

Socijalni domen. Tipični uzorci promena u socijalnom domenu su *sloboda govora i globalna povezanost*. Stvorene su realne mogućnosti da skoro svako može lako, brzo i jeftino da se poveže na Internet i da na njemu ima lični *Home page* na kojem može postaviti ili u *sobama za ćaskanje* reći sve ono šta želi i hoće, a potencijalni auditorijum za takvo prenošenje je vrlo velik. Takve povoljne, jeftine i stalne mogućnosti za slobodan govor su bez presedana. S druge strane lakoća sa kojom informaciona tehnologija dozvoljava građanima sveta da budu u vezi sa ljudima i događajima bilo gde unutar objedinjenog sveta je besprimerna.

[3] "Information Operations (the cyber threat)", Canadian Security Intelligence Service, CSIS/SCRS 1999, http://www.csis-scrs.gc.ca/eng/operat/io2e.html
[4] The Global Course of the Information Revolution: Political, Economic, and Social Consequences, Proceedings of an International Conference,2000 RAND, http://www.rand.org/pubs/conf_proceedings/ 2007/CF154.pdf; The Implications of Information and Communications Technologies for Distance Education: Looking Toward the Future, SRI Project Number P11913, June 2004, http://sri.com/policy/csted/reports/sandt/it/Distance_Ed_Lit_Review_FINAL_6-9-04.pdf

Državna uprava. U većini država, većina građana opravdano smatra da je njihova državna uprava *preglomazna, neefikasna i vrlo skupa*. Brojni pokušaji da se stanje promeni na bolje ostali su neuspešni. Međutim, informaciona tehnologija pružila je veliku šansu i mogućnost da se i u ovoj oblasti ostvare pozitivni efekti, odnosno da se državna administracija konačno približi građanima i da uveća kvantitet i kvalitet svojih usluga, da poveća efikasnost i smanji troškove u javnom sektoru, stimuliše uvođenje novih i poboljšanje postojećih servisa. U ovom kontekstu svakako je vredna pomena i najava održavanja prve elektronske sednice srpske vlade, što predstavlja prvi, ali vrlo značajan korak ka stvaranju jedne visprene, efikasne i jeftine (elektronske) vlade informacionog doba, organizovane po funkcijama i potrebama građana.

Ovo svakako uliva nadu da će i birokratija konačno biti svedena na razumnu veličinu i postavljena na pravo mesto. Rešenje ovog izuzetno velikog i za svaku državu preskupog problema nudi koncept elektronske vlade (e-Governmenta), zbog čega su sve vlade sveta, koje su shvatile i razumele mogućnosti i prednosti informacione tehnologije, pokrenule akciju realizacije ovog koncepta. Iz tih razloga informaciona tehnologija postala je centralni alat za vlade mnogih zemalja, jer su prepoznale vitalnu ulogu računara u izvršavanju administrativnih poslova. Ovo utoliko pre jer skoro da nema funkcije u bilo kojoj vladi – administrativne, naučne, vojne, policijske – koja ne zavisi od funkcionisanja računarskog hardvera i softvera.[5]

Ono što predstavlja drugu stranu medalje je činjenica, koja se u potpunosti uklapa u koncept ovog rada, da su državne uprave postale zavisne od informacione tehnologije do te mere da ugrožavanje i narušavanje primene ove tehnologije može stvoriti velike nevolje u radu vlade i njenih organa, sa posledicama koje nije teško pretpostaviti.

Poslovanje. Sve poslovne organizacije, u uslovima sve jače i brojnije konkurencije i brzih promena zahteva potrošača, u manjoj ili većoj meri ulažu napore da otkriju kako da korišćenjem informacione tehnologije brže i bolje iskoriste prilike i mogućnosti koje im ona nesebično pruža. Savremeno poslovanje bazirano na informacionoj tehnologiji ima mogućnost da smanji troškove proizvodnje i da poveća prihod kreiranjem novih tržišta za stare proizvode, da kreira nove proizvode na osnovu prikupljenih informacija o potrebama i željama potrošača za istim i da formira nove mogućnosti pružanja usluga svojim klijentima.

Novo poslovanje zahteva i nove metode upravljanja koje se odnose, pre svega, na upravljanje znanjem. Takvo upravljanje podrazumeva drugačiju organizacionu strukturu, a upravo informaciona tehnologija ima revolucionarne implikacije na promenu strukture organizacije. Ona suspenduje hijerarhiju eliminišući nivoe srednjih rukovodilaca čija je uloga bila da prikupljaju informacije i prenose ih naviše ili naniže u organizacionoj piramidi. Nove organizacione strukture koriste timove izvršilaca povezanih preko informacionih mreža sa onima koji oblikuju politiku, redukujući na ovaj način potrebu za internim posrednicima. Potreba za eksternim posrednicima se takođe redukuje. Proizvođači i potrošači i proizvođači i snabdevači su povezani mnogo direktnije, nezavisno od geografske lokacije, značajno reducirajući troškove i uveliko povećavajući korisnost i opticaj informacija koje se dvosmerno razmenjuju.[6]

Naučno-istraživački rad. Rapidna evolucija digitalne tehnologije prezentuje brojne izazove i mogućnosti naučno-istraživačkom sektoru i već je ostvarila nemerljivo snažan uticaj u oblasti naučno-istraživačkog rada. Inovacije na polju robotike, nano-tehnologije i genetike, kao i u mnogim drugim naučno-istraživačkim oblastima, omogućene su niskim troškovima računarskih operacija i kontrolnim mogućnostima koje pružaju računari i softveri. Internet, najznačajnija forma informacione tehnologije, posebno je popularan među naučnicima i verovatno predstavlja najznačajniji naučni instrument novijeg doba. Moćan, sofisticiran pristup koji on obezbeđuje u prikupljanju, sređivanju, skladištenju, ažuriranju, obradi, pretraživanju i razmeni podataka i informacija, kao i pogodnosti elektronske dokumentacije koju karakteriše jednostavnost dokumentovanja, lakoća upravljanja, modifikovanja, ažuriranja, čuvanja i distribucije, dostupnost i niski troškovi (hartija se koristi samo za finalnu verziju), i najzad, raznovrsne, efikasne i jeftine mogućnost međusobne komunikacije elektronskim porukama, trenutnim porukama, razmenom elektronskih dokumenata i videokonferisanjem, enormno olakšavaju, poboljšavaju i ubrzavaju naučna istraživanja.[7]

Edukacija. Informaciona tehnologija nas neumitno oslobađa tradicionalnog, ali istrošenog modela učenja *("iskusan" nastavnik ispred razreda usmeren na rasejavanje znanja zarobljenoj grupi studenata)*, jer podstiče druge modele razrednog učenja. Za razliku od industrijskog doba u informacionom dobu nastavnici i studenti neće morati biti na istom mestu u isto vreme, ali će, zahvaljujući informacionoj tehnologiji, moći i da se vide i da se čuju. Takođe, iz istog razloga, učenje neće morati da se zaustavi kada se student pridruži zaposlenima, već se može odigravati do kraja njihovog života (individualno doživotno učenje).

Tehnologija može kreirati jedan otvoren edukacioni ambijent u kojem studenti nisu više primorani da putuju do određene lokacije da bi participirali u pedagoškom procesu. Studenti se sada pomeraju od fizičkih ka virtuelnim lokacijama, globalno distribuiranim u kiber-prostoru. Čist dobitak koji iz ovog neposredno proizilazi je i u vremenu i kvalitetu. Na

[5] Haque A., Ethical Implications of Information Technology in Government: A Closer Look at GIS, School of Social and Behavioral Science, Department of Government and Public Service, The University of Alabama at Birmingham, http://www.netcaucus.org/books/egov2001/pdf/Ethicsin.pdf, str. 5.

[6] An introduction to e-business optimisation, http://www.weboptimiser.com/resources/index.html; Introduction to E-business, http://www.bgateway.com/bg-home/bg-services.htm

[7] Davidson T., Sooryamoorthy R., Shrum W., Kerala Connections: Will the Internet Affect Science in Developing Areas?, 2002, http://worldsci.net/EVERY4.pdf ; Finholt A. T., Collaboratories: Science over the Internet, 2002, http://www.aaas.org/spp/yearbook/2002/ch31.pdf ; Guice J., Duffy R., The Future of the Internet in Science, USRA Research Institute for Advanced Computer Science, NASA Ames Research Center, USA, http://ase.arc.nasa.gov/publications/pdf/2000-0174.pdf

žalost, visoko-obrazovne edukacione funkcije još uvek manje-više ostaju nepromenjene i učenje uveliko nastavlja da prati uzorak baziran na sedištu i centriran na učionicu, iako informaciona tehnologija omogućava pružanje edukacionih servisa bilo kome, na svakom mestu i u svako vreme. Ali, vreme će sigurno učiniti svoje.

Ekonomski domen. Rapidni napredak u informacionoj tehnologiji istovremeno znači i drastične promene u proizvodnoj tehnologiji, radnim mestima i strukturi poslova. U prerađivačkoj (posebno mašinskoj) industriji, industrijski roboti igraju značajnu ulogu u promovisanju tzv. automatizovanih fabrika, koje su nastale investiranjem u informacionu tehnologiju. Isto tako, automobilska industrija je značajno uspela u skraćivanju razvojnog perioda automobila, oslanjajući se na softver za računarski-potpomognuto dizajniranje (CAD). Isti softver je omogućio arhitektama da "šetaju" po "virtuelnim zgradama", ispituju ih i, ako je potrebno, remodeliraju ih, a sve pre nego što je zgrada i počela da se gradi. Rastuća upotreba sistema za naplatu (*point-of-sales* – POS) u maloprodaji i mašina za automatsku isplatu novca (ATM) u bankarstvu samo potvrđuju pomenuti trend.[8]

Investiranje u informacionu tehnologiju i tehnološki progres na radnim mestima, kao što pokazuju iskustva razvijenih zemalja, mogu imati vitalnu ulogu u ekonomskom razvoju. Površna observacija sugeriše da su se i radnici i firme, pa samim tim i društvo u celini, okoristili od informacione tehnologije.

Danas, uspešno poslovanje u sve većoj meri zavisi od kontinuiranog i pouzdanog funkcionisanja informacionih sistema. Ustanove, organizacije, korporacije i vladine institucije, koje su shvatile značaj tehnologije i njene primene, životno su zainteresovane da im njihovi računari pouzdano funkcionišu. Zato, svi oni čine sve da bi adaptirali svoje strategije i aktivnosti i prilagodili ih realnostima digitalnog doba.

Zdravstvena zaštita. Informaciona tehnologija ima potencijal da fundamentalno poboljša, i kvalitativno i kvantitativno, stanje u ovoj oblasti. Pored toga, ona sadrži i obećanje za značajnu redukciju ovog tipa troškova, koji ni malo nisu za potcenjivanje. Zato ne iznenađuje činjenica da oblast zdravstva predstavlja vrlo pogodno tle za veoma obimnu primenu informacione tehnologije. Ova tehnologija menja zdravstvenu zaštitu veoma radikalno: menja način na koji lekari međusobno komuniciraju, uključujući konsultacije specijalista; transformiše način na koji pacijenti pristupaju i dele informacije; nudi dodatne kanale kroz koje nega može biti dostupna pacijentima; i najzad, osetno umanjuje troškove.[9] Svaka ozbiljnija debata o zdravstvenoj zaštiti ukazuje na velike mogućnosti za osavremenjavanje i racionalizaciju njenih uslužnih i administrativnih aspekata, samo ih treba osmišljeno koristiti.

I u ovom slučaju potrebno je u razmatranom kontekstu ukazati da se uključivanjem informacione tehnologije i zdravstvena zaštita, poput drugih oblasti, sve više pomera prema većoj zavisnosti upravo od te tehnologije.

3. IMPLIKACIJE INFORMACIONE TEHNOLOGIJE

Pod uticajem burnog razvoja i sve šire i obimnije primene informacione tehnologije nastaje jedan novi paralelni svet u virtuelnom prostoru koji je označen prefiksom *kiber* i obeležen računarima, računarskim mrežama, informacionim procesima, tokovima i sadržajem u digitalnoj formi. Imajući u vidu činjenicu da je jedan od strateških ciljeva primene informacione tehnologije, s jedne strane, maksimalna automatizacija svih ljudskih aktivnosti i procesa, a sa druge strane, digitalizacija svega onoga što čovek ima i što vrednuje, *kiber-prostor*, koji je u stanju rapidne evolucije, postaje istovremeno i riznica nacionalnog bogatstva u elektronskoj formi – intelektualnog, duhovnog, materijalnog, finansijskog i informacionog, ali i opšte mesto događanja za najraznovrsnije ljudske aktivnosti, od najjednostavnijih i najbezazlenijih do najsloženijih i najopasnijih. U svemu tome informaciona tehnologija postaje glavni, a sve češće i jedini alat za obavljanje navedenih aktivnosti.

Ono što u razmatranom kontekstu svakako treba uočiti i zapaziti jeste da se ogroman uticaj informacione tehnologije na društvenu zajednicu ogleda u trajnim promenama u načinima komuniciranja, informisanja, obrazovanja, rada i zabave. S tim u vezi posebno zaslužuje pažnju trend ovih promena koji podrazumeva transformaciju poslova *od fizičkih ka mentalnim, od snage mišića ka snazi uma.* Zamena *fizičke* sa *umnom snagom* predstavlja grandioznu promenu koja je zaista i drastična i dramatična, i iz nje proizilazi i proizilaziće veoma širok spektar nacionalnih i međunarodnih političkih, ekonomskih i socijalnih pitanja, i sada i u budućnosti. Ovo utoliko pre, jer ogromna moć koja iz te i takve transformacije nastaje i koncentriše se u kiber-prostoru i koju informaciona tehnologija, pre svega preko Interneta, nesebično dezintegriše na nivo grupa i pojedinaca, uvećavajući njihove veštine i mogućnosti do neslućenih razmera, može da se upotrebi ne samo za dobrobit čovečanstva, već i za vrlo ozbiljnu zloupotrebu. A, svi moraju biti svesni potencijalnih posledica činjenice da se ta velika *nekontrolisana* moć nalazi u rukama grupa i pojedinaca.

Navedene promene izgledaju tako obimne i duboke da opravdavaju njihovo označavanje kao *"revoluciju veštine"*, koja omogućava grupama i pojedincima da u informacionom domenu, nezavisno od fizičkog rastojanja između lokacije napadača i lokacije cilja, vremenskih prilika i vremenskih zona, godišnjih doba i doba dana i noći, od otvorenosti ili zatvorenosti državnih granica, carinskih barijera i drugih prirodnih ili veštačkih prepreka, dosežu do bilo koje "tačke" na zemaljskoj kugli i izvršavaju veoma ozbiljne kriminalne akcije po celoj planeti, a da se nisu ni pomerili iz svoje radne, dnevne ili hotelske sobe ili bilo kojeg Internet kafea. Prošlost ovako nešto nije poznavala.

[8] Tribe H. L., The Constitution in Cyberspace, op. cit.
[9] Advocat J., Internet clinical trials: examining new disciplinary experiments in health care, Monash University, Australia, Anthropology Matters Journal 2005, Vol 7 (1), http://www.anthropology matters.com

Posebnu težinu u ovom kontekstu ima činjenica da informaciona tehnologija raspolaže i jednom dodatnom karakteristikom koja veoma podsticajno deluje na izvršavanje nelegalnih aktivnosti – u virtuelnom ambijentu pruža izuzetno visok stepen *anonimnosti*, koja rezultira vrlo niskim nivoom rizika koji treba prihvatiti, otvarajući time širok prostor "bezopasnog" delovanja. U fizičkom svetu o ovakvim pogodnostima se ne može ni sanjati. Zbog svega toga ne bi trebalo da nas iznenadi što će od 1,596,270,108 Internet korisnika, koliko ih trenutno ima, značajan procent zloupotrebu moći i mogućnosti koje su im postale dostupne usmeriti ka našem kiber-prostoru.

S druge strane, kao rezultat dramatičnog rasta primene informacione tehnologije, nacionalne infrastrukture postaju uvećano automatizovane i međusobno povezane. Danas, većina država ima suštinske resurse bazirane na informacionoj tehnologiji, uključujući odbrambene sisteme, sisteme državne uprave, kompleksne upravljačke sisteme i infrastrukture koje obuhvataju kontrolu električne energije, telefonskog sistema, tokove novca, vazdušni saobraćaj, naftu i gas, i druge informaciono zavisne oblasti. Oslanjane na informacionu tehnologiju u ovolikoj meri neminovno vodi do velike zavisnosti od te tehnologije, a samim tim i do osetljivosti – ranjivosti društvene zajednice u novom informacionom dobu. Kako se ova zavisnost bude uvećavala, tako će se takođe uvećavati i osetljivost društva na svako narušavanje ili kompromitaciju nacionalne informacione infrastrukture i automatizovanih aktivnosti i procesa.

Dakle, spoj rastuće moći i mogućnosti zloupotrebe i povećavajuće zavisnosti od informacione tehnologije, odnosno povećavajuće osetljivosti (ranjivosti) društvene zajednice, uslovio je da prvi pojedinačni slučajevi zloupotrebe tehnologije veoma brzo prerastu u talas zloupotrebe, čija tendencija preti da ga pretvori u digitalni cunami.

Iz istih razloga iz kojih je industrijsko društvo povezano sa zaštitom fizičkog kapitala i obezbeđivanjem zaštićenih ruta za transport resursa, i informaciono društvo mora biti povezano sa zaštitom informacija i transfera informacija. I kao što je destrukcija, na primer, mostova, fabrika ili centrala pretnja nacionalnoj bezbednosti industrijskog društva, destrukcija informacione infrastrukture, procesa koji se u njoj odvijaju i digitalnih sadržaja koji se obrađuju, skladište ili transportuju sigurno će biti isto toliko ozbiljna pretnja nacionalnoj bezbednosti informacionog društva.

Termin *nacionalna informaciona infrastruktura* se definiše kao fizička i virtuelna kičma informacionog društva i predstavlja generalnu oznaku za složeno komponovanu komunikacionu mrežu na nacionalnom nivou, unutar koje i preko koje se skladište, obrađuju i prenose podaci i informacije, čineći osnovu za ekonomsko, političko i vojno funkcionisanje.[10]

Ovakva jedna informaciona infrastruktura uključuje, na minimumu, sledeće:

– *Finansijske mreže za transfer informacija između finansijskih institucija;*
– *Mreže privatnih korporacija i institucija za njihovu međusobnu razmenu informacija, različitih vrsta i sadržaja;*
– *Javne mreže sa slobodnim pristupom;*
– *Kooperativne mreže koje povezuju edukacione i istraživačke mogućnosti za zajedničku dobit, kao što je slučaj sa Internetom;*
– *Pretplatne mreže koje obezbeđuju pristup na osnovu takse da objedine virtuelne zajednice, kao što je slučaj sa Prodigy, Compuserve i America On-line;*
– *Vladine i vojne mreže;*
– *Mreže za javne usluge: sistemi za snabdevanje električnom energijom, vodom i gasom, transportni i saobraćajni sistemi, sistemi za vanredne situacije i sl.*

Ova prilično široka lista sastavljena je da demonstrira tekuće oslanjanje na informacionu tehnologiju. Međutim, sa funkcionalnog, ali i sa bezbednosnog aspekta lista obuhvata mnogo širu sferu u kojoj se nalazi široka skala opreme, uključujući kompjutere, monitore, printere, tastature, kamere, skenere, faks mašine, svičeve, kompakt diskove, video i audio trake, optičke i klasične kablove, telefonske žice, satelite i još mnogo toga. Ljudi angažovani na rukovanju i upravljanju ovom strukturom, kao i podaci i informacije koji se skladište, obrađuju i prenose, takođe konstituišu kritične komponente nacionalne informacione infrastrukture.

Što se tiče informacionog sadržaja nacionalna informaciona infrastruktura koristi se za skladištenje, obradu i prenos javnih, ali i vitalnih podataka i informacija, od medicinskih slogova, preko informacionih sadržaja državnih organa, vojnih informacija, istraživačkih rezultata i poslovnih planova, podataka o kriminalnim aktivnostima pojedinaca, grupa i organizacija, pa do ličnih podataka pojedinaca.

U ovako formiranom strukturno, funkcionalno i sadržinski bogatom informacionom ambijentu, informaciona tehnologija kreira rastuću osetljivost društvene zajednice, stvara uslove i širi prostor za izvršavanje ne samo klasičnih kriminalnih, već i onih aktivnosti kojima je realno moguće ugroziti nacionalnu bezbednost jedne zemlje. S tim u vezi, zaista nije potrebno imati previše mašte da bi se zamislile potencijalne posledice po nacionalnu bezbednost koje bi mogle rezultirati iz namernih ataka na nacionalnu informacionu infrastrukturu, informacione procese i tokove i postojeći digitalni sadržaj.

Ilustracije radi navedimo neke od mogućnosti ugrožavanja nacionalne bezbednosti:

– *Uskraćivanje ili remećenje informacionih servisa;*
– *Neovlašćeno monitorisanje informacionih sistema;*
– *Neovlašćeno otkrivanje klasifikovanih podataka i informacija koji se obrađuju, prenose ili su uskladišteni unutar sistema;*
– *Neovlašćenu modifikaciju ili destrukciju umreženih baza podataka i podataka i informacija koji su uskladišteni, u obradi ili u prenosu;*

[10] Devost G. M., National Security In The Information Age, May, 1995, http://www.terrorism.com/documents/devostthesis.html; Freeh J. L., Threats to U. S. National Security, Congessional Statement, FBI, January 28, 1998, http://www.fbi.gov/pressrm/congress/congress98/threats.htm

– *Neovlašćenu modifikaciju ili destrukciju kompjuterskog programskog koda ili kompjuterskih mogućnosti;*
– *Manipulaciju informacionim servisima, koja bi rezultirala prevarom, finansijskim gubitkom ili drugim kriminalnim delom.*

Potencijalni ataci na vladine i vojne informacije, posebno one klasifikovane, predstavljali bi pretnju nacionalnoj bezbednosti sa strateške tačke gledišta, a ometanje ili uskraćivanje komunikacionih mogućnosti, izmena ili uništenje obaveštajnih podataka mogli bi imati duboke efekte na mogućnost uspešnog funkcionisanja državnih i vojnih organa. Isto tako, sinhronizovan i uspešan napad na samo nekoliko većih poslovnih informacionih sistema bi mogao izazvati ozbiljno zaostajanje nacionalne ekonomije. Ako bi, primera radi, Wall Street iznenada obustavio rad ili ako bi bankarske transakcije iznenada nestale – SAD bi izgubile stotine milijardi dolara. Procenjuje se da je dnevna vrednost telefonskih transakcija samo na Wall Street-u viša od teško zamislivih bilion dolara.[11]

S druge strane, pretnje koje potiču iz kiber-prostora mogu biti uzrokovane od strane klasičnih kriminalaca, organizovanog kriminala, konkurencije, terorista i tajnih službi prijateljskih i neprijateljskih zemalja. Dakle, jedna brojna i raznovrsna skupina. U razmatranom kontekstu od interesa su svakako teroristi i strane obaveštajne službe. Naravno, nikako se ne smeju zanemariti ni ostali (kriminalci, organizovan kriminal i konkurencija), ali je njihov doseg znatno niži i predstavljaju nacionalnu opasnost prvenstveno ako su u funkciji osnovne dve grupacije – terorista i obaveštajnih službi.

Iz napred izloženog očigledno proizilazi da mogućnosti napada na nacionalna kiber-dobra u informacionom ambijentu formiraju širok spektar pretnji koje se u cilju njihovog sagledavanja, analiziranja i razrešavanja, sa vrlo malo izuzetaka, mogu agregirati u jednu od četiri sledeće kategorije:

– *Kiber-kriminal;*
– *Kiber-terorizam;*
– *Obaveštajno delovanje;*
– *Informaciono ratovanje.*

Ključni kriterijum za ovu agregaciju je stepen društvene opasnosti u rastućem redosledu značajnosti sa aspekta nacionalne bezbednosti. Pri tome, mora se znati da svaka od ovih kategorija predstavlja složen pojam, posmatran sa aspekta načina realizacije, porekla (izvorišta), izvršilaca, motiva, upotrebljenih resursa i ciljnih meta, kao i da aktivnosti svake kategorije u datim trenucima, zavisno od potreba i okolnosti, postaju sastavni deo više – nadređene kategorije.

Kiber-kriminal. Najjednostavnije rečeno, kiber-kriminal, i pored određenih specifičnosti, podrazumeva *klasičan kriminal izvršen u informacionom ambijentu*. Sama činjenica da se izvršava u ambijentu u kojem informaciona tehnologija ima dominantnu ulogu, ukazuje na prisutnost određenih specifičnosti u odnosu na klasičnu situaciju. Te specifičnosti se ogledaju, pre svega, u činjenici da se ovaj u odnosu na klasičan kriminal, upravo zahvaljujući informacionoj tehnologiji i svemu onome što ona pruža i omogućava, izvršava *lakše, brže, obimnije, dalekometnije i anonimnije,* pa samim tim i *bezbednije*. Pomenimo samo najtipičnije oblike:

– *krađe;*
– *prevare;*
– *pronevere;*
– *falsifikovanje;*
– *iznude;*
– *ucene;*
– *narušavanje privatnosti;*
– *sabotaža;*
– *odavanje tajne;*
– *špijunaža;*
– *pornografija;*
– *propaganda;*
– *vandalizam;*
– *ubistva.*

Takođe, obogaćen je i novim formama koje ranije nisu postojale:

– *Generisanje i distribucija zlonamernih kodova;*
– *Neovlašćen upad u tuđe sisteme (hakiranje);*
– *Piratizacija softvera;*
– *Uskraćivanje servisnih usluga;*
– *Elektronsko uznemiravanje.*

Od tehnika koje se koriste pomenućemo samo one koje u kontekstu ovog rada imaju određenu težinu:

– *Trojanski konj;*
– *Logička (vremenska) bomba;*
– *Lovac (Sniffer) program;*
– *Prikriven ulaz (Trap Door);*
– *Virusi i crvi;*
– *Aktivna infiltracija (Piggybacking);*
– *Prisluškivanje (Wiretapping);*
– *Elektronsko prisluškivanje (Eavesdropping).*

Kiber-terorizam. Ne postoji standardna i opšteprihvaćena definicija ovog pojma, pa dok jedni koriste sažetu, drugi koriste široko opisnu definiciju. Autorov utisak je da se iz sažetih definicija (kao na primer: *... korišćenje informacione tehnologije od strane terorističkih grupa i pojedinaca da prošire svoj program rada*) teško može prepoznati suština kiber-terorizma i zbog toga se, radi jasnoće, opredelio za opisnu definiciju po kojoj je kiber-terorizam *smišljeno korišćenje remetilačkih aktivnosti, ili pretnji time, protiv računara i/ili telekomunikacione infrastrukture, s namerom da se u realnom svetu izazove šteta i ostvare neki društveni, ideološki, verski, politički ili slični ciljevi ili da se u širu javnost unese nesigurnost i strah radi ostvarivanja tih ciljeva*.[12]

Jasno je da u zavisnosti od toga koliko će informacioni sistemi biti značajniji za društvo, da će srazmerno tome oni biti i atraktivniji za terorističke napade. Reč je o jednoj veoma pretećoj pojavi koja zbog zloslutnih potencijalnih implikacija

[11] Devost G. M., National Security In The Information Age, May, 1995, http://www.terrorism.com/documents/devostthesis.html
[12] Šire o Kiber-terorizmu pogledati: Petrović R. S., Kiberterorizam, Vojno delo, god. LIII, br. 2/2001, str. 100-122.

na nacionalnu i međunarodnu bezbednost naprosto ne bi smela biti ignorisana, jer moderno društvo zahvaljujući informacionoj tehnologiji postaje krhka, lomljiva struktura ekstremno osetljiva na poremećaje, a to sigurno neće promaći pristalicama radikalnih metoda. Ovo utoliko pre jer smo svedoci nastajanja jednog novog virtuelnog sveta u kiber-prostoru, sveta koji se razlikuje od običnog fizičkog sveta materije i energije i u kojem vladaju znanje, elektronski impulsi i digitalni brojevi.

Prema tome, u kiber-terorizmu glavni cilj će biti *remećenje* umesto *destrukcije,* mada ni ona nije isključena, jer u društvima visoko zavisnim od informacione tehnologije remećenje informacionih sistema može izazvati kratkoročne probleme različitog obima i intenziteta, ali mnogo značajnije, dugoročno gubljenje poverenja u sposobnost i pouzdanost ovih sistema.

U skladu sa iznetim svakako će biti neophodno korigovati naše poimanje terorizma, pa čak menjati i njegovu definiciju koja konstituiše tradicionalni teroristički akt i prilagoditi je novonastaloj situaciji. Bez toga sadašnja razmišljanja, koja ceo terorizam vide kao politički motivisano i nasilno ponašanje, mogu limitirati mogućnost i sposobnost branilaca da predvide teroristično nasilje, konfrontiraju se sa njim i odgovore na adekvatan način.

Obaveštajno delovanje (špijunaža). Proces koji podrazumeva sistematično prikupljanje podataka i informacija za potrebe otkrivanja mogućnosti i namera rivala. Imalac takvih informacija, što je vrlo bitno, može sebe da zaštititi od svojih protivnika, ali, što nije manje bitno, i da eksploatiše slabosti protivnika.[13] Incidenti i pretnje špijunažom izvršeni korišćenjem softverskih alata su postali česti naslovi u vestima u poslednjih nekoliko godina i još češća tema u naučnim i stručnim radovima, tako da je postojanje kiber-špijunaže neporecivo. Kao snažne softverske alate za obaveštajno delovanje studije slučajeva posebno uključuju korišćenje Trojanskog konja i Sniffer programa.[14]

U zavisnosti od toga kome pripadaju podaci i informacije, obaveštajno delovanje može rezultirati podacima i informacijama različitog nivoa značajnosti i stepena tajnosti. U kontekstu ovog rada od interesa su strateške informacije o drugim državama koje za svoju vladu i njene organe prikupljaju obaveštajne službe za potrebe vođenja spoljne i unutrašnje politike. Strateške informacije obično obuhvataju nacionalnu bezbednost, političke, ekonomske i socijalne trendove u ciljanim državama.

Prema studiji SANS Instituta, istraživačke ustanove, kiber-špijunaža je označena sa brojem 3 na njihovoj Top listi pet najvećih opasnosti-pretnji za 2008. godinu.[15] Dakle, treba naglasiti da je u današnjem društvu kiber-špijunaža u osetnom porastu. Tokom poslednje decenije uvećanju špijunskih aktivnosti je značajno doprinela, s jedne strane, globalizacija, a sa druge strane, rapidni rast primene informacione tehnologije. Ova tehnologija je značajno uprostila način i skratila vreme potrebno za krađu podataka, jer pojedinac može da preuzme podatke u vremenu koje se meri sekundama, nasuprot časovima koji su potrebni pri tajnom dupliciranju dokumenata u klasičnoj situaciji. Pored toga, računari su povezani na Internet, što povećava broj ulaznih tačaka i pristupnih puteva preko kojih se može pristupiti informacijama. Čineći krađu poverljivih informacija lakšom, računari su poboljšali i druge oblike krađe.

Iskustva zapadnih zemalja, posebno SAD, nedvosmisleno pokazuju da novokomponovani termin *kiber-špijunaža* ima svoje puno opravdanje, jer su upravo one izložene serijama špijunskih napada „kroz žicu". To nikako ne znači da su one samo žrtva takvih napada. Naprotiv, razumno je pretpostaviti da i one uzvraćaju udarac i to, s obzirom na dostignuti nivo tehnološkog razvoja, sigurno žešće nego što ga primaju.

Informaciono ratovanje. Definiše se kao: *akcije preduzete da se ostvari informaciona superiornost napadanjem: protivničkih informacija, procesa baziranih na informacijama i informacionih sistema, dok se brane: sopstvene informacije, procesi bazirani na informacijama i informacioni sistemi*.[16] Reč je, dakle, o novoj formi ratovanja koja, opisno, uključuje prikupljanje taktičkih informacija, obezbeđenje validnosti sopstvenih informacija, širenje propagande i dezinformacija radi demoralizacije neprijatelja i javnosti, podrivanje kvaliteta informacija protivničke sile i uskraćivanje neprijatelju mogućnosti kolektiranja informacija.[17]

U razmatranom kontekstu interesantno je napomenuti da američko ratno vazduhoplovstvo od 1980. godine raspolaže eskadronom za informaciono ratovanje. Danas, njihova službena misija glasi: *"Omogućiti suverene opcije za odbranu Sjedinjenih Država i njenih globalnih interesa. Leteti i boriti se u vazduhu, kosmosu i kiber-prostoru"*, pri čemu se poslednji termin odnosi na njihovu ulogu u Informacionom ratovanju.[18]

Kako ratno vazduhoplovstvo često rizikuje avione i posade napadima na strateške ciljeve neprijateljskih komunikacija, daljinsko onemogućavanje takvih ciljeva pomoću softvera i drugih sredstava mogu obezbediti pouzdanije alternative. Osim toga, onemogućavanje takvih mreža elektronski (umesto razorno) takođe omogućava da se one brzo ponovo osposobe nakon zauzimanja neprijateljskih teritorija. Istovremeno, jedinice kontra-informacionog ratovanja se koriste da onemoguće takve sposobnosti neprijatelju. Prva primena tih tehnika je korišćena protiv iračke komunikacione mreže u prvom Zalivskom ratu 1991. godine.[19] Ono što svakako zaslužuje pažnju jeste činjenica da veliki broj zemalja danas intenzivno radi na razvoju informacionog oružja.

[13] Intelligence operations, http://www2.scholastic.com/browse/article.jsp?id=5213
[14] Cyber Espionage, http://www.oppapers.com/essays/Cyber-Espionage/178669
[15] Cyber Espionage, http://www.oppapers.com/essays/Cyber-Espionage/178669
[16] Haeni R., Information warfare – an Introduction, The George Washington University, Cyberspace Policy Institute, January, 1997, http://www.seas.gwu.edu/student/reto/papers/infowar.pdf
[17] Šire o Informaciojnom ratovanju pogledati: Petrović R. S., Kiber prostor - peta dimenzija ratovanja, Vojni informator, br. 4, jul-avgust 2001, str. 29-50; Borden A., What is Information Warfare?, 2 November 99, http://www.airpower.au.af.mil/airchronicles/cc/borden.html
[18] Information warfare, Wikipedia, The Free Encyklopedia, http://en.wikipedia.org/wiki/Information_warfare
[19] Information warfare, Wikipedia, op. cit.

Od brojnih karakteristika ove forme ratovanja navode se dve, koje, po oceni autora, i kontekstu ovog rada najbolje izražavaju njegovu suštinu:

– Bojište informacionog doba nije i neće biti fizički već virtuelni svet kiber-prostora, u kojem su napadač i napadnuti uvek države, pri čemu napadač, zavisno od razvoja situacije, može da koristi sav svoj naučni, tehnički, kadrovski i finansijski potencijal da bi ostvario željeni cilj, a napadnuti često može da i ne zna da je napadnut. Potencijalni ratnici na ovom bojištu mogu se rangirati od vojnih i obaveštajnih organizacija, terorista, kriminalaca i industrijskih konkurenata, do hakera i nezadovoljnih ili nelojalnih sopstvenih građana. Svaki od ovih protivnika motivisan je različitim ciljevima, ograničen različitim nivoima resursa, tehničkim iskustvom, pristupom do cilja i tolerancijom rizika. Pri tome, mnogi izvršioci nižeg nivoa (teroristi, kriminalaci, hakeri, ...) često neće biti ni svesni da su učesnici neke "ratne igre" u kojoj je ratni cilj narušavanje vojne efikasnosti i javne bezbednosti i podrivanje ekonomske moći napadnute države sa elementima iznenađenja i anonimnosti.
– Druga značajna karakteristika informacionog ratovanja je da on može biti dobijen ili izgubljen u kiber-prostoru sa minimalnim krvoprolićem, ali katastrofalnim konsekvencama.

ZAKLJUČAK

Radi jasnoće zaključka vratimo se malo u istoriju i u tom kontekstu pomenimo da se moć računara za poslednjih 30 godina duplirala svakih 18 meseci, da računar danas košta manje od jednog procenta od onog koliko je koštao početkom 1970-tih godina, da se komunikacije rapidno šire i ubrzavaju, a troškovi komuniciranja kontinuirano opadaju. U 1980. godini preko telefonske bakarne žice se mogla preneti jedna strana informacija za jednu sekundu. Za isto to vreme se krajem 1990-ih godina moglo preko optičkih kablova preneti informacija u obimu od 90.000 stranica.[20] Isto tako, ilustracije radi, ukoliko se u SAD plaćanje obavlja u nekoj bankarskoj filijali, trošak ove transakcije iznosi 1,07 dolara, posredstvom telefona upola manje, preko bankomata iznosi 0,27 dolara, ako se koristi kartica 0,18 dolara, dok Internet ovaj izdatak svodi na simboličan 1 cent. Troškovi slanja nekog dokumenta od, recimo, Njujorka do Tokija, najveći su ako se koristi telefaks (oko 29 dolara), a za to je potrebno u proseku pola sata. Slanje aviopoštom, iako staje znatno manje (7,4 dolara) uzeće čak 5 dana. Internet utrošak vremena svodi na dva minuta, a troškove na desetak centi. Poslovni telefonski razgovor između SAD i Singapura, koji bi inače koštao od 90 centi do 1,56 dolara za minut, posredstvom elektronske komunikacije obara ovu cenu na 10 do 45 centi.[21]

Izloženi podaci, iako nisu najnovijeg datuma, dovoljno jasno ukazuju na dinamiku i trend promena koje se odvijaju u informacionoj areni. S tim u vezi sa velikim stepenom izvesnosti se može pretpostaviti da će se mnogi tekući informaciono-tehnološki trendovi nastaviti bar u narednih 15 do 20 godina: računari će postajati minijaturniji, brži, moćniji i jeftiniji, komunikaciona propusnost će se uvećavati, računarske mreže će sve gušće prekrivati planetu, a u kiber-prostoru će se gomilati podaci i informacije u nepredvidivom, ali sigurno enormnom obimu, prilike i mogućnosti će se srazmerno prethodnim promenama takođe uvećavati, a sve zajedno će biti praćeno širenjem zloupotrebe informacione tehnologije u raznovrsnosti, obimu i intenzitetu.

Izazovi i prilike su zaista veliki, ali onaj ko želi da napreduje i da se razvija – izazove mora prihvatati, a prilike koristiti. Mada je rast primene informacione tehnologije dramatičan, većina eksperata se slaže da je to samo početak onog kako će biti nastavljen i rast i zavisnost. Sve to osetno uvećava ranjivost kritične infrastrukture i institucija koje ona podržava, pa samim tim i cela društvena zajednica postaje značajno osetljivija na sve vrste poremećaja. Uprošćeno rečeno, informaciona infrastruktura praktično postaje *Ahilova peta* savremene društvene zajednice.

Poremećaji koji bi nastali zbog izazvanih problema sa nacionalnom informacionom infrastrukturom za posledicu bi mogli, između ostalog, imati potrebu da se funkcionisanje državnih organa, ali i drugih značajnih entiteta, bar u nekim segmentima, vrati na stari – prevaziđen sistem rada. Ovo bi kod građana sigurno izazvalo visok stepen nerazumevanja, nespokojstva, pa i nezadovoljstva, a to svaka odgovorna vlast želi da izbegne.

Zato, zaštita kritične nacionalne infrastrukture i ključnih resursa, iako je izuzetno složen i težak problem za rešavanje, ne samo zbog obima infrastrukture, pretnji različite prirode i mnoštva izvora pretnji, mora imati vrlo visok nacionalni prioritet, posebno što je većina ovih pretnji prisutna i na nacionalnom nivou. Ova činjenica bi morala izazvati određene promene u konceptima nacionalne bezbednosti u svakom post-industrijskom društvu koje ozbiljno razmišlja o dugoročnom stanju sopstvene bezbednosti. Ovo utoliko pre jer će se nacije sve više suočavati sa ozbiljnom opasnošću da njihove informacione infrastrukture, na kojima će biti zasnivano njihovo ukupno funkcionisanje, budu uništene, izmenjene ili onesposobljene novom ofanzivnom tehnologijom. To će svakako uticati da najvažnije strategije moraju integrisati ove nove pretnje i osetljivosti u svoj generalni okvir, jer će nacionalna bezbednost, kako sada stvari stoje i kako ukazuju vidljivi trendovi, verovatno biti jedan od najvećih izazova sa kojima će se u novom informacionom dobu suočavati nacionalna rukovodstva.

Ono što ozbiljno zabrinjava je svakako činjenica da se sve te promene odvijaju obimno i možda previše brzo da bi se na sve njih moglo adekvatno i blagovremeno reagovati. Posebno ako se kasni u pripremnim radnjama. Ipak, odustati se ne može iz prostog razloga što kiber-prostor predstavlja i previše značajan prostor da bi olako bio prepušten samo njegovim korisnicima i slučajnim posetiocima. On mora biti stavljen pod kontrolu i u njemu moraju da važe pravila kao i u realnom fizičkom svetu. Ono što trenutno predstavlja problem je svakako činjenica da opštevažeća pravila industrijskog doba u novom informacionom ambijentu, zbog njegove specifičnosti,

[20] Keohane O. R., Nye S. J., "Power and Interdependence in the Information Age", Foreign Affairs, v. 77 no. 5 (September/October 1998), pp 81-94.
[21] Mijalković A., "Lepša strana globalizacije", Politika, 25- mart 2002. god., str. 4.

ili ne funkcionišu adekvatno ili uopšte ne funkcionišu, što nameće imperativnu potrebu posebnog regulisanja ovog prostora, kako bi se u njemu obezbedili neophodni funkcionalni i bezbednosni uslovi za nesmetano odvijanje svih legalno i moralno dozvoljenih aktivnosti i procesa.

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 i koriste ga ili će ga veoma skoro početi koristiti. Da nije reč samo o praznim pričama najbolje potvrđuje Strategija nacionalne bezbednosti Rusije do 2020. godine, u kojoj, prema pisanju Politike (14.05.2009.), između ostalog stoji i konstatacija da se *očekuje pojačanje globalnih informacionih sukoba, ...* , a kao posebna opasnost pominju se strane obaveštajne službe i terorističke organizacije.

U svemu tome Srbija ne može ostati izolovano ostrvo koje niko neće dirati. Naprotiv, a te činjenice moraju biti svesni pre svega oni koji su odgovorni za odbranu i bezbednost zemlje i koji su obavezni da u okviru svoje odgovornosti prate, otkrivaju, analiziraju, predviđaju i odlučuju. Kritičan pravac delovanja bi svakako bio detaljno preispitivanje mesta i uloge kriminalističkih, obaveštajnih i kontraobaveštajnih službi i njihovo adekvatno reoblikovanje saglasno bezbednosnim potrebama i zahtevima tekućeg i budućeg vremena. Kako su ove službe, kao i u većini drugih zemalja, formirane za neka bivša ili sadašnja vremena, to je očigledno da počivaju na skupu normi koje ih definišu za ta vremena i od kojih su neke sigurno zastarele i ne odgovaraju nastalim promenama stanja i odnosa, niti potrebama i zahtevima nacionalne bezbednosti kako dublje ulazimo u 21. vek. Upravo zbog toga, te norme treba revidirati ili zameniti i dopuniti novijim i adekvatnijim.

Sve promene bi morale biti celovito i vizionarski osmišljene i morale bi rezultirati rešenjima koja bi organizaciono, funkcionalno, tehnički i kadrovski zadovoljila bezbednosne potrebe i zahteve koji se mogu na ovom planu javiti u sadašnjem i bliskom budućem vremenu. Moraju se formirati jake službe, koje funkcionišu kao "zajednica" i što čvršće povezane sa onima kojima služe, posebno što njihove uloge i misije nisu statične, jer na njih utiču promene u svetu, u tehnologiji i u potrebama korisnika njihovih usluga. Dakle, fokus bi trebalo da bude na onom gde i kakve ove službe treba da budu u narednih 10-15 godina, a ne na onom gde su i kakve su sada. Jer, očigledno je da je na svetskoj sceni rođen i formiran kiber-prostor – novi ambijent u kojem se pojavljuju novi opasni igrači koji *sa novim igračkama igraju nove igre po novim pravilima*. Utakmice će gubiti onaj koji se na vreme i na pravi način ne prilagodi izmenjenoj situaciji.

Zato, spremnost, kao i širina i brzina delovanja onih koji na nacionalnom nivou odlučuju, iniciraju i usmeravaju ne bi smeli biti ograničeni ličnom ili institucionalnom inercijom i konzervativnim razmišljanjem, jer ulog je previše velik i ozbiljan da bi ovo bilo prepušteno spontanosti ili stihiji. Kratko rečeno, treba se suočiti sa brojnim aspektima sledećeg pitanja: Kako će društveni subjekti odgovorni za odbranu i bezbednost zemlje definisati i izvršavati svoje misije u 21. veku karakterističnom po rapidnom i sveobuhvatnom širenju i delovanju svemoćne informacione tehnologije? Odgovor na ovo pitanje niko nam neće pokloniti – moraćemo ga sami pronaći.

Naša šansa je u činjenici da je znanje u svemu ovome najjače oružje, a to znači da i male zemlje, iako nemaju ekonomsku moć, na polju znanja mogu da konkurišu i najrazvijenijim i najmoćnijim. Upravo zato ulaganje u znanje postaje *najisplativija nacionalna investicija*. Zbog svega toga, jedini pravi odgovor na ove izazove je organizovano, osmišljeno i sveobuhvato širenje bezbednosne kulture i razvijanje svesti na svim nivoima o potrebi zaštite nacionalnog kiber-prostora, bezbednosna obuka svih učesnika u informacionim procesima i edukacija različitih specijalista najvišeg nivoa i, što je imperativno, donošenje *nacionalne strategije* zaštite kiber-prostora u kojoj bi, u najkraćem, hitno, precizno i celovito bili definisani ciljevi, planovi, akcije i nosioci. Bez toga, mi u *elektronskom globalnom selu* postajemo *zaseok* u koji će svako moći *nesmetano da dođe, radi, ostavi i uzme šta hoće*. Ni jedna ozbiljna i odgovorna država to sebi ne bi smela da dozvoli.

Na kraju, autor i ovom prilikom ponavlja već više puta iznetu upozoravajuću konstataciju da će se ova zemlja sve manje braniti na geografski lociranim graničnim prelazima, a sve više u kiber-prostoru koji se i kod nas neumitno širi. Upravo zbog toga država jednostavno MORA da se pripremi da blagovremenim preduzimanjem svih raspoloživih mera i akcija uspešno odgovori na sve izazove osujećujući svaki pokušaj ugrožavanja nacionalnog kiber-prostora bez obzira odakle i od koga potiče.

LITERATURA

[1] Advocat J., *Internet clinical trials: examining new disciplinary experiments in health care*, Monash University, Australia, Anthropology Matters Journal 2005, Vol 7 (1), http://www.anthropologymatters.com

[2] *An introduction to e-business optimisation*, http://www.weboptimiser.com/resources/index.html

[3] *Awareness Of National Security Issues And Response (ANSIR) Program*, April 6, 1998., http://www.fbi.gov/hq/nsd/ansir/ansir.htm

[4] *CIA Official Assesses Information Warfare Threat*, 10 December 1998, http://www.fas.org/irp/news/1998/12/98121001_plt.html

[5] *Critical Infrastructure: Control Systems and the Terrorist Threat*, Report for Congress, 2003, http://www.fas.org/irp/crs/RL31534.pdf; *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report for Congress, 2004, http://fas.org/sgp/crs/RL32631.pdf

[6] *Cyber Espionage*, http://www.oppapers.com/essays/Cyber-Espionage/178669

[7] *Cybercrime and its Effects on the Asia Pacific Region*, CSCAP - Council for Security Co-operation Asia and Pacific, Transnational Crime Working Group, Sub Group Report, 2000.

[8] *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, National Academy of Sciences, National Research Council, Washington, D.C., ISBN: 0-309-08312-5, 2002, 50 pages.

[9] Davidson T., Sooryamoorthy R., Shrum W., *Kerala Connections: Will the Internet Affect Science in Developing Areas?*, 2002, http://worldsci.net/EVERY4.pdf

[10] Devost G. M., *National Security In The Information Age*, May, 1995, http://www.terrorism.com/documents/devostthesis.html

[11] *E-Government guideline*, The World Bank, http://siteresources.worldbank.org/INTEGOVERNMENT/ Resources/e-Gov_guideline.pdf

[12] *E-Government Handbook*, CDT/infoDev, http://www.cdt.org egov / handbook/
[13] Finholt A. T., *Collaboratories: Science over the Internet*, 2002, http://www.aaas.org/spp/yearbook/2002/ch31.pdf
[14] Forno F. R., *Hidden Threats And Vulnerabilities To Information Systems At The Dawn Of A New Century*, Special to Emergency-Net News; 11/22/98., http://www.emergency.com/techthrt.htm
[15] Freeh J. L., *Threats to U. S. National Security*, Congessional Statement, FBI, January 28, 1998, http://www.fbi.gov/pressrm/congress/congress98/threats.htm
[16] Guice J., Duffy R., *The Future of the Internet in Science*, USRA Research Institute for Advanced Computer Science, NASA Ames Research Center, USA, http://ase.arc.nasa.gov/publications/pdf/2000-0174.pdf
[17] Haeni R., *Information warfare – AN INTRODUCTION*, The George Washington University, Cyberspace Policy Institute, January, 1997, http://www.seas.gwu.edu/student/reto/papers/infowar.pdf
[18] Haque A., *Ethical Implications of Information Technology in Government: A Closer Look at GIS, School of Social and Behavioral Science*, Department of Government and Public Service, The University of Alabama at Birmingham, http://www.netcaucus.org/books/egov2001/pdf/Ethicsin.pdf, str. 5.
[19] *Information warfare*, Wikipedia, The Free Encyklopedia, http://en.wikipedia.org/wiki/Information_warfare
[20] *Intelligence operations*, http://www2.scholastic.com/browse/article.jsp?id=5213
[21] *Internet Hits 1,596 Million*, http://www.internetworldstats.com/pr/edi040.htm#3
[22] Keohane O. R., Nye S. J., *Power and Interdependence in the Information Age*, Foreign Affairs, v. 77 no. 5 (September/October 1998)
[23] Keohane O. R., Nye S. J., *Power and Interdependence in the Information Age*, Foreign Affairs, v. 77 no. 5 (September/October 1998), pp 81-94, http://www.uazuay.edu.ec/estudios/com_exterior/tamara/Keohane-Nye-Pwr_Interdepce_Info_Age.pdf
[24] McPhedran I., *Australia "Not ready" for Cyber-war*, Australia/New Zeland, The Canberra Times 16/09/97 P3, http://www.infowar.com/CLASS_3/class3_091997a.html-ssi
[25] Mijalković A., *"Lepša strana globalizacije"*, Politika, 25- mart 2002. god., str. 4.
[26] *Nation At Risk: Policy Makers Need Better Information to Protect the Country*, Task Force On National Security In The Information Age, March 2009, http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf
[27] Nishimura K. G., Minetaki K., Shirai M., Kurokawa F., *Effects of Information Technology and Aging Work Force on Labor Demand and Technological Progress in Japanese Industries: 1980-1998,* The University of Tokyo, January 2002, http://www.oecd.org/dataoecd/49/11/24726789.pdf, str. 1-5
[28] *Open Source Intelligence: Professional Handbook 1.0*, Proceedings, Volume I , Fifth International Symposium on "Global Security & Global Competitiveness: Open Source Solutions" 15-18, http://emmaf2.isuisse.com/96vol1/
[29] 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.
[30] Petrović R. S.**,** *Kiber-prostor – izvorište novih pretnji nacionalnoj bezbednosti,* Međunarodni naučno-stručni skup Informaciona bezbednost 2009, Beograd, februara 2009, Zbornik radova, str. 69-80.
[31] Petrović R. S., *Kiber-prostor – peta dimenzija ratovanja*, Vojni informator, br. 4, jul-avgust 2001, str. 29-50
[32] Petrović R. S., *Kiberterorizam*, Vojno delo, god. LIII, br. 2/2001, str. 100-122.
[33] Petrović R. S., *KOMPJUTERSKI KRIMINAL*, Vojnoizdavački zavod, Beograd, 2004, 564 st. III izdanje.
[34] 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.
[35] 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.
[36] Petrović R. S.*, O neophodnosti nacionalne strategije zaštite kiberprostora*, Nauka Bezbednost Policija (NTB), Beograd, vol. XI, no. 2, 2006, str. 3-28.
[37] *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, March 1, 1996, http://www.fas.org/irp/offdocs/report.html
[38] *Preparing for the Revolution: Information Technology and the Future of the Research University*, Panel on the Impact of Information Technology on the Future of the Research University, National Research Council, The National Academies Press, Washington, ISBN: 0-309-08640-X, 97 pages, (2002).
[39] Robert H'obbes' Zakon, *Hobbes' Internet Timeline v8.2*, http://www.zakon.org/robert/internet/timeline/
[40] *Safe Use Of The Internet For Defence Purposes*, DOC - C3I - 1 1997, A Report from the Panel on Secure Information Systems, STP-11, C3I Group, str. 1-2.
[41] *Security in cyberspace*, Staff Statement, U.S. Senate, Permanent Subcommittee On Investigations, june 5, 1996, http://www.fas.org/irp/congress/1996_hr/s960605t.htm
[42] Selwyn N, Facer K., *Beyond the digital divide – Rethinking digital inclusion for the 21st century*, 2007, www.futurelab.org.uk/openingeducation
[43] *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Committee on Offensive Information Warfare, National Research Counci, ISBN: 978-0-309-13850-5, 376 pages, (2009), http://www.nap.edu/catalog/12651.html
[44] *The Global Course of the Information Revolution: Political, Economic, and Social Consequences*, Proceedings of an International Conference, 2000 RAND, http://www.rand.org/pubs/conf_proceedings/ 2007/CF154.pdf
[45] *The Implications of Information and Communications Technologies for Distance Education: Looking Toward the Future*, SRI Project Number P11913, June 2004, http://sri.com/policy/csted/reports/sandt/it/Distance_Ed_Lit_Review_FINAL_6-9-04.pdf
[46] Tribe H. L., *The Consitution in Cyberspace*, http://www.sjgames.com/SS/tribe.html
[47] *U.S. Army War College Guide to National Security Issues*, Vol. I: Theory of War and Strategy, June 09, 2008, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=870
[48] *U.S. Army War College Key Strategic Issues List*, July 2008, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=860
[49] Warren M., *The Internet and rural communities: implications for health care?*, http://www.plymouth.ac.uk/ files/extranet/docs/HSC/abstract 2003 - Feb 13 health of rural communities.pdf

Prof. dr Slobodan R. Petrović, Fakultet bezbednosti Beograd
slobo.petrovic@nadlanu.com
Oblast interesovanja: kompjuterski kriminal, kiber-terorizam, informaciono ratovanje.