XXX Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2012, Beograd, 04. i 05. decembar 2012.

DEFINISANJE KRITIČNE TELEKOMUNNIKACIONE INFRASTRUKTURE U SRBIJI

Nataša Gospić[1], Goran Murić[1], Dragan Bogojević[2]
[1]Saobraćajni fakultet Univerziteta u Beogradu
[2]ICT-INFO, Beograd

Sadržaj: *Poslednjih godina fokus regulatornih aktivnosti u sektoru elektronskih komunikacija je bio na osiguravanju konkurencije i regulaciji tržišta. U regulatorne aktivnosti uključeni su elektronski sadržaji, zaštita cyber prostora, zaštita podataka, privatnost i zaštita životne sredine. U sklopu toga, kao i naglog povećanja opasnosti od pojave prirodnih nepogoda i drugih tipova napada, otvorila su se i pitanja kritičnih infrastruktura zemlje i širih regiona. Diskusije o kritičnoj infrastrukturi postavile su zahteve za njenom harmonizacijom. U Evropskoj Uniji, usvojena je Direktiva 2008/114/EC, a diskusije o uključivanju info-komunikacionog sektora, kao dela kritične infrastrukture zemlje članice, upućuju na potrebu razmatranja telekomunikacione kritične infrastrukture-KTI. Ovaj rad se bavi pitanjima koja treba postaviti u okviru definisanja i implementacije kritične telekomunikacione infrastrukture. Kroz pregled pristupa kritičnoj infrastrukturi telekom sektora i njenim uticajima na ostale kritične infrastrukture, u radu se ističe potreba za regulisanjem ove materije. Rad daje predlog koraka koje treba preduzeti u cilju definisanja i realizacije KTI u Srbiji.*

Ključne reči: *kritična infrsatruktura,kritična telekomunikaciona infrastruktura*

1. Uvod

Telekomunikacione mreže se na svim nivoima smatraju neodvojivim delom društvene interakcije. Treba posebno naglasiti da kompletna elektronska komunikaciona infrastruktura koja se sastoji od komunikacionih mreža, distribuiranih računarskih sistema, softvera i aplikacija igra ključnu ulogu u unapređenju ukupnog znanja i tehnologije. Zahvaljujući njenoj mogućnosti da okupi "kritičnu masu" ljudi, ideja i investicija, ona na različite načine doprinosi napretku na svim nivoima društvenog i ekonomskog života. Iz tog razloga, telekomunikaciona infrastruktura predstavlja veoma važnu imovinu i sredstvo koje mora biti zaštićeno i kao takva je neophodno da se prepozna kao deo nacionalne kritične infrastrukture. Zaštita ovih mreža od napada i prirodnih nepogoda, koje mogu dovesti do nedostupnosti mrežnih servisa, je veoma bitan aspekt koji se ne sme zanemariti. U ovom radu date su neke smernice u procesima

definisanja kritične telekomunikacione infrastructure - KTI bazirane na iskustvima i donetoj regulativi Evropske Unije, SAD i zemaljama u regionu. U radu su date definicije kritične infrastrukture - KI i iz toga izvedene definicije za KTI. Kao bitan element u definisanju KI prikazana je zavisnost između kritičnih infrastruktura različitih sektora. Kroz razmatranje procene rizika od različitih napada usmerenih ka telekomunikacionoj infrastrukturi (malicioznih, prirodnih katastrofa i sl.), ukazano je na neophodnost regulisanja KTI i koraka koje treba preduzeti .

2. Definisanje kritične infrastrukture

Postoji više definicija KI, ali u principu sve se one odnose na sredstva i imovinu koja je ključna za neometano funkcionisanje ekonomije i društva. Kao primer navode se seledeće definicije:

SAD: "Kritična infrastruktura i osnovni resursi (Critical infrastructure and key resources - CIKR) je pojam koji se odnosi na širok opseg različitih sredstava i imovine koji su neophodni za svakodnevno funkcionisanje društvenih, ekonomskih, političkih i kulturnih sistema u Sjedinjenim Američkim Državama. Bilo kakav prekid u elementima kritične infrastrukture predstavlja ozbiljnu pretnju za pravilno funkcionisanje ovih sistema i može dovesti do oštećenja imovine, ljudskih žrtava i značajnih ekonomskih gubitaka."[1]

Australija: "Kritična infrastruktura predstavlja one fizičke objekte, lance snabdevanja, informacione tehnologije i komunikacione mreže, koje bi ako se unište ili na duže vreme onesposobe, mogle značajno uticati na društveno ili ekonomsko blagostanje nacije, ili bi uticale na sposobnost Australije da održi nacionalnu odbranu i obezbedi nacionalnu sigurnost." [2]

Evropska Unija: (a)"Kritična infrastruktura predstavlja imovinu, sistem ili njegov deo koji se nalazi na teritoriji zemlje članice i koji je neophodan za održavanje ključnih društvenih funkcija, zdravstva, bezbednosti, sigurnosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na zemlju članicu".

(b)"Evropska kritična infrastruktura – EKI podrazumeva kritičnu infrastrukturu lociranu na teritoriji zemlje članice, čije bi ometanje ili uništenje imalo značajan uticaj na bar dve zemlje članice. Značaj poremećaja u funkcionisanju elemenata kritične infrastrukture treba da se proceni na osnovu kriterijuma međuzavisnosti. To podrazumeva efekte nastale kao rezultat međusektorske zavisnosti od drugih tipova infrastrukture." [3]

3. Glavni elementi nacionalne kritične infrastrukture i njihova međusobna zavisnost

U poslednjoj dekadi načinjeni su značajni koraci da se elementi kritične infrastrukture analiziraju sa aspekta rizika i pripreme za događaje koji mogu omesti njihov rad kroz izradu planova zaštite, tako da se ublaži ugroženost sistema na svim nivoima (regionalni, nacionalni i lokalni). Ipak, strategije koje su usmerene ka uspešnoj prevenciji krajnje negativnih scenarija (terorističkih napada ili prirodnih katastrofa većih razmera) iako veoma efikasne, ne moraju da znače da je izvršena optimalna alokacija resursa koji su potrebni za zaštitu. Ovo veoma složeno pitanje nivoa ugroženosti predstavlja veliki izazov za pravilno planiranje odgovora na prorodne ili druge nepogode.

Na osnovu pregleda literature [4], [5] , glavni elementi nacionalne kritične infrastrukture se mogu identifikovati kao:

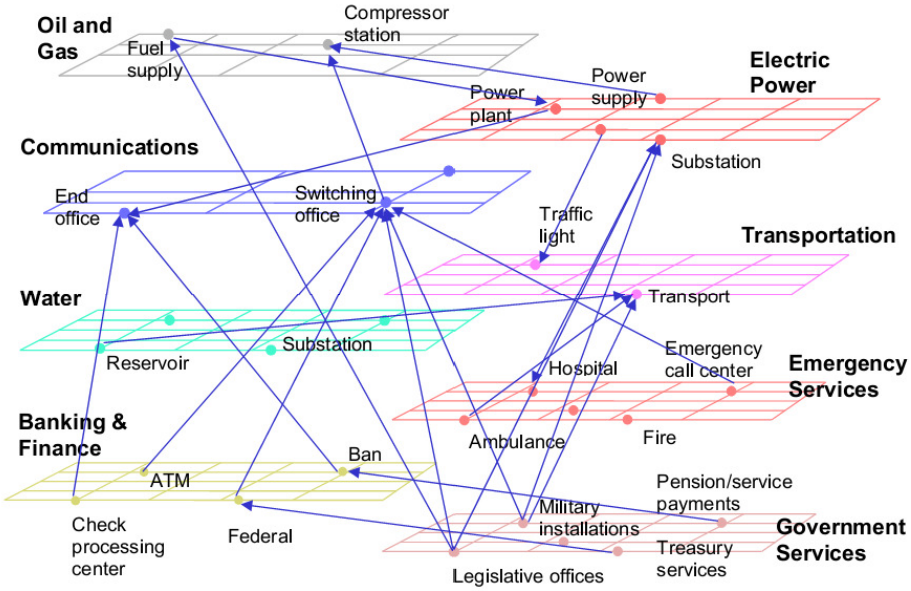
- Informacije i komunikacije (telekomunikacije, mreže, internet)
- Električna energija
- Transport
- Nafta i gas (snabdevanje, transport, rafinacija, distribucija)
- Bankarstvo i finansije
- Voda i službe za hitne slučajeve
- Vlada (+vojska)

U okviru direktive Saveta Evrope 2008/114/EC određeni su elementi / sektori za koje je potrebno definisati kritičnu infrastrukturu, kao što je prikazano u Tabeli 1 [1].

Sektor	**Podsektor**	
I Energija	1. Električna energija	Infrastruktura i objekti neophodni za proizvonju i prenoz električne energije
	2. Oil	Proizvodnja nafte i rafinisanje
	3. Gas	Proizvodnja gasa i rafinisanje
II Transport	4. Drumski transport 5. Železnički transport 6. Vazdušni transport 7. Transport unutrašnjim plovnim putevima 8. Prevoz okeanom i morima	

Tabela 1. *Sektori kritične infrastrukture u Evropskoj Uniji*

Imajući u vidu definicije, možemo reći da kritične infrastrukture u okviru jedne države predstavljaju složene "sisteme sistema". Veliki značaj koji infrastrukture identifikovane kao kritične imaju na društvo, obavezuje na stvaranje dovoljno dobrih sigurnosnih mera koje će služiti za umanjenje rizika od prekida rada. Međuzavisnosti obično nisu dovoljno dobro istražene i poremećaji u okviru jedne infrastrukture lako mogu da se prenesu u druge. Kritične infrastrukture su povezane na različitim nivoima i kvar na elementu jedne infrastrukture može lako da se odrazi na elemente druge i obratno [6]. Generalno, između kritičnih infrastruktura međuzavisnost je vrlo izražena, što je ilustrovano i Slikom 1.



Slika 1. *Međuzavisnost između različitih infrastruktura [7]*

Iz slike 1 jasno je uočljivo da između sektora telekomunikacija i velikog broja elemenata ostalih infrastruktura postoji veoma velika povezanost. Skoro svi elementi vezani za usluge proizvodnje i distribucije električne energije, vode, gasa i sl. imaju zahteve za komunikacijom u određenom obliku. Sa druge strane, komunikacioni sektor u mnogome zavisi od drugih sektora. Na osnovu toga možemo zaključiti da telekomunikacioni sektor predstavlja infrastukturu čija je pozicija centralna i da razumevanje i modelovanje rizika povezanih sa prekidom komunikacija treba da imaju prioritet u razmatranju KI, radi povećanja nivoa javne sigurnosti i otpornosti infrastruktura na neželjene uticaje [8].

4. Kritična telekomunikaciona infrastruktura

Telekomunikaciona infrastruktura jedne zemlje je kompleksan skup sistema koji uključuju veliki broj tehnologija i servisa, a koje se nalaze u vlasništvu više entiteta (države, privatnih kompanija). Infrastruktura obuhvata žične, bežične, kablovske i tehnologije za emitovanje, jezgrene mreže bazirane na Internet protokolu kao i interne informacione sisteme. Mnoge telekomunikacione kompanije/operatori koje poseduju i upravljaju telekomunikacionom infrastrukturom su tokom vremena implementirale mere zaštite od prirodnih katastrofa i nezgoda u okviru svojih arhitektura uvodeći redundantne čvorove i sisteme, biznis planove i strategije za sanaciju nakon napada ili prirodnih nepogoda. To ukazuje da i pored današnjeg veoma konkurentnog poslovnog okruženja zbog povezanosti i međuzavisnosti mreža različitih operatora/servis provajdera, svi činioci telekom sektora jedne zemlje treba da sarađuju, jer problemi u funkcionisanju

mreže jednog učesnika na tržištu često mogu da utiču na mrežu koja je u vlasništvu nekog drugog.

Kako je najveći deo telekomunikacione infrastrukture u vlasništvu privatnog sektora, bitno je ustanoviti zajednički strateški okvir kojim će se osigurati zaštita telekomunikacione infrastrukture jedne zemlje i osigurati njena bezbednost.

Vođeni opštom transformacijom i konvergencijom tehnologija početkom dvadeset prvog veka sektor telekomunikacija i IT-a su postali praktično nerazdvojivi. Telekomunikacioni sektor ne uključuje samo fizičke elemente kao što su žične, bežične, kablovske i sl. tehnologije, već i servise kao što su Internet saobraćaj i rutiranje, informacione servise i mreže kablovske televizije. Samim tim, komponente komunikacione infrastrukture koje su u vlasništvu države i privatnih kompanija su neraskidivo povezane u okviru ovih fizičko-logičkih struktura.

U definisanju telekomunikacione infrastrukture, uobičajeno je da se za osnovu uzima ono što je Međunarodna Unija za telekomunikacije (International Telecommunication Union – ITU) definisala. Međutim, u okviru familije ITU nije definisana KTI, iako mnogi dokumenti ITU-a pominju potrebu zaštite KTI (PP-10 Res. 130, PP-10 Res. 174, ITU CS/Art.38, ITU CS/Art.34, ITU CS/Art.35). Harmonizacija koja je urađena u okviru ITU-T sektora serijama preporuka E.408-409 i X.805 i X.1051 definiše zahteve za bezbednost, okvire i smernice za identifikaciju pretnji, smanjivanje rizika, organizaciju u slučaju incidenta i arhitekturu sigurnosti za sisteme koji pružaju kraj-kraj komunikaciju. I druge standardizacione organizacije kao što su Međunarodna standardizaciona organizacija (Internetional Standardisation Organization – ISO), 3GPP i 3GPP 2 (Group for Partership for Third Generation) takođe ne daju definicije KTI već samo okvire za sigurnost sistema mobilnih komunikacija i upravljačkih sistema,

Način definisanja KTI u mnogome zavisi od konteksta u kom se posmatra ne samo KTI već i druge KI u nekoj zemlji. Da bismo definisali KTI, kao osnovu smo koristili opšte definicije KI navedene u tački 2. U tom smislu KTI se može definisati kao javna ili privatna mreža koja prenosi informacije relevantne za nacionalnu bezbednost ili informacije velike materijalne vrednosti. U fizičkom smislu KTI može biti definisana kao celokupna mreža ili deo mreže preko koje se prenose informacije od velike važnosti.

5. Kritična infrastruktura u Evropskoj Uniji

Za podršku potrebama osiguranja dostupnosti, pouzdanosti i održivosti ključnih infrastruktura Evropska komisija je pokrenula Evropski program za zaštitu kritične infrastrukture (European Programme on Critical Infrastructure Protection - EPCIP) s naglaskom na identifikaciju i imenovanje Evropske kritične infrastrukture EKI, kao i procenu potreba za poboljšanje njene zaštite.

Istorijski, aktivnosti oko EPCIP započete su u EU početkom 2004. godine kada je Evropski Savet inicirao rad na programu zaštite kritične infrastrukture (Critical Infrastructure Protection –CIP). U narednim godinama usvojeni su: EU Zeleni papir (2005.), Evropski program za zaštitu kritične infrastrukture EPCIT (2006.), Direktiva 2008/114/EC (2008.), i EU Interna strategija zaštite (EU Internal Security Strategy, 2010.). Tokom 2012 rađena je revizija EPCIP programa i Direktive 2008/114/EC.

Direktiva Evropskog Saveta 2008/114/EC iz 2008. godine [9] predstavlja sastavni deo EPCIP programa. Ona definiše kritičnu infrastrukturu, zajedničke procedure

za identifikaciju i označavanje evropske kritične infrastrukture EKI, zajednički pristup u proceni potreba za poboljšavanje zaštite, kao i sve rizične pristupe sa prvim prioritetom pretnje od terorizma.

Direktiva Evropske Komisije 2008/114/EC je osnova za naredne korake u definisanju kriterijuma za kritičnu infrastrukturu. U Aneksu III istog dokumenta navdene su procedura, koje svaka zemlja članica treba da implementira, kroz nekoliko konsekventnih koraka (tabela 2):

Korak 1	Svaka zemlja članica treba da primeni sektorske kriterijume sa ciljem kreiranja inicijalne selekcije kritične infrastrukture u okviru sektora.
Korak 2	Svaka zemlja članica treba da primeni definiciju kritične infrastrukture shodno Članu 2(a) na potencijalne KTI identifikovane nakon Koraka 1. Za infrastrukture koje se koriste za pružanje osnovnih servisa, u obzir treba da se uzmu dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa.
Korak 3	Svaka zemlja članica treba da primeni prekogranični element za definisanje EKI shodno Članu 2(b) na potencijalne EKI koje su prošle prva dva koraka ove procedure. Za potencijalnu EKI koja zadovoljava definiciju prmenjuje se sledeći korak procedure. Za infrastrukture koje se koriste za pružanje osnovnih servisa, u obzir treba da se uzmu dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa.
Korak 4	Svaka zemlja članica treba da primeni unakrsne kriterijume za preostale EKI. Unakrsni kriterijum treba da uzme u obzir: ozbiljnost napada; i za infrastrukture koje se koriste za pružanje osnovnih servisa, dostupnost alternativne infrastrukture, kao i trajanje prekida/uspostavljanja servisa.

Tabela 2. *Koraci u definisanju kriterijuma za kritičnu infrastrukturu, prema direktivi 2008/114/EC [3]*

Kad je doneta ova direktiva, ona je predstavljala prvi korak u identifikaciji i određivanju Evropske kritične infrastrukture – EKI i potrebe da se unapredi njihova zaštita. U okviru nje naglašeno je da se odnosi na sektor energetike i transporta ali i da je treba razmotriti sa posebnim osvrtom na procenu među-uticaja sektora, između ostalog, posebno u odnosu na sektor informacionih i komunikacionih tehnologija. Prva revizija Direktive počela je januara 2012.

6. Evropski program zaštite kritične infrastructure (EPCIP): ciljevi i procesi revizije

Dokument [9] predstavlja osnovne preliminarne zaključke nakon započinjanja procesa razmatranja Evropskog programa za zaštitu kritične infrastrukture (EPCIP), a posebno direktive 2008/114/EC. Dokument pruža opštu analizu elemenata programa za zaštitu kritične infrastruktre i opisuje neprekidan razvoj metodologija za procenu rizika u ovoj oblasti [10].

Evropski program za zaštitu kritične infrastrukture ima utvrđeni horizontalni okvir, ilustrovan i Slikom 2. Ovaj okvir obuhvata

- Mere u cilju olakšavanja implementacije EPCIP: Informacioni sistem za uzbunjivanje u okviru kritičnih infrastruktura (Critical Infrastructure Warning Information Network - CIWIN); CIP ekspertske grupe; CIP procesi za deljenje informacija; identifikacija i analiza međuzavisnosti
- Podrška zemljama članicama vezano za nacionalnu kritičnu infrastrukturu
- Planiranje nepredvidivih situacija
- Spoljne dimenzije
- Prateće finansijske mere – EU program "Prevencije, planiranje i upravljanje posledicama terorizma i drugim bezbednosnim rizicima" za period 2007-2013
- Direktiva 2008/114/EC – procedure za identifikaciju i označavanje EKI

Kao podrška procesu dodatnog razmatranja, krajem 2011. godine lansirano je evaluaciono istraživanje implementacije i primene Direktive 2008/114/EC. Rezultati su objavljeni u martu 2012.

Pored toga, organizovana je serija sastanaka sa interesnim stranama, kao i ostalih sličnih događaja. Evropska komisija je 15. februara 2012. godine organizovala radionicu na kojoj su potvrđeni rezultati evaluacione studije, a ujedno su razmotrene potrebe za zaštitom pojedinih elemenata kritičnih infrastruktura.

U martu 2012. godine u Briselu održana je konferencija na temu zaštite kritične infrastrukture, čiji su učesnici bili predstavnici zemalja članica.

Dodatno razmatranje različitih do sada implementiranih elemenata EPCIP-a je dovelo do nekoliko važnih zaključaka koji će biti uključeni u oblikovani dokument za definisanje politike CIP-a (novembar 2012):

- Sve zemlje članice su zvanično implementirale Direktivu 2008/114/EC tako što su ustanovile proces identifikacije elemenata Evropske kritične infrastrukture, što je dovelo do podizanja svesti o potrebi zaštite kritične infrastrukture u Evropskoj Uniji i zemljama članicama.
- Iako postoje dokazi da je Direktiva pomogla u samoj proceni potrebe da se evropska kritična infrastruktura bolje zaštiti, ne postoje pokazatelji koji bi dokazali da se bezbednost ovih sektora povećala.
- Pristup predstavljen u ovoj Direktivi, a koji je orijentisan ka sektorima predstavlja izazov za veliki broj zemalja članica, jer u praksi analiza kritičnih segmenata nije ograničena na sektor već se često odnosi na sistem ili na servis.
- Iako je Direktiva doneta sa namenom da definiše jasan evropski okvir koji bi služio kao jedinstven forum svih država u okviru EU, u praksi je podstakao uglavnom bilateralne saradnje između zemalja članica.

Treba naglasiti da je u toku procesa revizije EPCIP i Direktive 2008/114/EC razmatrano i uključivanje IKT sektora, ali u smislu preplitanja definisanih KI sa IKT i uloge IKT u zaštiti EKI. Sektor IKT još nije uključen u EKI.

7. Situacija u Srbiji

Mnoge države su već identifikovale svoje kritične infrastrukture, a u okviru njih i kritičnu telekomunikacionu infrastrukturu (SAD, Kanada, Nemačka, Švedska, Norveška). Neke države su pokrenule projekte iz oblasti KTI-a (Brazil). U Srbiji i regionu se o ovoj temi veoma malo diskutovalo [11]. Veće aktivnosti je preduzela Hrvatska dok su BiH i Crna Gora formirali timove za odgovore na vanredne situacije u oblasti informacionih tehnologija [12].

U Srbiji se kritična infrastruktura pominje samo u okviru poglavlja 6.2. „Strategije razvoja informacionog društva u Republici Srbiji do 2020“ [13] kao “Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme, što pored IKT sistema mogu biti i drugi infrastrukturni sistemi kojima se upravlja korišćenjem IKT, poput elektro-energetskog sistema. U vezi toga je potrebno dodatno urediti kriterijume za utvrđivanje kritične infrastrukture sa stanovišta informacione bezbednosti, kriterijume za karakterizaciju napada primenom informacionih tehnologija na takvu infrastrukturu u odnosu na klasične oblike napada, kao i uslove zaštite u ovoj oblasti”.

Sledeći dokumenti koji bi trebalo da obrađuje pitanja KI su Nacionalna strategija zaštite i spasavanja u vanrednim situacijama i Zakon o vanrednim situacijama. Međutim u ovim dokumentima se ni ne pominje kritična infrastruktura, pa time ni KTI.

Treba naglasiti da institucionalni okviri za definisanje KI postoje a to su Sektor za vanredne situacije, nadležna ministarstva kao i nadležna regulatorna tela. Određene mere zaštite delova infrstrukture su preduzete od strane operatora ali nisu donesene ni strategija ni politika zaštite na nivou zemlje.

Potreba razmatranja KI prepoznata je u okviru projekta „Upravljanje kritičnom infrastrukturom za održivi razvoj u poštanskom, komunikacionom i železničkom sektoru Republike Srbije”, Osnovni cilj projekta je identifikacija kritičnih infrastrukturnih sistema čija je efikasnost ključna za neometan razvoj ekonomije i društva. Deo projekta se bavi kritičnom telekomunikacionom infrastrukturom i na njemu radi tim Saobraćajnog fakulteta Univerziteta u Beogradu u saradnji sa stručnjacima Telekoma Srbije. Uzimajući u obzir sve faktore koji mogu negativno uticati na telekomunikacionu infrastrukturu (prirodne nepogode, ciljane napade, nenamerne greške) i mešovitu vlasničku strukturu (državnu i privatnu), problemi kritične telekomunikacione infrastrukture postaju kompleksni i zahtevaju dobro upravljane regulatorne procese [12].

U okviru istraživanja u pomenutom Projektu predložena je sledeća metodologija u identifikovanju KTI:

- Formiranje međusektorskog tima (Sektor za vanredne situacije, Nadležno ministarstvo, RATEL, operatori, eksperti)
- Definisanje KTI sa svim kritičnim elementima u okviru infrastrukture
- Identifikovanje kritičnih tačaka telekomunikacione infrastrukture i procena rizika (Primena standarda ISO 31000)
- Identifikovanje međuveza sa ostalim KI
- Identifikovanje nacionalne KTI kao dela međunarodne KTI u skladu sa međunarodnim okvirom (EU okvir)
- Predlaganje preporuka za sprečavanje incidentnih situacija i osiguravanje održavanja usluge i stabilnosti servisa u slučaju da do takvih situacija dođe

- Priprema strategije i politike za zaštitu telekomunikacione infrastrukture; Priprema legislativnog okvira za zaštitu KTI

8. Zaključak

Razvoj sistemskog pristupa, kroz institucionalne i legislativne okvire predstavlja osnovni uslov za identifikovanje KTI i njeno integrisanje u širu (EU) KTI. Podizanje svesti o potrebi definisanja KTI i kritičnih sistema i mreža i načina njihove zaštite treba da bude deo politike razvoja KI, u kome će se jasno znati nadležnosti za disiminaciju informacija o značaju i zaštiti KI. Istraživanja iz projekta „Upravljanje kritičnom infrastrukturom za održivi razvoj u poštanskom, komunikacionom i Železničkom sektoru Republike Srbije", predstavljaju polazišta u podizanju svesti o KTI i identifikovanju kritičnih elemenata i njihovoj zaštiti.

Zahvalnost:

Ovo istraživanje je deo projekta "Upravljanje kritičnom infrastrukturom za održivi razvoj u poštanskom, komunikacionom i Železničkom sektoru Republike Srbije", podržanog od strane Ministarstva prosvete, nauke i tehnološkog razvoja u okviru naučnih istraživačkih projekata 2011-2014, Telekoma Srbije, Pošte Srbije i Železnice Srbije.

Literatura

[1] T. G. A.T. Murray, "Critical infrastructure protection: The vulnerability conundrum," *Telematics and Informatics,* vol. 29, no. 1, February 2012.

[2] "Critical Infrastructure Emergency Risk Management and Assurance," Emergency Management Australia, A Division of the Attorney-General's Department, 2003.

[3] "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," *Official Journal of the European Union L,* pp. 345-375, 23.12.2008..

[4] J. Moteff and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," Congressional Research Service, The Library of Congress, 2004.

[5] "National Infrastructure Protection Plan," Homeland Security, 2009.

[6] C. Rajmohan, G. Subramanya and N. Sharma, "Telecommunication Networks: Security Management," Tata Consultancy Services Limited, 2012.

[7] B. Lane, "Federal Communications Commission," [Online]. Available: http://transition.fcc.gov/pshs/techtopics/techtopics19.html. [Accessed 09 09 2012].

[8] S. M. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies," 2004.

[9] European Commission, "Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP)," European Commission, 2012.

[10 "Council Conclusions of 9-10 June 2011 on the development of the external dimension of the European Programme for Critical Infrastructure Protection".

[11 S. M. P. Š. Z. Kljaić, "Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama," in *TELFOR*, Beograd, 2010.

[12 N. Gospić, G. Murić and D. Bogojević, "Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia," in *International Conference on Applied Internet and Information Technologies*, Zrenjanin, October, 2012.

[13 Vlada Republike Srbije, "Strategija razvoja informacionog društva u Republici Srbiji do 2020," 2010.

Abstract: *In recent years the focus of regulatory activities in sector of electronic communications was oriented toward providing competition and market regulation. Regulatory activities cover electronic content, protection of cyber space, data protection, privacy and environment protection. Within the prior, and together with rapid increase of threats caused by natural disasters and various types of possible attacks, issues of critical infrastructures of country and wider regions emerged. The discussions on critical infrastructure set requirements for its harmonization. Within the European Union, a Directive 2008/114/EC was adopted, and discussions on inclusion of ICT sector, as a part of critical infrastructure of the Member State, pointing to the need of the consideration of critical telecommunication infrastructure – CTI. This paper deals with issues in terms of defining and implementation of critical telecommunication infrastructure. Through the review of the approach on critical infrastructure of the telecom sector and its influences on other infrastructures, this paper highlights the need of regulation of this field. The paper suggests a steps that should be conducted toward defining CTI in Serbia.*

Keywords: *critical infrastructure, critical telecommunication infrastructure*

DEFINING OF CRITICAL TELECOMMUNICATION INFRASTRUCTURE IN SERBIA

Nataša Gospić[1], Goran Murić[1], Dragan Bogojević[2]
[1]Faculty of Transport and Traffic Engineering, University of Belgrade
[2]ICT-INFO, Belgrade