

Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskim zemljama

Zdenko Kljaić, dipl.ing. *Member, IEEE*, Sadko Mandžuka, dr.sc. *Member, IEEE*,
Pero Škorput, mr.sc. *Member, IEEE*

Sadržaj - Današnja ekonomska i kulturna globalizacija, i u političkom kontekstu integracija s jedne strane, te liberalizacija proizvodnje i distribucije proizvoda i usluga s druge strane bitno problematizira upravljanje osnovnom infrastrukturom u tranzicijskim zemljama. I suvremena sociologija s puno uvjerljivih razloga govori o modernom društvu kao društvu rizika, u kojem proizvedeni rizici ugrožavaju pojedince i ljudske skupine znatno više od vanjskih generiranih rizika. Kada navedenu problematiku stavimo u recesijsko okruženje, gdje su financijski okviri i resursi vrlo ograničeni uočavamo bitno povećanje intenziteta rizika. Gdje je tu ICT industrija kao osnovna poluga razvoja poslovanja i da li ICT tehnologije mogu uspješno odgovoriti na rastuće izazove našega društva? Ovaj rad analizira, istražuje i daje niz tehničko-tehnoloških informacija, ukazujući na važne aspekte za povećanje sigurnosti kritične infrastrukture.

Ključne reči — ICT, kritična infrastruktura, upravljanje, sigurnost.

I. UVOD

PREMA tradicionalnom pristupu zaštita kritične infrastrukture je identifikacija specifičnih postrojenja i objekata od posebnog društvenog interesa, te razvoj planova za njihovu zaštitu. Suvremeni znanstveni pristup holistički je usmjeren na cijelokupan eko-sustav, mreže i njihove međuovisnosti, a upravo stručnjaci iz područja ICT-a imaju veliko znanje i iskustva iz područja umrežavanja.

ICT je neizostavan faktor u stvaranju razvijenog i konkurentnoga gospodarstva, s efikasnom, transparentnom i štedljivom lokalnom upravom. Živimo u doba sve veće proliferacije elektroničkih informacija, društvenih mreža ili pak raznih drugih inteligentnih zapisa. Takav snažan porast e-informacija definira i same dijelove ICT kao važnu „kritičnu infrastrukturu“ i s druge strane se nameće kao vrijedno rješenje za zaštitu kritične infrastrukture u

širem smislu. ICT rješenja mogu procesuirati široki spektar informacija neovisno o njihovom formatu, izvoru, jeziku i sl., i tako procesiranu informaciju učiniti humanom, iskoristivom u stvarnom poslovnom procesu ili incidentnoj situaciji, onda kada je to najpotrebnije - u realnom vremenu. Također, nedostatak strukturiranih, vremenski i lokacijski određenih informacija može ugroziti gospodarsko-društvenu infrastrukturu i učiniti je neracionalnom ili neupotrebljivom za korištenje, npr. opskrbu energijom, smanjenje sposobnosti službi za zaštitu i spašavanje za transportne, zapovjedno-komunikacijske, logističke i druge ciljeve u slučajevima prirodnih nepogoda, ekstremnih uvjeta za život i rad ili nekih drugih drugih akcidenata.

II. KRITIČNA INFRASTRUKTURA

Pojam „kritične infrastrukture“ u SAD-u se definira kao ona dobra, sustavi i mreže, bilo materijalne ili nematerijalne (tj. fizičke ili virtualne) toliko važne za SAD da bi njihovo onesposobljavanje ili uništenje oslabilo sustav nacionalne sigurnosti, nacionalnu ekonomsku sigurnost, javno zdravstvo i sigurnost, odnosno bilo koji od spomenutih sustava pojedinačno ili u kombinaciji sa spomenutim. Zaštita te osiguranje kontinuiranog djelovanja kritične infrastrukture i ključnih resursa SAD (eng. CIKR) neophodno je za očuvanje nacionalne sigurnosti, javno zdravstvo i opću sigurnost, te vitalnost ekonomskog sustava i očuvanje američkog načina života. Uredbom predsjednika SAD, oznake 7 (HSPD-7) utvrđene su odrednice za osnivanje sustava zaštite spomenutih resursa od mogućih napada i nefunkcionalnosti.

Definiranje pojma „kritične infrastrukture“ u EU je na sljedeći način: Kritičnu infrastrukturu čine djelatnosti, mreže, usluge i dobra materijalne i informacijske tehnologije čiji bi kvar ili uništenje značajno utjecalo na zdravlje, sigurnost ili ekonomski prosperitet građana ili na učinkovito djelovanje vlada država članica.

Kritična infrastruktura obuhvaća brojna područja gospodarstva, uključujući također i bankarstvo i financije, promet i distribuciju, energetiku, komunalne usluge, zdravstvo, opskrbu hranom i komunikacije, a također i ključne državne službe.

Definiranje okvira kritične infrastrukture u mnogim zemljama je različito i ovisi o raznim specifičnostima od političkih prilika do geografskih lokacija. Za lakše sagledavanje područja ovog pojma tablično su dani okviri za nekoliko zemalja (tabela 1.)

Zdenko Kljaić dipl.ing., Ericsson Nikola Tesla d.d., Krapinska 45, Zagreb, Hrvatska, (telefon: +385-1-3653086, e-mail: zdenko.kljaic@ericsson.com)

Sadko mandžuka dr.sc., Fakultet prometnih znanosti, Sveučilište u Zagrebu, Vukelićeva 4, Zagreb, Hrvatska, (telefon +385-1-2380224, e-mail: sadko.mandzuka@fpz.hr).

Pero Škorput mr.sc., Fakultet prometnih znanosti, Sveučilište u Zagrebu, Vukelićeva 4, Zagreb, Hrvatska, (telefon +385-1-2380224, e-mail: pero.skorput@fpz.hr).

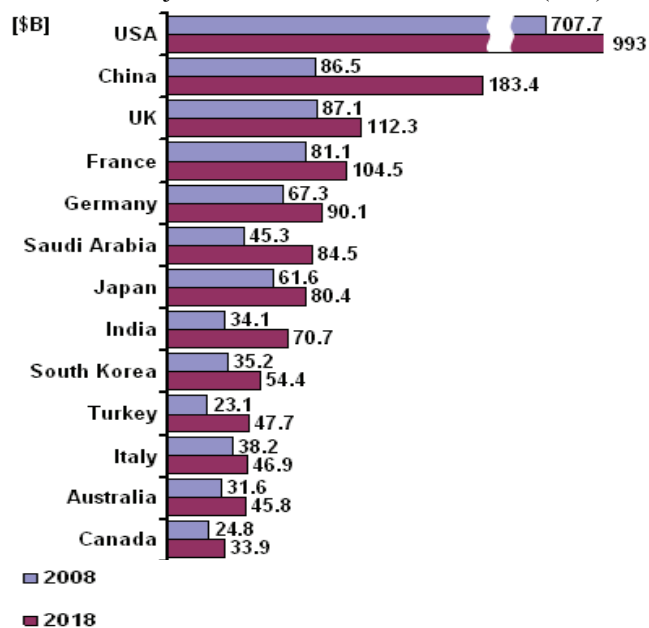
TABELA 1: INDIKATIVNA LISTA KRITIČNE INFRASTRUKTURE

KANADA	VELIKA BRITANIJA	AUSTRALIJA	SAD	NJEMAČKA	ŠVEDSKA	NORVEŠKA	NIZOZEMSKA	ŠVICARSKA
ENERGIJA (objekti električne i nuklearne energije, prirodni plin i nafta, proizvodni i transportni sustavi)	ENERGIJA	ENERGIJA (plin, naftna goriva, proizvodnja i distribucija električne energije)	ENERGIJA	ENERGIJA (električna, nafta i plin)	ENERGIJA	ENERGIJA I OBJEKTI	ENERGIJA I OBJEKTI	OBJEKTI I SLUŽBE
KOMUNIKACIJE	TELEKOMUNIKACIJE	KOMUNIKACIJE (telekomunikacije (tel., faks, internet, kablovska TV, sateliti) i masovni elektronski mediji)	INFORMACIJE I TELEKOMUNIKACIJE	TELEKOMUNIKACIJE I INFORMACIJSKA INFRASTRUKTURA	TELEKOMUNIKACIJE	OPSKRBA NAFTOM I PLINOM	TELEKOMUNIKACIJE	TELEKOMUNIKACIJE
SERVISI (financije, distribucija hrane, javno zdravstvo)	ZDRAVSTVENE SLUŽBE	ZDRAVSTVO (bolnice, javno zdravstvo i laboratoriji za istraživanje i razvoj)	JAVNO ZDRAVSTVO	JAVNO ZDRAVSTVO (uključivo i opskrbu pitkom vodom i hranom)	ELEKTRONSKE INFORMACIJSKE SLUŽBE	TELEKOMUNIKACIJE	JAVNO ZDRAVSTVO	DISTRIBUCIJA INFORMACIJA
TRANSPORT (zračni, morski, kopneni)	FINANCIJE	OPSKRBA HRANOM (poljoprivredna proizvodnja, skladištenje i distribucija)	HRANA	BANKARSTVO FINANCIRANJE I OSIGURANJE	JAVNO ZDRAVSTVO	JAVNO ZDRAVSTVO	HRANA	JAVNO ZDRAVSTVO
SIGURNOST (nuklearna sigurnost, službe spašavanja, hitne službe)	TRANSPORT	FINANCIJE (banke, osiguranje, burze)	POLJOPRIVREDA	TRANSPORTNI SUSTAVI	HRANA	BANKARSTVO I FINANCIJE	BANKARSTVO I FINANCIJE	HRANA
VLADA (bitni vladini objekti, službe i informacijski sustavi i mreže)	HITNE SLUŽBE	TRANSPORT (zračni, cestovni, morski, željeznica i robni distribucijski centri)	BANKARSTVO I FINANCIJE	HITNE I SPASILAČKE SLUŽBE	BANKARSTVO I FINANCIJE	TRANSPORT	TRANSPORT	FINANCIJE
	SREDIŠNJA VLAST	VLADINE SLUŽBE (objekti obrane i sig. službi, Parlament, bitna ministarstva, strane misije i bitne rezidencije, hitne službe (policija, vatrogasci, medicinska služba i druge))	HITNE SLUŽBE	VLAST I JAVNE SLUŽBE (uključivo policiju, carinu i oružane snage)	TRANSPORT	SPASILAČKE SLUŽBE	JAVNI RED I SIGURNOST	TRANSPORT
	VODA I ODVODNJA	USLUGE (voda, odvodnja i pročišćavanje otpadnih voda)	VLAST		VODA	OBRANA	VLAST	CIVILNA OBRANA
		PROIZVODNJA (vojna, teška i kemijska industrija)	OSNOVNA OBRAMBENA INDUSTRIJA		DRUŠTVENE VRIJEDNOSTI	POLICIJA	OBRANA	ADMINISTRACIJA
		NACIONALNE VRIJEDNOSTI (građevine, kulturne, sportske i turističke vrijednosti)	VODA			DRUŠTVENA SIGURNOST	PRAVOSUDE	VOJNA OBRANA
			KEMIJSKA INDUSTRIJA I OPASNE TVARI				PITKA VODA	OPSKRBA VODOM
			POŠTE I DOSTAVA ROBA				UPRAVLJANJE VODAMA	SOCIJALNA SIGURNOST
							DRUŠTVENI SEKTOR	INDUSTRIJA
							OBJEKTI VISKOG RIZIKA U IZVANREDNIM SITUACIJAMA	ISTRAŽIVANJE I OBRAZOVANJE

Trenutno, svjetsko gospodarstvo proživljava velike financijske izazove, ali u područje nacionalne i javne sigurnosti u smislu zaštite kritične infrastrukture ulažu se velika sredstva sa stalnim trendom rasta što govori o velikoj važnosti KI.

Slika 1. prikazuje istraživanja koja su provedena od strane Corporation HSRC. Prikazana je potrošnja na zaštitu kritične infrastrukture sa projekcijama na 2018 god. Najnovija istraživanja tržišta iz JP Freeman procjenjuju da je 38% integriranih sigurnosnih sustava temeljenih na mrežnim tehnologijama i 76% su integrirani sa postojećim IT mrežama za prijenos podataka i zakupljenih od tvrtki. Ovaj trend je potaknula recesija i želja za racionalizacijom sustava, te poboljšanjem sigurnosnih funkcionalnosti.

Sl. 1. Potrošnja na zaštitu kritične infrastrukture (\$Mr)



III. ZAŠTITA KRITIČNE INFRASTRUKTURE

Da bi se kritična infrastruktura kvalitetno definirala, nadzirala i razvijala minimalno je potreban institucijski sustav koji će preuzeti odgovornost i autoritet. Naravno, potrebna je i strategijska odrednica u ovom segmentu, zbog ulaska u nove integracije i zbog novih tehnoloških dostignuća koji uvelike mijenjaju društvene uvjete poslovanja, a sve zbog očuvanja i jačanja već postojeće infrastrukture. Moramo uzeti u obzir da je tehnološki razvoj promijenio način poslovanja, upravljanja i vođenja politike pa i shvaćanja nacionalne i javne sigurnosti. Također tehnologija je postala jeftinija, sofisticiranija i dostupnija, što je pretvara u potencijalno vrlo opasan instrument kojeg je teško nadzirati. Iz toga razloga neophodno je stvoriti preduvjete za smanjenje rizika od negativnih aktivnosti i posljedica na kritičnoj infrastrukturi. Poremećaji u kontinuiranom djelovanju institucija i kritične infrastrukture kao posljedicu mogu imati krajnje štetan učinak na obrambenu i ekonomsku sigurnost zemlje.

Kritična infrastruktura može obuhvaćati subjekte iz javnog i privatnog sektora, kanale distribucije, te „mreže“ osoba i informacija koje osiguravaju kontinuirani protok ljudi, roba, i usluga, što je ključno za stabilnost gospodarskog sustava, te javno zdravlje i strateške funkcije zemlje.

Sl. 2. Prikaz dijelova kritične infrastrukture



Prekid funkcioniranja u jednom segmentu ili infrastrukturnom sustavu može dovesti do prekida ili nefunkcioniranja u drugim sustavima, te kombinirano izazvati dugoročne posljedice na sustav vlasti, ekonomiju, javno zdravlje i sigurnost, nacionalnu sigurnost i povjerenje javnosti. U grupu „kritične infrastrukture“ ubrajaju se institucije telekomunikacija, elektroprivrede, skladištenja i prijenosa plina i nafte, bankarstva i financija, transporta, vodoopskrbe, hitne službe (uključujući medicinske, policijske, vatrogasne i spasilačke), te Vlada.

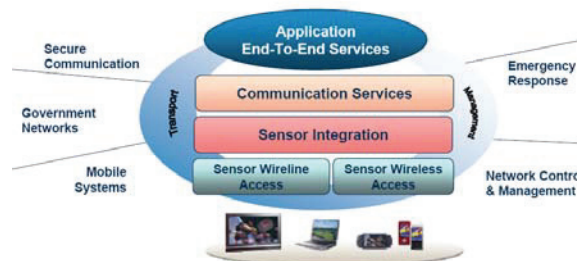
Tema kritične infrastrukture postaje, posebice posljednjih nekoliko godina, nezaobilazna u svekolikoj stručnoj literaturi, od prevencije rizika i katastrofa do mogućih štetnih učinaka ljudske aktivnosti. S elementima kritične infrastrukture susrećemo se u svim sferama naših svakodnevnih aktivnosti. Ne prepozna li se važnost tog zadatka kao prioritet na najvišim razinama odlučivanja, bojazan od nedovoljnog ulaganja u kritičnu infrastrukturu postat će opravdana, a gospodarstvo izloženije velikom riziku. Preduvjeti za kvalitativni napredak i povezanost svih segmenata sigurnosti kritične infrastrukture počiva u

specifičnim znanjima, posebno iz ICT područja u koja treba ulagati znatna sredstva da bi se preventivne mehanizme što prije povezalo u strateški okvir za kritičnu infrastrukturu.

Upravljanje kritičnom infrastrukturom stoga treba biti sastavnim dijelom razvojnih programa, a kategorije poput sigurnosti i prevencije rizika od nepogoda i katastrofa, moraju se integrirati u sve relevantne dokumente Vlade. Obično briga o kritičnoj infrastrukturi ne bude prepoznata kao jedan od prioriteta u procesima integracija pa su i početana ulaganja i tehnička pomoć nedostatni za optimalno osiguranje kritične infrastrukture. Nužno je zato osmisliti programe i zaštititi ključne resurse za upravljanje kritičnom infrastrukturom u vremenu provođenja strukturnih reformi kako bi gospodarstvo moglo stvoriti konkurentne sposobnosti za nove okolnosti na tržištu. Potrebno je upoznati europske i regionalne partnere ali i privatni sektor kako je ulaganje u jačanje kritične infrastrukture jedan od prioriteta i temelja za funkcioniranje gospodarstva i društvo u cjelini. U tom smislu, bojazan od prebrze deregulacije tržišta i daljnje liberalizacije pojedinih infrastrukturnih sektora, ponekad je i opravdana, posebno ako je cilj pravilnije relokacije postojećih resursa i izgradnja održivih sustava nasuprot kratkoročnom ostvarenju dobiti. Prema tome, koordinacija i priprema procedura za smanjenje rizika i preventivno djelovanje u slučajevima nepogoda i katastrofa koje se odnosi na sigurnost kritične infrastrukture predstavlja velik i široki dio aktivnosti gdje su važni nositelji industrija, posebno napredna ICT, te akademsko poduzetništvo u razvoju i tržišno orijentirane primijenjene znanosti zbog potrebnog visoko tehnološkog znanja.

Razvojem ICT industrije, a time i suvremenog informacijskog društva došlo se do spoznaja da neki ključni sektori, kao što je energija, telekomunikacije, financijski sektor, voda, javno zdravlje, te državni objekti od posebnog značaja koji su vitalni za nacionalnu sigurnost i ključni za ekonomsku i društvenu dobrobit, sadrže kritičnu infrastrukturu, koja počiva na čitavom spektru međusobno povezanih, nacionalnih i međunarodnih informacijskih sustava, koji se koriste u svrhu uspješnog i učinkovitog rada i upravljanja određene kritične infrastrukture.

Sl. 3. Simbolički prikaz kritične ICT infrastrukture



U tom smislu kritična infrastruktura je infrastruktura čija bi onеспособljenost ili uništenje imala utjecaj na slabljenja nacionalne sigurnosti, te ekonomske i društvene dobrobiti nacije, a kritična informacijska infrastruktura jest informacijska infrastruktura koja podupire višestruke elemente kritične infrastrukture. Kako su informacijski

sustavi u velikoj mjeri međusobno povezani ili povezani s javnim sustavima, kritična informacijska infrastruktura u današnje vrijeme postaje sve izloženija, ne samo otkazima i havarijama, već i raznim vrstama namjernih napada. Osnovni problem iz kojeg proizlazi nužnost prepoznavanja kritične infrastrukture, predstavlja činjenica da napad na određenu kritičnu infrastrukturu sam po sebi multiplicira još veću štetu, jer relativno mali napad na jedan infrastrukturni objekt može imati ogroman utjecaj i prouzročiti štetu na čitavom nizu međusobno povezanih infrastrukturnih subjekata.

IV. ZAKLJUČAK

Sa EU procesima integracije iniciraju se i zahtjevi interoperabilnosti između regionalnih infrastrukture i u cijelosti EU infrastrukture. Poseban naglasak je na kritičnoj infrastrukturi kao nositelju stabilnosti gospodarskog razvoja i društvenih odnosa. Preporuke i zakonski okviri za zaštitu kritične infrastrukture postaju nužnost u nacionalnim razvojnim programima.

Definiranjem okvira nacionalne kritične infrastrukture uvidamo da je to vrlo kompleksan sustav sastavljen od ljudskih potencijala, fizičkih objekata i njihove međupovezanosti kroz informacijsko komunikacijske sustave. Upravo ovo zadnje - ICT industrija, nužna je i ključna zbog svojih sinergijskih sposobnosti u povezivanju raznih gospodarskih i društvenih grana koji su po tradiciji konzervativni. Ovdje je također potrebno istaknuti i dosadašnju važnu ulogu informacijsko-komunikacijskog sektora u modernizaciji i transformaciji gospodarstva i društva.

ICT sektor se ne smije izolirati zbog svojih, ponekad prenaprednih tehnoloških rješenja i vrlo inovativnog pristupa novim izazovima.

Navest ću jedan primjer zbog pojašnjenja gore navedenih teza.

Svjedoci smo velikog trenda rasta društvenih mreža, poput Facebooka, YouTubea, raznih blogova i itd. Pojavom velikih kriznih incidenata ili katastrofa ljudi su reagirali na način da su koristili sve moguće resurse za spašavanje i zaštitu, pa i društvene mreže. Prema kasnijim izvješćima nekih organizacija, stanovništvo su i nove ICT tehnologije prepoznali kao faktor remećenja. Stanovništvo nikad ne smije biti dio problema već dio rješenja isto tako kao i ICT napredne tehnologije. Također kada su preživjele unesrećene ljude pitali što im nedostaje, odgovor je bio: voda i informacije.

Zaključno možemo konstatirati kako je za uspješnu zaštitu kritične infrastrukture, ne samo u ekstremnim uvjetima, potrebna informatizacija društva i stalno podizanje ICT znanja i svijesti o važnosti umrežavanja svih grana kritične infrastrukture.

LITERATURA

- [1] Architecture Development Team, National ITS Architecture Security, Federal Highway Administration, US Department of Transportation, May 2007.
- [2] Mandžuka S., Savi I., Kljaić Z. Inteligentni transportni sustavi i upravljanje krizama, III međunarodna konferencija Dani kriznoga upravljanja. Veleučilište Velika Gorica, Zagreb, 2010.
- [3] Moteff, J, Critical Infrastructure Protections: Commission Report and Congressional Response, Washington, 2005.
- [4] Mandžuka S., Kljaić, Z., Kordić, Z. Mobilne telekomunikacije u sustavima upravljanja incidentima, Konferencija TELFOR 2009.
- [5] Kljaić, Z., Mandžuka, S. Napredne telekom tehnologije u području sigurnosti gradova, Druga regionalna konferencija o sigurnosti gradova, Zagreb, 2010.
- [6] Perešin A., Klaić A., Kritična infrastruktura i kritična informacijska infrastruktura, III međunarodna konferencija Dani kriznoga upravljanja. Veleučilište Velika Gorica, Zagreb, 2010.
- [7] European Programme for Critical Infrastructure Protection
- [8] Tatalović, S., Grizold, A., Cvrtila, V., *Suvremene sigurnosne politike*, Tehnička knjiga, Zagreb, 2008.
- [9] Abele-Wigert, I., Dunn, M., *International CIIP Handbook 2006*, Center for Security Studies, ETH Zurich
- [10] Peltier, T.R., *Information Security Policies and Procedures*, Auerbach Publication, 2006.
- [11] PMI, *A Guide to the Project Management Body of Knowledge*, 3rd Ed., Project Management Institute, 2004
- [12] IT Governance Institute, *Information Security Governance*, 3rd Edition, 2007.
- [13] Lewis, T. G., *Critical Infrastructure Protection in Homeland Security*, Wiley-Interscience, 2006.
- [14] Črnko M., Šabić A., Uporaba društvenih mreža u kriznom menadžmentu, III međunarodna konferencija Dani kriznoga upravljanja. Veleučilište Velika Gorica, Zagreb, 2010.
- [15] Gerber, M., Von Solms, R., *Information security requirements – interpreting the legal aspects*, Computers&Security 27(2008)
- [16] Bošnjak, I., Mandžuka S., Vujić, M. Škorput, P. Razvoj inteligentnih transportno-logističkih sustava u RH, Drugi kongres znanstvenika iz zemlje i inozemstva, poster, Split, 2007.

ABSTRACT

Today's economic and cultural globalization, as well as, on the one hand, the political context of integration, and on the other, the liberalization of production and distribution of products and services, raises important questions on the management of basic infrastructure in transitional and developing countries.

Contemporary sociology too, with lots of compelling reasons, describes the modern society as a risk society, in which produced risks threaten individuals and groups more significantly than externally generated risks. When we put the mentioned issue in a recession environment, where the financial framework and resources are very limited, we can observe significant increase in the risk intensity.

Where is the ICT industry as a basic tool of business development, can ICT technologies successfully respond to the growing challenges of our society. This paper analyzes, investigates and provides a number of technical and technological information, pointing out the important aspects of increasing the security of critical infrastructure.

APPLICATION OF ICT IN MANAGEMENT OF CRITICAL INFRASTRUCTURE IN TRANSITIONAL AND DEVELOPING COUNTRIES

Zdenko Kljaić, Member, IEEE, Sadko Mandžuka, dr.sc, Member, IEEE, Pero Škorput, mr.sc. Member, IEEE