ZAŠTITA INFRASTRUKTURE U DOMOVINSKOJ SIGURNOSTI

CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY

Prikaz knjige

Majda Tafra-Vlahović*

Prikaz knjige/studija slučaja

Ted G. Lewis: Critical Infrastructure protection in Homeland Security, Defending a Networked Nation, third edition, 2020, John Wiley & Sons, Inc.

Ovaj gotovo pet stotina stranica dugi i na trenutke vrlo tehničkim jezikom pisan tekst o pitanjima infrastrukture u službi domovinske sigurnosti mogao bi obeshrabriti laike koji smatraju da je domovinska sigurnost stvar nekih dobro plaćenih umova ali ne i šire akademske zajednice, ukoliko mu ne bi prišli bez straha od izazova bavljenja svakim detaljem koji autor minuciozno razvija u knjizi. Usprkos očekivanoj kompleksnosti materije, ovaj tekst je tekst, međutim, od onih koji traže da mu se priđe otvorena uma već i zato jer se bavi pitanjima koja se tiču građana i njihove sigurnosti. Baš svih građana. U tom je smislu ovo treće izdanje publicirano 2020 godine osobito aktualno u vremenima kada, zbog epidemije Corona virusa koja ne jenjava niti obećava brzi oporavak, osobito zanimljivo ekspertima ali i manje ekspertnoj publici jer, u odnosu na prva dva izdanja, primarni naglasak stavlja na računalnu i mrežnu sigurnost a manje na numeričku i matematičku prezentaciju problema. Za autora tridesetak knjiga i više stotina znanstvenih tekstova, po profilu informatičkog i matematičkog eksperta, čini se logičnim da u tekstu koji je koncipiran i testiran, među ostalim, i kao udžbenik za studente kojima je sigurnosni aspekt obrane vitalni interes, ovaj je iskorak u cyber prostor, u većoj mjeri no u prethodnim izdanjima, logičan. Američki kontekst nije temeljan ali može biti osobito koristan kao uzorak osobito na planu konceptualnog okvira tako da je prednost teksta, osobito za čitaoca ili visokoškolskog nastavnika koji razmatra knjigu kao udžbenik, upravo njegova

* *Rochester Institute of Technology, Dubrovnik/Zagreb, Hrvatsk Majda.tafra@croatia.rit.edu*

široka primjenjivost i razumijevanje, pa i mogućnost učenja na tuđim greškama.

U recenziji pregnantnog teksta ovako obećavajućeg naslova kojoj je, po definiciji, cilj navesti čitatelje da požele osobno se upoznati s njime, utemeljena je odluka bila nikako preskočiti dva značajna predgovora, ne zato jer bi po stručnosti osobito doprinosili vrijednosti cijelog teksta, nego, moguće, prije svega zato, jer čitatelju koji nije ekspert sigurnosne struke, snažno ukazuju na gotovo sudbinsku važnost materije zaštite infrastrukture prije svega u kontekstu globalnih tektonskih poremećaja koje su i mali narodi balkanskog okruženja integralni dio, ma što se djeci i studentima o tome pripovijedali. U dva predgovora koja potpisuju jedan živući senator i bivši guverner (Mark Warner) i jedan matematičar i ekspertni akademik koji je i sam vodio Centar za kompjutorsku tehnologiju sveučilišta u Minnesoti i pripadajući Institut za računarstvo (Andrew Odlyzko), ta se važnost razvija u logičnim sljedovima potičući čitaočevu radoznalost. Političar po vokaciji, Mark Werner će upozoriti sugrađane Amerikance u pomalo dramatičnom narativu, da je u tijeku napad jednako opasan ili opasniji no što je bio Pearl Harbour ili 11 rujna, samo da nisu to osvijestili negirajući brojku da cyber napadi i cyber kriminal koštaju američku ekonomiju 175 milijardi dolara godišnje. Sami smo si krivi, ustvrdit će senator, jer smo društvo sve ovisnije od proizvoda i mreža koje su pod stalnim napadom a razina sigurnosti u proizvodima komercijalne tehnologije je neoprostivo niska. I konačno, otvoreno ističe da njihovi protivnici igraju potpuno drugačiju igru. Zemlje poput Rusije sve više spajaju tradicionalne cyber napade s informacijskim operacijama i taj rastući sve moćniji brand hibridnog cyber ratovanja upravo se hrani onim što Amerikanci smatraju svojim najvećim postignućem – otvorenošću i slobodnim protokom ideja. Predbacujući američkim političarima naivnost jer ne prepoznaju evidentnu rusku superiornost na ovom planu senator će ih upozoriti i na ekspanziju kineske doktrine cyber suvereniteta po kojoj država ima pravo na potpunu kontrolu informacija na svom teritoriju. To se naravno kosi s principima demokracije pa to senator neće ni preporučiti ali upozorava kako se ta doktrina uspješno izvozi u zemlje kao što su Venezuela, Pakistan ili Etiopija pa, naravno, i mnoge druge, da ekstenziju suvereniteta koji će protezati čak i do američkih divova u privatnom sektoru i ne spominjemo. Sjetimo se samo što je Google bio spreman učiniti da se domogne kineskog tržišta. Warner će zato preporučiti nova pravila za upotrebu cyber i informacijskih operacija, borbu protiv zloupotrebe informacija i dezinformacije: pojačane mreže, oružane

sustave i IOT (Internet of Things), ujedinjavanje obrambenog budžeta i, konačno, vodstvo koje bi sve to omogućilo. Knjiga kojoj je sve to napisao u predgovoru razvija do u detalja neke aspekte ovih mogućih strategija ali je, naravno, mnogo opširnija i sveobuhvatnija.

Informacijski i matematički ekspert Andrew Odlyzko, s druge strane, u istom tonu ali s detaljnijim argumentima objašnjava kako sada stvari stoje sa sigurnošću na globalnom planu, kako se ljudski prostor odnosi prema cyber prostoru i posebno upozorava na ekosustav cyber zločina te opasnosti zanemarivanja onog što bi trebale biti očite mjere sigurnosti. Jednako kritičan, moguće manje dramatičan, ali u tonu upozorenja kakvo daje i prvi uvodničar. Oba su teksta dobar uvod za knjigu u kojoj se znanstveno pristupa zaštiti ključnih infrastrukturnih komponenti nacije što znači analizu mreže elemenata infrastrukture nacije i identificiranje ranjivosti i rizika u različitim sektorima na način koji je djelomično preuzet iz teorijskog pristupa upravljanju incidentima i krizom a koji se već dosta dugo primjenjuje u raznim, a osobito izloženim i ranjivim industrijama u javnom i privatnom sektoru. Tekst kombinira mrežnu znanost, teoriju kompleksnosti, analize rizika te modeliranje i simulacije koje su studentima osobito bliske i metodički su prihvatljive u nastavi. Time se kompleksni problemi kao što su zaštita zaliha vode, energetskih cjevovoda, telekomunikacijskih stanica, električne mreže te internetskih i web mreža izučavaju na razumljiviji način svodeći ih na problem zaštite kritičnih čvorova.

Knjiga je podijeljena u tri dijela. Prvi se dio bavi povijesnim podrijetlom domovinske sigurnosti i kritične infrastrukture posebno se referirajući na aktualne političke okolnosti. U drugom dijelu autor ispituje teoriju i konceptualnu utemeljenost s naglaskom na pitanja rizika i otpornosti i kontekstu teorije kompleksnosti, znanosti o mrežama i prevladavajućih teorija katastrofe. U trećem dijelu obrađeni su pojedinačni sektori uključujući i komunikacije, Internet cyber prijetnje, informacijsku tehnologiju, društvene mreže, SCADA, zaštitu i pročišćavanje voda, energiju i ostala pitanja zaštite infrastrukture. Autor se bavi i teorijama katastrofe i radom pojedinih sektora kao i pitanjem veličine i složenosti zaštite kritične infrastrukture. Velik naglasak se stavlja na računalnu sigurnost i odgovor cijele zajednice. Kako je riječ o knjizi koja služi i kao udžbenik, izdavač nudi i slajdove za predavanja, vodič za instrukcije i vježbe te opširne dodatke koji dopunjuju nematematička poglavlja dubljima objašnjenjima i matematikom. Riječ je o bogatoj knjizi koja je i doživjela treće dopunjeno izdanje jer se cyber prostor nameće kao jedna od

vodećih tema sigurnosti, pa u tom smislu je dragocjen izvor ne samo za nastavu već i za sve profesionalne stručnjake za sigurnost i ali i one koji nisu posebno stručni na tom planu ali imaju moć da stvaraju politike i uvode mjere o kojima ovisi sigurnost države.