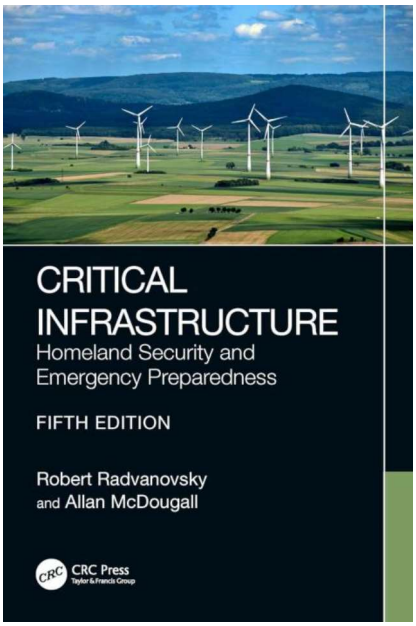
Јана МАРКОВИЋ, сарадник у настави*

ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ КАО УСЛОВ ОЧУВАЊА ЖИВОТА И ОПСТАНКА ДРУШТВА

Robert Radvanovsky, and Allan Mcdougall. *Critical Infrastructure: Homeland Security and Emergency Preparedness*, Fifth Edition. CRC Press, 2023, 294 pp.



Књига *Критична инфраструктура: Државна безбедност и спремност за ванредне ситуације*, која се налази пред читаоцем, представља пето издање и наставак дугогодишњег истраживања. Аутори Роберт Радвановски (Robert Radvanovsky), стручњак у области безбедности, управљања ризицима, континуитета пословања, планирања опоравка од катастрофа и сајбер безбедности, и Алан МекДугал (Allan McDougall), стручњак у области заштите имовине и безбедности, настоје да кроз дванаест поглавља дају одговоре на следећа питања: Да ли је инфраструктура неопходна за очување живота или опстанак заједнице? Да ли инфраструктура функционише у веома ограниченом контексту или у много ширем контексту, односно да ли је инфраструктура

* Факултет безбедности, Универзитет у Београду, markovicfb22@gmail.com

специфична само за локалну заједницу, или се повезује са другим заједницама како би створила много већу заједницу? Да ли инфраструктура функционише као појединачна или јединствено организована целина, или је то заједница координисаних напора које улаже неколико страна? Чини се да аутори настоје да, поред приказа тренутног стања, понуде увиде за сагледавање трендова у домену заштите критичне инфраструктуре и њеном значају за националну безбедност. Таква сазнања би значила истраживачима, студентима, стручњацима, заинтересованим странама у индустрији, попут власника и оператера критичне инфраструктуре било у приватном, јавном или непрофитном сектору.

Прво поглавље аутори користе да читаоце упознају са значењима одређених појмова и понуде објашњења за феномене без чијег разумевања даље читање овог штива не би имало смисла. Објашњени су развој, појам и елементи критичне инфраструктуре, њена заштита, приватни и јавни сектор као власник критичне инфраструктуре и улога ових сектора у њеној заштити, као и незаобилазно јавно-приватно партнерство приватног и јавног сектора у области заштите „физичких и логичких система који су неопходни за минималне операције привреде и владе". Кроз књигу се провлачи прагматичан приступ разумевању супротстављених интереса јавног и приватног сектора око заштите критичне инфраструктуре.

Критична инфраструктура има одређена својства или карактеристике. Једно од својстава јесте капацитет одређен као „способност система да производи, дистрибуира и испоручује услуге". Међутим, у конкурентном окружењу, за успех система није довољан само капацитет, већ и уверење или сигурност да ће ти капацитети задовољити потражњу. Онда када капацитет система задовољи потражњу онда се каже да је систем у равнотежи. Са друге стране, систем ван равнотеже може да доспе у стање крхкости и дестабилизације, или чак да изгуби могућност комуникације и координације између својих активности, што систем води до фрагментације и распадања. Друго поглавље, поред одређених карактеристика, указује и на подложност критичне инфраструктуре утицајима који могу деловати на међузависности, као и поремећајима унутар њеног умреженог окружења.

Трећи део књиге посвећен је међународном карактеру критичне инфраструктуре, а у првом реду међународним стратешким интересима и ланцима снадбевања као једном виду економских веза који повлаче за собом и уједно захтевају кретање изван националних ка

међународним оквирима. У таквом окружењу, аутори подвлаче да „владе задржавају *de facto* коначни ауторитет … али оне више нису водећи играч на сцени". Тада на сцену ступају међународни споразуми који не обавезују само на дељење информација, већ и на заједничке захтеве по питању одређених активности као што су управљање ризиком и ланцима снабдевања који прелазе међународне границе. Посебно питање које се отвара јесте и подела одговорности између влада као јавног сектора (сектора који регулише) и приватног сектора (сектора који се регулише).

Јавно-приватно партнерство у области заштите или осигурања критичне инфраструктуре долази у први план у наредном поглављу где се, поред одређења и врста јавно-приватног партнерства, повлачи паралела између улоге влада и улоге приватног сектора у тој заштити, а посебно у областима успостављања нових капацитета и одржавања постојећих.

Пето поглавље посвећено је улози коју подаци и информације имају у заштити критичне инфраструктуре. Подаци, као основна запажања, након што се обраде постају информације које се интелигенцијом даље синтетизују у функцији доношења одлука, а све то уважавајући контекст. Аутори не само да разматрају нове трендове када су у питању прикупљање, коришћење и заштита информација и обавештајних података већ разматрају и употребу такозваног облака (енгл. *Cloud*) за складиштење података или повезивање поуздане рачунарске базе и корисничких заједница за размену података, уз указивање на евентуалне ризике коришћења истог и могућа решења. На крају, у ери све бржег развоја отворених извора података (енгл. *Open Sources*), истраживачи треба да воде рачуна између информација које се само преписују и знања које је генерисано.

Функционисање сваке заједнице почива на основним услугама, које су све више резултат конкуренције на отвореним тржиштима. Улога владе јесте да заштити пружање тих услуга и уједно заштити безбедност и економско благостање својих грађана. И на овом месту аутори указују на кључну разлику између јавног и приватног сектора, усмерености на јавно добро и усмерености на профит кроз теме као што су балансирање јавне безбедности и пословних операција и балансирање отпорности и финансијске одговорности.

Шта је отпорност? Шта она значи за критичну инфраструктуру? Да ли је довољно чекирати контролне листе и строго се придржавати правила и „добре праксе" да бисмо били сигурни да је критична инфра-

структура коју штитимо заиста заштићена и осигурана. Суштина заштите критичне инфраструктуре јесте обезбедити да „услуга очувања здравља, безбедности или економског благостања буде присутна, у употребљивом стању, када је то потребно и по разумној цени". Како томе треба приступити? Одговоре на ова, али и друга повезана питања могуће је пронаћи у седмом поглављу ове књиге, где аутори дају критички осврт на строго поштовање стандарда и уско посматрање контекста и ризика који се у њему јављају.

Поред отпорности, значајно место у разумевању критичне инфраструктуре има њена међузависност, којој аутори посвећују наредно поглавље. Аутори упозоравају на то да, с обзиром на растућу међусобну повезаност инфраструктуре, „способност да се идентификује, процени, управља и надгледа комплетан пакет зависности и међузависности било које организације постаје све сложенији и изван домета било којег самосталног ентитета". У овој ери „повећаног груписања инфраструктура" од изузетне је важности регулисање и усаглашавање међузависности, а посебно у четири кључна сектора: енергетике, транспортних система, комуникација и финансијских услуга… У супротном, може се догодити „савршена олуја" – потпуни колапс неколико инфраструктура на најмање регионалним нивоима.

Стручност и искуство аутора у областима физичке и сајбер безбедности огледа се и у размишљању о конвергенцији физичких и сајбер претњи критичној инфраструктури. Док су сајбер претње, односно сајбер безбедност обухваћени кроз више поглавља, аутори су разматрању физичке безбедности посветили девето поглавље књиге. Физичка безбедност, која се протеже на стратешком, оперативном и тактичком нивоу, није изгубила на значају услед јачања сајбер безбедности. Разумевање топографије мреже која пружа критичне услуге, процена ризика, која омогућава разумевање ризика, поштовање прописа и стандарда, а тек онда пројектовање и имплементирање мера физичке безбедности елементи су успешног одговора на ризике са овог аспекта заштите.

У десетом поглављу главна тема јесте промена парадигме управљања критичном инфраструктуром изазвана догађајима попут пандемије. Низ „тренутака из којих се може учити" произвео је промене у радној снази, измешта „локације" управљања, увећава значај дигиталне инфраструктуре, отвара питања заштите критичних информација и мрежа, као и сертификације у функцији свеобухватне процене управљачких, оперативних и техничких контрола неког система.

Наредно, или једанаесто поглавље се надовезује на промену парадигме обухватајући неке аспекте које би та промена парадигме требало да обухвати.

Последње поглавље аутори су посветили климатским променама као једној од претњи по критичну инфраструктуру и изазову за оне који се баве њеном заштитом. Неизвесности које доносе климатске промене, те неповољни временски услови условљавају управљање ванредним ситуацијама неизоставним елементом заштите критичне инфраструктуре. Способност да се издржи (да се идентификују критичне услуге на сваком нивоу стратешког, тактичког и оперативног нивоа), способност да се реагује и способност да се опорави три су кључна елемента у суочавању са елементарним непогодама. Аутори, избегавајући политичку дебату која постоји око ове теме, пишу још и о ПООД петљи (енгл. *OODA Loop*), која укључује посматрање, оријентисање, одлучивање и деловање, а може се користити у процесу доношења одлука.

Аутори су користили јасан језик за писање, што је садржај ове књиге учинило лаким за читање. Ова књига представља корисно штиво за заинтересоване читаоце како у научним тако и у стручним круговима, у јавном и приватном сектору, који желе да разумеју заштиту критичне инфраструктуре и импликације, те заштите на националну безбедност.

Значајан сегмент ове књиге јесу прилози у виду линкова значајних владиних и јавних интернет страница који омогућавају читаоцима да дубље истражују питања која их интересују. Међутим, имајући у виду брзу промену Интернет ресурса, као и могућност нестанка интернет адреса аутори су обезбедили секундарни извор референтног материјала како би се обезбедила конзистентност онога што је написано. Уз то, садржај књиге је употпуњен и мноштвом примера које аутори користе да поткрепе изнете ставове.