

ЕДИЦИЈА АΣΦΑΛΕΙΑ

Књига VIII

**СУПРОТСТАВЉАЊЕ
САВРЕМЕНОМ
ОРГАНИЗОВАНОМ
КРИМИНАЛУ И
ТЕРОРИЗМУ**

VI

КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКА АКАДЕМИЈА

БЕОГРАД, 2015

Издавач
КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКА АКАДЕМИЈА
Београд, Цара Душана 196, Земун

За издавача
Проф. др Младен Бајагић,
в. д. декана Академије

Главни и одговорни уредник
Проф. др САША МИЈАЛКОВИЋ,
Руководилац научноистраживачког пројекта

Уредници
ВЛАДИМИР ЦВЕТКОВИЋ, МА, секретар Пројекта
МАРИЈА ПОПОВИЋ, МА, секретарка Пројекта
Доц. др ТАЊА КЕСИЋ
Проф. др ЖЕЉКО НИКАЧ

Рецензенти
Проф. др РАДОМИР МИЛАШИНОВИЋ
Др ЈОВАН ЂИРИЋ, научни саветник
Др МАРКО НИКОЛИЋ, научни сарадник

Лектор
Милена Шећеровић

Компјутерска припрема слога
Сигнатуре Д.о.о.

Тираж
150 примерака

Штампа
Пекограф, Земун

©2015 Криминалистичко-полицијска академија, Београд

ISBN 978-86-7020-333-4

This book (thematic collection of papers) is the result of the realisation of the Scientific Research Project entitled "Development of Institutional Capacities, Standards and Procedures for Fighting Organized Crime and Terrorism in Climate of International Integrations". The Project is financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia (No 179045), and carried out by the Academy of Criminalistics and Police Studies in Belgrade (2011–2015). The leader of the Project is Full-time Professor Saša Mijalković, PhD.

КАРАКТЕРИСТИКЕ ИНФРАСТРУКТУРНИХ СИСТЕМА

Марија Мићовић¹

Криминалистичко-полицијска академија, Београд

Апстракт: Инфраструктурни системи представљају основ функционисања људског друштва. Састоје се из индивидуалних или међусобно повезаних структура, опреме, извора струје, контролних система итд. Због увећања ризика повредљивости и лаког искључивања из редовног функционисања инфраструктурног система, потребно је предвидети појединачно за сваки систем одговарајуће мере. Функционисање модерног друштва како у редовној тако и у ванредној ситуацији није могуће замислити без ефикасне заштите значајних инфраструктурних објеката те се као један од примарних и најзначајнијих безбедносних изазова новог доба намеће проблем заштите критичних инфраструктура. Инфраструктуре као што су саобраћајне мреже, воде, енергије, хемијске и нуклеарне индустрије, и информационих и комуникационих технологија пружају основне услове за функционисање појединаца па и друштва у целини.

Кључне речи: критична инфраструктура, инфраструктурни системи, рањивост.

Увод

Пре него што је критична инфраструктура постала термин од интересовања за расправе о тероризму и унутрашњој безбедности, сличан појам „инфраструктура“ био је предмет расправа креатора јавне политике у Америци. Током 1980-их, на пример, дискутовало се о томе да ли је дошло до националне кризе у стању америчке инфраструктуре – путева, мостова, брана, система отпадних вода, итд. Без икаквих стандарда или заједничке дефиниције, концепт инфраструктуре у контексту политике био је флуидан, на начин на који тако изгледа данас.

Извршна наредба 13010², коју је потписао председник Клинтон 1996. године, а која успоставља председничку комисију за заштиту критичне инфраструктуре, односи се на оно што одређену инфраструктуру чини критичном а то су одређене националне инфраструктуре које су толико

1 Истраживач-сарадник, marija.blagojevic@kpa.edu.rs

2 Executive Order 13010 – Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138. pp 37347-37350. Str. 37347.

виталне да би ометање њиховог рада или уништење имало ефекат ослабљивања одбрамбене или економске сигурности САД³.

Према овој извршној наредби, ове инфраструктуре су обухватале:

- телекомуникације;
- системе електричне енергије;
- складиштење и транспорт нафте и гаса;
- банкарство и финансије;
- транспорт;
- системе за снабдевање водом;
- хитне службе (медицинске, полицијске, ватрогасне и за спасавање) и
- континуитет власти.⁴

1. Особине инфраструктурних система

Инфраструктурни системи обухватају широк спектар виталних сектора, као што су саобраћај, транспорт, производња и дистрибуција енергије, информациони и комуникациони системи, здравствене службе, системи за снабдевање водом и храном, финансијске службе, државна инфраструктура (агенције и организације влада, административни сектор) итд. Делимично или потпуно отказивање ових инфраструктура може да угрози друштво, националну безбедност и да доведе до најразличитијих криза. Развијене земље, а последњих година и оне мање развијене, настоје да идентификују и анализирају критичне секторе, подсекторе, процесе и објекте коришћењем различитих методолошких и политичких приступа. Невероватна комплексност инфраструктурних система је дефинитивно највећи заједнички проблем свих земаља које су се упустиле у анализирање и идентификовање критичне инфраструктуре, као и оних које покушавају да формирају политику заштите критичне инфраструктуре. Основне карактеристике инфраструктурних система су:

Ослабљеност: Стање одбрамбене или економске сигурности које карактерише неефикасност.

Одбрамбена сигурност: Стање у којем су живот и лична сигурност грађана, како у земљи, тако и у иностранству, заштићени, а суверенитет,

3 Ibid. стр. 37347.

4 Ibid.

политичка слобода и независност, заједно с њеним вредностима, институцијама и очуваном територијом одржани.

Економска сигурност: Стање у којем национална добра и услуге могу успешно да конкуришу на глобалним тржиштима, док се истовремено одржава или увећава доходак грађана.⁵

2. Дефинисање инфраструктурних сектора

Један од основних инфраструктурних сектора за опстанак човека дефинитивно је и сектор производње и снабдевање становништва електричном енергијом. Поремећај функционисања мреже снабдевања електричном енергијом може да има јако негативан утицај на националну безбедност, националну економију и на живот сваког човека посебно. Пошто је мрежа дистрибуције електричне енергија врло разграната, велики изазов представља очување нормалног функционисања те инфраструктуре. Ванредне ситуације, саботаже попут сајбер-напада могу у великој мери да оштете сектор производње и дистрибуције електричне енергије и да спрече успут и нормалну комуникацију и рад информационих система и то не само на националном већ и на међународном нивоу.⁶

Сведоци смо све већег броја инфраструктурних сектора који постају транснационални. То је првенствено сектор информационих и комуникационих технологија који је све више утицајнији и одавно је превазишао националне границе. Такви су и сектори саобраћаја (друмски, железнички, ваздушни, водни), затим телекомуникација, хемијске индустрија, као и нуклеарне индустрије.

Зелени документ⁷ о европском програму заштите критичне инфраструктуре дефинише даје и преглед критичних инфраструктурних сектора. У критичне инфраструктуре се према овом документу убрајају:

- Енергетика (производња нафте и гаса, рафинисање, прерада и складиштење укључујући и гасоводе и нафтоводе; производња струје; трансмисија струје, гаса и нафте; дистрибуција струје

5 President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure, October 1997.

6 A. Massoud, "Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)". *Computer* (IEEE computer society), 2002-04

7 Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final, документ је доступан на интернет адреси: http://www.liberty-security.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf

нафте и гаса), Електране и мреже за пренос и дистрибуцију који производе и снабдевају електричном енергијом крајње кориснике тако да они постижу и одржавају номиналну функционалност, укључујући транспорт и складиштење горива које је неопходно за овај систем.

- Информационе и комуникационе технологије – ИКТ (информациони системи и мрежна заштита; интернет; пружање услуга у области фиксне телефоније; пружање услуга у области мобилне телефоније; радио комуникација и навигација; сателитска комуникација),
- Вода (извори воде, резервоари и постројења за складиштење, водоводи и други транспортни системи, системи за филтрацију, чишћење и прераду воде, цевоводи, расхладни системи и други механизми испоруке који обезбеђују воду домаћинствима и индустријским потрошачима, укључујући системе за рад са отпадним водама, као и системе за заштиту од пожара.
- Храна (снабдевање храном и очување безбедности и квалитета хране),
- Здравство (медицинска и болничка нега; лекови, серуми, вакцине; био-лабораторије; био-агенси),
- Финансијски системи (ентитети као што су малопродаје и комерцијалне организације, инвестиционе институције, брокерске куће, трговачке куће и системи резерви, и придружене оперативне организације, владине операције и активности подршке које су укључене у све аспекте монетарних трансакција, укључујући штедне улоге, инвестиције, безготовинске исплате и исплате у форми зајмова и других финансијских инструмената.
- Органи јавног реда и мира, јавне безбедности и судство (очување јавног реда, мира, безбедности; судска администрација),
- Цивилна администрација (владино органи; оружане снаге; службе цивилне администрације; службе за реаговање у ванредним ситуацијама; поштанске и курирске службе),
- Саобраћај и транспорт (друмски саобраћај; железнички саобраћај; ваздушни саобраћај; речни саобраћај; поморски и океански саобраћај и транспорт),
- Хемијска и нуклеарна индустрија (производња, складиштење и прерада хемијских и нуклеарних супстанци; цевоводи за транспорт опасних материја).⁸

8 Ibid.

Упркос сталном развоју и напретку безбедних технологија, у непрекидној трци са нападачима у реалном животу и даље постоје бројне слабости (мобилни терминали, персонални рачунари, приступне мреже, транспортне мреже, сигнализациони канали, интерне инфраструктуре оператора и корпоративних корисника, базе података и друге компоненте система). Динамично пословно окружење и жестока тржишна утакмица, мобилност корисника, конвергенција мобилних терминала и персоналних компјутера, разуђеност корпорација, нови пословни модели електронског пословања, јединствен глобални виртуелни простор и други спољашњи фактори само отежавају позицију бранилаца мрежа и дигиталних граница.⁹

Када говоримо о инфраструктурним системима свакако треба обухватити чиниоце који могу довести до угрожавања нормалног функционисања истих и нормалног обављања дужности од стране оператора, као и власника система, социјалну климу и интерперсоналне односе између свих људи неопходних за функционисање КИ, као и обезбеђеност објеката, техничких и информационо-комуникационих система и осталих средстава, и правила функционисања самог процеса КИ. Такође, треба водити рачуна о томе да су ризици међусобно условљени и испреплетени и да промене временских, просторних и фактора средине, односно окружења доводе до појаве нових и промене постојећих ризика. Другим речима, ризици су варијабилна категорија, тако да редуковање једне врсте ризика може да доведе до настајања новог или до повећања вероватноће остварења другог ризика, што не би требало занемарити у процесу анализе, идентификације и класификације ризика. Треба напоменути да приступ идентификацији и класификацији ризика мора бити заснован на објективности, систематичности и непристрасности, с тим да је пожељно узети у обзир субјективне доживљаје свих одговорних за нормално функционисање КИ о степену и врсти угрожавања, па је препоручљиво процес идентификације и класификације ризика прилагодити специфичностима једне КИ, њеног окружења и локалне заједнице. У идентификовању и класификовању ризика врло су битне релевантне и ажуриране информације и посебна стручна знања.¹⁰

9 L. Bouwmans, M.P. C. Weijnen, A. Gheorghe, *Critical Infrastructures at Risk, Securing the European Electric Power System*, Springer, 2006.

10 J. Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating and Managing Threats, Vulnerabilities and Consequences*, Report for Congress, Science and Industry Division, Congressional Research Service, 2005.

Рањивост је динамична, својствена одлика инфраструктурног система која садржи много компоненти. Степен до којег је утврђена рањивост одређује озбиљност догађаја. Рањивост указује на потенцијалну штету и променљива је која је усмерена ка напред. Рањивост подразумева предвидљивост као особину и би требало да буде у ствари начин предвиђања шта се може десити одређеној популацији у условима одређеног ризика и хазарда. Одредити рањивост значи поставити питање шта ће се десити ако одређени догађај (или догађаји) утиче на елементе који су изложени ризику.

Рањивост је унутрашња карактеристика заједнице, чак и у периоду између догађаја. Она се не појављује и не нестаје како догађај дође и прође, већ је особина која је стална и динамичка и испољава се у одређеној мери, у зависности од јачине штетног догађаја. Ово доводи до закључка да се рањивост може мерити само индиректно или ретроспективно, што подразумева да је тада главни показатељ рањивости настала штета. Оно што се обично види након катастрофе није рањивост сама по себи, већ причињена штета. Сагледавајући само штету која је настала услед штетног догађаја, без претходног сазнања о магнитуди догађаја, не дозвољава доношење закључка о рањивости одређене заједнице или друштва. У том смислу веза између јачине догађаја и штете рефлектује рањивост елемента који је угрожен (заједница, домаћинство, инфраструктура...). У општем смислу, рањивост се може дефинисати као „степен до кога ће систем, подсистем или компонента система вероватно бити оштећена због своје изложености хазарду, притисцима или стресорима различитог порекла.¹¹

Осим тога, још један важан параметар представља фактор независности, зависности или узајамне зависности инфраструктуре. Ово такође утиче на вероватноћу и врсту каскадног и појачаног ефекта:

- у каскадном неуспеху, поремећај у једној инфраструктури изазива поремећај и друге инфраструктуре;
- у нарастајућем неуспеху, поремећај у једној инфраструктури погоршава другу инфраструктуру (на пример време за опоравак и обнову инфраструктуре се повећава због недоступности друге инфраструктуре);

11 B. Ezell, Infrastructure Vulnerability Assessment Model (I-VAM), Risk Analysis Vol. 27, No.3., 2007.

- могућа је и дисфункција две или више инфраструктуре у исто време, која се јавља због заједничког узрока (природне катастрофе и сл.).¹²

Системи критичне инфраструктуре делују у окружењу које у великој мери одређује њихово функционисање. Окружење се може описати са неколико карактеристика, и то:

- прво, то је пословно окружење које највише утиче на деловање критичних инфраструктура. Иновације и технологија осигуравају развој и на разне начине креирају међузависности, са трендом синергетског повећавања учинака. Често су својства међузависности повезана са власништвом над инфраструктурама, при чему државно и власништво локалних заједница чешће усмеравају инфраструктуре на осигуравање услуга, док приватни сектор тежи повећању профита. Уз то јавне политике су друга димензија окружења,
- Законодавна и нормативна решења или прописивање услова за пословно инвестирање одређују деловање инфраструктура. Већ по дефиницији и сами су критичне инфраструктуре, па се морају утврдити међузависности са другим инфраструктурама,
- Трећи важан чинилац сваке инфраструктуре су техничка и сигурносна питања која такође битно утичу на њихово функционисање. На деловање критичних инфраструктура битно утиче и њихова повезаност, односно међузависност. Зависност је посебна индивидуална веза између две инфраструктуре, кроз коју стање једне мреже утиче на другу или је повезано са стањем друге, а може бити једносмерна или двосмерна. Инфраструктуре су често повезане као „системи система“, па се међузависности морају увек узимати у обзир приликом њиховог разматрања,
- Инфраструктуре су често повезане на више чворишта кроз низ различитих механизма, у чему постоје двосмерне везе између било којег пара инфраструктура. Међузависност је дакле двосмерна веза између две инфраструктуре, кроз коју стање једне утиче на стање друге и обрнуто. Теоретски то је једноставно, али у пракси то драматично утиче на сложену топологију мрежа, са различитим односима на појединим

12 C. Roper, Risk Management for Security Professionals, Butterworth-Heinemann, 1990

- тачкама укупне мреже. Као у пауковој мрежи шокови се могу пренети на сасвим други крај мреже, који наизглед нема никакве везе са местом иницијалног шока.¹³

Закључак

Систем критичне инфраструктуре обухвата поједине институције јавног и приватног сектора, канале дистрибуције те мреже особа и информација које гарантују несметан и континуиран проток људи, роба, сервиса, услуга, што је кључно за стабилност економског и безбедносног система земље. У систем критичне инфраструктуре убрајају се телекомуникације, електропривреда, складиштење и пренос плина и нафте, банкарство и финансије, транспорт, водоснабдевање, хитна служба (укључујући медицинске, полицијске, ватрогасне и спасилачке службе) и друге институције.

У оквиру једног инфраструктурног система, нема свака структура или подсистем исту важност за одржавање функционалности читавог система. Током катастрофе не мора сваки јавни сервис тј. услуга да функционише у оном обиму као када су у питању нормални услови: нпр. за одржавање система јавног здравља у току ванредних периода нема свака болница исту важност или подједнаке капацитете када су у питању хитне или ванредне ситуације. Физичка рањивост подразумева рањивост инфраструктурних елемената, као што су путеви, зграде, пруге итд. Уколико је посебно рањива инфраструктура сконцентрисана на једном месту, то може значајно да утиче на степен оштећења уколико дође до неког катастрофалног догађаја, било да су у питању последице природних хазарда или хазарда неког другог порекла. Ови догађаји могу имати различите потенцијалне утицаје на инфраструктуру, у зависности од врсте догађаја, његове локације, као и делова инфраструктуре који се налазе на том месту.

Литература

1. Bouwmans, I; Weijnen, M.P.C; Gheorghe, A; Critical Infrastructures at Risk, Securing the European Electric Power System, Springer, 2006.

13 C. Hofer, *Turnaround Strategies*, *The Journal of Business Strategy*, vol. 1 (1), ss.19. - 31., 1990.

2. Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final.
3. Executive Order 13010 - Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138. pp 37347-37350.
4. Ezell, C.B; Infrastructure Vulnerability Assessment Model (I-VAM), Risk Analysis Vol. 27, No.3, 2007.
5. President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure, October 1997.
6. Moteff, J; Risk, Management and Critical Infrastructure Protection: Assessing, Integrating and Managing Threats, Vulnerabilities and Consequences, Report for Congress, Science and Industry Division, Congressional Research Service, 2005.
7. Roper C; Risk Management for Security Professionals, Butterworth-Heinemann, 1999.
8. Hofer, C. V; Turnaround Strategies, The Journal of Business Strategy, vol. 1 (1), ss.19. - 31., 1990.

CHARACTERISTICS OF INFRASTRUCTURAL SYSTEMS

Marija Mićović

The Academy of Criminalistic and Police Studies, Belgrade

Abstract: Infrastructural systems represent the basis for the functioning of human society. They consist of individual or interconnected structures, equipment, power sources, control systems, etc. Due to an increased risk of fragility and light exclusion from regular functioning infrastructure system should be planned individually for each system correspond- measures. The functioning of a modern society both in regular and in an emergency situation can not be imagined without efficient protection of important infrastructure facilities, as well as one of the primary and most important security challenges of the new age raises the problem of protecting critical infrastructure. Infrastructure such as transport networks, water, energy, chemical and nuclear industries, and information and communication technologies provide the basic conditions for the functioning of individuals and the whole society.