КРИТИЧНА ИНФРАСТРУКТУРА

КОНЦЕПТ И БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ

МАРИНА МИТРЕВСКА
ТОНИ МИЛЕСКИ
РОБЕРТ МИКАЦ

FRIEDRICH EBERT STIFTUNG

МАРИНА МИТРЕВСКА
ТОНИ МИЛЕСКИ
РОБЕРТ МИКАЦ

КРИТИЧНА ИНФРАСТРУКТУРА: КОНЦЕПТ И БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ

Проф. д-р Марина Митревска
Проф. д-р Тони Милески
Доц. д-р Роберт Микац

**КРИТИЧНА ИНФРАСТРУКТУРА:
КОНЦЕПТ И БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ**

Рецензенти:
Проф. д-р Роберто Сетола
Проф. д-р Јонас Јохансон

Издавач: Фондација Фридрих Еберт, Канцеларија Скопје
Лектура: д-р Жанет Ристоска
Превод: Кирил Шарламанов
Печати: Контура
Тираж: 150

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

355.45(497.7)
355.45(100)

MITREVSKA, Marina
Critical infrastructure : concept and security challenges / Marina Mitrevska, Toni Mileski, Robert Mikac. - Skopje : [Friedrich Ebert Stiftung - Office Skopje], 2019. - 174 стр. : табели, граф. прикази ; 25 см

Фусноти кон текстот. - About authors: стр. 173-174. - Библиографија: стр. 159-162. - Регистар

ISBN 978-9989-109-93-5
1. Mileski, Toni [автор] 2. Mikac, Robert [автор]
а) Критична инфраструктура - Државна безбедност - Македонија COBISS.MK-ID 111119370

Искажаните ставови на експертите не мора да соодветствуваат на ставовите на организаторите.

МАРИНА МИТРЕВСКА
ТОНИ МИЛЕСКИ
РОБЕРТ МИКАЦ

КРИТИЧНА ИНФРАСТРУКТУРА: КОНЦЕПТ И БЕЗБЕДНОСНИ ПРЕДИЗВИЦИ

Скопје, 2019

Содржина

Листа на кратенки

ANSI	American National Standards Institute (Институт за национални стандарди на Америка)
ASME	American Society of Mechanical Engineers (Американско друштво на машински инженери)
BS	British Standards (Британски стандарди)
CEN	Comité Européen de Normalisation (French) – European Committee for Standardization (Европски комитет за стандардизација)
CENELEC	Comité Européenne de Normalisation Électrique (French) – European Committee for Electrotechnical Standardization (Европски комитет за електротехничка стандардизација)
CEPS	Central European Pipeline System (Централноевропски цевководен систем)
CI	critical infrastructure (критична инфраструктура)
CIP	critical infrastructure protection (заштита на критичната инфраструктура)
CIPP	Critical Infrastructure Protection Plan (план за заштита на критичната инфраструктура)
CIWIN	Critical Infrastructure Warning Information Network (Информативна мрежа за предупредување на критичната инфраструктура)
CPNI	Centre for the Protection of National Infrastructure (United Kingdom) (Центар за заштита на националната инфраструктура - Велика Британија)
CSDP	Common Security and Defence Policy (Заедничка безбедносна и одбранбена политика)
DHS	Department of Homeland Security (Оддел за државна безбедност)
DIN	Deutsches Institut für Normung (German) – German Institute of Standardization (Институт за стандардизација на Германија)
DOT	Department of Transportation (Оддел за транспорт)
ECAC	European Civil Aviation Conference (Европска конференција за цивилно воздухопловство)
ELEM	Macedonian Electric Power Plants (Електрани на Македонија)
EO	Executive Order (Извршна наредба)
EPA	Environmental Protection Agency (Агенција за заштита на животната средина)
ERNCIP	European Reference Network for Critical Infrastructure Protection (Европска референтна мрежа за заштита на критичната инфраструктура)

ETSI	European Telecommunications Standards Institute (Европски институт за телекомуникациски стандарди)
EU	European Union (Европска унија)
FINRA	Financial Industry Regulatory Authority (Регулаторно тело за финансиска индустрија)
GAO	Government Accountability Office (Владина канцеларија за одговорност)
G-8	Group of eight – Forum of governmental leaders of eight large and industrialized nations (Група од осум - Форум на владини лидери од осум големи и индустријализирани држави)
HIPAA	Health Insurance Portability and Accountability Act - Акт за подвижност и одговорност на здравствено осигурување
IEA	International Energy Agency (Меѓународна агенција за енергија)
IEC	International Electrotechnical Commission (Меѓународна електротехничка комисија)
ISAC	Information Sharing and Analysis Center (Центар за споделување и анализа на информации)
ISC	Interagency Security Committee (Меѓуагенциски комитет за безбедност)
ISIL	Islamic State of Iraq and the Levant (Исламска држава на Ирак и Левант)
ISO	International Organization for Standardization (Меѓународна организација за стандардизација)
IT	Information technology (Информатичка технологија)
JSC MEPSO	Macedonian Electricity Transmission System Operator (Македонски електропреносен систем оператор А.Д.)
MCS	Mercalli-Cancani-Sieberg (Меркали-Канкани-Сиебергова скала)
MI5	Military Intelligence, Section 5 (United Kingdom domestic intelligence agency) - Воено разузнавање, Оддел 5 (Агенција за разузнавање на Велика Британија)
MSB	Myndigheten för samhällsskydd och beredskap (Swedish) – Swedish Civil Contingencies Agency (Шведска агенција за цивилни вонредни состојби)
NATO	North Atlantic Treaty Organisation (Северноатлантски сојуз)
NCISAC	National Council of Information Sharing and Analysis Center (Национален совет на Центарот за споделување и анализа на информации)
NERC	North American Electric Reliability Corporation (Северноамериканска корпорација за електрична сигурност)
NIAC	National Infrastructure Advisory Council (Советодавен одбор за националната инфраструктура)

NIPP	National Infrastructure Protection Plan (Национален план за заштита на инфраструктура)
NIST	National Institute of Standards and Technology (Национален институт за стандарди и технологија)
NPR	National Preparedness Report (Национален извештај за подготвеност)
NPRD	National Protection and Rescue Directorate (Национална дирекција за заштита и спасување)
OSCE	Organization for Security and Co-operation in Europe (Организација за безбедност и соработка во Европа)
PCCIP	President's Commission on Critical Infrastructure Protection (Претседателска комисија за заштита на критичната инфраструктура)
PPD	Presidential Policy Directive (Директива за претседателска политика)
RC3	Regional Consortium Coordinating Council (Регионалниот конзорциумски координативен совет)
RECIPE	EU funded critical infrastructure protection project (Проект за заштита на критичната инфраструктура финансиран од ЕУ)
SCADA	Supervisory Control and Data Acquisition (Систем за мерење, следење и контрола на индустриски системи)
SCC	Sector Coordinating Council (Совет за секторско координирање)
SEE	South East Europe (Југоисточна Европа)
SLTT	state, local tribal and territorial (државен, локален, племенски и територијален)
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council (Државен, локален, племенски и територијален владин координативен совет)
SSA	Sector-Specific Agencies (Агенции за специфични сектори)
SSP	Sector Specific Plan (План за специфичен сектор)
TSA	Transportation Security Administration (Администрација за безбедност на транспорт)
UK	United Kingdom (Велика Британија)
UN	United Nations (Обединети нации)
USA	United States of America (Соединетите Американски Држави)
USD	United States Dollar (Американски долар)
USCG	US Coast Guard (Американска крајбрежна стража)
WTO	World Trade Organization (Светска трговска организација)

Предговор

При крајот на оваа година, кога НАТО прославува 70 години од постоењето, се очекува да биде завршен процесот на ратификација на Пристапниот протокол за членство на Република Северна Македонија во НАТО, со што и официјално ќе стане 30-тата земја-членка на Сојузот.

Членството во НАТО, покрај безбедносните, но и економските и социјалните придобивки, значи и многу работа и обврски за сите: граѓани, институции и организации во Северна Македонија, владеење на правото, независно судство, развиен образовен и здравствен систем.

Токму од таа причина, Фондацијата „Фридрих Еберт" одлучи да даде свој придонес преку поддршка на одредени процеси кои би можеле да бидат корисни за земјата и политиките во следните фази на интегрирање во НАТО. Темата на заштита на критичната инфраструктура беше иницирана од групата на автори на оваа публикација, и преку инклузивен процес кој подразбираше јавна расправа и вклучување на ставовите на експертите по ова прашање, е издадена финалната верзија на материјалот за заштита на критичната инфраструктура.

Во ваквите процеси, значајни се информациите и искуствата од поновите земји-членки, како Хрватска во случајов, во однос на нивниот процес на интегрирање во Алијансата и нивните искуства во однос на функционирање како полноправна членка на НАТО. Ваквата размена на искуства и добри практики ќе биде особено корисна сега, во финалната фаза на интеграцијата на нашата земја во НАТО, но и понатаму, во фазите на имплементација на политиките.

Искрено се надеваме дека оваа публикација, која има за цел да ги претстави и образложи сите аспекти поврзани со заштитата на критичната инфраструктура и, воедно, да иницира активности за креирање на стратегија и носење на закон за заштита на критичната инфраструктура, ќе наиде на интерес кај експертската публика и ќе биде од особена корист за надлежните институции.

Нита Старова
Фондација „Фридрих Еберт" – канцеларија Скопје

Вовед

Идејата да напишеме книга како оваа што ја имате пред себе ***„Критична инфраструктура: концепт и безбедносни предизвици“*** е храбар научен и стручен чекор. Нашата долгогодишна научно-истражувачка и стручна кариера ја насочивме кон неколку премиси. Првата базична премиса на оваа книга тргнува од концептот за критична инфраструктура како воопштен збир на вредности и добра кои се од суштинско значење за економијата, за државата и за општеството и чие нарушување во функционирањето или уништување би можело да создаде долгорочни штетни последици за основните вредности на општеството, од каде што јасно се препознава потребата од градење на координиран пристап при креирање на современ концепт за заштита на критичната инфраструктура.

Втората премиса со која се одликува оваа книга е со цел да покаже дека безбедносните проблеми со кои денес со соочуваат државите достигнаа ниво на сериозност и ургентност, при што станува јасно дека брзите поправки и ад хок решенија не се доволни и оттука е потребно да се размислува за зафати кои ќе помогнат, или пак, ќе бараат ефикасен начин за менување на пристапот кон заштитата на критичната инфраструктура.

Третата базична премиса на оваа книга е доменот на заштитата на критичната инфраструктура на национален развој, односно индивидуално и за таа цел ги издвоивме примерите на САД и Хрватска и политиките и процесите кои ЕУ и НАТО ги имаат иницирано и истите се трудат да ги координираат. Овие искуства се драгоцени за идните правци во креирањето на системот за заштита на критичната инфраструктура во Република Северна Македонија.

Во интерес на сеопфатна анализа вклучивме и двајца странски еминентни експерти од областа на критичната инфраструктура, и тоа Рик Ларкин и Мат Ватер (Rick Larkin end Matt Vatter). Нивното учество во овој проект, преку нивната анализа на заштита на критичната инфраструктура во САД, дава посебно значење на книгата во барањето на целисходно решение во креирање на систем за заштита на критичната инфраструктура во Република Северна Македонија.

Проблематиката на ***„Критична инфраструктура: концепт и безбедносни предизвици“*** е систематизирана во шест глави.

Во рамките на **првиот дел *„Поимно определување на терминот критична инфраструктура“,*** акцентот е ставен на поимното определување на инфраструктура за критична. Во овој контекст се разработени и заканите врз критичната инфраструктура и потребата од заштита на критичната инфраструктура. Исто така, во овој дел е поместен и делот кој се однесува на анализата на Индикативната листа на критичната инфраструктура.

Во **вториот дел *„Заштита на критичната инфраструктура во Европската унија“,*** фокусот од истражувањето е посветен на развојот на заштита на критичката инфраструктура од аспект на Европската унија, работата на институциите на Унијата и ориентацијата на овој домен за соработка со

приватниот сектор. Исто така, во овој дел е поместен делот кој се однесува на Директивата 2008/114/ЕК за идентификација и одредување на европските критични инфраструктури и процена на потребата да се подобри нивната заштита.

Во **третиот дел** насловен како „***НАТО и заштитата на критичната инфраструктура***", во фокусот на интерес се местото и улогата на Алијансата во заштитата на критичната инфраструктура, при што преку критичка анализа на еден сегмент од вклученоста и улогата на НАТО во заштитата на критичната инфраструктура се прави обид да се одговори на неколку значајни прашања. Едно од нив е дали НАТО прави прекумерна секуритизација и милитаризација на енергетскиот сектор, кој доминантно се поима како исклучително економско прашање, и дали постои соодветна улога и можност за вклучување на НАТО во заштитата на критичната инфраструктура во рамките на стратегиските концепти, особено по завршувањето на Студената војна.

Во рамките на **четвриот дел *„Заштита на критичната инфраструктура во Соединетите Американски Држави",*** акцентот е ставен на анализа на една од водечките земји во развојот на заштитата на критичната инфраструктура. Во тој контекст, мошне внимателно е разработен концептот и системот за заштита на критичната инфраструктура, при што мошне внимателно се разработени трите базични сегменти, и тоа функционалните, политичките и техничките механизми за заштита на критичната инфраструктура.

Во **петтиот дел од книгата *„Заштита на критичната инфраструктура во Хрватска",*** се анализирани досегашните постигнувања во развојот на критичната инфраструктура во Хрватска. Во тој контекст е разработен пристапот на Хрватска при донесувањето на Законот за заштита на критична инфраструктура и подзаконските акти, како и организацијата на системот за заштита на критична инфраструктура.

Во **шестиот дел** насловено како „***Република Северна Македонија и заштитата на критичната инфраструктура***", направен е приказ и преглед на актуелните состојбите во Република Северна Македонија поврзани со градењето ефикасен систем за заштита на критичната инфраструктура. Во овој дел, идентификувани се приоритетните сектори од критичната инфраструктура, како што се енергетиката, информатичките технологии, водните системи и воздушниот сообраќај. Во секој од посочените сектори, како резултат на реформските зафати на државата, постојат определени законски и подзаконски акти кои можат да овозможат ефикасно регулирање на заштитата на критичната инфраструктура. Врз основа на таквите состојби, се нудат соодветни мерки и препораки кои би биле најцелисходни во организацијата на заштитата на критичната инфраструктура. Како пример, понуден се начинот и можностите за креирање ефикасна стратегија за заштита на енергетската критична инфраструктура. Стратегијата, после идентификација на постојните ризици, треба да даде вистинска насока за надминување на состојбите околу немањето позитивно законодавство за енергетската критична инфраструктура. Сепак, авторите потенцираат дека се идентификувани парцијални решенија во различни сектори на критичната инфраструктура, кои не се погрешни, но многу веројатно можат да придонесат кон „задушување" на целиот процес за креирање и

ефикасно функционирање на оптималниот систем за заштита на критичната инфраструктура. Како резултат на таквите состојби, на крајот од поглавјето, дадени се поширок препораки кои треба да ги конкретизираат практичните чекори во насока на изградба на ефикасен систем за заштита на критичната инфраструктура.

Им изразуваме благодарност на рецензентите професор Јонас Јохансон, директор на центарот за истражување на заштитата на критичната инфраструктура од Лунд Универзитетот во Шведска и професор Роберто Сетола, од биомедицинскиот универзитетски кампус во Рим, Италија, кои ни укажаа чест со прифаќањето да бидат рецензенти на овој труд, за нивната стручна, академска и искрена поддршка за објавувањето на оваа книга.

Изразуваме голема благодарност на Фондацијата „Фридрих Еберт-Скопје", која го помогна овој проект и публикувањето на оваа книга на македонски и на англиски јазик.

Авторите и натаму остануваат благодарни за сите добронамерни сугестии, што ќе ги имаме предвид за евентуално ново издание.

Автори

Скопје, август 2019 година

ГЛАВА 1

КРИТИЧНА ИНФРАСТРУКТУРА: ПОИМ И КОНЦЕПТ

ГЛАВА 1

КРИТИЧНА ИНФРАСТРУКТУРА: ПОИМ И КОНЦЕПТ

Проф. д-р Марина Митревска
Универзитет Св. Кирил и Методиј - Скопје
Филозофски факултет, Институт за безбедност, одбрана и мир

1.1. Дефинирање на поимот критична инфраструктура

Терминот „критична инфраструктура" е релативно нов и теоретичарите ги наоѓаат неговите корени во средината на деведесеттите години и е тесно поврзан со енергетската безбедност, телекомуникациите, енергетските системи, гасоводите и нафтоводите, економијата, транспортот, водоводот и сл. (DCSINT 2006:1). Токму од тие причини „критичната инфраструктура" и нејзината ефикасност се од големо значење за квалитетот на животот, стопанството и функционирањето на јавниот сектор. Секако дека денешниот турбулентен свет и динамичен развој, со сè поголема пенетрација на модерните технологии и вештачката интелигенција, со зголемен број на неспецифични закани и ризици, како и сè поголемиот ефект од климатските промени кој резултира со зачестени катастрофи и со зголемен интензитет и огромни штети и загуби, влијаат поимот „критична инфраструктура" да е сè поприсутен во секојдневниот живот.

Интересот од истражувачки аспект за значењето на поимот „критична инфраструктура" може да се согледа и преку поедноставен пристап. Имено, доколку на веб-пребарувачот за истражување на „Гугл" (scholars google.com) се внесе поимот „критична инфраструктура" со цел пребарување, ќе се види дека во моментот се идентификуваат 298.000 истражувачки резултати, што претставува една огромна база на трудови поврзани со поимот „критична инфраструктура" (пристапено на 1април 2019 година).

Последователно се граделе и терминолошките и теориските рамки на дефинирањето на „критичната инфраструктура" во литературата. Разбирањето на „критична инфраструктура" се движи во рамките на опишувањето на критичната инфраструктура како важна компонента на националната безбедност на секоја држава бидејќи загрозувањето на таквите објекти/инфраструктури го доведува во прашање нормалниот тек на животот и безбедноста на граѓаните, но и општото функционирање на државата (Mikac, Cesarec&Larkin, 2018:23) или како збир на сите објекти, системи, мрежи и функции, витални за опстанокот на државата, чиешто уништување ќе влијае негативно врз безбедноста, националната безбедност, јавното здравје и др. (Dawson, Omar, 2015:97).

Според Мотеф и Парфомак (Moteff, Parfomak, 2004:5), критичната инфраструктура претставува базична физичка и организациска структура која му е потребна на општеството за да функционира. Од друга страна, во процесот

на целокупниот современ развој и доминантната автоматизација и дигитализација на сите сегменти во општествата, критичната инфраструктура претставува комплексен систем кој специфично е изложен и ранлив првенствено на природните закани, техничко-технолошките опасности и антропогените закани. Во овој контекст, Мотеф и Парфомак сметаат дека поимот „критична инфраструктура" треба да се прошири и тоа од она што е примарно за националната одбрана, економската безбедност до она што е од витално значење за јавното здравје, безбедноста и националниот морал.

Доколку овие системи се во ризик, односно во дефицит или пак се уништени, ќе настане импакт на економијата, психологијата и сигурноста на нацијата и општеството. (Levis, 2006:1). Ова може да се воочи во бројни дефиниции за „критична инфраструктура" во литературата, а нејзината заштита и потребата од јакнење на отпорноста на општеството станува предизвик и атрактивна тема за истражување. Но, најчесто сè се сведува на тоа дека инфраструктурата, системите и ресурсите се од витално значење за едно општество. Високата меѓузависност на овие системи со останатите системи од социјалниот живот, налага потреба да се обрне поголемо внимание на нивната заштита (Keković, Z., 2013:203). Токму можеби затоа, различни земји критичната инфраструктура ја дефинираат на различен начин. Да разгледаме некои од нив.

САД започна да го развива оваа подрачје во средината на 1990 година, а во 1998 година во Претседателската директива NSC-63 критичната инфраструктура ја дефинира како „физички и информатички системи нужни за минималното функционирање на стопанството и Владата". Непосредно по терористичкиот напад на Њујорк и Вашингтон на 11 септември 2001 година, Конгресот го донесе Патриотскиот закон (Patriot Act, 2001) во кој критичната инфраструктура се определува како „системи и средства, физички или виртуелни, од витално значење за државата, каде што нивното онеспособување или уништување ќе има негативен ефект врз националната, економската и социеталната безбедност, стабилноста на стопанството и др.". (Patriot Act, 2001). Како надополнување на ова е и аргументот дека со донесувањето на Патриотскиот закон активностите на САД за заштита на критичната инфраструктура се во тесна врска со одбраната од тероризмот.

Австралија е земја која заедно со САД го започнаа теоретскиот развој на областа критична инфраструктура. Австралија критичната инфраструктура ја дефинира како ,,физички капацитети, системи за снабдување, информатички технологии и комуникациски мрежи, кои, ако се уништени, онеспособени или ослабени на долго време, може значително да влијаат на социјалната или на економската благосостојба на народот, или да влијаат врз способноста на Австралија да ја одржи националната одбрана и да ја обезбеди националната безбедност (National Guidelines for Protection Critical infrastrukture from terrorism, 2011:3).

Во Велика Британија, во критична национална инфраструктура се вбројуваат средствата, услугите и системите кои го поддржуваат социјалниот, економскиот и политичкиот живот и нивното уништување може да предизвика жртви, да има влијание врз националната економија, социјални последици или пак, да биде приоритетна цел на Владата.

Во Германија, под поимот „критична инфраструктура се подразбира организациската структура и објектите од витално значење за општеството, така што нивната деградација или дефицит ќе резултира со недостатоци, ќе предизвика значително намалување во снабдувањето, нарушување на јавниот ред или други последици".

Во националната критична инфраструктура во Хрватска спаѓаат „системите, мрежите и објектите од национална важност, при што нивното престанување со работа или услуга може да има сериозни последици за националната безбедност".

Во Бугарија, пак, под критична инфраструктура се подразбира систем на објекти, услуги и информациски системи, чиешто откажување или пак, уништување ќе има негативно влијание врз безбедноста на луѓето, животната средина, економијата или на целокупното ефективно функционирање на Владата.

Во овој контекст, од особено значење се и неколкуте „институционализирани" обиди за дефинирање на критичната инфраструктура. Во еден од тие обиди, под покровителство на Европската унија, се наведува дека критичната инфраструктура претставува „систем или негов дел лоциран во земјата-членка, кој е од суштинско значење за виталните општествени функции, здравјето, безбедноста, економската и социјалната благосостојба и нивното оштетување или пак, нивното уништување би имало значителни последици во земјата-членка на ЕУ" (European Union Council Directive 2008).

Ваквото дефинирање е под силно влијание на терористичките напади на САД во 2001 година и глобалната војна против тероризмот која следеше по терористичкиот напад во Мадрид во 2004 година. Сите тие случувања доведоа до Иницијативата за усвојување на „комуникации за заштита на критичната инфраструктура во борба против тероризмот", во која се наведени предлозите што треба Европа да ги преземе во спречувањето на терористичките напади на критичната инфраструктура, на кој начин треба да се подигне нивната отпорност и да се развие способност за одговор на потенцијалните напади (Communication from Commission to the Council and the European Parliament-Critical Infrastructure Protection in the fight against terrorism, 2004).

Имајќи го предвид примерот од големиот терористички напад во Лондон во 2005 година, Комисијата иницираше и ја усвои Зелената книга за Европска програма за заштита на критичната инфраструктура, која посебно се фокусира на предлогот за воспоставување на програмата за заштита на критичната инфраструктура. Но, она што ја прави ова програма поактуелна, е нејзиниот предлог за формирање на информатичка мрежа за тревожење во случај на загрозување на критичната инфраструктура. (Green Paper on a European programme for critical infrastructure protection, 2005). Исто така, Комисијата во 2006 година усвои Европска програма за заштита на критичната инфраструктура од сите опасности, но фокус е ставен на тероризмот како примарна закана (Communication from the Commission on a European Programme for Critical Infrastructure Protection, 2006).

Следниот чекор на Европската унија кој заслужува внимание, а се однесува на заштитата на критичната инфраструктура, е донесувањето на Директивата

2008/114/ЕК за идентификација и одредување на европските критични инфраструктури и процена на потребата да се подобри нивната заштита. Според оваа Директива, „критичната инфраструктура значи имот, систем или дел од него кој се наоѓа во земјите-членки и е од суштинско значење за одржување на виталните општествени функции, здравјето, сигурноста, безбедноста, економската и општествената благосостојба на луѓето, а чие нарушување или уништување би имало значително влијание во една земја-членка како резултат на неуспехот да се одржат тие функции. „Европската критична инфраструктура означува критична инфраструктура која се наоѓа во земјите-членки, а чие нарушување или уништување би имало значително влијание на најмалку две земји-членки. Значењето на влијанието ќе биде оценето во однос на вкрстени критериуми. Ова ги вклучува ефектите кои произлегуваат од меѓусекторската зависност од други видови инфраструктура". (Council of the European Union (2008) *Directive on the identification and designation of Europe)*.

Во НАТО, пак, за критични се сметаат објекти, услуги и информациски системи кои се од витално значење за една нација, а нивното уништување може да ги загрози безбедноста, економијата, здравјето, односно генерално безбедноста на нацијата или да се попречи ефективното функционирање на државите (Bognar, B., 2009:552).

И на крај, можеме да извлечеме неколку заклучоци, и тоа: во академската средина се прават напори да се утврди една прифатлива дефиниција за критичната инфраструктура, но сè уште не постои универзално прифатена дефиниција за поимот критична инфраструктура. Критичната инфраструктура претставува имот, систем, средства, услуги и сл., кои се клучни за нормално функционирање на државата во поглед на економските, здравствените, социјалните и безбедносните потреби.

Различни национални власти имаат подготвено листа на стопански гранки кои се опфатени во наведените дефиниции. Конкретно, тие ги вклучуваат водата, храната, енергијата, транспортните средства, а приоритет се дава на аеродромите и железниците, финансиските институции, здравството и сл.

Владите на државите ѝ посветуваат сè поголемо внимание на критичната инфраструктура. Позитивен пример се американската влада, германската влада, владата на Велика Британија. Овие држави ја организираат критичната инфраструктура подеднакво на национално, на регионално и на локално ниво. Додека пак, слабо развиените држави, како на пр. Хрватска и Романија, со критичната инфраструктура се занимаваат исклучиво на национално ниво.

Оттука, можеме да извлечеме генерален заклучок дека силно е изразена потребата за контролирање и развивање на критичната инфраструктура. Притоа, акцентот треба да се стави на целта да се промовира институционален пристап, насочен кон креирање на стратегиска рамка за критичната инфраструктура.

1.2. Закани и ризици за критичната инфраструктура

Современите општества денес се соочуваат со голем број закани и ризици коишто ја надминуваат првобитната рамка на подготвеност и одговор кон истите и затоа е неопходно отпорноста и организираноста на општеството да се анализираат и во контекст на неговите статични и динамични карактеристики. Затоа е во право Аристотел кога тврди дека „Целото е повеќе отколку збирот на неговите делови". Ова можеме да го примениме и во контекст на отпорноста на општеството кон голем број закани и ризици, бидејќи самото општество претставува збир на повеќе посебни комплексни системи кои интерактивно се поврзани како систем (на пример инфраструктурата, здравството, енергетиката и др.). Имено, секој од овие засебни системи има свои карактеристики и динамики, но кога се интегрираат во општествениот систем, тогаш пренесуваат од своите и примаат од карактеристиките на другите системи. Со други зборови, суштината на општеството е неговата комплексност како систем изграден врз сложени внатрешни и надворешни односи и како систем кој постојано е во развој и прилагодување кон новата иднина. (Popovski, 2019: 45). Оттука, токму таа изменета слика може да се опише како ново безбедносно опкружување во кое заканите и ризиците сè повеќе произлегуваат и од невоената сфера на безбедноста и таквото безбедносно опкружување станува многу подинамично и понеизвесно, исполнето со предизвици и опасности кои ја наметнуваат потребата општествата да понудат сеопфатен одговор. За нашата анализа значајно е да се напомене дека драстичните промени во безбедносното опкружување, особено по завршувањето на Студената војна, предизвикани од енормната дистрибуција на закани и ризици предизвикаа промени во разбирањето и перцепирањето на заштитата и градење на отпорно општество. Всушност, според ова значајно е да се нагласат неколку прашања кои во одредена мерка влијаат врз управувањето со ризикот и во правецот на дебатите кои придонесоа да се искристализира она што денес се нарекува проширен и продлабочен пристап на идентификување на т.н. организации од висока доверливост (High Reliability Organizations) кои всушност претставуваат посебни системи кои се дел од општествениот систем, а кои имаат континуирана оперативност без грешки, дури и во време на околности кои се повеќеслојно турбулентни и опасни (Roberts, 1990) а кои може да се идентификуваат како систем за контрола на воздушниот сообраќај (Weick, 1990), здравствени институции (Chassin and Loeb, 2013), односно како дел од критичната инфраструктура. Затоа е важно да се потенцира дека во услови на глобализирано и меѓузависно општество безбедноста не е само атрибут на државата и резултат на динамиките на меѓународното безбедносно опкружување. Затоа е неопходно подготвеноста да биде разбрана во целата своја комплексност од превенција до заштита, од мултисекторски пристап во намалувањето на ризиците и заканите по критичната инфраструктура, па сè до индивидуална надлежност и одговорност на институциите, да ги обезбеди неопходните нормативни, институционални и оперативни услови за воспоставување на заштитата на критичната инфраструктура. Истражувањата докажуваат дека безбедноста е конструкција и последица на фактори кои дејствуваат на различити нивоа и влијаат врз не/сигурноста. Ова карактеристика му дава широчина, бидејќи во контекст на

класификација на заканите и ризиците конкретно за критичната инфраструктура особено е значаен придонесот на Богнар (2009), кој за разлика од минатото, наведува повеќе сектори како економија, и тоа со посебен акцент на банкарството и финансиите, транспортот (со посебен акцент на аеродромите и железниците), дистрибуцијата, енергетиката, здравството, комуникациите, комуналните услуги, снабдувањето со храна, како и клучните владини услуги. Анализата покажува дека некои од критичните елементи во наведените сектори не се конкретно „инфраструктура", туку се мрежа или пак, снабдувачки синџири директно поврзани со суштински производи и услуги. Токму затоа, се зголемуваат факторите кои им се заканuваат на различни елементи од инфраструктурата, затоа што критичната инфраструктура ги претставува мрежите, објектите и системите дистрибуирани во просторот, чиј континуитет во работата е под влијание на бројни природни, техничко-технолошки и антропогени фактори. Во одмос на аспектот на заштита, потребно е да се земат предвид најзначајните закани и ризици категоризирани во горенаведените групи. Од друга страна, посебно внимание треба да се посвети на зависноста и меѓузависноста на оперативноста на критичката инфраструктура која произлегува од ефектите на самата нејзина природа, структурата и деловните процеси кои влијаат на критичната инфраструктура. Затоа е важно да се потенцира дека разни области во светот имаат свои специфични природни закани и ризици кои се повторуваат, се во интеракција со други и претставуваат потенцијална и – или директна закана за критичната инфраструктура. Истражувањата докажуваат дека е потребно е да се набљудуваат и поединечни анализи и пресметки на трошоците за да се добие ситуациска слика на заканите и ризиците кои, покрај другите вредности, ги загрозуваат критичните инфраструктури. Затоа, во право е Микац (2017) кога тврди дека поради нејзината природна положба, областа на Југоисточна Европа е зона која е исклучително ранлива на природни закани како што се поплави, земјотреси и пожари. Во последните десет години, поплавите се најголемата закана. Од техничко-технолошките ризици потребно е да се споменат: катастрофи и големи несреќи во економски објекти; техничко-технолошки катастрофи и големи сообраќајни несреќи; нуклеарни опасности. И антропогените фактори се разликуваат на следниов начин: дела поврзани со тероризам, саботажа и криминал. Оттука, од особена важност е да се потенцираат емпириски докази, ќе бидат користени примери од регионот на Југоисточна Европа и повремено поширокиот контекст.

1.2.1. Природни закани и ризици за критичната инфраструктура

Во природни закани за критичната инфраструктура спаѓаат: поплави, пожари, земјотреси, суши, бури, топлотни бранови.

Обединетите нации во своето истражување наведуваат дека регионот на земјите-членки на Организацијата за безбедност и соработка во Европа е многу подложен на природни непогоди како што се земјотреси, поплави, суши, бури, топлотни бранови, шумски пожари. Ваквите закани влијаат на повеќе од 76 милиони луѓе во последните 25 години. Со анализа на прецизните податоци во периодот од 1990 до 2014 година, бурите (34%) и поплавите

(31%) се најчести природни непогоди. Според нив, поплавите (35%), бурите (29%) и сушите (19%) влијаат врз повеќето луѓе во наведената област, а со тоа и најголем број луѓе останале без своите домови, и тоа поради земјотресите (54%), поплавите (26%) и бурите (16%). Горенаведените настани во изминатите 25 години резултираа со смрт на 182.075 луѓе и економски загуби од над трилион американски долари. (United Nations Development Programme, 2014:8) Специјален претставник на генералниот секретар на ООН за намалување на ризиците од катастрофи, ***Маргарета Валстром*** идентификува дека според проценатa, глобалните годишни економски загуби предизвикани од природни непогоди се поголеми од 100 милијарди УСД и трендовите покажуваат дека тие ќе продолжат да растат. Според ***Кристијан Фриз Бах,*** генерален секретар на ООН на Економската комисија за Европа, во изминатите 10 години загубите предизвикани од природни катастрофи изнесуваат 100 милијарди евра во Европска унија. Тука би можело да се вбројат и природните катастрофи во Европската унија меѓу 2002 и 2014 година кои предизвикале повеќе од 80 илјади смртни случаи и повеќе од 100 милијарди евра економски штети (European Commission, 2014:1). Помеѓу бројните големи природни катастрофи, статистички, поплавите го претставуваат феноменот кој многу често и кумулативно предизвикува голема штета, економски и човечки зауби, значителни безбедносни и здравствени предизвици, бројни последици за луѓето, економијата, критичната инфраструктура, услужниот сектор, животната средина и историското наследство (Mitrevska M., Mikac R., 2017:28), Анализите на извештајот на Европската агенција за животна средина, за периодот од 1998 до 2009 година укажуваат на фактот дека биле пријавени 213 поплави во Европа, кои предизвикале 1126 смртни случаи и економски загуби од повеќе од 52 милијарди евра. (European Environment Agency, 2011) Некои области во Европа се повеќе подложни на поплави отколку други, така на пример во изминатите неколку години поплавите доминираа во областа на Централна и Југоисточна Европа. Во таа смисла, анализата укажува дека во последните десетина години се забележува историскиот максимум на водата во големите европски реки како што се Дунав, Тиса, Драва, Мура, Сава и други реки и нивните притоки. Особено е важно да се знае дека поплавите предизвикаа пробивање на повеќе насипи, поплавување на голема заштитена област, човечки жртви и масовно оштетување на имот во десетици држави. Следен податок на Европската комисија кој заслужува внимание е 100-годишната поплава во Централна Европа во 2013 година, односно поплавата со веројатност да се случи еднаш на сто години, а се случува по втор пат за само 13 години. (European Commission, 2014:1) Во овој контекст може да се очекува дека ќе се појават поинтензивни и почести поплави како резултат на ефектите од климатските промени и постојаната деградација на животната средина (European Commission ,2014 *The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience)*. Конкретно, слична ситуација се случи во Југоисточна Европа, каде што најзначајните последици се манифестираа во 2014 година, односно во поплавите во мај, кои беа такви што се појавуваат еднаш на секои 1000 години, а најтешко беа погодени бројни области во Босна и Херцеговина, Србија и Хрватска. Во сите три држави загинаа 53 лица. Во Босна и Херцеговина повеќе од 1,5 милиони луѓе

беа погодени од поплавите, а повеќе од 90 илјади мораа да ги напуштат своите домови. Во Србија, над 1,6 милиони луѓе беа погодени од поплавите, а 31 илјада беа евакуирани. Во Хрватска поплавите загрозија 38 илјади луѓе (United Nations Development Programme (2014)). Од аспект на критичната инфраструктура, наведените поплави предизвикаа многу проблеми во функционирањето на системот за водоснабдување, транспортот и преработувачкиот сектор, земјоделството, образованието и здравствениот систем. Некои поплавени области ги исцрпија локалните, регионалните, па дури и индивидуалните државни капацитети и ресурси и државите добија меѓународна помош (Mitrevska M., Mikac R., 2017:32).

Во овој контекст, од големо значење е да се анализира и областа на Југоисточна Европа, како дел од медитеранско-транзициониот појас, која се одликува со изразена сеизмичка активност. Во таа смисла, ова особено важи за крајбрежните области и делови од внатрешноста кои биле погодени од катастрофални земјотреси. Примери, кои често пати се аналитички експлоатирани, се однесуваат на неколку многу силни земјотреси кои ја означуваат оваа област и тоа земјотресот кој се случи во 1667 година, со интензитет од 10 степени според Меркали-Канкани-Сиберг (МКС) скалата, кога Дубровник беше речиси целосно уништен, а загинаа повеќе од 3000 луѓе (Government of the Republic of Croatia, 2009), во Скопје во 1963 година, уништи 75 до 80 проценти од градот и предизвика повеќе од 1000 смртни случаи, повеќе од 3000 лица беа повредени, а помеѓу 120.000 и 200.000 луѓе останаа без нивните домови. Земјотресот во Црна Гора во 1979 година, освен во црногорската област, предизвика жртви и материјална штета и во Хрватска и Албанија. Во земјотресот, 101 лице загина во Црна Гора, 35 во Албанија, а повеќе од 100 илјади луѓе останаа без својот дом. Сите овие примери, од аспект на критичната инфраструктура, значат нанесена значајна штета, забележана на бројни објекти, мрежи и системи на локалната и државната инфраструктура. Исто така, големи штети беа причинети во образовните, културните, здравствените, социјалните и објектите на јавната администрација, во економијата, дури и до степен одредени бизниси целосно да престанат со нивните активности.

Пожарите од различен вид претставуваат потенцијална опасност за сите нивоа и облици на општеството, бидејќи потенцијално загрозуваат голем број на луѓе, средства во сите видови на објекти, во различни начини на транспорт, во тунели, во технолошки капацитети и инфраструктури кои складираат опасни стоки. Тука би можеле да се вбројат пожарите на отворен простор кои се случија во последните десет години во областа на Југоисточна Европа и тоа во Босна и Херцеговина, во Србија, во Северна Македонија и во внатрешноста на Грција.

Пожарите предизвикуваат значителна директна и индиректна штета, а нивното гаснење понекогаш бара ангажирање на големи материјални, технички и човечки ресурси на домицилните држави, прекугранична соработка и помош, како и активирање на механизмот на цивилна заштита на Европската унија за да се обезбеди потребниот човечки и материјален капацитет за тие да се изгаснат. Пожарите имаат директни последици за одредени сектори на критичната инфраструктура како што се: енергија (производство, вклучувајќи

акумулации и брани, пренос, складирање, енергија и енергетски транспорт, дистрибутивни системи), сообраќај (патен, железнички, воздушен, поморски и речен) и јавни услуги (обезбедување јавен ред и мир, систем на цивилна заштита, итна медицинска помош). Секако, постојат индиректни последици и за други сектори на критичната инфраструктура (Mitrevska M., Mikac R., (2017:34).

1.2.2. Техничко-технолошки опасности за критичната инфраструктура

Заканите од техничко-технолошка природа можат да бидат предизвикани од знаење или незнаење, ненамерна човечка грешка или пак, од технолошка грешка. Во нив спаѓаат: сообраќајни несреќи, катастрофи, нуклеарни експлозии, ослободување на биолошки агенси кои можат да предизвикаат масовни инфекции, пандемии, болести и да влијаат врз голем број критичен персонал. (Bognar, 2009:500). Од исклучително значење е да се сфати дека**,** меѓу другото, големите техничко-технолошки несреќи и катастрофи со сериозни последици за луѓето, материјалните и културните добра, како и за критичната инфраструктура. Имено, тие можат да настанат поради бројни причини, но и како домино-ефект после првичните несреќи. Од теориска гледна точка, најопштата класификација на големите техничко-технолошки несреќи и катастрофи ја покажува целата ширина на потенцијалните сценарија за загрозување на вредностите кои треба да се заштитат. Гореспоменатите се поделени на: техничко-технолошки катастрофи и големи несреќи во економски објекти; техничко-технолошки катастрофи и големи сообраќајни несреќи; нуклеарен ризик. Конкретно, од собраните информации производството и складирањето на опасни материи во бројни постројки и складишта е постојан ризик од индустриски несреќи со катастрофални последици. На глобално ниво, постојат два познати примери кои го одбележаа овој домен: големата катастрофа во Севесо во 1976 година и катастрофата во Бопал во 1984 година. Градот Севесо во северниот дел на Италија беше местото на една од најголемите хемиски несреќи во историјата на човештвото. Голема количина на диоксин била ослободена од хемиски објект заради технолошки дефект. Околу 2000 луѓе добиле медицинска помош, повеќе од 80 илјади животни биле еутаназирани за да се спречат потенцијално штетните последици по луѓето, околу 1800 хектари почва била контаминирана и во месеците по несреќата во регионот бил пријавен зголемен број на спонтани абортуси. Најголемата хемиска катастрофа се случи во индискиот град Бопал кога голема количина на хемикалии протекла од фабриката за пестициди поради технолошки дефект. Последиците биле ужасни. Повеќе од 25.000 луѓе загинале, а повеќе од 150.000 луѓе се здобиле со сериозни болести и до денес во таа област се раѓаат деца со тешки физички и ментални пречки почесто отколку каде било на друго место. Несреќата во Севесо ја натера Европската унија да ги зајакне деловните прописи и контролата на хемиските постројки. Ова беше направено преку Директивата Севесо[1] којашто обезбедува систематска контрола и следење на потенцијалните

1 Првата Директива наречена Севесо I беше усвоена во 1982 година. Севесо II беше усвоена во 1996 и ја вклучи и катастрофата во Бопал. Додека Севесо III беше усвоена во 2012 година. Секоја нова директива ја заменуваше претходната и дополнително ги заоструваше прописите за работа на хемиските постројки, кои моментално се над 10.000 во Европската унија.

извори на опасност од хемиско загадување и штетни ефекти врз животната средина и луѓето, што е исто така транспарентно за општата јавност[2]. Специфичноста на овој пристап во врска со разгледувањето на аспектот на заштитата на критичната инфраструктура е во тоа што ние имаме потреба за колку што е можно поголема транспарентност и јавно достапни индикатори за сите процеси во хемиските постројки, додека од друга страна, концептот за заштита на критичната инфраструктура бара одредено ниво на доверливост на податоците за структурата и процесот. Кога законодавецот во исто време ќе одреди една постројка задолжително да ја примени Директивата Севесо и ќе ја назначи постројката како објект на национална критична инфраструктура, постројката се соочува со предизвици во процесот на исполнување на двете обврски, при што ниту една не е едноставна, а примената е делумен судир во принципите на акција. (Mitrevska, Mikac 2017:36).

Искуството покажува дека техничко-технолошки катастрофи и големи сообраќајни несреќи (патни, железнички, воздушни, поморски и речни) можат да се појават поради бројните процеси кои што се случуваат при транспортот на опасните материи. Како можни причини за опасност од неочекувани настани се истакнуваат: несоодветно ракување на возила во транспортот; непрецизиран товар; дефектни делови за транспорт; невнимание, занемарување или небрежност при работа или несоодветно ракување; недостаток на контрола на процесот; штета предизвикана од механички удари; дефект на уреди или грешки при повлекување и полнење на садот; пожари во објектите, човечки намерни активности за предизвикување несреќи. (Benjamin K. Sovacool ,2010:369-400)

1.2.3. Антропогени закани и ризици за критичната инфраструктура

Како антропогени закани и ризици за критичната инфраструктура се сметаат дела поврзани со тероризам, злоупотреба за политичка корист, злоупотреба за економска корист, поттикнување на вооружени конфликти, немири и протести, саботажа и криминал насочени кон функционирањето на целата или некои делови на критичната инфраструктура.

Критичната инфраструктура претставува огромен, глобален сектор и не е можно да се обезбеди нејзина целосна заштита во секое време и на сите места. Оттука, веројатно е дека некои терористички напади врз критичната инфраструктура ќе успеат. Терористите имаат цел да шират страв, вознемиреност и паника, создавајќи перцепција дека секој граѓанин и главен јазол во инфраструктурата на земјата се подложни на напад. Примери за ова има многу, на пример случајот на 22 март 2016 година, кога два тима на оперативци на ИСИЛ

2 За повеќе информации види: The **Council** of the European Communities (1982) ***Council Directive 82/501/EEC of 24 June 1982 on the major-accident hazards of certain industrial activities,*** http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1982:230:FULL&from=EN***;*** The **Council** of the European Union (1996) ***Council Directive*** *96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01996L0082-20120813&from=EN; The European Parliament and the Council (2012) ***Directive 2012/18/EU*** *of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC,* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018&from=EN, (цитирано 23 април 2019).

извршија симултани напади во Брисел на аеродромот „Завентем" (убиени 11 лица) и во метрото „Мајлбег" (убиени 20 лица). Околу 300 луѓе беа повредени (United Nations Security Council Counter-Terrorism Committee, 2017:3-4). „Ал каеда" и нејзините приврзаници нападнаа објекти и персонал на нафтени компании во Алжир, Ирак, Кувајт, Пакистан, Саудиска Арабија и Јемен, а исто така заробија многу нафтени полиња. ООН проценува дека приходот генериран од ИСИЛ од нафта и нафтени производи во 2015 година бил помеѓу 400 и 500 милиони долари (United Nations Security Council ,2016). Иако некои автори забележуваат дека енергијата привлекува само мал дел на терористички напади, трендот покажува брз раст на интерес на терористите за нафта и гас (Brookings Doha Center Analysis (2016). Според бројни студии, повеќе напади во светот се насочени кон критичните инфраструктури (Mitrevska, Mikac, 2017:37).

Како што нагласуваат истражувачите на критичната инфраструктура, следната важна антрополошка закана е чинот на саботажа, што е гранична појава помеѓу терористички акт и кривично дело. Според нив, рангирањето на овие напади најчесто се насочени кон инфраструктури како што се производството на енергија и преносните системи, мрежите за снабдување со храна и вода, телекомуникациските мрежи, транспортните мрежи итн. Имено, во континуитет се потврдува дека методите за извршување на такви дејства можат да бидат подметнување пожар, предизвикување експлозии, употреба на оружје за масовно уништување до најчести форми на напад, разни сајбер-напади. Но подеднакво е важно да се има предвид дека непријателските сајбер-напади доаѓаат и во државна и во недржавна варијанта, а како можни се странски разузнавачки агенции, терористи, погрешни активисти или едноставно поединци кои дејствуваат сами. Сепак, како што технологиите се развиваат и стануваат покомплексни исто така тоа се случува и со предизвиците за откривање и заштита од сајбер-напади. Има бројни показатели кои укажуваат дека главните цели се високотехнолошките индустрии, вклучувајќи го и телекомуникацискиот сектор, индустријата за нафта и гас и други елементи од секторот за природни ресурси, приватниот сектор, како и универзитетите кои се вклучени во истражување и развој. Исто така, познато е дека државните актери користат сајбер-напади за да ја нарушат политичката и економската активност како средство за влијание врз владините носители на одлуки. Закани од сајбер-шпионажа, сајбер-саботажа и други сајбер-операции се дел од една поширока економска закана за клучните сектори на критичната инфраструктура (Canadian Security Intelligence Service, 2017). Криминалните активности кон критичната инфраструктура пак, се делат на внатрешни и надворешни. Внатрешните закани се дел од секоја организација и најчесто се случува кога доверлив вработен ги издава неговите обврски и лојалност кон работодавецот вршејќи саботажа или шпионажа против нив. Конкретно, како „внатрешни предавства" можат да бидат кражби како суптилни форми на саботажа или поагресивни дејства како насилство на работното место. Заканата што ја претставуваат инсајдерите е термин кој најчесто се користи во случај на злоупотреба на ИТ мрежата. Ова често доведува до понатамошна конфузија во врска со природата и сериозноста на заканата (Thomas Noonnan and Edmund Archuleta (2008). Надворешните закани претставуваат разновидни обиди за инфилтри-

рање во системот, било физички или преку интернет, а мотивот може да биде различен, во зависност од мотивацијата на напаѓачот. Конкретно, физичките упади претставуваат обид за отуѓување на дел од опрема или добивање важни информации директно преку соработка со вработените во компанијата или со одреден вид измама или изнуда, со инвазии да се нападне сајбер-просторот. Оттука, такви напади на критичната инфраструктура се случуваат секој ден на глобално ниво и за жал нивниот тренд постојано се зголемува. Токму затоа се тврди дека, сајбер-просторот и критичната инфраструктура станаа неразделни, безбедносните предизвици се појавуваат исто како и размислувањата на кој начин е најдобро да се заштитат виталните делови на критичната инфраструктура од надворешен упад. Со оваа силна корелација помеѓу интернетот и критичните инфраструктури се доаѓа по цена на зголемена комплексност и како последица на тоа, зголемен ризик на случајни грешки.

1.3. Потреба од заштита на критичната инфраструктура

Во современи услови, сфаќањето и примената на заштитата на критичната инфраструктура е под силно влијание на повеќе фактори, и тоа сложеноста на критичната инфраструктура, регулативата за надлежности, недостатокот на одговорност во секторите, каде пред сè се ангажирани повеќе државни и приватни институции, недоволна размена на информации, пред сè помеѓу институциите, што пак, од друга страна, ја зголемува ранливоста и директно влијае на ефикасниот пристап во заштитата на критичната инфраструктура, квантумот на знаење и вештини во однос на заштита на критичната инфраструктура и меѓузависноста на секторите од критичната инфраструктура и др. (Prezelj., I., 2008:13). Токму затоа, авторите заклучуваат дека заштитата на критичната инфраструктура е многу широка и динамична активност и се остварува по два различити начини. Првиот ги извршуваат јавни тела, како што се различни законодавни институции, агенции за спроведување на законот, инспекциски и судски органи и организации за приватна безбедност. Вторите се активности што ги извршуваат меѓународни тела како што се Европската унија и НАТО. Други теоретичари, на сличен начин, аргументираат дека секој случај е посебен, па затоа е неопходно да се посвети посебно внимание и да се согледа фактот дека многу актери учествуваат во заштитата на критичната инфраструктура и тоа во различни фази и процеси. Застапникот на ова теза Микац, смета дека за да се илустрира степенот на дискусија по ова прашање, потребно е да се наведат примери за критичната инфраструктура: 1. енергетски сектор – национално значајни рафинерии за нафта и гас; 2. транспортен сектор – најголемите аеродроми; 3. информациско-комуникацискиот сектор – најважните бази на податоци на секоја земја; 4. економски сектор – системите на националната централна банка; 5. здравствен сектор – клинички болнички центри; 6. прехранбен сектор – силоси за складирање на жито; 7. сектор за водостопанство – водоцрпилишта; 8. сектор за производство, складирање и транспорт на опасни материи – интегриран систем за следење и контрола на транспорт на опасни материи; 9. јавни услуги – итна медицинска помош; 10. сектор за туризам – национални споменици кои се причината за доаѓањето

на голем број туристи (Mitrevska M., Mikac R., 2017: 35). Оттука, заеднички став е дека е очигледно дека критичната инфраструктура е многу разновидна и е претставена во мрежи, објекти и системи кои не се секогаш физички видливи, туку се состојат од многу компоненти и меѓузависности, најчесто во веб-светот. Причините за ова се различити. Ние можеме да го посочиме примерот со зградата на Народната банка, која како зграда, сама по себе, не е критична инфраструктура, но, структурите и процесите кои се одвиваат во зградата се. Од тие причини, ние повторно правиме дополнително расчленување и мора да определиме кои процеси се незаменливи, дали постои алтернатива за нивно дејствување и што ќе се случи ако тие престанат или привремено престанат да работат. Исто така, во настојување да се елаборира потребата од заштита на критичната инфраструктура, треба да се има предвид дека тие се комплексни системи за кои е потребен холистички пристап во разгледувањето на нивното функционирање, со акцент на изворите на нивните внатрешни и надворешни закани, значењето за самиот сектор и зависноста и меѓузависноста со други сектори и критични инфраструктури, зајакнување на нивниот отпор и нивна заштита.

Во однос на описот на состојбата и она што треба да се прави, постои основна позиција според која целокупната заштита на државата и општеството од аспект на зачувување на функционирањето на критичната инфраструктура мора да се заснова на „пакетот за заштита" на сите инфраструктури, како и на секој поединец. Ваквиот пристап, на прв поглед наведува на заклучокот дека секоја инфраструктура и целата земја ќе бидат најдобро заштитени ако се преиначат патиштата за снабдување и испораката, колку што е можно, да се создадат и зајакнат алтернативи за критичната инфраструктура и да се зајакне нивната отпорност. Всушност, таквите објекти ќе бидат заштитени ако се изградат во области каде што постои најмал ризик од поплави, пожари и земјотреси. Ако на тоа се надоврзе изградбата според правилата на професијата и со користење на квалитетни материјали, почитувајќи ги сите стандарди за градба и одржување, тогаш е јасно зошто пакетот на заштита ќе биде поефикасен и поефективен. Но подеднакво е важен и следниот чекор и тоа да се креира комплетна придружна документација и познавање на процесите за да се избегнат застои и домино-ефекти. Сепак, треба да се има предвид генералниот впечаток дека постои и отпор на самиот систем, неговата робустност и висока функционалност. Анализата на прашањето дали остварувањето на заштитата на критичната инфраструктура низ призма на сите потребни процени, анализи и планови кои се бараат со други закони, од кои зависат националните закони кои се директно поврзани со прашањето на критичната инфраструктура се само надградба на сè што е претходно направено. Анализата на потребата од заштита на критичната инфраструктура е добар пример за да се укаже дека постои цел спектар на потребни и претходно преземени активности преку кои со структурни мерки може да се избегне и намали ранливоста на критичната инфраструктура. Конкретно, има бројни показатели кои укажуваат дека станува збор за многу широк спектар на работни места и области на одговорност, со јасно определување на институции, со јасно утврдени програми и процедури за работа компетентни за заштита на критичната инфраструктура.

1.3.1. Организација на заштитата на критичната инфраструктура

Во теоријата и практиката доминира ставот дека пристапот кон заштитата на критичната инфраструктура треба првенствено да се заснова на анализа на ризик, притоа јасно да се прецизира кои ризици го загрозуваат работењето на критичната инфраструктура и како да се одговори на нив. Некои автори предлагаат анализата на ризикот да се однесува на процесите кои се користат за процена на тие веројатности и последици, како и за проучување на тоа како да се инкорпорираат добиените процени во процесот на донесување одлуки. Вториот предлог е процесот на процена на ризикот, да служи како алатка за донесување одлуки, со тоа што неговите резултати ќе се користат за обезбедување насоки за областите со најголем ризик и за изготвување на политики и планови за да се осигура дека системите се соодветно заштитени. (Myriam, 2006:2)

Слично внимание на овој организациски пристап кон имплементацијата на заштитата на критичната инфраструктура се посветува и во Европската унија и во земјите кои се стремат кон полноправно членство (како што е случајот со Република Северна Македонија) и тоа е имплементирано во *Директивата 2008/114/ЕК за идентификација и утврдување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита* (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection). Така, во Воведот на Директивата јасно се укажува дека примарната и клучната одговорност за заштита на европските критични инфраструктури е кај земјите-членки и сопствениците/операторите на таквите инфраструктури (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 6). Овој принцип, исто така важи и за заштитата на националната критична инфраструктура. Додека пак, од аспект на соработка помеѓу јавниот и приватниот сектор важна е одредбата од Воведот на Директивата каде е наведено како вклучувањето на приватниот сектор во надгледувањето и управувањето со ризиците, планирањето на континуитетот во работењето и закрепнувањето после катастрофа, пристапот на заедницата, треба да поттикне целосно вклучување на приватниот сектор (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 8). Сепак, како што добро забележуваат некои автори, Директивата наведува дека во организирањето на заштитата на критичната инфраструктура е неопходно да постојат три важни компоненти: да се направат оперативни безбедносни планови; да се назначат офицери за врска за безбедност и да се номинираат точки за контакт за заштита на критичната инфраструктура. Во сите назначени критични инфраструктури треба да бидат поставени оперативни безбедносни планови или еквивалентни мерки кои опфаќаат идентификација на важни средства, процена на ризикот и идентификација, селекција и приоретизација на контрамерките и процедурите. Со цел да се избегне непотребната работа и дуплирање, секоја земја-членка прво треба да процени дали сопствениците/операторите на назначените критични инфраструктури поседуваат ре-

левантни оперативни безбедносни планови или слични мерки. Онаму каде што не постојат такви планови, секоја земја-членка треба да ги преземе неопходните чекори за да се осигура дека се преземени соодветни мерки. Секоја земја-членка треба да одлучи за најсоодветната форма на дејствување во врска со воспоставувањето на оперативни безбедносни планови (Council of the European Union, *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, paragraph 11). За да се олесни соработката и комуникацијата со релевантните национални органи за заштита на критичната инфраструктура, треба да бидат идентификувани офицери за врска за безбедност за сите назначени критични инфраструктури. Со цел да се избегне непотребната работа и дуплирање, секоја земја-членка прво треба да процени дали сопствениците/операторите на назначените критични инфраструктури веќе имаат офицер за врска за безбедност или еквивалент. Онаму каде што не постои таков офицер за врска за безбедност, секоја земја-членка треба да ги преземе неопходните чекори за да биде сигурна дека се преземени соодветни мерки. Секоја земја-членка треба да одлучи за најсоодветната форма на дејствување во однос на назначувањето на офицери за врски за безбедност (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 13).

Ефикасната заштита на критичните инфраструктури бара комуникација, координација и соработка на национално ниво. Ова најдобро се постигнува преку номинирање на точки за контакт за заштита на критичната инфраструктура во секоја земја-членка, кои внатрешно треба да ги координираат прашањата за заштита на критичната инфраструктура, како и со други земји-членки и Комисијата (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 17). Потоа следува процес на непосредна имплементација на заштитата на критичната инфраструктура во три чекори: 1. идентификација; 2. утврдување; 3. заштита. Идентификацијата на потенцијалната критична инфраструктура ја вршат секторските носители (надлежни министерства) во соработка со регулаторни агенции. Еднаш кога овие заинтересирани страни ќе ја идентификуваат потенцијалната критична инфраструктура во рамките на нивниот сектор, тие ја составуваат листата и ја доставуваат до владата за потврда. Во следниот чекор, владата ги разгледува предложените листи на потенцијални критични инфраструктури и со одлука одредува индивидуална критична инфраструктура или сите предложени. Таа одлука потоа се доставува до сопственикот или менаџерот на критичната инфраструктура и до релевантното министерство или регулаторни агенции. По приемот на одлуката, сите горенаведени актери се должни да комуницираат и да соработуваат едни со други. Првото ниво на соработка е да се види дали постои оперативен безбедносен план и дали е тој соодветен за нивото на заштита на критичната инфраструктура. Исто така е неопходно да се назначат и заемно да се поврзат офицери за врска за безбедност кои ќе вршат предметни задачи помеѓу релевантното министерство, критичната инфраструктура, регулаторните агенции, а и ќе соработуваат со другите засегнати страни во

овој процес и системот за заштита на критичната инфраструктура. Што се однесува до чекорите за заштита, ова се прави во согласност со оперативниот безбедносен план, кој мора да се постави според четирите основни принципи на управување со кризи: превенција, подготвеност, реакција и закрепнување. Споменатиот план мора да ја оцени анализата на деловниот ризик на критичната инфраструктура, нејзините закани, силата за одговор, соработката со надлежните институции, имплементацијата на мерките за заштита, сценариото за можен и најлош можен настан или повеќе такви настани кои може да се случат во критичната инфраструктура. Освен тоа, тој мора да содржи план за комуникација како и адресар на најважните контакти.

Во рамките на системот за заштита на критичната инфраструктура секоја земја самостојно ја одредува организацијата и спроведувањето на сите процеси, како и нивото на вклучени актери. Не постои универзална форма која треба да се следи при воспоставувањето на системот, но постојат одредени принципи кои беа наведени погоре, а кои треба да се почитуваат за да биде системот поефикасен, поекономичен и самоодржлив (Mitrevska, Mikac 2017:42).

1.3.2. Институции кои се компетентни за заштита на критичната инфраструктура

Издиференцирани се два основни пристапи кон ориентацијата на нивото на утврдување на критичната инфраструктура. Првиот пристап се однесува на територијално помалите држави каде што критичната инфраструктура е утврдена само на национално ниво и системот е поедноставен за координација бидејќи релевантните тела на единиците на регионална и локална самоуправа не се вклучени во процесите. Додека пак, вториот пристап е претставен од поголемите земји каде што критичната инфраструктура е утврдена на национално, на регионално и на локално ниво.

Од анализа на институциите кои се компетентни за заштита на критичната инфраструктура ја издвојуваме улогата на Владата на секоја држава, која треба да е вклучена во системот на заштита на критичната инфраструктура и тоа од неколку причини. Прво, Владата е предлагач на закони и подзаконски акти. Второ, таа има можност да им даде овластување на одредени министерства и/или централни владини тела да бидат координатори на целиот систем и носители на секторските процеси. Трето, Владата обезбедува стратегиска рамка која е од суштинско значење за успешно функционирање на системот, соработката, комуникацијата и координацијата на сите вклучени актери. Четврто, Владата има ингеренции да ги одреди секторите од кои централните владини тела идентификуваат одредени критични инфраструктури со цел да обезбедат холистички пристап за заштита и намалување на негативните влијанија во случај на закана за критичната инфраструктура.

Како следен важен актер кој е компетентен за заштита на критичната инфраструктура ја издвојуваме улогата на *координаторот* на целиот систем за заштита на критичната инфраструктура. Постојат различни примери и практики за тоа кое тело е соодветно за оваа улога, на пример во САД оваа функција ја врши Министерството за внатрешна безбедност. Додека пак, во повеќето

европски земји функцијата е доделена на Министерството за внатрешни работи. Но постојат примери, како оној на Република Словенија, каде Министерството за одбрана ја има таа должност или пак, Република Хрватска, каде таа е доделена на Дирекцијата за национална заштита и спасување (независно тело на централно државно ниво под министерствата). Улогата на координаторот на системот е да комуницира директно со сите актери на системот, со меѓународните актери, да доставува извештаи до Владата и најчесто ја претставува својата земја на координативните состаноци организирани од Европската комисија. Споменатата институција, во соработка со надлежните централни органи на државната администрација од чиј опсег е индивидуалната критична инфраструктура, постојано ги надгледува и ги проценува заканите и предлага оперативни и други мерки за процена на критичноста и потребата од предложените мерки за управување и заштита на критичната инфраструктура.

Следниот важен актер кој е компетентен за заштита на критичната инфраструктура е во рамките на *централните органи на државната управа* назначени од владата, најчесто релевантните министерства кои се одговорни за имплементацијата на секторските политики. Овие институции во соработка со надлежните регулаторни агенции се одговорни во рамките на нивниот опсег за идентификување (утврдување) на посебни системи или нивните компоненти како критични инфраструктури, обезбедувајќи управување со критичната инфраструктура и нејзина заштита. Како пример ќе го земеме енергетскиот сектор. Надлежна институција е претежно Министерството за економија (или Министерството за енергетика во некои земји), кое обезбедува секторски политики за развојот на релевантниот сектор, соработува, комуницира и се грижи за бизнисот на сите актери на пазарот, врши надзорно надгледување, посветувајќи посебно внимание на областите на секторската критична инфраструктура и нивната секторска зависност и меѓузависност со други критични инфраструктури од други сектори. Постои претпоставка, што зависи од развојот на државата, дека сите сектори немаат воспоставено регулаторни агенции. Меѓутоа, бидејќи енергетскиот сектор е еден од најважните сектори на критичната инфраструктура, сите држави имаат воспоставено енергетски регулаторни агенции. Овие агенции имаат јавен авторитет и нивните активности се: издавање, продолжување и пренесување на дозволи за вршење на енергетски дејности и привремено и трајно одземање на дозволи; надзор на енергетските субјекти во вршење на енергетските дејности; надгледување на управувањето со деловните книги; надгледување на принципот на транспарентност, објективност и непристрасност во работата на операторите на енергетскиот пазар; издавање на одлука за стекнување на статус на квалификуван производител на енергија и одземање на наведеното решение; издавање или одобрување на цените на енергијата; соработка со меѓународни регулаторни агенции итн. Идентификација на критичноста на инфраструктурата, по правило, се прави за секој систем, мрежа и инфраструктурен објект во рамките на надлежноста на централното тело на државната управа, во кое соработуваат релевантното министерство и регулаторната агенција (или повеќе од нив доколку се присутни во конкретниот сектор). Критериуми за процена на критичноста на инфраструктурата можат да бидат: животот и здравјето – одреду-

вање на влијанието на нарушувањето и/или прекинот на работа врз животот и здравјето; временската рамка – во случај на нарушување/прекин на работата ќе се утврди за колку време тоа нарушување/прекин на работата ќе има последици врз вкупниот бизнис/испорака на услуги (за пократко време, поголема критичност); опсегот – одредува колку вкупниот производ и/или услуга ќе биде погоден во случај на нарушување или целосно прекинување на работата; правно, регулаторно и договорно значење; економска/финансиска штета. (Митревска, Микац, 2017: 43).

Потоа следниот актер е *сопственикот или менаџерот* на критичната инфраструктура. Тие се директно одговорни за управување и заштита на критичната инфраструктура во сите услови. Тие треба да направат анализа на ризикот како основа за создавање на оперативен безбедносен план. При развивањето на анализите на ризик, тие соработуваат со централните органи на државната управа, чиј опсег е критичната инфраструктура, надлежните регулаторни агенции и централниот орган на државната управа, кој е координатор на целокупниот систем. Оперативниот безбедносен план исто така ги идентификува оние субјекти кои се одговорни за заштита на критичната инфраструктура во сите фази и исто така, заедно со агенциите за спроведување на законот, има голема улога за компаниите кои обезбедуваат приватна безбедност. Предизвикот што е присутен насекаде во светот е да се обезбеди размена на информации, посебно на оние кои се чувствителни, па сопствениците/менаџерите може да имаат сознание за тоа дали тие се загрозени. Самата Директива 2008/114/ЕК го препознава гореспоменатото и одредува дека сопствениците/операторите на критичната инфраструктура треба да добијат пристап до најдобрите практики и методи поврзани со заштитата на критичната инфраструктура, првенствено преку релевантните тела на земјите-членки и дека размената на информации треба да се одвива во услови на доверба и безбедност. Размената на информации бара доверлив однос во кој компаниите и организациите знаат дека нивните чувствителни и доверливи податоци ќе бидат доволно заштитени. Ова е најсложениот дел од аранжманот за заштита на критичната инфраструктура и индикатор за општиот развој на општеството и државата (Mikac, 2017:44).

1.3.3. Заштита на критичната инфраструктура преку јавно-приватно партнерство

Теоретичарите на критичната инфраструктура се согласуваат дека при заштита на критичната инфраструктура посебно место треба да имаат јавниот и приватниот сектор. Но, некои автори внесуваат и дополнителни аргументи и тоа тргнувајќи од дефиницијата дека јавно-приватното партнерство е заедничка иницијатива на јавниот и приватниот сектор каде секој субјект придонесува за специфичните ресурси на системот и учествува во планирањето и донесувањето одлуки (White House 1998). Конкретно, првиот аргумент укажува дека е потребно системите на јавно-приватно партнерство да се стремат на полето на јакнење на отпорноста и заштитата на критичната инфраструктура. Вториот аргумент укажува дека со зголемена свест за важноста на заштитата на критичната инфраструктура за секојдневно функционирање на сите субјекти, националната безбедност и меѓународната соработка, како и размената на

знаење, искуства и најдобри практики помеѓу приватниот и јавниот сектор, директно се влијае врз зголемувањето на отпорноста и заштитата на системот на критичната инфраструктура.

Аналитичарите укажуваат дека во практиката создавањето соодветен систем за заштита на критичната инфраструктура е многу тешка задача за која било земја и тоа во кој било степен на развој. Општиот заклучок е дека заканите стануваат посложени и го загрозуваат функционирањето на инфраструктурите, што е голем предизвик за државата. Но, како што ќе видиме во елаборацијата на другите глави преку примерите на Хрватска и САД, станува евидентно дека секоја земја има свој пристап кон заштитата на критичната инфраструктура, во зависност од степенот на приватна сопственост во компаниите, стабилноста на државната структура и минатите искуства. Општиот заклучок е дека ќе биде потребно да помине извесно време државите да го прифатат јавното-приватно партнерство во заштитата на критичната инфраструктура во целосна смисла како незаменлив и неопходен концепт за развој и подобрување на бизнисот и нивото на услуги. Најдобар пример за ова пред сè се земјите од Источна и Јужна Европа. Оттука, потребно е да се стимулира и воспостави соодветен систем на јавно-приватно партнерство во областа на заштитата на критичната инфраструктура. За оваа потреба се нудат неколку типа решенија, и тоа: потребно е да се обезбеди најшироко можно учество на предлози, значајно е обезбедување на соодветно ниво на свест, јасно да се дефинираат надлежностите и одговорностите на ниво на самите оператори на критичната инфраструктура и размената на информации (информациите кои се од суштинско значење за обезбедување на националната безбедност и информациите кои во деловното опкружување претставуваат важни деловни податоци, што може да ја намали конкурентската предност на компанијата која управува со критичната инфраструктура). Исто така, неопходено е јавно-приватното партнерство да се фокусира на одредени елементи за успех и одржливост на соработката со цел спроведување на целите за јакнење на отпорноста и заштита на критичните инфраструктури, како што се:

- **Дефинирање на улогите и одговорностите**. Конкретно, јавно-приватното партнерство треба да ги регулира обврските и правата на јавните и на приватните партнери, истовремено почитувајќи ги основните принципи во подготовката и имплементацијата на проектите за јавно-приватно партнерство, т.е. принципот на јавни набавки, принципот на јавен интерес и принципот на економичност.
- **Примена на ресурси.** Ова е насочено кон намалување на критичноста и/или зголемена флексибилност на инфраструктурите при што заинтересираните страни од јавно-приватното партнерство треба да ги вклучат ресурсите кои им се на располагање. Исто така, покрај постојните јавни и приватни финансиски ресурси, потребно е да се планира можно користење на европските структурни и инвестициски фондови за поддршка на јавните-приватни партнерства во заштитата на критичната инфраструктура.
- **Отвореност за развој на капацитети и промени** се однесува во случај кога ќе се јави потреба за институционални промени во процесот на

управување со ризикот за критичните инфраструктури на ниво на давателот на услуги или тела.

- **Реални очекувања** кои се однесуваат на краткорочните планови со ограничени временски рамки кои резултираат со решенија кои тешко се применуваат. Оттука, не е реално да се очекува дека вклучувањето на приватниот сектор во краток временски период ќе ги надомести недостатоците во однос на ресурсите или активноста на јавните институции воопшто (RECIPE, 2015).

Приватниот сектор има уште една од главните улоги за заштита на критичната инфраструктура која се базира на јавно-приватното партнерство и се однесува на високото ниво на квалитет и услуга и затоа треба да биде признаен како доверлив партнер од страна на надлежен јавен орган и од сопственикот/менаџерот на критичната инфраструктура. На пример, на ниво на ЕУ сè уште не постои сеопфатен сет на мерки за регулирање на активностите за заштита на критичната инфраструктура од приватниот сектор и надлежноста е во доменот на националното законодавство. Од друга страна, постојат посебни ISO стандарди за заштита за услугите на приватната безбедност кои треба да се разгледаат и имплементираат во работата на приватниот сектор пред да влезат во областа на заштитата на критичната инфраструктура.

Ова се бројни показатели кои укажуваат дека сето ова мора да се земе предвид кога станува збор за изградба на ефикасен систем за заштита на критичната инфраструктура.

1.4. Индикативна листа на критичната инфраструктура

Во рамките на ЕУ е утврдена прецизна спецификација на критичните инфраструктури. Така на пример, Индикативната листа на Европската комисија на ЕУ ги вклучува: енергијата, информациските и комуникациските технологии, водата, храната, финансиите, јавната администрација, транспортот, хемиската индустрија и др. (Green paper on a European Programme for critical infrastructure protection, 2005 , Annex II).

Исто така, во повеќето држави-членки на НАТО е утврдена прецизна индикативна спецификација на критичната инфраструктура. Така на пример, во Германија таа ги вклучува: енергијата, телекомуникациите, информатичката инфраструктура, јавното здравство, снабдувањето со вода и храна, банкарството, финансиите, транспортот, итните и спасувачките служби, владините институции, полицијата, царината, вооружените сили и др.

Во *Франција* листата ги вклучува: државниот сектор (цивилни активности, правото и воени активности), потребите на луѓето (храна, вода, здравје), економијата (енергетика, прометот и финансиите), технологии (индустрија, комуникациските технологии и радиодифузија) и истражувања (Ducamin 2016; 5).

Во *Велика Британија* ги вклучува: енергијата, телекомуникациите, владините институции, здравството, финансиите, транспортот, итните служби, водата и одводните системи и др.

Во *Шведска*, ги вклучува: енергијата, транспортот, водата и комуналните услуги, храната, здравствената заштита, информациите и комуникациите, итните

служби, индустријата и трговијата, финансиските услуги, владините институции и социјалните осигурувања.

Во *САД* ги вклучува: енергијата, информациите, телекомуникациите, јавното здравство, храната, водата, финансиите, итната помош, владините институции, основната одбранбена индустрија, хемиската индустрија и опасните материи и др.

Во *Хрватска* листата се однесува на транспортот (копнен, железнички, воздушен и поморски), енергетиката (електрична енергија, гас, нафта и нафтени производи), комуникации и информациски технологии.

Словенија со помош на критериумите за идентификација (објавени во 2012 година како Основни и секторски критериуми за одредување на критичната инфраструктура од национално значење за Република Словенија и Измените и дополнувањата од 2014 година) ја идентификува, препознава и ја одредува критичната инфраструктура. Издиференцирани се основни критериуми, и тоа:

- Критична инфраструктура којашто поради прекин или нарушување на работата може да предизвика смрт на повеќе од 50 лица.
- Критична инфраструктура којашто поради нефункционалност може да влијае врз здравјето на луѓето до таква мера што ќе биде неопходно да се хоспитализираат повеќе од 100 луѓе за повеќе од една недела.
- Критична инфраструктура којашто поради прекин или пак нарушување на редот на работата и услугите, предизвикува оштетување или уништување на објекти или подрачја со влијание врз националната безбедност на Република Словенија и тоа до тој степен да биде отежнато спроведувањето на националната безбедност, внатрешната безбедност и заштита од природни или други непогоди.
- Критична инфраструктура којашто поради нефункционалност влијае врз спроведувањето на стопанските и другите активности, со што ќе доведе до прекин во снабдувањето со вода за пиење или храна за населението од над 100.000 луѓе за повеќе од една недела.
- Критична инфраструктура којашто поради нефункционалност влијае на прекин во снабдувањето со електрична енергија за три дена или за повеќе од една недела за над 100.000 луѓе.
- Критична инфраструктура којашто поради нефункционалност влијае на прекин во снабдувањето со нафтени производи за повеќе од една недела, за над 100.000 луѓе.
- Критична инфраструктура којашто поради нефункционалност предизвикува голема штета поради влијание на водата и загрозува живеалишта и почва во површина од над 100 хектари.
- Критична инфраструктура којашто поради нефункционалност предизвикува информациски или комуникациски прекини во поддршка за работа на друга критична инфраструктура во времетраење до 24 часа.
- Критична инфраструктура којашто поради нефункционалност предизвикува значајни последици во други држави, во согласност со претходните критериуми (Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012: 1-2).

Исто така, донесени се и критериуми за секој од осумте сектори на критичната инфраструктура: енергетика, транспорт, храна, вода за пиење, здравствени услуги, финансии, заштита на околината, комуникациите и ИТ технологии. Овие критериуми се прикажани во Табела бр.1.

ТАБЕЛА БР.1: Листа на сектори на критична инфраструктура во Република Словенија

Сектор	Критериуми
Енергетика	• Распад на енергетскиот систем на подрачје на Република Словенија за чија санација е потребно повеќе од 7 дена. • Прекин во снабдување со електрична енергија за три дена за над 100.000 луѓе. • Прекин во снабдување со нафтени производи и природен гас за времетраење повеќе од една недела во обем над 100.000 луѓе и трошоци во висина од 10.000.000 евра дневно.
Транспорт	• Оневозможување на железничкиот сообраќај на клучни правци повеќе од неколку недели и штета од 10.000.000 евра дневно. • Оневозможено одвивање на воздушен сообраќај во Република Словенија подолго од 12 часа.
Храна	• Оневозможено снабдување со основни прехранбени продукти за времетраење од една недела за население во обем над 100.000 луѓе.
Вода за пиење	• Оневозможено снабдување со вода за пиење за времетраење од една недела за население во обем над 100.000 луѓе.
Здравство	• Оневозможено давање на итна медицинска помош и услуги во јавно здравство за население во обем над 100.000 луѓе.
Финансии	• Оневозможен дотур на пари подолго од 3 дена на подрачје во обем над 50.000 луѓе. • Нефункционирање на државните финансии подолго од 7 дена. • Нефункционирање на платен промет подолго од 1 ден.
Заштита на околината	• Причини за загаденост со кратки штетни влијанија врз здравјето на населението на подрачје над 50.000 луѓе.
Комуникации и ИТ технологии	• Нефункционирање на комуникациската опрема, мрежата и услугите од кои зависат клучните функции во државата и работата на повеќе сектори од критичната инфраструктура, системот на националната безбедност, електро-енергетскиот сектор и финансии подолго од 6 или 24 часа.

Извор: Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012: 2-3.

Република Северна Македонија нема формално утврдена листа на критична инфраструктура, таа е законски нерегулирана и нема идентификација и заштита на критичната инфраструктура. Оттука, утврдена ЕУ прецизна спецификација на критичните инфраструктури и наведените решенија во земјите-членки на ЕУ и НАТО од кои би ги издвоиле примерите со Словенија и Хрватска, ќе бидат од голема полза за идните активности при создавање формална рамка за заштита на националната критична инфраструктура.

1.5. Стандарди за заштита на критичната инфраструктура

Компаративно набљудувано, постојат одредени разлики во стандардизацијата на рамката за секторите на критичната инфраструктура помеѓу Европската унија и САД. Сепак, покрај тие разлики, ефективните стандарди за заштита на критичнаата инфраструктура претставуваат камен-темелник на секоја успешна програма за заштита на критичната инфраструктура. Стандардите и нормите за заштита на критичната инфраструктура вклучуваат методологија за проценка на ризици кои се неопходни за идентификување на заканите, проценка на ранливоста и оценка на влијанието врз средствата, инфраструктурата или системите земајќи ја предвид веројатноста на нивното појавување. Постои значителен број на методологии за проценки на ризик на критични инфраструктури. Во принцип, пристапот што се користи е прилично вообичаен и се состои од неколку главни елементи. Прво, идентификација и класификација на заканите, идентификација на разнливоста и проценка на влијанието. Ова е добро познат и веќе воспоставен пристап за проценка на ризици и претставува столб на речиси сите методологии за проценка на ризици. Сепак, постои голема разлика во методологиите за проценка на ризици врз основа на обемот на методологијата, популацијата за која е наменета (носители на политики, креатори на одлуки, истражувачки институти) како и на нивниот домен на применливост (ниво на средства, инфраструктурно/системско ниво и сл.)

Генерално гледано, стандардите играат голема улога во дефрагментирачките пазари и помагаат на индустријата да достигне одредени економски вредности. Стандардите се исто така од голема важност за страната на побарувачката, особено во однос на интероперабилноста на технологиите што ги користат првите одговорни лица, органите за спроведување на законот, итн. Дополнително, стандардите се од суштинско значење за да се обезбеди единствен квалитет во обезбедувањето на безбеден сервис. Креирањето на стандарди на ЕУ и нивно промовирање на светско ниво исто така е витална компонента на глобалната конкурентноста на безбедосната индустрија на ЕУ. Меѓутоа, неколку ЕУ стандарди постојат во безбедносната сфера. Изгледа дека различни национални стандарди претставуваат голема пречка за создавање на вистински внатрешен пазар за безбедност, со што се попречува конкурентноста на индустријата на ЕУ. Европската комисијата веќе има објави во својата порака за стратегиска визија за европските стандарди нагласувајќи ја потребата да се забрзаат напорите за стандардизација во безбедносниот сектор. Затоа, со издавање на документот М/487 на Комисијата ги овласти во 2011 година Европските организации за стандардизација (CEN, CENELEC и ETSI) да направат детален преглед на постојните меѓународни, европски и национални стандарди во безбедносната област, како и да се утврди листа на празнини во стандардизацијата и да се предложи изработка на програма за стандардизација Мандатот е прифатен од Европските организации за стандарди. Работата беше доделена на CEN/TC 391 "Општествена и граѓанска безбедност" чиј секретаријат е обезбеден од страна на Холандски институт за стандардизација (NEN). Од извештајот се појавуваат неколку вообичаени закани (мандат) и тие можат да се сумираат на следниов начин:

- Доверливост - посебно внимание е потребно за стандардизација на безбедноста.
- Интегритет во име на сите засегнати страни.
- Работа базирана на ризик - ISO 31000 е широко прифатен стандард во секторот.
- Услови и дефиниции - потребни се јасни дефиниции.
- Стандардизација и иновации - иновацијата може многу да има корист од раната стандардизација.
- Предлози за временската рамка треба да бидат приоритетни и патоказот е само почеток на развојот.
- Политиката на ЕУ - стандардизацијата во безбедносниот сектор е одлична алатка за поддршка на политиката на ЕУ.
- Реакциите на засегнатите страни - засегнатите страни генерално беа позитивни во врска со мандатот и активно учествуваа.
- Потребата да се исполнат целите и критериумите на ЕУ преку разгледување од страна на експерти.

Најчесто се повторуваат стандардите, најдобрите практики и упатства извлечени од Инвентарот на Европската референтна мрежа за заштита на критичната инфраструктура (ERNCIP). Инвентарот е подреден според репрезентативните тематски области и секторски критериуми како Автентикација и биометрија, крос секторска, детекција на експлозиви, ИТ и сајбер безбедноста, отпорност на структури од експлозиви, безбедност во сообраќајот и вода и животна средина. Најрепрезентативни стандардите за секоја од горенаведените тематски области се следните:

А. Вода и Животна средина

- ISO 15839: 2003 Квалитет на вода - Он-лајн сензори / опрема за анализа на вода - Спецификации и тестови за изведба;
- ISO 24510: 2007 Активности во врска со услугите за вода за пиење и отпадни води - Упатства за проценка и подобрување на услугата за корисниците;
- ISO 24511: 2007 Активности во врска со вода за пиење и услуги за отпадни води - Упатства за управување со комунални услуги за отпадни води и проценка на отпадни води;
- ISO 24512: 2007 Активности во врска со услугите за вода за пиење и отпадни води - Упатства за управување со комунални услуги за вода за пиење и проценка на услугите за вода за пиење.

В. Безбедност на транспортот

- PAS 68 Спецификации за тест на влијание за пречки во безбедноста на возилото;
- ASTM F2656 – 07 Стандарден метод за тестирање на несреќи со возила на периметарски бариери;

- CWA 16221: 2010 Безбедносни бариери на возилото. Барања за изведба, методи на тестирање и упатство за примена;
- BS EN 1317-1:2010 Системи за ограничување на патот. Терминологија и општи критериуми за методи на тестирање;
- BS EN 1317-2:2010 Системи за ограничување на патот. Класи за изведба, критериуми за прифаќање на тест на удар и методи за тестирање за безбедносни бариери, вклучително и парапети за возила
- BS EN 1317-3:2010 Системи за ограничување на патот. Класи за изведба, критериуми за прифаќање на тест на удар и методи за тестирање на перничиња за судар.;
- DD ENV 1317-4:2002 Системи за ограничување на патот. Класи за изведба, критериуми за прифаќање на тест на удар и методи за тестирање за терминали и преминување на безбедносни бариери;
- NCHRP Извештај 350 Препорачани процедури за проценка на безбедноста на перформансите на висок пат;
- BS EN 12767:2007 Пасивна безбедност на структурите за поддршка за опремата за патиштата. Барања, класификација и методи за тестирање;
- PAS 69:2006 Упатства за спецификација и инсталација на бариера за безбедност на возилото;
- ISO 13492-2007 Преземен ISO 13492-2007 Финансиски услуги - Елемент на податоци поврзани со клучното управување - Примена и употреба на ISO 8583 елементи 53 и 96;
- ISO 22902-2:2006. Моторни возила - Автоматски мултимедијален интерфејс - Дел 2: Употребете случаи;
- ISO 28000:2007 Спецификација на системите за управување со безбедност на синџирот на снабдување.;
- ISO/TS 10891:2009, Топлински контејнери - Идентификација на радиофреквенцијата (RFID) - ознака за регистарски таблички;
- ISO/IEC 9797-2:2011, ИНФОРМАТИЧКА ТЕХНОЛОГИЈА - ТЕХНИКИ ЗА БЕЗБЕДНОСТ - КОДОВИ ЗА АВТЕНТИКАЦИЈА НА ПОРАКА (MACS) -- ДЕЛ 2: МЕХАНИЗМИ КОИ КОРИСТАТ ПЕРСОНАЛИЗИРАНИ ХАШ-ФУНКЦИИ;
- ISO 11064-4:2013, ЕРГОНОМСКИ ДИЗАЈН НА КОНТРОЛНИ ЦЕНТРИ - ДЕЛ 4: РАСПОРЕД И ДИМЕНЗИИ НА РАБОТНИТЕ СТАНИЦИ;
- ISO/PAS 16917:2002. Бродови и морска технологија - Стандард за пренос на податоци за поморски, интермодален транспорт и безбедност..

С. Автентикација и биометрија

- BSI TR-03104 Технички упатства за прибирање на податоци за производство, тестирање на квалитетот и пренесување на службени документи;
- BSI TR-03105 Тестови за совпаѓање со официјални елетронски лични документи;

- BSI TR-03121 Техничко упатство биометрија за апликации во јавниот сектор;
- BSI-TR 03132 Технички упатства и заштита на профили со електронски лични документи.

D. Инфроматичка технологија и Сајбер безбедност

- ISO/IEC 27001:2005 Информатичка технологија – Безбедносни техники – Системи за управување со информатичка безбедност -- Барања;
- ISO/IEC 27002:2005 Информатичка технологија – Безбедносни техники -- Кодекс на практика за управување со информатичката безбедност;
- ISO/IEC 13335-1:2004 Информатичка технологија – Безбедносни техники – Управување со информатичката безбедност и безбедноста на комуникациската технологија -- Дел 1: Концепти и модели за управување со информатичка безбедност и комуникациската технологија;
- ISO/IEC 20000-1:2011 Информатичка технологија – Управување со услуги – Дел 1: Барања на системот за управување со услуги;
- ISO 9241-110:2006 Ергономија на интеракција човек- систем -- Дел 110: Принципи на дијалог;
- ISO 9241-11:1998 Ергономски барања за канцелариска работа со терминали за визуелен приказ (VDTs) - Дел 11: Упатство за употребиливост;
- ISO/IEC DIS 25051 Софтверско инженерство – Барања и оценка на квалитетот на софтверските производи (SQuaRE) -- Барања за квалитет на софтверски производ Off-The-Shelf (COTS) и упатства за тестирање;
- ISO 9241-210:2010 Ергономија на интеракција човек-систем -- Дел 210: Дизајн на интерактивни системи за човекот;
- BS EN 45011:1998 Општи барања за тела кои управуваат со системи за сертификација на производи;
- NIST HANDBOOK 150-17 Национална програма за доброволна акредитација на лабораторија;
- IEC 60870-5-104 Телеконтрола опрема и системи - Дел 5-104: Протоколи за пренос - Мрежен пристап за IEC 60870-5-101 со користење на стандардни транспортни профили;
- IEC 61850-SER ed1.0 Комуникациски мрежи и системи во трафостаниците;
- NIST IR 7628 Упатства за паметна мрежа (Smart Grid) сајбер безбедност;
- NIST 800-53 rev3
- ISO 22311:2013 Видео надзор на интероперабилност на извозот
- IEC 62676-2:2013 Видео надзор за употреба во безбедносни апликации.

E. Отпорност на структури на експлозиви

- DIN EN 13541:2012 Стакло во зграда - Безбедносно застаклување -Тестирање и класификација на отпорност на притисок при експлозија;
- DIN EN 14449:2005 Стакло во зграда - Ламинирано стакло и ламинирано безбедносно стакло - Оцена на сообразност / Стандард на производ;

- ISO 16934:2007 Стакло во зграда -- Безбедносно застаклување отпорно на експлозија - Тест и класификација со шок цевки;
- DIN EN 13123-1:2001 Прозори, врати и ролетни - Отпорност на експлозија; Барања и класификација – Дел 1: Шок цевка; Англиска верзија на DIN EN 13123-1;
- DIN EN 13124-1:2001 Прозори, вратии ролетни - Отпорност на експлозија; Тест на методот - Дел 1: Шок цевка; Англиска верзија на DIN EN 13124-1.

F. Откривање на екслозиви

- ECAC Заедничка програма за проценка на опремата за безбедност – Систем за откривање на експлозиви;
- ECAC Заедничка програма за проценка на опремата за безбедност – Течно експлозивно откривање;
- ECAC Заедничка програма за проценка на опремата за безбедност – Безбедносни скенери.

G. Меѓу-секторски

- ISO/IEC 17025:2005 Општи барања за компетентност на лабораториите за тестирање и калибрација;
- ISO 14001:2004 Системи за управување со животната средина – Барања со упатства за употреба;
- ISO 22301:2012 Социјална безбедност – Системи за континуирано бизнис управување – Барања;
- EN 14383- 1:2006 Превенција на криминал – Урбано планирање и дизајн на згради – Дел 1: Дефиниција на специфични термини.

Заклучок

Имајќи го предвид досега кажаното, може да се констатира дека сè уште не постои универзално прифатена дефиниција за поимот критична инфраструктура. Ова може да се воочи во бројни дефиниции за „критична инфраструктура" во литературата. Различни земји, критичната инфраструктура ја дефинираат на различен начин. Но, најчесто сè се сведува на тоа дека инфраструктурата, системите и ресурсите се од витално значење за едно општество. Тргнувајќи од потребата да се обезбедат виталните функции на државата постои можност и да се одреди значењето на критичност на одредена инфраструктура, бидејќи таа е тесно поврзан со енергетската безбедност, телекомуникациите, енергетските системи, гасоводите и нафтоводите, економијата, транспортот, водоводот и сл. Во тој контекст треба да се потенцира дека „критичната инфраструктура" опфаќа ресурси кои се неопходни за функционирање на општествата, и тоа: енергетски капацитети и мрежи, комуникациска и информатичка технологија, финансии, здравство, храна, вода, транспорт, производство, складирање и транспорт на опасни материи и владини објекти. Заштитата на критичната инфраструктура, како водата, енергијата и телекомуникациите, е

од најголема важност. Доколку овие системи се во ризик, односно во дефицит или пак, се уништени, ќе настане импакт на економијата, психологијата и сигурноста на нацијата, односно на општеството. Високата меѓузависност на овие системи со останатите системи од социјалниот живот, налага потреба да се обрне поголемо внимание на нивната заштита. Потребата од заштита на критичната инфраструктура, во основа, произлегува од потребата секоја држава да има систематизиран пристап кон постојната инфраструктура и потребно е инфраструктурата да се дефинира како критична, заради можноста да биде потенцијална цел. Постојат многу различни решенија и практики, но секоја земја треба сама да го препознае најсоодветниот модел за заштита на критичната инфраструктура. Токму затоа, потребно е заштита на критичната инфраструктура да се регулира преку интегрален пристап, почнувајќо од идентификување, спречување и подготовка за справување со заканите врз критичната инфраструктура, па преку намалување на ранливоста на критичната инфраструктури да се дојде до ублажување на последиците врз критичната инфраструктура. Паралелно со определување на стратегиските императиви, неопходно е да се обезбеди и добра процена на заканите, на ранливоста, индикативната листа и стандарди за заштита на критичната инфраструктура и на последиците врз критичната инфраструктура, а пред сè, подобрување на отпорноста на критичната инфраструктура, односно безбедна критична инфраструктура од можни човечки, физички и сајбер-закани.

ГЛАВА 2

ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО ЕВРОПСКАТА УНИЈА

Глава 2

ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО ЕВРОПСКАТА УНИЈА[3]

Доц. д-р Роберт Микац
Факултет за политички науки при Универзитетот во Загреб

Додека некои земји како Велика Британија, Шведска, Германија, Холандија и Франција напредуваа во развојот на националните политики за заштита на критичната инфраструктура, Европската унија сè уште го бара своето место и улога во оваа област. Меѓу институциите на Европската унија, најактивна на овој план е Европската комисија, која настојува да ја промовира важноста на оваа тема, да обезбеди соработка меѓу земјите-членки, да ја забрза размената на знаења и искуства и да ги насочува земјите-членки во нивните напори за развој на областа на зајакнување на отпорноста и заштитата на критичната инфраструктура. Предизвиците на ниво на Европската унија се повеќеслојни и нивното решавање се одвива под притисок на временските рокови, бидејќи, како што одлично забележуваат Хемерли и Ренда (2010), неопходно е Европа да се усогласи по „неколку линии", како и да се усогласат различните политики и во сето тоа да се најде и да се создаде сопствен идентитет во оваа област. Затоа, Унијата се обидува со забрзано темпо да развие своја препознатливост и да постави стандарди што треба да ги следат сите земји-членки.

Дадено во определена временска рамка, ова поглавје започнува со следување на активностите на одредени поединечни држави и начините на кои ја развиваа областа на заштита на критичната инфраструктура, за понатаму да се сврти кон активностите на Европската унија како целина и напорите на обврзаните држави, процеси, критични инфраструктури и стручни лица на тој план. Она што најмногу ги карактеризира ваквите активности, како во поединечните држави, така и на ниво на Унијата, е тоа што тие речиси секогаш започнуваат со првично разгледување, т.е. нормативно уредување, потоа следува одредено (очекувано) доцнење во спроведувањето предизвикано од бројни фактори, а по ова развојот продолжува во фази кои пред сè зависат од имагинацијата и посветеноста на поединци (ние овие ги сметаме за клучни фактори) кои работат во рамки на организациите, а кои, со своите идеи и настојување, овозможија развојот на одредени активности да продолжи.

Важно е да се истакне дека постои значајна разлика меѓу концептот на критична инфраструктура и концептот на критична информатичка

3 Начелното истражување во оваа област чија цел беше да се истакне целокупната слика и да се анализираат активностите кои се преземаат во тој поглед во Република Хрватска беше изготвено за потребите на книгата Микац, Р.; Цезарец, И. и Ларкин. Р. (2018), *Критична инфраструктура: Платформа за успешна национална безбедност*, Загреб: Јесенски и Турк
За потребите на ова истражување, текстот на наведеното начелно истражување беше преработен и дополнет.

инфраструктура. Под критична инфраструктура главно подразбираме средства, системи или некои физички елементи. Додека, пак, критичната информатичка инфраструктура претставува „еден од составните сектори на целокупната критична инфраструктура кој, всушност, е особен по тоа што овозможува меѓусебно поврзување на секторите, а честопати обезбедува и механизам за меѓусекторска контрола" (Лопез и др., 2012: 1). Во целите на овој труд, фокусот ќе го ставиме на критичната инфраструктура.

Структурата на поглавјето е поделена на следните четири дела: 1. Концептот на заштита на критичната инфраструктура во одделни земји-членки на Европската унија; 2. Нормативната рамка на Европската унија за заштита на критичната инфраструктура; 3. Активности за соработка во рамките на Европската унија; 4. Заклучок.

Првиот дел е одбран како почеток на поглавјето токму со цел да се покажат решенијата на поединечни држави кои започнаа да ја развиваат областа на заштита на критичната инфраструктура пред самата Унија и кои потоа се прилагодуваа на неа на постепена основа. Во натамошниот текст на поглавјето, сакавме најпрво да ги посочиме главните активности кои ги презема Европската унија и начините на кои истите се реализираат, додека, на самиот крај на текстот, се обидовме да извлечеме и еден вид заклучок од целото поглавје.

2.1. Концептот на заштита на критичната инфраструктура во одделни земји-членки на Европската унија

Пред да се појави поттикот за заштита на критичната инфраструктура од страна на Европската унија, во текот на целата втора половина на XX век, сите постари земји- членки на Унијата постепено ја откриваа сами за себе потребата од заштита на нивните соодветни национални критични инфраструктури. Тие го препознаа значењето и важноста на функционирањето на критичната инфраструктура за одвивањето на секојдневниот живот на граѓаните, за опстојувањето на формите на општествено организирање и за одржувањето во работа на сите значајни системи во државата. Но, според некои автори (Сетола и др., 2016 година), заштитата и отпорноста на критичната инфраструктура како такви повторно се вратија во фокусот дури во последните две децении.

Важноста на проучувањата во овој дел може да се согледа преку тоа што во него е прикажано следното: 1. Пресек на поединечните напори на анализираните земји - предизвиците со кои тие се соочуваа и начини на кои ги решаваа истите; 2. Градење на нормативната рамка; 3. Преглед на опсегот на оваа област; 4. Дополнителни предизвици со кои се соочуваат државите кога треба да ги усогласат нивните политики со политиките на ЕУ во областа на критичната инфруструктура; 5. Водечка идеја кај други држави што се на почетокот на овој процес. Подолу се поместени пресеци на главните активности во тој поглед во Велика Британија, Кралството Шведска и во Германија.

Велика Британија припаѓа на групата земји кои почнаа да ја развиваат областа на заштита на критичната инфраструктура пред Европската унија да започне да се фокусира на оваа тема и таа ги пренесе во своето законодав-

ство обврските кои ѝ беа наложени од страна на Унијата преку воведување процедурални промени во активностите кои веќе ги преземаше за заштита на критичната инфраструктура на национално ниво (Лазари, 2014: 75). Постојната стратегиска рамка на земјата се заснова на безбедносни стратегии како што се: *Националната безбедносна стратегија на Велика Британија* за 2008, 2009, 2010 и 2015 година и *Националната стратегија за борба против тероризмот* за 2009 и 2011 година, додека оперативната рамка е содржана во законите со кои се регулираат клучните функции во земјата во различни интердисциплинарни области како што се: заштитата на информациите, енергетската и сообраќајната инфраструктура, функционирањето на службите за итна помош при вонредни ситуации и други. Во рамките на *Националниот регистар на ризици од граѓански вонредни состојби* (2008, 2010, 2012, 2013, 2015 и 2017), заедно со другите услови, Велика Британија ги разгледува ризиците, заканите и слабостите во функционирањето на критичната инфраструктура. Тој документ потоа им служи на сите фактори во заштитата на критичната инфраструктура како основа за разгледување на сите можни закани и како платформа за планирање на мерките за заштита.

Заштитата на критичната инфраструктура е во политичка надлежност на следниве две тела: Министерството за внатрешни работи (министерство во Владата надлежно за прашања поврзани со имиграцијата, безбедноста и за законот и редот во земјата), кое е одговорно за политиките за заштита во однос на терористичките закани; и Канцеларијата на Владиниот кабинет (генералниот секретаријат на Владата - општ и заеднички внатревладин оддел кој е задолжен за поддршка на политиките и активностите на премиерот и членовите на Владата на Велика Британија), која се занимава со прашања за зајакнување на отпорноста и заштитата од последиците од природни непогоди и катастрофи. На овој начин се остварува стратегикиот преглед и влијанието врз оваа област во земјата. Централниот орган надлежен за оперативно дејствување со цел да се намали ранливоста, да се заштитат националните критични инфраструктури, како и да се координираат активностите и факторите кои доаѓаат од повеќе дисциплини е Центарот за заштита на националната инфраструктура (ЦЗНИ). Овој Центар е владин орган (основан во 2007 година) кој му одговара директно на генералниот директор на Службата за безбедност МИ5 (ЦЗНИ, 2017 година) за својата работа. Центарот за заштита на националната инфраструктура е одличен пример на воспоставување на владино непрофитно тело кое спроведува меѓусекторски координативни дејности со компании и организации од индустријата, со академската заедница и со бројни министерства и институции на државната управа. Центарот обезбедува советодавни услуги со цел да се намали ранливоста на националните инфраструктури од тероризмот и другите закани. Тој ги поддржува институциите и организациите и преку градење и пренесување знаења за соодветните стандарди и нивното спроведување.

Во Велика Британија беа формирани девет сектори на критична инфраструктура и дваесет критични услуги. Министерствата одговорни за секој сектор ја вршат првичната селекција на средства и оператори (операторите се избираат врз основа на нивниот соодветен пазарен удел). Центарот за заштита

на националната инфраструктура паралелно спроведува сопствена процена и селекција. Врз основа на комбинираните придонеси од страна на операторот, надлежното министерство и ЦЗНИ, средствата (кои исто така може да бидат и процеси) ги мапираат според големината на последиците од нивното потенцијално неизвршување на услугата. Во процесот на идентификација, исто така, се земаат предвид шест нивоа на критичност (од КАТ-0 - „инфраструктура чиј прекин на дејството би имал мало влијание" до КАТ-5 „инфраструктури чиј прекин на дејството би имал катастрофално влијание врз Велика Британија") кои се разгледуваат во однос на три специфични критериуми: влијание врз животот, економско влијание и влијание врз основните (виталните) услуги. За поширокатa јавност, достапни се само описни и субјективни критериуми, додека на ниво на класифицирани информации, на секој критериум му се доделуваат квантитативни и објективни вредности (мерила). Ваквата сегментација се спроведува во комбинација со секторски критериуми (специфични за секој сектор) кои се единствени за секој од деветте сектори. Во крајна мера, идентификувани се само мал број средства на кои им е доделено највисоко ниво на критичност, имајќи предвид дека само оние средства што се наоѓаат во категоријата „КАТ-3" и повисоко се сметаат за навистина критични. Потоа, се спроведува приоретизација врз основа на „категоризацијата според ознаките за КАТ" и веројатноста за подложност на напад, која всушност претставува збир од ранливоста (на пр. леснотијата на пристап до имот) и заканите по средствата (на пр. видот на напад).

Кралството Шведска исто така го започна процесот на заштита на критичната инфраструктура пред иницијативите кои дојдоа од ЕУ и се прилагоди преку усвојување измени и дополнувања на постојните закони и подзаконските акти во областа на енергетиката и транспортот (Лазари, 2014: 75). „Од шведска гледна точка, не постои јасна дефиниција за тоа што претставува критична инфраструктура "(Јохансон, 2010: 27). Шведска го поврзува поимот критични инфраструктури со изразот *витални општествени функции* и истите ги согледува преку еден единствен концепт. При ваквото поврзување на поимите, критичните инфраструктури претставуваат физички структури чие функционирање придонесува за обезбедување на виталните општествени функции. Тоа се функции што се толку важни што нивното прекинување или сериозно нарушување на работата може да претставува голем ризик или опасност по животот и здравјето на луѓето, функционирањето на општеството или основните општествени вредности. Овој пристап кон концептот се заснова на сеопфатно разгледување на сите ризици, закани и слабости и обезбедувањето заедничка и сеопфатна реакција кон сите нив (Шведска агенција за граѓанска подготвеност, 2011). Заштитата на виталните функции на општеството и критичната инфраструктура претставува дел од системот за подготвеност за граѓански вонредни ситуации (Шведска агенција за граѓанска подготвеност, 2016) и укажува на мерки и активности што се преземаат за да се обезбеди ефикасноста и дејствувањето на критичните инфраструктури и виталните општествени функции и општеството како целина (Шведска агенција за граѓанска подготвеност, 2014).

Централен орган надлежен за координирање на главните активности за заштита на виталните функции на општеството и критичната инфраструктура

е Шведската Шведска агенција за граѓанска подготвеност (Myndigheten för samhällsskydd och beredskap - MSB).

МСБ е владин орган надлежен за прашања во врска со цивилната заштита, јавната безбедност, управувањето со итни случаи и цивилната одбрана за кои нема надлежност ниеден друг орган. Надлежноста се однесува на мерките кои се преземаат пред, за време на и по вонредни состојби или кризи (Шведска агенција за граѓанска подготвеност, 2019 година). Во Шведска се означени единаесет сектори во кои може да се откријат и обележат витални општествени функции и критична инфраструктура.

Заштитата на виталните општествени функции и критичната инфраструктура е дел од системот за подготвеност за вонредни состојби и ги подразбира мерките и активностите што се преземаат за да се обезбеди ефикасноста и функционирањето на инфраструктурата од важност и виталните општествени функции, како и на општеството како целина. Шведската агенција за граѓанска подготвеност ја идентификуваше и анализираше зависноста на критичните инфраструктури врз основа на надлежноста која ѝ беше доделена и водството кое ѝ го понуди Владата за тоа во периодот 2006-2008 година. Во таа анализа беше истакнато дека наместо инфраструктурите, се разгледуваат виталните општествени функции, затоа што улогата на инфраструктурата е само да поддржува одредени функции на заедницата. Резултатите од анализата на зависност се користат при носењето одлуки за мерките за приоретизирање, распределбата на средствата и одбирањето на предметот на студиите и истражувањата. Шведскиот пристап кон заштитата на критичната инфраструктура подразбира соработка меѓу голем број фактори, од органите за спроведување на законот, разузнавачките и безбедносните служби, Шведската агенција за граѓанска подготвеност, секторските агенции, регионалните и локалните власти, до засегнатите страни од приватниот сектор кои се сопственици или оператори на критични инфраструктури.

Германија е пример за земја која, исто како Велика Британија и Шведска, го направи првичното усогласување на националното законодавство во 2001 година во областа на енергетиката и во 2002 година во областа на системите за трансмисија со цел да одговори на барањата на ЕУ (Лазари, 2014: 74) . И покрај тоа што критичната инфраструктура е заштитена со бројни регулативи, мерки и активности, Германија сепак одлучи одделно да ја уреди оваа област. Најпрво, во 2007 година, беше усвоен *Планот за спроведување на заштитата на критичната инфраструктура*, кој претставува национален план за заштита на критичната информатичка инфраструктура. Овој пристап е избран со цел обезбедување заштита на виталните национални функции преку соодветна заштита на информациите (Сојузно министерство за внатрешни работи, 2007 година). Една година подоцна, усвоен е *Концептот за основна заштита на критичните инфраструктури*, кој беше разработен на интердисциплинарна основа од страна на јавните органи со цел да се обезбедат препораки за компаниите за начините на кои може зајакнат јавната безбедност преку соработка во заштитата на критичната инфраструктура (Сојузно министерство за внатрешни работи, 2008). Потоа, во 2009 година беше донесена *Националната стратегија за заштита на критичната инфраструктура*, каде јасно беше

истакнато дека заштитата на критичната инфраструктура претставува клучна функција на мерките за подготвеност во склоп на безбедносните активности кои ги преземаат сите засегнати чинители, додека споменатите активности претставува основен интерес на безбедносната политика на државата (Сојузно министерство за внатрешни работи, 2009). Кратко потоа, во 2011 година беше донесена *Стратегијата за сајбер-безбедност на Германија*, која, покрај другите одредби, ја смета и заштитата на информатичката инфраструктура како главна задача на областа за компјутерска безбедност (Сојузно министерство за внатрешни работи, 2011а; 2016), како и *Националниот план за заштита на информатичката инфраструктура* кој истакнува три стратешки цели за заштита на критичната информатичката инфраструктура (Сојузно министерство за внатрешни работи, 2011 б).

На сојузно ниво, институционалната одговорност за координирање на системот за заштита на критичната инфраструктура е кај Сојузното министерство за внатрешни работи, градежништво и заедница. Министерството е исто така национална точка за контакт и е одговорно за сите прашања што вклучуваат меѓусекторски перспективи и управува со Центарот за ИТ ситуации и ИТ кризниот центар, кои, пак, ги следат сите важни активности поврзани со критичната инфраструктура. Во рамките на Министерството, две канцеларии се надлежни за некои од сегментите на заштитата на критичната инфраструктура - Сојузната канцеларија за цивилна заштита и помош при непогоди е одговорна за разгледување на сеопфатни активности, додека Сојузната канцеларија за безбедност на информации се занимава со компјутерската заштита на критичните инфраструктури. Покрај тоа, за секој сектор е определено надлежно министерство кое носи одговорност за спроведување на секторските политики и насочување на активностите на засегнатите страни во рамките на соодветниот сектор. Во Германија, беа формирани вкупно девет сектори на критична инфраструктура. На ниво на сојузните држави, исто така е воспоставен систем на јасни надлежности и одговорности за спроведување на политиките, управување со системот и заштита на критичната инфраструктура.

Во Германија има бројни закони кои регулираат специфични секторски надлежности кои се однесуваат на заштита на критичната инфраструктура, а во кои исто така се вградени и одредби за управувањето со кризи (Џон-Кох, 2017). Кога станува збор за законски одредби, треба да се нагласат два закони. Прво, *Законот за цивилна заштита и хуманитарна помош* пропишува одредби за заштита на критичната инфраструктура гледана како задача за цивилна заштита (Браубах и др., 2014). Второ, *Законот за компјутерска безбедност*, кој ѝ пристапува на заштитата на критичната инфраструктура преку пропишување одредби кои се однесуваат на примената на минималните стандарди за безбедност на информациите во работењето на сите засегнати национални компании (Германски Бундестаг, 2015). *Законот за цивилна заштита и хуманитарна помош* се занимава со функционирањето на системот како целина при што истакнува јасно дадени надлежности. Додека *Законот за компјутерска безбедност* конкретно се однесува на повеќе од две илјади компании кои обезбедуваат витални функции и услуги како што се сообраќај, управување со водите, здравствени услуги, телекомуникации, одржување, финансиски и

осигурителни услуги. Одреден е двегодишен рок за спроведување, во кој период е неопходно да се преземе процес на сертификација за нови стандарди за компјутерска безбедност и да се обноват безбедносните сертификати. Со цел да се постигне поголема отпорност и заштита од сајбер-напади, доколку не ги исполнуваат бараните услови, компаниите ќе се соочат со високи казни (Форд, 2015; Сантилан, 2015). Ваквиот пристап може да послужи како модел за другите земји да ја регулираат областа на заштита на критичната инфраструктура преку обезбедување поцврста компјутерска безбедност, имајќи предвид дека ИТ системите ја прават критичната инфраструктура вмрежена во огромна мера и затоа нивната заштита е од клучно значење (Кандек, 2015).

Овие три примери ја илустрираат разновидноста на пристапите при воспоставувањето на нормативна рамка во областа на критичните инфраструктури. Од британскиот пример, каде што се направени само мали измени во постојните закони со цел да се усогласи концептот на критична инфраструктура со барањата од одредбите на Европската комисија, коешто беше првото нешто што го презеде и Германија, до случајот на Шведска, каде поврзувањето на овој со концептот на виталните општествени функции оформи единствен концепт на заштита. До денес, Велика Британија и Шведска ја одржуваат рамката за заштита на критичната инфраструктура преку голем број документи на различни нивоа на имплементација, додека Германија по првичното усогласување воспостави комплетно нова регулаторна рамка за оваа област. Покрај споменатите делумни разлики, сите три земји делат многу повеќе заеднички елементи. Заедничкиот именител за сите три држави е силната поддршка за развивање јавно-приватни партнерства и неопходното стапување во соработка со приватниот сектор во областа на заштита на критичната инфраструктура. Потоа следи идентификацијата и означувањето на критичните инфраструктури на сите три нивоа на политичко организирање на земјата (локална, регионална, национална власт), што бара секојдневна соработка помеѓу горенаведените нивоа на власт. Акцентот при спроведувањето на оваа активност е ставен врз проценатa на ризиците и ранливостите кај критичните инфраструктури и, следствено, врз управувањето со ризиците и деловните процеси преку примена на деловни, индустриски и секторски стандарди. Сите три земји се стремат кон поголема соработка меѓу сите вклучени чинители, како и кон одржувањето на транспарентност на системот. Секој од горенаведените модели или комбинациите од нив претставуваат примери за други земји бидејќи, како што е неопходно, така е и навистина возможно да се развие своја национална рамка за заштита на критичната инфраструктура и соработка меѓу сите засегнати страни во системот.

2.2. Нормативната рамка на Европската унија за заштита на критичната инфраструктура

Под силно влијание на терористичкиот напад во САД во 2001 година, Глобалната војна против тероризмот што следуваше и големите терористички напади во Европа (2004 година во Мадрид, 2005 година во Лондон), Европската унија, ги насочи своите согледување и дискусија за заштитата на критичната инфраструктура кон одбраната од тероризмот.

Во јуни 2004 година, Европскиот совет побара од Европската комисија да подготви сеопфатна стратегија за областа на критичната инфраструктура во Европската унија и да воспостави нормативна рамка за нејзина заштита. Врз основа на гореспоменатиот услов, во октомври 2004 година Европската комисија го усвои првиот документ во оваа област под наслов *Комуникација за заштита на критичната инфраструктура во борбата против тероризмот*, во кој беа посочени предлози околу тоа што треба Европа да направи за да спречи терористички напади врз критични инфраструктури, за подобрување на нивото на подготвеност за вонредни ситуации, за подигање на нивото на отпорност кај таквите инфраструктури, како и за развивање на нивната способност за одговор на напади (Европска комисија, 2004). Со овој документ започнаа интензивни напори кај телата на Европската унија, како и соработката со земјите-членки и со поединечните експерти за развој на нормативната рамка и идентитетот на Унијата во областа на критичните инфраструктури.

Една година подоцна, Комисијата изработи *Зелена книга за Европската програма за заштита на критична инфраструктура*, во која се понудени можни политики за тоа како Комисијата може да воспостави програма за заштита на критичната инфраструктура и Информативна мрежа за предупредување за критична инфраструктура (CIWIN), (Европска комисија, 2005 година). Дискусиите што се водеа по усвојувањето на *Зелената книга* ја подвлекоа додадената вредност која се добива со воспоставувањето стратегиска рамка на Унијата за заштита на критичната инфраструктура. Исто така, истакнати се клучните насоки за развој на оваа област, како што се: потребата да се подобрат можностите за заштита на критичната инфраструктура во Европа и да се помогне во ублажување на недостатоците поврзани со критичната инфраструктура. Понатаму, беше истакната важноста на клучните принципи на супсидијарност, пропорционалност и комплементарност, како и на дијалогот меѓу засегнатите страни во системот на зајакнување на отпорноста и заштита на критичната инфраструктура (Совет на Европската унија, 2008).

Следниот придонес дојде од Советот за правда и внатрешни работи, кој во декември 2005 година ја повика Комисијата да даде предлог за *Европска програма за заштита на критична инфраструктура*. Упатствата за изготвување нагласуваат дека Програмата треба да ги земе предвид сите опасности, при што приоритет треба да се даде на борбата против терористичките закани. Ваквиот пристап кон заштитата на критичната инфраструктура ги зема предвид технолошките закани предизвикани од човечка активност и природни непогоди, но приоритет треба да се даде на заканите од тероризам (Совет на Европската унија, 2008). Затоа, во 2006 година, Европската комисија усвои *Европска програма за заштита на критична инфраструктура*, која ги зема предвид сите ризици кога станува збор за заштитата на критичната инфраструктура, но која најмногу се занимава со тероризмот, како што и се бараше во спомнатите упатства (Европска комисија, 2006) .

Во април 2007 година, Советот на Европската унија ја разгледа *Европската програма за критична инфраструктура* и донесе заклучоци во кои се наведува дека крајната одговорност за управување со клучните решенија за заштита на инфраструктурата е кај земјите-членки во рамките на нивните државни

граници. Покрај ова, тој побара од Комисијата да развие европска постапка за идентификација и означување на европски критични инфраструктури и процена на потребата за подобрување на нивната заштита. Ова е важна одредница во развојот на оваа област, бидејќи на тој начин се препознава податокот дека во Унијата постојат голем број критични инфраструктури чие нарушување на работата или уништување би можело да произведе значителни прекугранични ефекти. Прекините во работата може да вклучуваат прекугранични меѓусекторски ефекти предизвикани од меѓузависноста на меѓусебно поврзаните инфраструктури. Програмите за билатерална соработка помеѓу земјите-членки во областа на заштитата на критичната инфраструктура претставуваат добро оформена и ефикасна алатка за справување со прекугранични критични инфраструктури, но се препознава и потребата за интегрални решенија на ниво на целата Унија. Затоа, беше неопходно да се утврдат условите за идентификација и означување на европската критична инфраструктура преку заеднички процес во кој учествуваат сите земји-членки, како и да се воспостави нивна меѓусебна соработка и вклучување на сопствениците или операторите на критичните инфраструктури во наведените процеси (Совет на Европската унија, 2008).

Паралелно со работата на Комисијата, во 2007 година, Советот на Европската унија усвои посебна програма за *Превенција, подготвеност и управување со последиците од тероризмот и други ризици поврзани со безбедноста*. Оваа програма идентификува голем број ризици поврзани со безбедноста, ставајќи акцент на поддршката на напорите на земјите-членки за спречување терористички напади и спроведување на подготовки за заштита на луѓето и критичната инфраструктура од ризици поврзани со терористички напади (Совет на Европската унија, 2007 година).

Веднаш потоа, земајќи го предвид предлогот на Комисијата, Советот на Европската унија го усвои клучниот документ во областа на критичните инфраструктури во Европската унија - *Директивата на Советот 2008/114/ЕЗ од 8 декември 2008 година за идентификација и означување на европската критична инфраструктура и процена на потребата за подобрување на нивната заштита* (во натамошниот текст *Директивата 2008/114/ЕЗ*), која повеќе не е насочена кон заканата од тероризам, туку има за цел да воспостави сеопфатен процес на заштита на критичната инфраструктура како на ниво на земјите членки, така и на Унијата во целост (Совет на Европската унија, 2008). Правна основа за Директивата 2008/114/ЕЗ е Членот 308 од *Договорот за основање на Европската заедница*. Како што беше посочено, првичната дискусија во Унијата за заштитата на критичната инфраструктура, пред сè беше насочена кон одбраната од тероризмот. Со текот на времето, другите ризици сè повеќе се препознаваа и дискутираа, но, до усвојувањето на *Директивата 2008/114/ЕЗ*, кога беше преземен еден сеопфатен пристап кон согледувањето на сите ризици и закани, тероризмот остана најголемата посочена закана.

Иако споменатите документи на Европската унија, како и многу други кои таа ги усвои, предложија дефинирање на поимот критична инфраструктура, со донесувањето на *Директивата 2008/114/ЕЗ*, дефинициите кои беа понудени во нив станаа еден вид теоретско ограничување во однос на националните

критични инфраструктури и европската критична инфраструктура, како во институциите на Унијата, така и во нејзините земји-членки. Државите започнаа да користат идентични или многу слични дефиниции за критичната инфраструктура во своите документи. Според *Директивата 2008/114/ЕЗ*, под критична инфраструктура се подразбираат „средствата, системите или деловите од нив кои се наоѓаат во земјите-членки и кои се од суштинско значење за одржувањето на виталните општествени функции, здравјето, сигурноста, безбедноста, економската или социјалната благосостојба на луѓето и чие нарушување или уништување би имало значително влијание во една земја-членка како резултат на неисполнувањето на тие функции". Под европска критична инфраструктура, пак, се подразбира „критичната инфраструктура која се наоѓа во земјите-членки и чие нарушување или уништување би имало значително влијание врз најмалку две земји- членки. Значењето на влијанието се проценува врз основа на вкрстени критериуми. Ова вклучува ефекти кои произлегуваат од меѓусекторската зависност од други видови инфраструктура" (Совет на Европската унија, 2008). *Директивата 2008/114/ЕЗ* се применува од 12 јануари 2009 година, додека земјите-членки имаа рок да ја пренесат во нивните национални законодавства до 12 јануари 2011 година во секторите енергетика и транспорт, додекаа земјите-кандидати за полноправно членство во Европската унија мора да ја спроведат истата пред нивното официјално пристапување кон Унијата.

Предлогот дека членките на Европската унија, по усвојувањето на *Директивата 2008/114/ЕЗ,* се должни да ги вклучат одредбите од неа во нивните национални законодавства стана повеќеслоен предизвик затоа што „постарите" земји членки на ЕУ го започнаа процесот на заштита на критичната инфраструктура пред усвојувањето на *Директивата 2008/114/ЕЗ*, кое претставуваше можна пречка за нив во спроведувањето на нивните сопствени политики додека од нив се бараше да ја усогласат нивната национална политика со политиката на Унијата во оваа област. Кај новите земји- членки, пак, се појави потребата за брзо прилагодување или започнување на процесот од почеток, иако некои од нив сè уште не беа целосно организациски подготвени за таа цел. Но, *Директивата 2008/114/ЕЗ* не остави простор спроведувањето на одредбите од неа да се одложи и го забрза прилагодувањето кон истите. Прашањето што се поставува е колку ова им претставуваше проблем и предизвик на земјите членки и колку тоа ги забрза нивните подготовки и ги насочи кон директно регулирање на материјата. Предноста при усвојувањето на *Директивата 2008/114/ЕЗ* за новите земји членки на Унијата доколку немаа развиено свои политики, мерки и активности за заштита на критичната инфраструктура се состоеше од тоа дека тие не беа оптоварени со претходните пристапи и, врз основа на регулативите на ЕУ, тие имаа можност да развијат и применат нови идеи кои можеа да бидат од корист за Унијата во целост и за постарите членки при градењето на политиките за заштита на критичната инфраструктура.

Бидејќи критичните инфраструктури се поврзани и сè повеќе зависат од Интернетот и процесите во сајбер-просторот, Унијата мораше да преземе чекори за регулирање на оваа област. Во 2013 година, Европската комисија, заедно со Високиот претставник на Европската унија за надворешни работи и

безбедносна политика, промовираше *Стратегија за сајбер-безбедност на Европската унија: Отворен, сигурен и безбеден сајбер-простор,* што претставуваше сеопфатна визија на ЕУ за тоа како најдобро да ги поддржи земјите-членки и другите засегнати страни во спречувањето и реагирањето на компјутерските нарушувања и напади (Европска комисија и високиот претставник на Унијата за надворешни работи и безбедносна политика, 2016 година). „Идејата беше да се поттикнат европските вредности на слобода и демократија и да се обезбеди безбеден раст на дигиталната економија. Конкретни активности насочени кон слабеење на компјутерската отпорност на информатичките системи, намалување на компјутерскиот криминал и зајакнување на политиката на ЕУ за меѓународна сајбер-безбедност и сајбер-одбрана." Стратегијата ја артикулираше визијата на ЕУ за сајбер-безбедност преку пет приоритети: 1. Постигнување на компјутерска отпорност; 2. Драстично намалување на компјутерскиот криминал; 3. Развој на политика за сајбер-одбрана и можностите поврзани со Заедничката политика за безбедност и одбрана (CSDP); 4. Развивање на индустриски и технолошки ресурси за компјутерска безбедност; и 5. Воспоставување доследна политика за меѓународниот сајбер-простор за Европската унија и промовирање на основните вредности на ЕУ. Стратегијата се спроведува преку низа законодавни и незаконодавни инструменти, како и активности за финансирање (Европска комисија, 2017: 2-3). Стратегијата претставува суштинска основа за преземање натамошни заеднички активности во регулирањето на сајбер-просторот, како и за заштита на критичната инфраструктура во тој домен, имајќи во вид дека „обезбедувањето на мрежните и информатичките системи во Европската унија е од суштинско значење за продолжување на одржувањето на он-лајн економијата и обезбедување напредок" (Европска комисија, 2019).

Врз основа на *Стратегијата за сајбер-безбедност на Европската унија*, донесена е *Директивата 2016/1148 на Европскиот парламент и на Советот во врска со мерките за високо заедничко ниво на безбедност на мрежните и информатичките системи низ Унијата* (натамошна *Директива за МИС*). Таа беше донесена на 6 јули 2016 година со обврска да се примени во националните законодавства на сите земји членки до 9 мај 2018 година (Европски парламент и Совет, 2016 година). *Директивата за МИС* претставува основен законодавен документ на *Стратегијата за сајбер-безбедност на Европската унија* и, во поглед на нејзината природа и примена, претставува акт од исклучително значење. Правна основа за *Директивата за МИС* е Членот 114 од *Договорот за функционирање на Европската унија*.

2.2.1. Директивата на Советот 2008/114/ЕЗ од 8 декември 2008 година за идентификација и означување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита

Имајќи предвид дека *Директивата 2008/114/ЕЗ* претставува централна точка за развој на политиката на ЕУ, земјите-членки, земјите во преговори за пристапување и земјите-кандидати за членство во ЕУ, таа ја поставува логиката за воспоставување деловни процеси и основата за голем број други активности

(како што се проектите кои се финансирани од страна на ЕУ, развојот на соработка меѓу државите и операторите на критични инфраструктури, воспоставувањето јавно-приватни партнерства, развојот на наставни програми, основањето центри и летни курсеви посветени конкретно на критичните инфраструктури итн.), па затоа неопходно е да се посвети посебно внимание на нејзиното анализирање, значење, достигнувања и предизвици при примената.

Во воведните одредби од *Директивата 2008/114/ЕЗ*, Советот на Европската унија презеде чекори за истакнување основни упатства за сите засегнати страни. Беше потенцирано дека првиот чекор во повеќефазниот пристап е насочен кон идентификација и означување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита. Притоа, фокусот првенствено паѓа врз секторот за енергија и транспорт, но треба да се земат предвид и другите значајни сектори како што се секторите за информатичко-комуникациска технологија Исто така, а следново е и особено важно, земјите-членки и сопствениците или операторите на горенаведените европски критични инфраструктури треба да ја подседуваат основната и конечна одговорност за заштита на критичната инфраструктура во Европа. Ова претставува продолжување на обврската за заштита издадена од Советот во април 2007 година, кога истиот ја разгледуваше *Европската програма за заштита на критична инфраструктура,* притоа донесувајќи заклучоци за заштитата на националните критични инфраструктури во кои беше нагласено дека конечната одговорност за заштитата лежи кај земјите-членки. Бидејќи во крајна линија европските критични инфраструктури се првенствено национални, и кога тие се од заемно значење за две земји членки, тие се сметаат како европски.

Следниот важен аспект на *Директивата 2008/114/ЕЗ* е дека таа стана заедничка платформа за соработка на сите засегнати чинители во системот за заштита на критичната инфраструктура на ниво на Унијата. Пред нејзиното усвојување, не постоеше обврска за службена соработка меѓу различни засегнати страни, ниту пак форум за постигнување на оваа соработка. Силата на Директивата лежи во барањето за нејзина задолжителна примена, а секоја земја-членка го одбира начинот на кој таа ќе биде транспонирана во нејзиното национално законодавство. Државите претходно соработуваа на билатерална основа, но не можеа во целост да постигнат повисоко ниво на функционалност во развојот на процесот за идентификација и означување на заедничка (европска) критична инфраструктура, како и заеднички пристап кон проценатa на потребата од подобрување на заштитата на ваквите инфраструктури, па така се појави неопходност за координативно дејствување од страна на самата Унија, за кое основата беше поставена со усвојувањето на *Директивата 2008/114/ЕЗ*.

Главниот дел на *Директивата 2008/114/ЕЗ* се занимава со постапката за идентификација и означување на европските критични инфраструктури. Постапката за идентификација беше уредена во Членот 3 од Директивата и прилогот кон него. Се состои од неколку чекори кои подразбираат терминолошко усогласување на набљудуваната инфраструктура според утврдената дефиниција и исполнување на вкрстените и секторските критериуми. Првиот чекор

подразбира дека секоја земја- членка треба да применува секторски критериуми за да изготви примарна квалификација на критичната инфраструктура во рамките на соодветниот сектор во склоп на територијата на државата. Секторските критериуми се користат за правење првична селекција на потенцијалните критични инфраструктури. Вториот чекор е да се применат дефиниции за инфраструктурата која се разгледува за да се увиди дали таа ги исполнува барањата и условите за „критична инфраструктура" или „европска критична инфраструктура". Третиот чекор е да се разгледа прекуграничното влијание на дефиницијата за „европска критична инфраструктура" и да се утврди дали одредена инфраструктура е заемно значајна за двете соодветни земји-членки без оглед на тоа дали и двете ја определиле како значајна или една од членките открила дека на територијата на другата земја-членка има инфраструктура што е значајна само за таа земја. Четвртиот чекор се состои од примена на вкрстени мерила кои вклучуваат почитување на следниве три критериуми:

а) критериум жртви (процена на потенцијалниот број на жртви или повредени);

б) критериум економски ефекти (процена на значењето на економската загуба или деградацијата на производите или услугите; вклучувајќи ги и потенцијалните ефекти врз животната средина);

в) критериум ефекти врз јавноста (процена на влијанието врз самодовербата на јавноста, како и на физичките страдања и нарушувањата на секојдневниот живот, вклучувајќи ја и загубата на основните услуги) (Совет на Европската унија, 2008).

Доколку се укаже потреба, Европската комисија може од секакви можни причини да им помогне на земјите членки да идентификуваат потенцијални европски критични инфраструктури, меѓу кои причини може да се вбројуваат недостатокот на административен и професионален капацитет, недостатокот на процедури, нејаснотиите во толкувањето на одредени критериуми, недостатокот на соработка со друга земја-членка, или, пак, неактивноста, при што Комисијата може да им посочи на некои земји-членки потенцијални критични инфраструктури кои може да се сметаат дека ги исполнуваат условите, кои најпрво ќе се идентификуваат, а потоа ќе бидат означени како европски критични инфраструктури.

Постапката за означување на европски критични инфраструктури е уредена во Членот 4 и истата може да се примени по претходно спроведување на постапката за идентификација на потенцијалните европски критични инфраструктури. Кога една земја-членка идентификувала потенцијална критична инфраструктура на територијата на други земји-членки или открила дека има своја инфраструктура на нејзината територија што е значајна за соседните земји, таа истите е задолжена да ги информира за тој податок. Се разгледува само инфраструктурата која е од суштинско значење за одржување на виталните функции на општеството, здравјето, сигурноста, безбедноста и економската или социјалната благосостојба на луѓето, а чие нарушување или уништување би имало значително влијание врз една или две земји-членки. Потоа, следи процес на билатерални или мултилатерални дискусии меѓу државите со

цел да се разгледаат состојбите и потенцијалните негативни ефекти од застојот или дефектот во работењето на утврдената инфраструктура. На покана на земјите-членки, Европската комисија може да учествува во овие дискусии. По извршената анализа, за да се идентификува потенцијалната критична инфраструктура како европска критична инфраструктура, потребна е согласност од земјата-членка на чија територија е откриена и назначена како европска критична инфраструктура. Во случај на неможност да се постигне договор меѓу земјите-членки, тие можат да се обратат до Комисијата, која може да се вклучи во дискусијата и да го олесни постигнувањето на договор меѓу државите (Совет на Европската унија, 2008).

По успешните преговори меѓу земјите-членки, следниот чекор е да се информираат сопствениците или операторите на критичната инфраструктура дека нивната инфраструктура е идентификувана и означена како европска критична инфраструктура. Земјата-членка на чија територија се наоѓа оваа европска критична инфраструктура е одговорна за информирање на сопственикот или операторот и исто така е должна на годишно ниво да ја известува Комисијата за бројот на означени европски критични инфраструктури по сектор и за бројот на земји-членки кои зависат од секоја означена европска критична инфраструктура. Информациите за означените инфраструктури се класифицираат според соодветното ниво на тајност на податоците и нивниот идентитет им е познат само на земјите-членки кои ги делат или на каков било начин зависат од истите. Интерес на Комисијата е да добие колку што е можно посеопфатни информации од земјите-членки за ризиците, заканите и слабостите во секторите каде се означени европски критични инфраструктури, како и информации за меѓусекторските зависности и преземените чекори за намалување на ризиците, заканите и слабостите, со цел да се разработат соодветни предлози за заштита на набљудуваните инфраструктури.

После тоа, во означените европски критични инфраструктури, неопходно е да се утврдат безбедносни планови за операторите на критични инфраструктури или соодветни документи кои вклучуваат идентификација на важните средства, процена на ризикот и селекција и приоретизација на противмерките и постапките за заштита на тие средства. За да се избегне непотребен напор и удвојување на документи, секоја земја- членка треба прво да утврди дали сопствениците или операторите на одредени европска критични инфраструктури веќе имаат воспоставено безбедносни планови за операторите или други еквивалентни документи. Таму каде што постојат такви планови, неопходно е истите да се анализираат и да се увиди дали тие треба да се надоградат, додека, пак, таму каде што не постојат, секоја земја-членка треба да ги преземе неопходните мерки за да обезбеди нивно воспоставување.

Следната важна одредба се однесува на назначувањето офицер за врски за безбедност. Државата треба да овозможи секој сопственик или оператор да назначи безбедносен координатор во рамките на европската критична инфраструктура или офицер за врски задолжен за безбедносни работи. Споменатиот претставува важна хоризонтална и вертикална врска меѓу елементите на системот на критични инфраструктури, како и лице за контакт со законодавецот и другите критични инфраструктури. Понатаму, државата треба

да назначи национална контакт-точка која ќе биде одговорна за соработка со Комисијата, другите држави, како и со сопствениците или операторите на европските критични инфраструктури означени на нејзината територија.

Директивата 2008/114/ЕЗ понуди голем број практични решенија кои, покрај регулаторните обврски од областа на заштитата на европската критична инфраструктура, им служат на државите за разработување внатрешни процеси поврзани со заштитата на нивните национални критични инфраструктури. Пример за ова е воспоставувањето на законодавната рамка во Република Хрватска каде законодавецот во голема мера одлучи целосно да го следи духот и содржината на *Директивата 2008/114/ЕЗ* при изготвувањето на *Законот за критична инфраструктура*.

По усвојувањето на *Директивата 2008/114/ЕЗ*, земјите-членки се соочија со предизвикот да ги прилагодат националните рамки или за прв пат да воспостават цел пакет на програми поврзани со заштитата на критичната инфраструктура. Некои извори кои беа консултирани во целите на овој труд (Лазари и Симончини, Хемерли и Ренда) сметаат дека по усвојувањето на *Директивата 2008/114/ЕЗ*, недостасуваа следните чекори што ги бара Комисијата за развој на областа и постоеше вакуум во кој, повеќе или помалку, членките беа оставени самите на себе. Иако *Директивата 2008/114/ЕЗ* содржи јасни одредби, следењето на нејзината примена во националното законодавство изостанува. Алесандро Лазари и Марта Симончини посочуваат дека иако *Директивата 2008/114/ЕЗ* е транспонирана во националните законодавства на секоја од 28-те земји членки на Унијата во форма на: „измени и дополнувања на постојните закони и подзаконски акти (4 држави); нови закони (9 држави); резолуции (4 држави); процедурални промени во постојните активности за заштита на критичната инфраструктура (3 држави); извршни укази и уредби (8 држави)", не во сите земји е транспониран духот на Директивата на потребниот начин (Лазари и Симончини, 2014: 13). По усвојувањето на *Директивата 2008/114/ЕЗ*, Комисијата немаше јасна цел како да го води и обликува процесот. Недостасуваше кохезивен фактор со кој Комисијата треба да им овозможи на земјите-членки да ги усвојат стандардите на што е можно подобар начин и да ги спроведат одредбите од *Директивата 2008/114/ЕЗ* во потребниот дух (Хемерли и Ренда, 2010). Истите автори (2010: 7) понатаму сметаат дека, дури и години по усвојувањето на *Директивата 2008/114/ЕЗ,* „земјите членки на ЕУ сè уште ги следат фрагментираните политики за заштита на критичната (информатичка) инфраструктура и сè уште постои значаен недостаток на соработка помеѓу националните влади и институциите на ЕУ во воспоставувањето координиран одговор за итни случаи на потенцијални закани ".

Директивата 2008/114/ЕЗ треба да се согледува според обемот и времето кога е донесена. Секако, таа претставуваше огромен чекор напред, но јасно е дека не можеше да одговори на сите барања за целосно регулирање на областа на идентификација, означување и заштита на европската критична инфраструктура. Во исто време, таа требаше делумно да ги израмни веќе развиените национални политики на со оние на земјите кои не обрнуваа доволно внимание на оваа област или тукушто започнаа, под нејзино влијание, да ја регулираат оваа област. *Директивата 2008/114/ЕЗ* првично беше искористена

за да ги води земјите-членки во меѓусебната соработка и директно како пример за тоа како тие можат да ја воспостават и организираат националната рамка за идентификација и означување на критичните инфраструктури, но и индиректно за нивната заштита. Понатаму, земјите-членки треба да ја развијат оваа област со помош на Комисијата, наместо таа да ја игра главната улога. Илустрација на горенаведеното може да биде кратката анализа на три земји: Италија, Романија и Хрватска - и како тие одговориле во раните години по усвојувањето на *Директивата 2008/114/ЕЗ*. Италија не го препозна духот на *Директивата 2008/114/ЕЗ*, ниту пак ја искористи можноста за зајакнување на транспарентноста, како и ефективноста на соработката во заштитата на критичната инфраструктура и не ги дефинираше јасно обврските и одговорностите на сопствениците или операторите на критичните инфраструктури во рамките на земјата. Романија, пак, го препозна духот на *Директивата 2008/114/ЕЗ* и го уреди своето законодавство во согласност со одредбите од *Директивата 2008/114/ЕЗ*. Воспостави процеси, изгради систем за заштита на критичната инфраструктура, разработи функционални форми на поддршка на јавните институции и за сопствениците или операторите на критични инфраструктури во вршењето на нивните задачи, и сето тоа функционира и во практика во државата (Лазари и Симончини, 2014). Хрватска воспостави нормативна рамка во согласност со *Директивата 2008/114/ЕЗ*, изгради системска архитектура и назначи офицери за врска за безбедност во надлежните органи на централната државна управа и со години инвестираше во напорите за воспоставување национални критични инфраструктури, едукација на Офицерите за врска за безбедност, оствари средби со Словенија и Унгарија за воспоставување на европска критична инфраструктура и спроведе проект кој беше финансиран од ЕУ под наслов РЕЦИПЕ 2015, кој имаше цел да ги доразвие започнатите активности за изградба на споменатиот систем за заштита на критичната инфраструктура. Сепак, бидејќи ништо од овие напори не даде конкретни резултати, по неколку години се случи целосно замирање на процесот. За да се избегне недоразбирање, овој коментар ги согледува активностите на наведените три земји по донесувањето на *Директивата 2008/114/ЕЗ* во однос на обврската за нејзино спроведување во националните законодавства и е заснован на анализата на напорите ко треите земји ги презедоа во текот на неколку години, т.е. до 2014 година во случајот на Италија и Романија и до 2015 година на Хрватска. По овој период, сите три држави спроведоа конкретни активности и резултати, при што најзначајно место во тој поглед зазема Романија.

2.2.2. Директивата 2016/1148 на Европскиот парламент и Советот во врска со мерките за високо заедничко ниво на безбедност на мрежните и информатичките системи низ Унијата

Мрежните и информатичките системи и услуги играат клучна улога во општеството. Нивната сигурност и безбедност се од суштинско значење за економските и општествените активности, а особено за функционирањето на внатрешниот пазар. Обемот, честотата и влијанието на безбедносните инциденти се зголемуваат и претставуваат голема закана за функционирањето на мрежните и информатичките системи. Овие системи исто така може да станат

цел на намерни штетни активности насочени кон оштетување или прекинување на работата на системите. Ваквите инциденти можат да го попречат извршувањето на економски активности, да создадат значителни финансиски загуби, да ја поткопаат довербата на корисниците и да предизвикаат голема штета на економијата на Унијата (Европски парламент и Совет, 2016: 2). Затоа беше донесена *Директивата за МИС* за да ги поврзе клучните области, чинители и процеси, а со цел да се зголеми нивото на заштита и воведување на минимум заеднички стандарди во оваа област.

Директивата за МИС опфаќа две групи на актери: оператори на суштински услуги и даватели на дигитални услуги. Под оператори на суштински услуги се подразбираат оние кои обезбедуваат клучни услуги за општеството или економијата на земјата во следниве седум сектори: енергетика, транспорт, банкарство, финансиски пазар, здравство, снабдување и дистрибуција на вода за пиење и дигитална инфраструктура. Давателите на дигитални услуги се сметаат дека се од општо значење кога станува збор за сајбер-безбедност и меѓу нив се вбројуваат даватели на услуги во следниве три сектори: пазари, клауд-услуги и интернет-пребарувачи.

Основна цел на *Директивата за МИС* е да обезбеди заедничко ниво на безбедност на мрежните и информатичките системи во сите земји-членки, чии неправилности предизвикани од безбедносни инциденти може да имаат силни последици врз општеството или економијата на земјата. Притоа, *Директивата за МИС* воведува регулаторни елементи кои овозможуваат трајно следење на состојбата со автоматизацијата и дигитализацијата во одбележаните сектори. Покрај тоа, таа воведува обврска за спроведување на технички и организациски мерки за управување со ризици и мерки за спречување и минимизирање на ефектите од инциденти во безбедноста на мрежните и информатичките системи, воведувајќи и обврска за известување за инциденти кои можат да имаат значителни ефекти врз континуитетот во давањето услуги.

Споредувајќи ја *Директивата за МИС* со *Директивата 2008/114/ЕЗ*, неопходно е да се потенцираат неколку важни прашања. Можеме да кажеме дека *Директивата за МИС* е разработена како одговор на потребата да се надополни нормативната рамка, земајќи ги предвид недостатокот на соодветна заштита на критичната инфраструктура и активности во секторите информатичка и комуникациска технологија. *Директивата 2008/114/ЕЗ* првенствено се фокусира на секторите енергија и транспорт, но исто така ја потенцира потребата да се земат предвид и другите значајни сектори, како што се информатичките и комуникациските технологии. Потоа, операторите на критична инфраструктура и операторите на суштински услуги не мора да се совпаѓаат, но постои голема веројатност тие да се преклопуваат во многу случаи. *Директивата 2008/114/ЕЗ* повеќе се фокусира на средствата, додека *Директивата за МИС* на услугите. Главната цел на *Директивата 2008/114/ЕЗ* е ограничена на зајакнување на безбедноста на конкретни критични инфраструктури коишто се важни за ЕУ како целина, додека главната цел на *Директивата за МИС,* од друга страна, е зајакнување на безбедноста на земјите-членки на ЕУ преку безбедносна соработката меѓу ЕУ и земјите-членки.

2.3. Активности за соработка во рамките на Европската унија

Работната група за критична инфраструктура на Центарот за европски студии за политики смета дека, иако Комисијата усвои бројни иницијативи за политики во оваа област, остануваат голем број на нагласени проблеми. „Прво, земјите-членки имаат различен степен на зрелост во однос на развојот на сеопфатна и ефективна политика за ЗКИ. Второ, постојат изолирани случаи на соработка низ земјите-членки на ЕУ, но нема целосен концепт на работење на ниво на ЕУ. Трето, партнерствата и односите се распрскани низ државите (секоја поединечна земја има и ќе продолжи да одржува единствени односи со операторите и сопствениците од приватниот сектор и глобалните компании кои ги овластуваат). Четврто, критичната инфраструктура на ЕУ е исто така распрскана низ многу различни земји" (Хемерли и Ренда, 2010: 3). Треба да се напомене дека некои од споменатите предизвици веќе се разрешени, но други сè уште опстојуваат.

Предизвици секако дека постојат, бидејќи тие се присутни во секое деловно опкружување и процес. Тие се составен дел од деловните активности, соработката, размената на знаења, како и од воспоставувањето нови системи и унапредувањето на постојните. Динамичниот свет во кој живееме е таков што очекува брз напредок во сите области и активности со кои се занимаваме. Но, реалноста на усогласување на мозаикот што го нарекуваме европска критична инфраструктура и која е исткаена од мноштво различни чинители со повеќе улоги, физички и виртуелни структури, големи количини на информатичко-технолошки решенија (кои застаруваат уште пред повеќето луѓе да научат како функционираат), застрашувачки количини на информации кои треба да се складираат, заштитат и анализираат, различни нивоа на регулација, како и безброј сфери на влијание и интерес, а со што можеме со сигурност да кажеме дека истиот претставува „жив организам" кој постојано се менува, расте и „цица" нови количини на информации, технологија, сензори и финансии, па сè до луѓе и кој не можеме да го ставиме во „рамка" и да очекуваме брзи решенија. Таквиот организам едноставно не подлежи на мерливост или управување со целиот негов обем, но пристапот кон него треба да се заснова на анализа на одделни делови, нивниот севкупен придонес и управувањето со споменатите.

Според тоа, ниту една институција на Унијата не може едноставно да биде конкретно прозвана дека не вложила повеќе напори во развојот на областа на заштита на критичната инфраструктура. На крајот на краиштата, сè е резултат на работата на луѓето кои работат на позиции во критичната инфраструктура и нивната продуктивност. Сведоци сме на различни активности кои се спроведоа на ниво на Унијата или во рамките на поедниечните земји-членки, каде постигнатото беше недоволно за постигнување на предвидените цели, непроизведувајќи резултати и напредок. Сето ова е составен дел од животот и дава увид во животните приоритети на луѓето. Така, при анализата на досегашните постигнувања во развојот на подрачјето на заштита на критичната инфраструктура, потребно е да се разгледаат антрополошките, културните, организациските и другите фактори поврзани со единствената околина, поединечните организации, држави и сектори, но и да се согледа зошто некои

средини се поуспешни од другите. Наша цел не е да ги браниме институциите на ЕУ, туку да ги покажеме нивните главни активности во оваа област, што, пак, потоа сведочи за многуте пропуштени можности од страна на корисниците без оглед дали истите се држави, сопственици или оператори на критична инфраструктура, регулаторни агенции, научната заедница или поединци. Унијата ја развива оваа област со голема транспарентност, при што секој има можност да добие информации и да биде дел од активностите, но прашање е дали донел таква одлука.

За да ги поддржи земјите-членки, Комисијата основаше и свој Заеднички центар за истражување, кој во 2008 година изготви документ под наслов *Необврзувачки упатства за примена на Директивата на Советот за идентификација и означување на европски критични инфраструктури и процена на потребата за подобрување на нивната заштита*. Документот има за цел да им помогне на земјите-членки во правилната примена на техничките одредби за утврдување на европските критични инфраструктури (Лазари, 2014: 52). Тој е насочен кон она што претставува најголем предизвик за сите земји-членки кога тие првпат ќе го започнат процесот на идентификација и означување на критичните инфраструктури и претставува подробно објаснување за правилната примена на секторските и вкрстените критериуми. Се предлага да се користат следните четири различни критериуми или услови за кумулативно следење на секторските критериуми:

1. Препишување конкретни својства (според неопходноста за функционирањето на целиот систем, сектор или организација).
2. Идентификација на мрежите во кои мора ќе се означат „клучните елементи" (според потенцијалните негативни ефекти што можат да се појават во земјите- членки).
3. Директно именување конкретни инфраструктурни средства.
4. Овозможување на земја-членка директно да идентификува средство (во случаи кога не постојат секторски критериуми) (Заеднички центар за истражување, 2008: 23-24).

Горенаведените критериуми или услови претставуваат, како што се вели во насловот на документот, необврзувачки насоки кои треба да им ја олеснат работата на земјите-членки кои прв пат започнуваат таква постапка. Доколку државите веќе имаат развиено критериуми за подобар квалитет, тие дефинитивно треба истите и да ги користат, а во документот се предлагаат идеи од кои може да се започне. Во толкувањето на вкрстените критериуми (такви критериуми се: а) критериум жртви; б) критериум економски ефекти; в) критериум јавни ефекти) даден е детален опис на квалификацијата и квантификацијата на горенаведените критериуми и се дава исклучително важното објаснување дека е доволно да се задоволи само еден од трите критериуми за да се исполнат условите за примена на вкрстените критериуми (четвртиот чекор се смета дека е исполнет со утврдувањето на европската критична инфраструктура) (Заеднички истражувачки центар, 2008: 25-35).

Понатаму, Комисијата се концентрираше на развој на различни платформи за соработка помеѓу земјите-членки, сопствениците или операторите на

критични инфраструктури и заинтересираните експерти. Една конкретна мерка во таа насока е одржувањето состаноци меѓу националните точки за контакт во рамките на официјалниот формат на Европската комисија, кој обично се организира двапати годишно. На овие состаноци земјите-членки имаат можност да разменуваат најдобри практики и достигнувања во сите фази на заштита на националната и европската критична инфраструктура. Во рамките на овој процес, Комисијата игра улога на организатор и модератор, ги плаќа трошоците за сите национални точки за контакт, подготвува материјали за состаноците, ги претставува најновите релевантни резултати од разни програми и проекти, поддржува иницијативи и, што е најважно, им овозможува на земјите-членки да соработуваат. Колку е успешна оваа соработка и сè што им е овозможено на земјите-членки зависи од бројните фактори врз кои Комисијата нема директно влијание, меѓу кои се вбројуваат некои од следните: какво значење се дава на конкретниот процес кој е посочен во националната рамка, како националните контактни точки го разбираат и прифаќаат процесот, квалитетот на соработката меѓу безбедносните координатори во националната рамка и слично.

Покрај оваа формална мрежа, Комисијата силно ги охрабрува земјите-членки да учествуваат со нивни претставници во неформалната мрежа на експерти во рамките на Европската референтна мрежа за заштита на критична инфраструктура (ЕРМЗКИ). Мрежата има цел да обезбеди рамка во која истражувачките капацитети и лабораториите споделуваат знаења и експертиза со цел усогласување на протоколите за тестирање низ цела Европа, што доведува до подобра заштита на критичната инфраструктура од сите видови закани и опасности и создавање на единствен пазар за безбедносни решенија. Во моментов, во рамките на споменатото, работата се одвива во дванаесет работни групи, од кои сите имаат должност постојано да ги испитуваат и подобруваат бројните стандарди и процедури во критичната заштита на инфраструктурата (Заеднички центар за истражување, 2017 година). Мрежата претставува вистинско извориште на научна извонредност кој објавува многу значајни студии, организира едукации, развива нови програми и обезбедува поддршка за сите заинтересирани. Иако претставува добар извор на знаење и потенцијална соработка, изненадувачки е што само нешто повеќе од половина од земјите-членки активно учествуваат преку нивните претставници на работни состаноци, а само мал дел од нив активно соработуваат. Ова може да се поврзе со претходниот исказ во врска со факторите за соработка на кои Комисијата нема директно влијание, а исто така влијание врз ова има и индивидуалното разбирање на важноста од инвестирањето во знаење и истражувања. Со оглед на ова, можеме многу лесно да заклучиме дека државите кои и онака инвестираат во истражување и развој се активни и во овој дел, додека други остануваат пасивни набљудувачи.

Следната значајна можност што Европската комисија им ја обезбедува на сите заинтересирани актери во областа на заштита на критичната инфраструктура се проектите. Преку програмата *Превенција, подготвеност и управување со последиците од тероризам и други ризици поврзани со безбедноста*, во периодот 2007-2012 година беа кофинансирани 111 проекти (70 ди-

ректно поврзани со заштитата на критичната инфраструктура, 32 поврзани со управување со кризи и 9 мешани) со издвоени вкупно 45 милиони евра во тие цели. Проектите имаа многу широко опсег и ги опфатија сите сектори во кои може да се идентификува критична инфраструктура. Нивната главна цел е: да се обезбеди подобрување на знаењето, подобро разбирање на функционирањето на критичната инфраструктура на сите нивоа, давање препораки за јавните политики и обезбедување на научна основа за тековните и идните истражувања. Меѓу некои од областите во кои беа понудени пректи се вбројуваа: анализа на секторски и меѓусекторски критериуми и одредници, дефинирање на различни методологии за процена на меѓузависноста помеѓу критичните инфраструктури; изготвување на упатства за најдобри практики за креаторите на јавните политики во заштитата на критичната инфраструктура; модели за размена на најдобри практики за ефективна заштита на критичната инфраструктура; режими на размена на податоци и алармни системи; развој на симулациски модели и алатки за критериуми за следење (Европска комисија, 2013: 6). По овој период, Комисијата продолжи да инвестира во проекти што им овозможуваат на сите заинтересирани кофинансирање на најголем дел од трошоците за проектот и, што е најважно, да го пренесуваат потребното знаење и технологија. Неодамнешните податоци покажуваат дека вкупно 140 милиони евра се инвестирани во оперативна соработка и активности во периодот 2007-2013 година, при што досега се финансирани повеќе од 120 проекти (Енгдал, 2016: 4). Повторно, како и во претходните случаи, колку некој ги користи горенаведените опции зависи само од крајниот корисник. Комисијата ја поддржува секоја добра идеја.

Следниот важен чекор за воспоставување соработка и размена на знаење и искуство на европско ниво беше разработката и започнувањето на Информативна мрежа за предупредување за критична инфраструктура (ИМПКИ). Ова веќе беше објавено во *Зелената книга за Европската програма за заштита на критична инфраструктура во 2005 година*, а беше обликувано постепено применувајќи модуларен пристап и влезе во функција во јануари 2013 година. Целта на мрежата е размена на информации за стратегии и мерки за намалување на ризикот при заштита на критичната инфраструктура. Развиена е како заштитена веб-платформа на Европската комисија за сите заинтересирани експерти од земјите-членки на ЕУ кои се занимаваат со областа на критичната инфраструктура. Одобрувањето пристап до мрежата е многу едноставно и овозможува бројни услуги како преглед на нормативните решенија, студии, најдобри практики и контакти со други експерти. Како и во претходните случаи, Комисијата обезбеди платформа за соработка и оние кои се заинтересирани можат да ги користат горенаведените опции.

Ова се само дел од активностите на Комисијата за создавање претпоставки и поврзување на различни фактори во системот на заштита на критичната инфраструктура. Голем дел од овие активности навистина постојат и продолжуваат да се одвиваат, но сметаме дека овде ги посочивме токму поважните и во доволна мера ја прикажавме работата на Комисијата во оваа област.

Исто така, Комисијата го призна застојот во нормативната област на процесот на развој на подрачјето за идентификација и означување на европските

критични инфраструктури, како и во соработкат меѓу земјите-членки, а во 2012 година започна да врши еден вид ревизија на претходните активности и да изготвува работен документ посветен на новиот пристап во заштитата на критичната инфраструктура. Кон средината на 2013 година, Комисијата го презентираше *Работниот документ на персоналот при Комисијата за Европската програма за заштита на критична инфраструктура: Како да ги направиме европските критични инфраструктури посигурни*. Горенаведената е ажурирана верзија на *Европската програма* која беше првично усвоена во 2006 година. Во неа се разгледани досегашните решенија, презентиран е нов преглед на начините и моделите за тоа како да продолжи да се развива оваа област, вклучувајќи и неколку податоци меѓу кои е и тој дека се означени помалку од 20 европски критични инфраструктури и меѓу нив не е главната мрежа за дистрибуција на енергија (Европска комисија, 2013). До 2016 година, определени се вкупно 89 европски критични инфраструктури (Енгдал, 2016: 3). Најновите податоци од почетокот на 2019 година велат дека во моментов, вкупниот број на европски означени критични инфраструктури изнесува 92.

Работниот документ претставува нов поглед кон попрактичното спроведување на *Европската програма за заштита на критична инфраструктура*, дава анализа на елементите на тековната програма и предлага трансформација на пристапот кон заштитата на европската критична инфраструктура заснована врз спроведување на практични активности во областа на превенција, подготвеност и одговор. Дел од новиот пристап е да се разгледа меѓузависноста помеѓу критичната инфраструктура, индустријата и државните субјекти, бидејќи се забележува дека меѓусебната зависност досега не била доволно согледувана. Имајќи предвид дека многу од критичните инфраструктури се во приватна сопственост, документот го потврди ставот дека е потребна подобра соработка со приватниот сектор и развој на јавно-приватно структуриран дијалог.

Дополнително се истакнуваат четири приоритетни области на европскиот критички модел за заштита на инфраструктурата, кои треба дополнително да се разработат: 1. Постапки за идентификација и означување на европски критични инфраструктури и процена на потребата за подобрување на нивната заштита; 2. Мерки изработени да помогнат во имплементацијата на *Европската програма за заштита на критична инфраструктура*, вклучително и Акциски план, воспоставување на *Информативна мрежа за предупредување за критична инфраструктура* (ИМПКИ), употреба на експертски групи за заштита на критичната инфраструктура на ниво на Унијата, размена на информации, идентификација и анализа на меѓузависноста; 3. Финансирање на мерки поврзани со заштита на критичната инфраструктура и проекти поврзани со специјалната програма за *Превенција, подготвеност и управување со последиците од тероризмот и другите ризици поврзани со безбедноста*; 4. Развој на надворешната димензија на *Европската програма за заштита на критична инфраструктура* (Европската комисија, 2013).

На тој начин, применувајќи еден нов пристап, Комисијата се обидува да ја подобри заштитата на критичната инфраструктура низ целата Унија, да го постави целиот процес на повисоко ниво и да создаде платформа за споделу-

вање информации и најдобри практики преку назначување експертски групи за секој сектор. Во новиот пристап беше поставен пилот-проект за *Европската програма за заштита на критична инфраструктура* која ја разгледува меѓузависноста помеѓу различните критични инфраструктури од значење за Европа и како такви ги означува следниве: „Еуроконтрол", „Галилео", мрежа за пренос на електрична енергија и мрежа за дистрибуција на гас. Овие системи се избрани заради нивното значење за Европската унија и со цел да се оптимизира нивната заштита и отпорност (Европска комисија, 2013). Целта на проектот е да се покаже дека Европската комисија самостојно ќе спроведе анализа на меѓузависноста на овие системи, кое, пак, треба да им помогне на земјите членки во нивната работа. Проектот е одложен неколку пати од неговиот почеток и сè уште не е завршен.

Во моментов, клучна активност која се спроведува во последните неколку години на иницијатива на Комисијата е ревизијата на *Директивата 2008/114/ЕЗ*. Досега, Комисијата го спроведуваше ваквото оценување за да ја провери ефикасноста на Директивата во постигнувањето на целите (идентификација и означување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита); нејзината релевантност со оглед на тековните и идни предизвици за критичните инфраструктури и колку таа е кохерентна и комплементарна во однос на ЕУ и националните политики во областите од интерес (енергетика и транспортни сектори), т.е. која е нејзината додадена вредност во таа смисла. Евалуацијата исто така дава препораки за тоа како да се подобри операционализацијата на национално ниво истовремено задржувајќи го стратешкиот фокус, како и следењето, синергијата на национално ниво (секторско законодавство), размената на информации, соработката со трети земји и др. Во текот на неколкумесечна подготовка за вршење на евалуацијата, во ноември 2018 година, земјите-членки, заедно со оператори и сопственици на критични инфраструктури, одржаа работилница во Брисел на која, во рамките на една студија на конкретен случај, беше извршена симулација на процесот за идентификација и означување на европската критична инфраструктура која се спроведува во согласност со *Директивата 2008/114/ЕЗ*. Беа изработени голем број на прашалници за имплементацијата (за идентификуваните и означените европски критични инфраструктури, ризиците, заканите и ранливостите на секторите на европските критични инфраструктури, итн.) со цел да се добијат што е можно повеќе информации од сите засегнати страни кои се клучни за спроведувањето на *Директивата 2008/114/ЕЗ*. Како краен производ, евалуацијата овозможи препознавање на предизвиците во спроведувањето, најдобрите практики кај одделните земји-членки и истакна заклучоци и препораки кои се помесетени во нејзиниот конечен и многу сеопфатен документ (90 страници со 500 страници во прилози). Врз основа на оваа процена, ќе се утврдува што ќе се случи со *Директивата 2008/114/ЕЗ* во следната фаза, т.е. дали таа ќе претрпи измени или ќе се создаде целосно нов документ (за чиј формат ќе се решава понатаму) кој целосно ќе ја замени (Цезарец, 2019).

Заклучок

Заштитата на критичната инфраструктура во Европската унија е сложен и динамичен процес кој се одвива на дневна основа на мноштво различни нивоа и аспекти. Во него главни актери и иницијатори се државите и одделните институции на Европската унија, иако некои сопственици или оператори на критични инфраструктури поседуваат поголеми знаења и способности за тоа од наведените. Ова е логично затоа што тие ја претставуваат суштината на системот и најдобро ги знаат своите специфики, ризици, секторска логика и начини на согледување на нештата. Покрај горенаведеното, експертите од областа на заштита на критичната инфраструктура сè повеќе се профилираат и преку нивните интердисциплинарни знаења и вештини додаваат нова вредност на системот.

Ова поглавје имаше цел да го претстави историскиот пресек на индивидуалните активности на неколку држави кои пред доаѓањето на иницијатива за тоа на ниво на ЕУ први започнаа да се справуваат со прашањето на заштитата на нивната критична инфраструктура. Она што беше потребно за понатаму беше сето тоа да се усогласи со напорите на институциите на ЕУ да ја стандардизираат заедничката област, да им помагаат на земјите-членки во нивните предизвици, да започнат да ги разгледуваат местото и улогата на европските критични инфраструктури и јасно да ја реализираат својата видливост и препознаеност во оваа област.

Во овој труд се прикажани и анализирани главните нормативни решенија и предлози на институциите на Унијата во оваа област. Унијата направи многу во развојот на оваа област и причините зошто одредени процеси не се одвивале побрзо и поефикасно можеме да му се припишат на човечкиот фактор, и тоа пред сè во земјите- членки, наместо во институциите на Унијата. Како што побараа од неа земјите-членки, Унијата вложи силни напори на овој план и тргна во потрага по нови и подобри решенија. Без да се обидуваме да бидеме критични, направено е навистина многу, но, исто така, пропуштени се некои некои убави можности во тој поглед. Сепак, ова е динамична и крајно интерактивна област која ќе добива сè поголем простор и време во сите сфери на политичката, општествената и безбедносната активност, имајќи предвид дека секој ден сè повеќе и повеќе зависиме од ефективното функционирање на критичните инфраструктури.

ГЛАВА 3

НАТО И ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Глава 3

НАТО И ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Проф. д-р Тони МИЛЕСКИ
Универзитет „Св. Кирил и Методиј" – Скопје
Филозофски факултет, Институт за безбедност, одбрана и мир

Пристапот и придонесот на НАТО во заштитата на критичната инфраструктура сè уште претставува тема на бројни политички дебати и научни анализи. Иако комплексната улога на НАТО после распадот на биполарниот светски поредок е главна карактеристика во годините потоа, можеме да констатираме дека со неговата еволуција, еволуираат и дискурсите на неговиот интерес. Евидентно е дека обидите за политизација и секуритизација на енергетското снабдување, вклученоста и улогата на НАТО на полето на енергетската безбедност и заштитата на критичната инфраструктура отвораат широк спектар насоки за улогота на НАТО.

Она што веднаш треба да се напомене, а воедно ја профилира структурата и карактерот на Алијансата во постстуденовоениот период е Коминикето од Самитот во Рига каде се стави посебен акцент на заштитата на енергетската инфраструктура како дел од енергетската безбедност. Во оваа насока, важно е да се напомене дека НАТО поседува и оперира со значителни стратегиски средства и тоа 10 различни цевководи за транспорт на авионско гориво кои се во должина од 12.000 км, кои минуваат низ 12 земји на НАТО и поврзуваат складишни депоа, воздушни бази, цивилни аеродроми, бензински пумпи, рафинерии и пристаништа, вклучувајќи го тука и најголемиот гасоводен систем на НАТО, Централноевропскиот цевководен систем (CEPS). НАТО веќе четири децении управува со CEPS и водејќи се од комерцијални и бизнис интереси, истиот се изнајмува за индустриски цели и обезбедување на авионско гориво за големите комерцијални аеродроми во Европа. Преку CEPS се добива целото авионско гориво за потребите на авиокомпаниите на бриселскиот аеродром, како и најголем дел од горивото за аеродромите во Франкфурт (Германија) и Шипхол (Холандија). Сеќавањата од Втората светска војна сè уште биле многу свежи кога започнала изградбата на CEPS и тој бил дизајниран да издржи и најсурови воени услови, има бројни пумпни станици, зајакнат е на критичните места, има вкопани цевководи, а на располагање стојат и тимови за итни реакции и поправки. Во услови на засилен дијалог помеѓу евроатлантските партнери за безбедноста на енергенсите и нивните транспортни системи, НАТО има навистина многу да понуди (Bell, G.R., 2009: 268).

Следејќи ги овие неспорни факти, во ова поглавје, преку критичка анализа на еден сегмент од вклученоста и улогата на НАТО во заштитата на критичната инфраструктура ќе се обидеме да одговориме на неколку значајни прашања. Едно од нив е дали НАТО прави прекумерна секуритизација и милитаризација

на енергетскиот сектор, кој доминантно се поима како исклучително економско прашање и дали постои соодветна улога и можност за вклучување на НАТО во заштитата на критичната инфраструктура во рамките на стратегиските концепти, особено по завршувањето на Студената војна.

3.1. Стратегиска рамка на концептот за заштита на критичната инфраструктура

Генерално можеме да се согласиме дека НАТО ги регулира и строго ги заштитува своите критични инфраструктури уште од своето основање. Според основачкиот документот на Алијансата, постојат неколку можни сценарија во кои НАТО треба да има улога во заштитата на критичната инфраструктура. Прво, поддршка на воените операции на Алијансата во рамки на одредбата од Членот 5. Второ, поддршка на операциите за одговор на криза надвор од одредбата во Членот 5. Трето, поддршка на националните авторитети во вонредни состојби од невоен карактер. Четврто, поддршка на националните авторитети во заштитата на нивното население од последиците на оружјето за масовно уништување. И петто, ко-партнерство со партнерите во полето на цивилното планирање за итни ситуации. (Babos, 2016).

Според Протоколот креиран во периодот на Студената војна, НАТО обезбедува сигурност на критичната инфраструктура на Алијансата и на нејзините земји-членки. Во насока на обезбедување координиран пристап за цивилно планирање на итни ситуации, клучната улога му е доделена на Високиот комитет за цивилно планирање на итни ситуации, кој директно го известува Северноатлантскиот совет.

Цивилното планирање на итни ситуации е важна активност во процесот на предвидување и е насочена кон координирање на националните ресурси. Во контекст на природните и од човек предизвикани катастрофи, договорите ја зацврстуваат улогата на НАТО во итните ситуации. Како примери можат да се напоменат „НАТО политиката за асистенција при несреќи во мирни услови" ("NATO Policy on Disaster Assistance in Peace Time") од 9 мај 1995 година или изјавата „Подобрена практична соработка во полето за помош при катастрофи" ("Enhanced Practical Cooperation in the field of Disaster Relief") од 29 мај 1998 година. Покрај тоа, Стратегискиот концепт на НАТО од 1999 година ги признава големите катастрофи како извор на загриженост за безбедноста и стабилноста.

Терминот „заштита на критичната инфраструктура" – според Директивата на Клинтон од 1998 година, а по терористичкиот акт од 11 септмеври 2001 година, веднаш бил ставен на дневниот ред на Северноатлантскиот совет. По нападите од 11 септември 2001 година, НАТО-самитот во Прага го иницираше „Акциониот план за вонредни состојби". Конкретно во Членот 4, точка б од Декларацијата за одржаниот самит стои: „...ние сме посветени, во соработка со нашите партнери, целосно да го имплементираме Акциониот план за планирање на вонредни состојби за подобрување на граѓанската подготвеност против можни напади врз цивилното население со хемиски, биолошки или радиолошки агенси. Ние ќе ја зголемиме нашата способност да обезбедиме

поддршка, кога тоа ќе биде побарано, да им помогнеме на националните власти да се справат со последиците од терористичките напади, вклучувајќи ги и нападите со хемиско, биолошко, радиолошко и нуклеарно оружје на критичната инфраструктура, како што е предвидено во Акциониот план на цивилното планирање на вонредни ситуации". (Prague Summit Declaration, 2002). Покрај тоа, се планирале вежби за тестирање и евентуално подобрување на интероперабилноста. Во исто време, беше објавен и Партнерскиот акционен план против тероризмот.

По 11 септември беше разгледана подготвеноста на земјите-членки на НАТО во сферата на заштитата на критичната инфраструктура. Резултат на таквата активност претставува концепт-документот за заштита на критичната инфраструктура, подготвен од Високиот комитет за цивилно планирање на вонредни ситуации. Главните цели се сумирани во размена на информации помеѓу засегнатите страни, помош и развој на програми за обука и едукација кои придонесуваат кон идентификација на критичната инфраструктура, одредување на истражувања за поддршка на заштитата на критичната инфраструктура и помош во текот на вежбовните активности. Планирачките одбори и комитети на Високиот комитет за цивилно планирање на вонредни ситуации ги започнале неопходните студии. Националните експерти од владите и индустријата, како и воените претставници, координираат планирање на осум технички домени: цивилен воздушен сообраќај, цивилна заштита, безбедност на храна, индустриско производство и логистика, внатрешен копнен транспорт, работи од областа на медицината, испорака, и на крај, цивилни електронски комуникации. Во 2005 година Високиот комитет за цивилно планирање на вонредни ситуации го усвои и прилагоди Акциониот план во насока да ги покрие напорите за време и после терористички напади со хемиско, биолошко, радиолошко и нуклеарно оружје. Планот се фокусирал на заштита на критичната инфраструктура и поддршка на жртвите.

Консеквентно на ова, зголемената активност на европските сојузници на полето на заштитата на критичната инфраструктура е резултат на терористичките напади во Мадрид од 2004 година, сајбер-нападите на Естонија од 2007 година, руско-грузискиот конфликт од 2008 година, пиратските напади кои во континуитет се случуваат од 2008 година во Аденскиот Залив и брегoвите на Сомалија, како и ескалацијата на руско-украинските односи. НАТО, денес, покрај концепциските и стратегиски документи за заштита на критичната инфраструктура, исто така креира и спроведува политика и практики на оперативно ниво (Babos, 2016: 12).

На стратегиско ниво, почетоците на интересот и активностите на НАТО во сферата на заштитата на критичната инфраструктура датираат уште од 1990 година и Самитот на НАТО одржан во Лондон. Како резултат на насоките дадени на Лондонскиот самит се креира нов стратегискиот концепт на НАТО во 1991 година. Во овој стратегиски документ, Алијансата започнува со промовирање на безбедноста на критичната инфраструктур поврзана со енергетските витални ресурси. Имено, според Стратегискиот концепт на НАТО од 1991 година, нарушувањето на протокот на виталните ресурси е дефиниран како потенцијална безбедносна закана по интересите на Алијансата (Параграф 12)

(The Alliance's New Strategic Concept, 1991). Истата оваа констатација, Алијансата на Самитот во Вашингтон во 1999 година ја напоменува и во тогаш одобрениот нов стратегискиот концепт (Параграф 24) (The Alliance's Strategic Concept, 1999).

Според содржината на Стратегискиот концепт на НАТО усвоен на Самитот во Лисабон од 2010 година, критичната инфраструктура за прв пат јасно и недвосмислено се напоменува во делот за сајбер-заканите. Во Параграф 12 се потенцира дека сајбер-заканите стануваат сè почести, повеќе организирани и поскапи за штетата што ја предизвикуваа врз владината администрација, бизнис-заедницата, економијата и потенцијално врз транспортот и мрежите за снабдување, како и друга критична инфраструктура. Притоа, се потенцира дека сајбер-заканите достигнуваат праг кој претставува закана на националниот и евроатлантскиот просперитет, безбедност и стабилност. Странските воени иразузанвачки служби, организирани криминални групи, терористи и/или ектремисти, секој може да биде извор на сајбер-напади.

Во Параграфот број 19 од Стратегискиот концепт се потенцира заложбата за развивање на капацитети кои ќе придоенесат за енергетската безбедност, вклучувајќи ја и заштитата на критичната енергетска инфраструктура и транзитните области и правци, соработка со партнерите и консултации меѓу сојузниците врз основа на стратегиски процени и планирање на непредвидени ситуации (Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2010: 11-17).

Стратегиските определби за критичната инфраструктура на НАТО втемелени во неговите стратегиски концепти се одраз на интензивните дебати за енергетската безбедност како предмет околу кој интензивно се дебатира на меѓународно рамниште. Активноста на НАТО во оваа сфера практично датира и пред истата да е вклучена во стратегиските концепти. Имено, за време на Студената војна, Алијансата одржувала и обезбедувала гасоводен систем за снабдување со природен гас на сопствените сили и критичната инфраструктура во Европа.

Токму овој дискурс ќе ни послужи подетално да ја објасниме комплексната содржина за местото, улогата и вклученоста на НАТО во заштитата на критичната инфраструктура.

3.2. Вклученоста и улогата на Алијансата во заштита на критичната енергетска инфраструктура

Како што претходно напоменавме, проблемите поврзани со енергетската безбедност, вклучително и заштитата на критичната инфраструктура, од поодамна не претставуваат базични тематски содржини единствено на економските форуми. Тоа значи дека овие теми сè повеќе претставуваат главни содржини во рамките на меѓународните политички средби на највисоко ниво. Трговската размена на основните енергетски ресурси не претставува само само економско прашање, туку сè повеќе станува и политичко прашање. Уште повеќе, имајќи предвид дека НАТО како воено-политичка алијанса сè повеќе во своите работни агенди ја стават редовноста и стабилноста со снабдување на

енергенси, јасно е дека може да се заклучи дека снабдувањето со енергенси и сѐ она што е поврзано со тоа снабдување, претставува тема и на безбедносниот дискурс, но и интерес на НАТО.

Сепак, вклученоста на НАТО во заштитата на критичната инфраструктура има и своја критичка компонента. Истата, ќе се обидеме да ја анализираме преку корпусот на прашања поврзани за енергетската безбедност и енергетската критична инфраструктура.

Можноста за вклучување и улогата на НАТО во сферата на енергетската безбедност има два круцијални момента. Првиот момент има повеќе воено-безбедносен фокус кој ја рефлектира дуалната потреба на Алијансата за спроведување практично и логистичко планирање на заштитата на енергетските резерви, посебно на нафтата, притоа одржувајќи поширока безбедност на нејзините земји-членки и стабилност на сопствената оперативна способност.

Ваквата констатација подразбира разгледување на воените закани на енергетските постројки, како и рутите за снабдување со енергетските ресурси. Можностите за ескалација на заложбите за воспоставување контрола над производителите, транзитните земји во поглед на енергенсите (нафтоводи, гасоводи), како и сопствената безбедност, се релевантни фактори на можните воени конфронтирања. Одредени аналитичари оценуваат дека можноста за пристап кон енергетските ресурси може да стане предмет на големи воени конфронтирања и претставува сериозен проблем во функционирањето на современиот меѓународен систем. Пиратските и терористичките напади го зголемуваат овој ризик.

Според извештај на Обединетите нации во периодот од 2010 до 2014 се укажува дека енергетскиот сектор е исклучително ранлив на терористички напади. Најголемиот број на терористички напади во дадениот период се случиле во Пакистан (439), потоа во Јемен (170), Колумбија (161), Ирак (146), Филипини (73), Индија (42), Нигерија (38), Тајланд (37), Турција (28) и сл. (CTED Trends Reports, 2017: 4-5). Ваквата широка географска дисперзираност на феномените тероризам и енергетска критична инфраструктура, овозможува маритимната енергетска безбедност да има витално значење. Тоа бара ефективно справување со нелегалните активности и прекини на снабдување со енергенси на релативно голем оперативен простор. Познато е дека повеќе од две третини од светот е покриен со солена вода и околу 80% од светската трговија се одвива по воден пат. Она што можеме дс го воочиме како енергетски безбедносен проблем е фактот што најголемиот дел од светските океани не се под државна јурисдикција (Wilson, B., 2012).

Вториот момент за вклучувањето на НАТО во дискусиите за енергетската безбедност повеќе се фокусира на политичкиот притисок и закани за енергетската безбедност. Ваквиот став може да се идентификува и нагласи особено по спорот помеѓу Украина и руската компанија „Газпром". Политички притисок кој се манифестираше со прекин на испораката на гас, на почетокот од 2006 година. Руските авторитети ваквиот чин го објаснувале исклучиво со економски причини. Поскапувањето на цената на чинење на нафтата и гасот за земјите од

поранешниот Советски Сојуз го означиле крајот на ерата во која тие енергенсите ги купувале по пониска цена. На тој начин, официјална Москва настојува дебатата да ја задржи на економски терен, нагласувајќи дека зголемувањето на цената има економско, а не политичко значење. Руските министри за финансии и економија истакнувале дека усогласувањето на руските цени на енергенсите со светските цени до 2011 година претставува еден од условите за прием на Русија во Светската трговска организација. Русија станува членка на СТО во 2012 година (Radoman, J., 2007). Ваквите настани ја стимулираа дискусијата за енергетската безбедност и заштитата на енергетската критична инфраструктура во рамките на НАТО.

Двата момента несомнено резултираа со концептуална разлика во поглед на реализирањето на главната цел. Имено, дилемата е поставена на следното ниво: дали треба Алијансата да усвои поширок „тематски" пристап кон енергетската безбедност и заштитата на енергетската критична инфраструктура, во кој интересите на држава „произведувач", „транзитната" држава и државата „потрошувач" се гледаат ефективно во слично светло — против заканите кои ги поткопуваат интересите на сите, како што е напад на главна снабдувачка рута? Или треба да усвои повеќе регионален и директен пристап, во кој интересите на „произведувачот" и „потрошувачот" се разликуваат - што во основа го носи влијанието на моќна Алијанса во поддршката на земјата „потрошувач" во она што се смета натпреварувачки дијалог на „производител" и „потрошувач"?

Практичната акција на НАТО поврзана со енергетската безбедност датира од 30 јули 2007 година кога флотата составена од шест земји-членки на Алијансата (Данска, САД, Германија, Португалија, Канада и Холандија) се упатиле на долго патување кон Африка. Изјавата на поранешниот генерален секретар на НАТО, Јап де Хоп Шефер, дека висок приоритет на членките на НАТО претставува поморската безбедност, како и овозможување безбедни премини за транспорт на енергенси, ја детерминира појдовната основа на делувањето на Алијансата во контекстот на енергетската безбедност и заштитата на рутите и енергетската критична инфраструктура.

Основната цел на НАТО-мисијата била насочена кон делтата на реката Нигер, каде што криминалните банди ги напаѓале нафтените инсталации и киднапирале работници кои работеле на нафтените платформи. За првпат во историјата на НАТО, заедно со Јужноафриканската морнарица, се реализирани заеднички поморски вежби, кои во месец септември 2007 година се преселија и во опасните води во близина на брегот на Сомалија, каде што нападите на пиратите зачестиле. Намерата на оваа двомесечна мисија била да се покажат способностите на НАТО за примена на воени средства и да се гарантира Законот за отворено море, кој меѓу другото вклучува и заштита на правото на премин на виталните енергетски ресурси (Милески, 2014: 47-48).

Во контекстот на потребата од вклучувањето на Алијансата во енергетската безбедност и заштитата на енергетската критична инфраструктура, особено е важен Самитот во Рига, одржан во ноември 2006 година. Есента 2006 година, НАТО ги правеше последните подготовки за мисијата, а на Самитот во Рига,

сојузниците сè уште беа прилично поделени за тоа дали енергетската безбедност е дел од мисијата на Алијансата. Неколку земји-членки во оваа улога на НАТО препознаа интереси на Европската унија. Но, по една година убедувања, тогашниот генералниот секретар успеал да ја постави енергетската безбедност на агендата на НАТО. Прво, Шефер успеал да го наметне ова прашање на еден неформален состанок помеѓу претставниците на НАТО и министрите за надворешни работи на земјите-членки на Европската унија, а потоа во февруари 2006 година на Минхенската конференција за безбедносна политика, тој ги повторил заложбите за проширување и продлабочување на формалните политичко-безбедносни дискусии во рамките на НАТО за да се опфатат повеќе клучни прашања, притоа несомнено алудирајќи и на енергетската безбедност. Заради продолжување на понатамошните дискусии, челниците на НАТО закажале НАТО-форум за енергетска безбедност во Прага, и го најавиле присуството на голем број премиери, министри за енергетика, високи претставници на НАТО, како и високи претставници од глобалната енергетска заедница (Bell, G.R. 2009: 261-262). По бројните забелешки од неколку сојузнички влади, особено Франција, генералниот секретар се соочил со нови проблеми на кои се надоврзала и забраната за членовите на Меѓународниот штаб на НАТО да одржат презентации на таа конференција. Во тогашното соопштение од НАТО се потенцирало дека НАТО нема формална улога во областа на енергетската безбедност и безбедноста на нафтоводите и гасоводите и дека НАТО не размислува за какво било воено инволвирање за заштита на нафтената и гасната инфраструктура во кавкаскиот или кој било друг регион. Сепак, до Самитот на НАТО во Рига, залагањата на САД, како и засегнатоста на Европа од руското користење на гасот и нафтата како инструмент за политичко влијание, јасно ставиле до знаење дека енергетската безбедност повеќе не може да биде игнорирана од страна на НАТО. Во документот усвоен на Самитот, насловен како „Сеопфатно политичко лидерство", лидерите на НАТО посочуваат дека нарушувањето на нормалното движење на виталните ресурси ќе претставува една од главните закани за Алијансата во наредните 10 до 15 години. Благодарение на залагањата на генералниот секретар на НАТО, донесен е консензус имплементиран во Декларацијата од Самитот на НАТО во Рига.

Декларацијата од Рига претставува значајна почетна точка за каква било анализа за улогата на НАТО во рамките на енергетската безбедност и заштитата на енергетската критична инфраструктура. Имено, во Членот 45 од Декларацијата се наведува дека безбедносните интереси на НАТО можат да бидат погодени со прекин на протокот на виталните ресурси. Алијансата ги поддржува координираните меѓународни напори за процена на ризиците за енергетската инфраструктура и промовирањето на безбедност на енергетската инфраструктурна. Идивидуалниот ангажман на државите-членки на НАТО е идентификуван и пред дискусијата за улогата на Алијансата на полето на енергетската безбедност. Истиот можеме да го детектираме уште во периодот на Иранско-ирачката војна од 1980-1988 година. Тогаш, Велика Британија, Франција и Холандија партиципираа во операцијата „Earnest Will", во која ги обезбедувале рутите на танкерите во Персискиот Залив (Varwick, J., 2008: 39).

По Самитот во Рига останаа евидентни сериозните политички несогласувања помеѓу сојузниците во врска со улогата на НАТО во сферата на енергетската безбедност. Во рамките на состаноците на разните политичко-воени тела постоеле повеќе прашања отколку одговори. Во февруари 2007 година за првпат е составена Работна група за енергетска безбедност во рамките на НАТО. Нејзина задача била да се посочат сите прашања на кои Алијансата мора да одговори пред да изгради каква било рамка или политика за енергетската безбедност и тоа:

- дефинирање на улогата на силите на НАТО во заштитата на енергетската инфраструктура;
- идентификување на проблемите во сите мисии на НАТО за обезбедување безбедни транзитни коридори за нафта и гас низ Ормутскиот Теснец и други специфични локации, како и обезбедување на непровокативно присуство на чувствителните локации за производство на нафта и гас;
- интегрирање на политиките за безбедност во снабдувањето помеѓу сите членки на Алијансата (Милески, 2014: 50).

Имено, Декларација од Самитот во Рига вклучи краток параграф експлицитно најавувајќи (за првпат) дека енергетската безбедност е грижа на НАТО, давајќи ѝ задача на Алијансата да ги истражи специфичностите на таа улога. Во Декларацијата на тој начин се промени природата на дискусијата, таа веќе не е за тоа дали Алијансата има улога, односно таа потврдува дека има. Прашањето сега се поставува за природата на таа улога. Втор значаен момент претставува говорот на американскиот сенатор Ричард Лугер на маргините на Самитот во Рига. Во говорот се укажува на заканите од тероризмот, како и на фактот дека енергијата веројатно ќе биде извор на вооружени конфликти на европската сцена, како и во околните региони. На тој начин, Лугер потенцира дека би било неодговорно од НАТО да го намали својот ангажман на полето на енергетската безбедност. Но, неговиот фокус беше насочен кон потенцијалот од политички манипулации со ресурсите и употребата на „енергетското оружје". Говорот на Лугер беше предмет на внимание на речиси целата меѓународна јавност.

Политичкиот момент, по донесувањето на Декларацијата од Рига, продолжи да добива поголемо значење, особено по спорот со прекин на испораката на гасот помеѓу Русија и Белорусија во декември 2006 година и јануари 2007 година. Истото се случуваше и наредните години. На 31 јануари 2008 година Русија ја прекинува испораката на гасот за Украина, поради неплатените сметки и поради цената на гасот. Руско-украинскиот спор околу цената на гасот остави без тој енергент десетина земји од Централна и Источна Европа. Без гас за греење и производство на струја останале Молдавија, Словачка, Бугарија, Србија, Хрватска, Македонија, додека со недостаток од гас се соочиле Турција, Грција, Чешка, Полска, Унгарија и Австрија. Својот врв, политичкиот момент го имаше, по сè изгледа, во јануари 2009 година. Прекинот на испораката на рускиот гас преку Украина, предизвика голема нелагодност во Европската унија затоа што 40% од потребите за природен гас Европската унија ги задоволува од Русија, а 80% од тој гас поминува преку Украина. Кризата е завршена на 19 јануари по преговорите на тогашниот премиерот на Русија, Владимир Путин

и тогашниот премиер на Украина, Јулија Тимошенко. Договорено е Украина во 2009 година да го плаќа рускиот гас 20% пониско од пазарната вредност, а од 2010 година да почне да ја плаќа цената како и другите земји од Европа, односно 470 долари за 1000 кубни метри. До тогаш Украина имала повластена цена за рускиот гас од 179,5 долари за 1000 кубни метри (Милески, Т., 2014: 51).

Генерално гледано, пред Самитот во Рига, Алијансата укажуваше на проблематиката на енергетската безбедност прилично нејасно, односно активностите на НАТО оделе во насока на оневозможување на попречувањето на протокот на виталните ресурси. Дефинирањето на попречувањето е клучниот предизвик за Алијансата, илустрирајќи го јазот во консензусот помеѓу воените загрозувања на виталните ресурси и оние со политичка мотивација. Мандатот на НАТО дефиниран со Декларацијата од Рига обезбедува одредено појаснување на интересите на Алијансата и нивно фокусирање кон безбедност на енергетската инфраструктурна, но не и кон другите димензии на енергетската безбедност. Фокусираната и ограничена агенда дефинирана со Декларацијата од Рига формираше подлога за официјални разговори во 2007 и почетокот на 2008 година. Тогашниот генерален секретар на НАТО, Јап де Хоп Шефер, повтори дека Алијансата ја смета енергетската безбедност како „колективен" предизвик за кој мора да биде обезбеден „колективен" одговор. Одговор, кој во голема мерка е проследен со координација помеѓу националните влади и меѓународните организации. Понатаму, улогата на НАТО во таквиот колективен одговор би се фокусирала таму каде што истата би можела да даде придонес, односно Алијансата треба да ја разгледа сопствената улога во заштитата на рутите на испорака, особено кај транспортот на течниот природен гас со танкери на отворено море и заштита на критичната енергетска инфраструктура кога постои одредено високо ниво на закана.

На Самитот во Букурешт во април 2008, истиот пристап беше потврден. Алијансата ќе настојува да даде придонес и потполно да се координира со активностите на меѓународната заедница, која содржи бројни организации кои се специјализирани во сферата на енергетската безбедност. Иако сè уште постојат некои нејасни фрази - Алијансата ќе се ангажира во „проектирање стабилност" и унапредување на меѓународната и регионалната соработка. Притоа, фокусот насочен кон цивилната одбрана и справувањето со кризи и енергетската инфраструктура, останува јасен. Тоа нè води до разгледување на „продлабочената" улога која НАТО би можел да ја реализира.

Во тој контекст, улогата на НАТО би можела да биде насочена во давањето придонес во координираниот меѓународен напор заради подобрување на енергетската безбедност во две широки подрачја, и тоа: споделување на информации и планирање и одговор.

Прво, споделувањето информации претставува еден од клучните принципи на енергетската безбедност. НАТО може да придонесе делувајќи како важен мост помеѓу енергетската и безбедносната заедница. Ова е јасно назначено со Декларацијата од Рига, и потврдено со Декларацијата од Букурешт, односно, НАТО може да придонесе за размената на информации делувајќи како форум за размена на известувања. Одредени размислувања се движат во

насока на зајакнување на линкот помеѓу безбедносната и енергетската заедница преку создавање постојан мониторинг и оценување на механизмите за делување во соработка со Меѓународната енергетска агенција (ИЕА) и сличните на неа организации, вклучувајќи ги и компаниите. Исто така, НАТО може да даде свој придонес во размената на податоци преку практичната употреба на нејзините средства и капацитети. Односно, средствата за поморски надзор и рано предупредување можат да се користат за давање моментални информации за главните поморски транспортни рути кои не се доволно покриени од националните капацитети на одредени држави. Како второ, Алијансата може да даде свој придонес во остварувањето на енергетската безбедност преку ставање на располагање на сопствените воени капацитети и стручност онаму каде што тоа е потребно. Првенствено се мисли на физичката заштита, патролирање и придружба на патиштата на критичната инфраструктура. НАТО веќе има јасно дефинирана улога во заштитата на нафтените и гасните капацитети во Северното Море, во случај на вооружени напади. Морнаричките капацитети на НАТО (и на ЕУ) веќе се користат за заштита на пратките на нафта и гас во подрачјето на Рогот на Африка и Западна Африка, особено од нападите на пиратите и терористичките напади. Ваквите можности за одговор на заканите се манифестирани со операцијата „Steadfast Jaguar 06", одржана на Зелено'ртските Острови во јуни 2006 година.

Енергетската безбедност има соодветна позиција во новиот стратегиски концепт на НАТО од 2010 година, донесен на Самитот на НАТО, одржан во Лисабон. Како продолжение на претходно наведените параграфи во делот на стратегиската рамка која го позиционира концептот за заштита на критичната инфраструктура на НАТО, во Член 13 од основните начела и принципи на новиот Стратегиски концепт на НАТО, се потенцира дека сите држави сè повеќе се потпираат на виталните комуникации, транспортот и транзитните рути од кои зависат меѓународната трговија, енергетската безбедност и просперитетот. Тоа подразбира поголеми меѓународни напори за обезбедување на нивната отпорност од напади или прекини. Одредени држави, членки на НАТО сè повеќе ќе стануваат зависни од надворешни снабдувачи со енергија, додека во одредени случаи од надворешни снабдувачи со енергија и дистрибутивни мрежи за сопствените потреби. На светско ниво, енергетското снабдување ќе се соочи со зголемена изложеност на прекини во дистрибуцијата (Strategic Concept for the Defence and Security of the Members of the NATO).

Овие определби претставуваат континуитет на ставови на НАТО наведени во Стратегискиот концепт донесен 1999 година. Евидентно е дека тој претставува основа за сите понатамошни процеси на носење одлуки од страна на Алијансата, а се во врска со енергетската безбедност. Параграф 24 од овој Стратегиски концепт донесен на 50- годишнината од основањето на НАТО во Вашингтон, гласи: „Секој вооружен напад на територијата на сојузниците, без оглед на тоа од кој правец доаѓа, ќе резултира со активирање на Членот 5 и Членот 6 од Вашингтонскиот договор. Но, Алијансата, исто така, мора да води сметка и за глобалниот контекст. Безбедносните интереси на Алијансата може да бидат загрозени и од други ризици од поширока природа, вклучувајќи ги тука и актите на тероризам, саботажа и организираниот криминал, како и со

пореметување на текот на ресурсите од витално значење. Неконтролираното движење на голем број луѓе, особено како последица на вооружените конфликти, исто така, може да резултира со проблеми по безбедноста и стабилноста и да ја погоди Алијансата. Со Членот 4 од Вашингтонскиот договор се регулира координацијата на напорите на земјите-членки, вклучувајќи го и нивниот заеднички одговор на овие ризици".

Значи, државите-членки на НАТО, со консензус се согласни дека терористичките напади би можеле да претставуваат основа за повикување на колективните безбедносни гаранции содржани во Членот 5 од Договорот на НАТО. До 1999 година, Клинтоновата администрација се справуваше со бомбашките напади на американските амбасади и воените сили во странство од страна на „Ал Каеда", и ги поовикуваше сојузниците да се договорат за проширување на традиционалниот концепт и за тоа што би можело да предизвика активирање на Членот 5. Две години подоцна, со нападите од 11 септември 2001 година, со проследувањето на ужасните сцени од терористичките напади на кулите-близначки, следеше соопштение на Северноатлантскиот совет во кое се потенцира дека Советот е согласен дека доколку се утврди дека овој напад против САД е диригиран од странство, истиот ќе резултира со активирање на Членот 5 од Вашингтонскиот договор, во кој се наведува дека вооружен напад против еден од сојузниците во Европа или Северна Америка ќе се смета за напад против сите нив. Заложбата за колективна самоодбрана која е отелотворена во Вашингтонскиот договор за првпат се соочуваше со околности различни од оние кои постоеле претходно, но сепак таа и понатаму останува не помалку валидна и е од суштинско значење.

Она што треба да се напомене е дека Параграфот 24 од Стратегискиот концепт не завршува и не го опфаќа единствено „терористичкиот акт", туку и нарушувањата на текот на виталните ресурси претставуваат дополнителна основа за повикување на Членот 4, па дури и координиран одговор (доколку е тоа потребно) преку колективната безбедност во согласност со Членот 5. Ова не значи дека постои механизам за автоматски одговор доколку дојде до вакви ситуации. Постоењето на овој параграф не значи дека секоја нафтена криза ќе резултира со повикување на Членот 5 од страна на НАТО. Тоа ќе зависи пред сè од природата на околностите, успехот/неуспехот на дипломатските мерки, но и способноста да се постигне консензус во рамките на НАТО.

Што се однесува на Декларацијата од Лисабон, содржините од сферата на енергетската безбедност се потенцираат во Членот 41. Имено, во членот се укажува дека стабилното и сигурно снабдување со енергија, диверзификација на рутите, снабдувачите и енергетските ресурси, како и поврзаноста со енергетските мрежи, останува да биде од критично значење. Алијансата ќе продолжи со консултациите за најнепосредните ризици во областа на енергетската безбедност во согласност со одлуките донесени на претходните самити и во согласност со новиот стратегиски концепт од Лисабон. Алијансата и понатаму ќе развива капацитети за да придонесе во областа на енергетската безбедност, концентрирајќи се на области за кои се дискутирало на Самитот во Букурешт. Во унапредувањето на работата на Алијансата, ќе се зајакнува соработката и консултациите со партнери и други меѓународни актери за да

може да се интегрираат сите целосходни размислувања во политиките и активностите на НАТО. Ќе биде побарано да се подготви извештај за напредокот постигнат во сферата на енергетската безбедност кој ќе се разгледа на Состанокот на министрите за надворешни работи во декември 2011 година, и понатамошен извештај за разгледување на идниот самит на НАТО. (Lisbon Summit Declaration, 2010).

На Самитот во Чикаго, континуитетот на интересот за енергетската безбедност продолжува. Во Декларацијата која произлезе од Самитот во Чикаго, во Член 52 се наведува, исто како и на претходниот Самит во Лисабон, дека стабилно и сигурно енергетско снабдување, диверзификација на рутите, снабдувачите и енергетските ресурси, како и конектираноста со енергетските мрежи и понатаму ќе претставува задача од критично значење. Овие прашања првенствено се однесуваат на националните влади и другите меѓународни организации кои се занимаваат со истите, додека НАТО внимателно ќе ги следи сите релевантни случувања во сферата на енергетската безбедност. На Самитот во Чикаго нотиран е извештај во кој се забележува напредок во процесот на преземање конкретни чекори од последниот самит на Алијансата и кој го опишува начинот на кој Алијансата очекува да се интегрираат сите размислувања на полето на енергетската безбедност во политиките и активностите на НАТО. И понатаму ќе се продолжи со консултациите за енергетската безбедност и идниот развој на капацитетите за соодветен придонес кон енергетската безбедност, концентрирајќи се на областите каде што НАТО може да даде значаен придонес. Понатаму, се истакнува дека за претходно наведените цели, Алијансата ќе работи на значително подобрување на енергетската ефикасност на сопствените воени сили; развој на способноста за поддршка на заштитата на критичната енергетска инфраструктура и понатамошен развој на теренските активности во консултација со партнерите, врз основа на принципот „од случај до случај". Во оваа прилика, Алијансата ги поздравува напорите за создавање на НАТО-акредитиран центар за енергетска безбедност во Литванија како придонес кон напорите на НАТО во сферата на енергетската безбедност. Се определува задача на Советот да продолжи да ја насочува улогата на НАТО во рамките на енергетската безбедност во согласност со принципите и насоките договорени на Самитот во Букурешт и во корелација со насоките имплементирани во новиот стратегиски концепт како и одлуките од Лисабон. Повторно се задолжува Советот да изготви извештај за напредокот за следниот самит на НАТО (Chicago Summit Declaration, 2012).

На Самитот на НАТО одржан во Кардиф, Велс, во 2014 година во завршната Декларација од Самитот во Член 109 се напоменува следното: За НАТО од критично значење и перманентна заложба се постојаното и сигурно снабдување со енергија, диверзификација на правците, добавувачите и енергетските ресурси, како и меѓусебната поврзаност на енергетските мрежи. Додека овие прашања претставуваат првенствено одговорност на националните влади и другите меѓународни организации, НАТО внимателно ги следи релевантните случувања во сферата на енергетската безбедност, вклучително и во врска со кризата Русија-Украина и растечката нестабилност на регионот на Средниот Исток и Северна Африка. НАТО ќе продолжи да се консултира и понатаму да

ги развива сопствените капацитети за да придонесе кон енергетската безбедност, концентрирајќи се на области каде што НАТО може да се придонесе. Притоа, особено се потенцира зголемувањето на свеста за енергетскиот развој со безбедносни последици за сојузниците и Алијансата; понатамошно развивање на компетентноста на НАТО во поддршката на заштитата на критичната енергетска инфраструктура; и ангажман кон подобрување на енергетската ефикасност на воените сили, при што е потенцирана Рамката за „зелена одбрана". (Wales Summit Declaration, 2014).

Рамката за „зелена одбрана", претставува значаен исчекор кој е направен на Самитот во Кардиф. Накусо, таа рамка обезбедува основа за зголемена размена на знаења и координација на истражувањата кои можата да го поддржат развојот на поевтини и поефикасни „зелени решенија" за одбранбена способност и справување со голем број на современи и нови безбедносни предизвици како што се енергетската безбедност, глобалните климатски промени, одбранбените трошоци и логистичките предизвици за добивање енергија на бојното поле (Larsen, K.K, 2015).

Во 2016 година, домаќин на НАТО-самитот беше Полска, односно Варшава. Завршната декларација од Самитот во член 135 потенцира дека енергетскиот развој и движење можат да имаат значителни политички и безбедносни импликации и за Алијансата, како што и се покажа во кризите на истокот и југот на НАТО. Се констатира дека од исклучително значење за НАТО се стабилното и безбедно снабдување со енергија, диверзификација на правците за увоз, добавувачите и енергетски ресурси, како и меѓусебна поврзаност на енергетските мрежи. Постигнувањето на овие заложби ќе овозможат зголемување на отпорноста од политички и економски притисоци. Додека овие прашања се првенствено одговорност на националните влади и другите меѓународни организации, НАТО внимателно ги следи безбедносните импликации од релевантните енергетски развојни процеси и придава особено значење на диверзификација на снабдувањето со енергија во евроатлантскиот регион. Од тие причини, се потенцира дека, НАТО ќе продолжи да ја зголемува сопствената стратегиска свест во тој поглед, вклучително и преку размена на разузнавачки информации и проширување на врските со другите меѓународни организации како што се Меѓународната агенција за енергија и ЕУ. Притоа, од особена важност ќе бидат консултациите и ќе споделувањето информации за прашањата на енергетската безбедност кои се од особена важност за сојузниците и Алијансата, со цел да се обезбеди сеопфатна слика за развојот на енергетскиот пејзаж, концентрирајќи се на области каде што НАТО може да даде соодветен придонес. Исто така, НАТО ќе продолжи да ги развива сопствените капацитети, преку размислувања за енергетската безбедност во обуките, вежбите и планирањето. Основната цел е во насока на поддршка на националните власти во намерата за заштита на критичната инфраструктура, како и подобрувањето на нивната отпорност кон пореметувања во снабдувањето со енергија кои понатаму можат да влијаат врз националната и колективна одбрана, вклучувајќи хибридни и сајбер-закани. Заложба на НАТО ќе биде понатамошното подобрување на енергетската ефикасност на воените сили преку воспоставување на заеднички стандарди, намалување на зависноста од фосилните горива и

демонстрирањето на енергетски ефикасни решенија за војската. На Самитот во Варшава забележан е Извештај за напредокот на улогата на НАТО во енергетската безбедност (Warsaw Summit Communiqué, 2016).

На последниот самит на НАТО, одржан во Брисел во 2018 година, во официјалната завршна декларација се наведува дека енергетската безбедност игра важна улога во заедничката безбедност. Притоа се повторуваат наводите од претходниот самит, дека стабилно и безбедно снабдување со енергија, диверзификацијата на правците, добавувачите и енергетските ресурси, како и меѓусебната поврзаност на енергетските мрежи се од клучно значење и ја зголемуваат отпорноста на Алијансата од политички и економски притисоци. Додека овие прашања се првенствено одговорност на националните власти, развојот на енергијата може да има значителни политички и безбедносни импликации за сојузниците, а исто така ќе влијае и на НАТО-партнерите. Како резултат на тоа, НАТО ќе продолжи со редовни сојузнички консултации за прашања поврзани со енергетската безбедност. Особено се потенцира дека од суштинско значење е да се обезбеди дека членовите на Алијансата не се ранливи на политичка или принудна манипулација со енергија, што претставува потенцијална закана. Затоа, сојузниците ќе продолжат да бараат диверзификација на нивните енергетски резерви, во согласност со нивните потреби и услови. НАТО ќе ја ублажи улогата на НАТО во енергетската безбедност во согласност со воспоставените принципи и насоки и ќе продолжи да ги развива капацитетите на НАТО за поддршка на националните власти во заштитата на критичната инфраструктура, вклучително и против злонамерни хибридни и сајбер-активности. Ќе продолжиме да ја подобруваме нашата стратешка свест, вклучително и преку размена на разузнавачки податоци и проширување на врските со релевантните меѓународни организации, како што се Меѓународната агенција за енергија, Меѓународната агенција за обновлива енергија и Европската унија, како што е соодветно. Исто така, ќе ја подобриме енергетската ефикасност на нашите воени сили, вклучително и преку употреба на одржливи извори на енергија, кога тоа ќе биде соодветно. Овие наводи укажуваат дека помеѓу двата самита на НАТО во Варшава и Брисел не се промениле насоките на делување на НАТО во сферата на енергетската безбедност и заштитата на критичната инфраструктура (Brussels Summit Declaration, 2018).

Континуираниот интерес на Алијансата за заштитата на критичката (енергетска) инфраструктура претставува константа која може да се препознае од насоките кои произлегуваат од завршните декларации на самитите. Од нив воочливо е барањето изготвување на извештаи од страна на Северноатлантскиот Совет за напредокот на Алијанската на полето на заштитата на критичната инфраструктура и енергетската безбедност.

3.3. Критички осврт кон комплексната улога на Алијансата

Според претходно изнесеното, НАТО добива мандат да ја преиспита својата потенцијална улога во сферата на енергетската безбедност во меѓународни рамки. Декларацијата од Рига, поточно делот кој се однесува на енергетската безбедност се соочува со редица сложени елементи кои го успоруваат прак-

тичното дефинирање на улогата на Алијансата. Официјалните лица и аналитичари од повеќето држави-членки на НАТО се на мислење дека енергетската безбедност останува национален проблем, и дека како таков треба да се третира. Значи, според нив, незамисливо е сценариото за распоредување на НАТО трупи на нафтените платформи или чување на нафтоводите и гасоводите. Во тој контекст, еден НАТО-дипломат одговарајќи на шпекулациите за распоредувањето трупи како „полиција на нафтоводите" во региони како што е Кавказот, ќе потенцира дека енергетската безбедност и безбедноста на инсталациите и транспортните рути претставуваат национална одговорност. Ангажманот на Алијансата првенствено треба да биде насочен кон давањето совети и помош, отколку активно да се ангажира на теренот (Милески, Т. 2014: 56).

Слични ставови имаат и турските експерти и аналитичари кои истакнуваат дека турската држава борејќи се против Курдите направила многу повеќе од Алијансата во поглед на заштитата на критичната енергетска инфраструктура. Исто така, Азербејџан низ чија територија поминува значајна енергетска траса (Баку-Тбилиси-Џејхан нафтоводот) преку поранешниот заменик премиер Абид Шарифов потенцира дека Алијансата нема искуство во заштитата на нафтоводите и комуникациите кои поминуваат преку земјите кои не се членки на НАТО. Ваквите ставови за немањето потреба за помош од страна на НАТО, конкретно за посочениот нафтовод, произлегуваат од фактот што истиот е заштитен и од азербејџанската влада и од компаниите кои сметаат дека заштитата е остварена и преку други мерки како што се: длабоко вкопување на нафтоводите и укажувањето на локалното население за важноста на безбедноста на нафтоводите.

Од друга страна, доколку се преместиме на северот од планетата, поточно северноатлантскиот регион, и ги анализираме тамошните дискусии на експертите и аналитичарите ќе увидиме поинакви размислувања. Имено, Норвешкото Море и транспортните рути на нафтата и природниот гас кои тука поминуваат, промовираат дискусии за потребата од разгледување на прашањата за поморската безбедност. Се потенцира дека НАТО-членките од двете страни на Атлантикот мораат заедно да работат на енергетската безбедност, како централен дел на безбедносната политика на Алијансата, и тоа првенствено на безбедноста на транспортот, а потоа и на енергетската безбедност. Според Бјорн Бјарнасонар, енергетската безбедност претставува нова димензија која ги редефинира северните предели на Атлантскиот регион на политичката и воената сцена на НАТО, односно го реафирмира поморскиот идентитет на НАТО.

Според други мислења, енергетско-безбедносната улога би ја разводнила или нарушила агендата на НАТО на штета на постоечките мисии. Енергетската безбедност, исто така е поврзана со други прашања од сложениот дневен ред на НАТО, како на пример, расправата за понатамошно проширување на Членот 5 со вклучување на енергетската безбедност. Во својот говор на маргините на Самитот во Рига, веќе споменатиот сенатор Лугер предложил делотворните енергетски стратегии да ги вклучат и новите односи со државите од Кавказ и Централана Азија и тоа особено односите со Казахстан и Азербејџан, при што евентуалното членство во НАТО мора да се стави на маса. (Милески, Т. 2014: 59).

Аргументите за проширувањето на Членот 5 се однесуваат на можноста за уништување на националните економии доколку енергијата се користи како „оружје". На овој начин Алијансата би се обврзала на соодветен одговор на обидите и користењето на енергијата како „оружје" против своите земји-членки.

Иако соработката со други меѓународни организации е важна намера нотирана во Рига, Лисабон, Чикаго, Кардиф, Варшава и Брисел, таа, исто така, се покажува и како доста проблематична. Дефинирањето на улогата на НАТО во рамките на енергетската безбедност, овозможува поширока дискусија и изнесување на различни мислења кои честопати не се на иста „фреквенција". Оваа може да се илустрира, на пример, со разликата во дефинирањето на заканите по енергетската безбедност на национално и институционално ниво. Земајќи ги предвид различните географски региони, изворите на ресурсите и инфраструктурните капацитети, а со тоа и нивните поединечни енергетски стратегии, повеќето земји во ЕУ и НАТО гледаат на различен начин на ситуацијата со енергијата. Според тоа во рамките на секоја организација, постои проблем за дефинирање на било кој напреден степен на разјаснување и консензус за природата на заканата и за кого таа се однесува.

Сè уште поголемиот број држави-членки на ЕУ и НАТО на енергетската криза гледаат како на економски проблем кој првенствено треба да се регулира на пазарот, а не со надворешно-политички и безбедносни мерки. Генерално, би можеле да се согласиме дека САД се стремат кон прифаќање на енергетската безбедност како заштита на снабдувањето со енергенси, додека ЕУ тоа го дефинира во смисла на менаџирање со побарувачката на енергенси. Ваквите различни стојалишта во дефинирањето на енергетската проблематика, претставува дополнително комплицирана состојба, особено по различните реакции внатре во ЕУ и НАТО на некои од прашањата кои ја донесоа енергетската безбедност на дневниот ред на Алијансата. Сето тоа ги поткопува изгледите за воспоставување комплементарни енергетски односи помеѓу НАТО и ЕУ.

Дополнителен проблем претставува и рускиот поглед на дискусиите за вклучувањето на енергетската безбедност во агендата на НАТО. Алијансата се труди расправата за енергетската безбедност да не биде протолкувана од страна на Москва како антируски сигнал. Во оваа насока особено е интересна изјавата на рускиот министер за надворешни работи кон крајот на 2007 година, Сергеј Лавров, кој ја осуди политизацијата на енергетската безбедност на штета на земјите производители и потенцира дека она што претставува чисто економски се политизира со обид за обединување на потрошувачите за да му се спротивстават на рускиот енергетски монопол (Monaghan, A. 2008). Како што НАТО почнува да разговара за енергијата како безбедносно прашање, истото го прави и Москва, која состави нова воена доктрина во која енергетската безбедност има свое место. Конкретно, во новата воена доктрина на Русија од 2014 година, во делот за спроведување на главните задачи на градење и развој на вооружените сили и другите трупи и органи, меѓу другото, се постигнуваат и со формирање територијални трупи за заштита и одбрана на воени, владини и специјални објекти, објекти кои ги обезбедуваат витални функции на населението, функционирање на транспортот, енергетски постројки, како и објекти кои претставуваат зголемена опасност по животот и здравјето на луѓето (Military Doctrine of the Russian Federation, 2014).

Во процесот на редефинирањето на НАТО како безбедносен гарант на своите членки, сè повеќе се наметнува потребата од сериозно разгледување на безбедноста на снабдувањето со енергенти. Заканите по енергетската безбедност нашироко се етаблираат во меѓународната политика, но и на национално ниво. Покрај тоа, проблемот сериозно се елаборира и во академската заедница. Сепак, сè уште доминираат ставовите кои не се на релација на прифаќањето на улогата на НАТО во разрешувањето на заканите за енергетската безбедност.

Што се однесува на постоечките основи на Алијасата, се мисли на Членот 5, можеме да воочиме дека енергетската безбедност на некој начин е содржана во истиот. Членот 4 од Вашингтонскиот договор пропишал дека страните „ќе се консултираат заедно, секогаш кога, според мислењето на кој било од нив, нивниот територијален интегритет, политичка независност или безбедност е загрозен". Членот 5, исто така, е потенцијално релевантен, земајќи ја предвид природата на повеќето закани „страните се сложни дека вооружен напад против една или повеќе од нив во Европа или Северна Америка се смета за напад на сите нив". (The North Atlantic Treaty). Земајќи го предвид фактот дека со ова не се дистанцираат енергетските постројки од останатите цели, а од друга страна природата на заканите за енергетската инфраструктура од страна на терористите, пиратите, па дури и државите, најверојатно ќе бидат во форма на вооружени напади, можеме да претпоставиме дека вооружен напад на енергетска постројка може да биде причина за повикување на Членот 5. Единствен исклучок би биле намерните престанувања на производство потребни количини енергенти и нивна испорака до крајните потрошувачи, со што би се влијаело на националните економии и би се заземале одредени политички позиции на земјата производител. Во овој случај би било симптоматично повикувањето на Членот 5.

Негативните конотации во поглед на предложената агенда за улогата на НАТО во енергетската безбедност се чини дека е премногу поедноставено разбрана. Односно, шпекулациите генерално одат во насока на единствено воен одговор на Алијансата во случај на загрозување на енергетската безбедност. Ако на тоа се надоврзе и нереалната агенда или провокацијата за дискусија за менување на постоечкиот член 5 од Вашингтонскиот договор и потенцијалното членство на Казахстан и Азербејџан, евидентен е новиот стратегиски хоризонт кој може да го креира идниот меѓународен контекст во кој Алијансата ќе функционира.

Алијансата при дефинирањето на сопствената улога во рамките на енергетската безбедност се соочува со две паралелни дебати насочени кон дефинирањето на прекинот на снабдувањето со енергенти. Дали тоа ќе биде воен прекин, предизвикан од вооружени напади или можеби во контекстот на натпреварот за пристап кон одредени ресурси?. Тоа треба да ги детерминира напорите на Алијансата заради изнаоѓање најсоодветни решенија. Односно нејзиниот ангажман би одел во насока на соработка со партнерите, изградба на капацитетите, реформи во одбраната и обука на партнерските земји. Во екстремни случаеви можно е вклучување и на воена заштита на инфраструктурата од вооружени напади. Втората дебата оди во насока на детерминирање

на прекинот во снабдувањето со енергенти преку вклучување на политичките причини за таквиот чин, кои најчесто тешко се дефинираат и докажуваат. Во ваков случај многу тешко може да се смета на консензус на сите партнери при евентуално преземање на одредени мерки. Од друга страна, таквата состојба може да мотивира разгледување одредени решенија внатре во рамките на Алијансата, каква што би можела да биде намерата за подобрување на сопствената ефикасност во потрошувачката на енергенти како средство за намалување на зависноста од надворешни услови.

Како и да е, Алијансата ќе мора поактивно да работи на сопствената улога во енергетската безбедност, во контекстот на нејзината еволуирачка патека на опстојување и функционирање на меѓународната безбедносна сцена. Еден од тие правци на делување, се чини дека се етаблира со формирањето на НАТО-акредитираниот центар за енергетска безбедност во Литванија. Овој чин, јасно покажува дека дебатите за енергетската безбедност од теоретски елаборации, полека но сигурно, резултираат со практични акции на теренот. Имено, центарот почнува да функционира во 2012 година како меѓународна воена организација под менторство на НАТО. Со тој чин, појасно се определува улогата на НАТО во сферата на енергетската безбедност. Концептот за овој центар е на линија со зацртана стратегија за т.н. „паметна одбрана" на НАТО, етаблирана на самитот во Лисабон. Центарот ќе работи на полето на техничките, научните и академските истражувања кои треба да придонесат во соодветните проценки и анализи на конретните ризици. Исто така, Центарот треба да даде свој придонес преку соодветни препораки и предлози за ефективни и економични решенија за оперативните енергетски проблеми како поддршка за воените барања. Центарот треба да ги поддржува истражувањата на алтернативните енергетски ресурси и развој на еколошки пријателските и ефикасни воени сопсобности. Понатаму, треба да обезбди ангажирање во образованието и вежбовни активности како и да обезбедува научни, технички и академски анализи од различни аспекти на снабдувањето со енергија и критичката енергетска инфраструктура (NATO ENSEC COE).

Преку неколку примери ќе посочиме како Алијансата би требало да се постави во случај на потенцијални енергетски кризи. Согласно одредени сценарија кои се хипотетички, но не и невозможни, одредена земја-членка на НАТО може да побара дополнителни консултации во согласност со Член 4, а како резултат на загрозување на безбедноста на снабдувањето со енергенти. На пример, во јануари 2006 година, Бугарија (членка на НАТО од 2002 година), го отфрли барањето од „Газпром" за преиспитување на цената која таа треба да ја плаќа за природниот гас. Доколку „Газпром" го исклучел дотокот на природен гас за Бугарија (како што се случи со Украина, Молдавија и Грузија), се поставува прашањето дали Бугарија ќе побарала дополнителни консултации согласно Член 4? Единствен начин да се дознае одговорот на едно такво прашање е тоа навистина да се изнесе во рамките на НАТО. А, Бугарија не е единствената членка на НАТО со многу висока зависност од увозна нафта или природен гас. Во слична ситуација се наоѓаат Словачка со 100% зависност, балтичките држави со 100% зависност, Полска со 99% зависност, Бугарија со 94% зависност, Чешка со 82% зависност и Унгарија со 81% зависност. (Bell, G.R., 2009: 266).

Украина не е членка на НАТО, барем не до денес. Полска и Соединетите Американски Држави силно се заложија за нејзино пристапување во Алијансата во 2009 година, на 60-годишнината од основањето на НАТО. Сепак, без оглед на временската рамка околу фаворизирањето на украинското членство во НАТО, тешко е да се замисли како сојузниците на НАТО ќе се придржуваат до Стратегискиот концепт на Алијансата, доколку по евентуално украинско членство Русија одлучи повторно да го прекине снабдувањето со гас. Слична загриженост постои и за Грузија (која исто така е аспирант за членство во НАТО). Неодамнешниот воен судир меѓу Грузија и Русија, во август 2008 година го нагласи ризикот од вклучување на поранешните руски сојузници (кои имаат клучна улога во енергетската безбедност) во Алијансата. Доколку Грузија беше членка на НАТО, рускиот напад од 2008 година ќе ја ставеше Алијансата под притисок да ги исполни своите воени обврски. Акцентот е ставен и на Иран и на моменталната нуклеарна криза која се случува таму.

Европската унија и САД нагласија дека никогаш нема да дозволат Иран да се здобие со нуклеарно оружје. Шпекулациите за можната превентивна воена насочена кон иранските нуклеарни капацитети се сè погласни, но паралелно со тоа се преземаат и мерки од страна на Советот за безбедност на ОН, но и од страна на САД и Европската унија, главно изразени преку економски санкции, со кои се настојува да се притисне Иран кон конечно стопирање на својата нуклеарна програма. Меѓутоа, иранската влада јасно стави до знаење дека евентуалните поригорозни мерки кон Иран, усвоени од Советот за безбедност на ОН, ќе резултираат со намалување или целосно стопирање на извозот на иранската нафта кон западните земји. Евентуалното попречување на транзитот на нафтата низ Ормутскиот Теснец ќе резултира со катастрофални последици по многу светски економии. Интересни ќе бидат и случувањата на Арктикот. Со глобалното затоплување, огромните нафтени и гасни ресурси во тој дел од светот конечно ќе станат достапни (се претпоставува дека Арктикот крие 25% од вкупните резерви на нафта и гас), а дури 4 земји-членки на НАТО (САД, Норвешка, Данска и Канада), но и Русија ќе бидат директни партиципиенти, но и конкуренти за пристапот до овие ресурси. Па така, во услови на нецелосно дефинирање на позицијата на НАТО кон енергетската безбедност, единствен начин да дознаеме што ќе се случува во иднина е да се препуштиме на настаните кои ни претстојат, а одговорите ќе си дојдат сами по себе. По сојузничките напади врз Ирак, стана јасно дека НАТО ќе ја има улогата на клучно место за дијалог за стратегиски и политички консултации и координации помеѓу сојузниците од Европа и Северна Америка. Во иднина, се претпоставува дека тоа партнерство ќе се зајакнува, а уште повеќе ќе се интензивираат дијалозите, како и потребата од политички и безбедносни консултации и координации на највисоко ниво во Алијансата бидејќи ќе има малку прашања кои ќе бидат поважни од енергетската безбедност. Најверојатен извор на вооружени конфликти на европскиот простор и околните региони во иднина ќе биде недостатокот на енергенси и манипулацијата со истите. Затоа, логично е да се претпостави дека членките на НАТО ќе бидат сè повеќе ангажирани во мисии кои се директно или индиректно поврзани со енергетската безбедност. Ако Алијансата сака да ја зачува својата улога и да продолжи да биде релевантна

за развојот на глобалната безбедност на средината од 21 век, таа ќе мора да ја разјасни својата позиција и да ги продолжи координациите со други владини и невладини организации кон реализирањето на една заедничка и сеопфатна трансатлантска енергетска безбедносна политика. Со други зборови, НАТО треба да го користи и својот статус на меѓувладина организација, но и компаративната предност во однос на другите меѓународни организации, а тоа е неговата воена способност.

Заклучок

Анализирајќи ги стратегиските концепти на НАТО, можеме веднаш да констатираме дека Алијансата ја регулира и ја штити својата критична инфраструктура. Широкиот спектар на можности и сценарија за вклучување на НАТО во заштитата на критичната инфраструктура оддава впечаток дека во одредени моменти премногу милитаристичкиот пристап е надвор од стратегиските определби на Алијансата. Сепак, дилемите кои беа анализирани, поврзани со сферата на енергетската безбедност и енергетската критична инфраструктура, сè уште не даваат прецизен одговор дали енергетската сфера е чисто економско прашање и дали може исклучиво со воена сила да се регулираат прашањата поврзани со енергијата. Во оваа насока, акцентот на НАТО треба да биде поставен на поддршката на националните авторитети, нивно зајакнување и поддршка заради успешна и ефикасна заштита на критичната инфраструктура. Дебатата околу промена на Членот 5 и објаснувањето за колективната безбедност на земјите-членки, повеќе делува дека е форма на зајакнување на напорите за вклучување на Алијансата во оперативните акции заради конкретно инволвирање во практика.

Анализите од релевантни авторитети велат дека главната одговорност за прашањата поврзани со енергетската безбедност треба да се препушти на Европската унија, а НАТО да се држи настрана. Европската унија има клучна улога која може и мора да ја одигра. Тоа пред сè се однесува на активирање на неопходните дипломатски мерки кон Русија и максимизирање на напорите за да се обезбеди руско ратификување на Енергетската повелба и нејзините транзитни протоколи. Исто така, потребни се и интензивирања на напорите за дефинирање на енергетската безбедност во рамките на Европската унија, како и нови иницијативи насочени кон создавањето единствен европски енергетски пазар, решавање на пазарните нарушувања, поттикнување на диверзификацијата и развојот на нови технологии, како и иницирање програми за заштита на европската критична инфраструктура. Европската унија може и мора да го прошири својот дијалог и соработка со Соединетите Американски Држави на полето на енергетската безбедност. Но, Норвешка и Турција (сè уште) не се членки на Европската унија, а тоа значи дека на состаноците на министрите на Европската унија, никој формално не го претставува снабдувањето со нафта од Северното Море, ниту пак можноста за намалување на Европската зависност од руската нафта и гас претставена преку реализацијата на нафтоводот Баку-Тбилиси-Џејхан (Bell, G.R., 2009: 267).

Дијалогот помеѓу ЕУ-САД не ја вклучува и Канада, со што уште една држава со огромни ресурси се држи настрана од овие процеси. Меѓутоа, овие три земји (Норвешка, Канада и Турција) се членки на НАТО и во негови рамки егзистираат како рамноправни партнери. Па така, координацијата помеѓу НАТО и Европската унија ќе биде добитна комбинација и за двете страни. Ако ништо друго, неизбежен е дијалогот (како на неформално ниво, така и на редовните средби помеѓу Северноатлантскиот совет и Комитетот на Европската унија за политичка безбедност) околу прашањата за заштитата на критичната инфраструктура. Дијалог може да се оствари и на многу други места, пред сè во рамките на ОБСЕ, но и во Г-8 (Русија беше претседавач во 2007 година, а тогашниот претседател Путин ја наметна енергетската безбедност како клучна тема за разговор). Советот НАТО-Русија е уште едно место на кое може да се остварува политички дијалог по овие прашања. Советот не е наменет исклучиво за разговори за кои постои согласност помеѓу двете страни. Тој претставува и место на кое се изнесуваат сите прашања за кои постојат длабоки несогласувања и токму тука треба да се изнесат сите ставови на евроатлантските сојузници околу руската употреба на енергентите како инструмент на надворешната политика.

ГЛАВА 4

ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО СОЕДИНЕТИТЕ АМЕРИКАНСКИ ДРЖАВИ

Глава 4

ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО СОЕДИНЕТИТЕ АМЕРИКАНСКИ ДРЖАВИ

Метју Ватер, MSS, MSST US Army Colonel (Retired)
Assistant Commissioner for Enforcement,
Minnesota Department of Commerce

Ричард (Рик) Ларкин, MA, CEM
Emergency Management Practitioner Minnesota, USA

4.1. Организациската структура на критичната инфраструктура во Соединетите Американски Држави

Во практична смисла, критичната инфраструктура ја претставува електричната енергија што ја користиме во нашите домови и бизниси, водата која ја пиеме, како и транспортот што го користиме за движење на луѓе и стоки. Тоа се патиштата и мостовите низ целата земја, трговските центри во кои купуваме и спортските објекти што ги посетуваме. Тоа се нашите комуникациски системи и нашите банкарски и финансиски системи. Сè на сè, тоа е структурата која го овозможува секојдневниот живот каков што го знаеме во САД.

САД препознава 16 сектори на критична инфраструктура. Системите и средствата во овие сектори се од витално значење за општата структура и функционирањето на националното стопанство, јавното здравје и безбедноста и целокупната безбедност и сигурност на американските граѓани. Претседателската директива за спроведување политики бр. 21 (ПДСП-21) ја истакнува политиката која обезбедува силен, отпорен и безбеден систем за заштита на американската критична инфраструктура. (Белата куќа, 2013) Претседателската директива за спроведување политики бр.7 (ПДСП-7) воспостави национална политика која треба да ја спроведуваат сојузните секретаријати и институции во идентификувањето и приоретизирањето на критичната инфраструктура (Секретаријат за државна безбедност, 2003). Поседувањето насоки на сојузно ниво за начинот на насочување на напорите на сојузните институции помага да се утврдат улогите и задолженијата ширум органите на државната управа и создава основа за спроведување на заштитните активности.

Слика 1: Закани по критичната инфраструктура

Извор: НПЗИ 2013

Раздвојувањето на критичната инфраструктура на 16 сектори го олеснува доделувањето на секторските задолженија во рамките на државната управа и на засегнатите страни од приватната индустрија. Идентификувани се секторски специфичните институции (ССИ) кои треба да го претставуваат водечкиот капацитет за организирање на напорите на повеќе институции и засегнати страни за обезбедување на клучните секторски средства. ССИ, во координација со секретарот за внатрешна безбедност, ја вршат приоритетизацијата на критичната инфраструктура којашто е заснована на анализа на заканите и ранливоста, соработуваат со сопствениците и операторите на секторски специфичните критични инфраструктури, спроведуваат управување со инциденти, обезбедуваат техничка поддршка и помош, а помагаат и во ублажувањето на инцидентите. ССИ исто така се одговорни за редовното информирање на Секретаријатот за домашна безбедност за севкупната состојба на подготвеност во рамките на секторите кои им се доделени, како и за идентификувањето на областите кои предизвикуваат загриженост. ССИ се задолжени да ја разгледаат заштитата на критичната инфраструктура и пристапот на „Согледување на сите опасности". Изразот „сите опасности" значи дека инцидентите и заканите кои се согледуваат доаѓаат од природни и човечки извори и се однесуваат на животот, имотот, животната средина и јавното здравје и безбедност. Во „сите опасности" се вбројуваат природните непогоди, индустриските несреќи, терористичките чинови, пандемиите, сајбер-инцидентите, саботажите и деструктивните криминални активности кои се насочени кон критичната инфраструктура. (Секретаријат за државна безбедност на САД. 2019).

Во табелата се посочени 16-те сектори на критична инфраструктура и секторски специфичните институции за секој поединечен сектор, а даден е и краток опис на областите на надлежност во секој сектор.

Табела 2: Сектори на критична инфраструктура и секторски специфични институции во САД

Сектор и специфична институција вршител	Опис
Хемиски сектор: Секретаријат за внатрешна безбедност	Хемискиот сектор е одговорен за производството, складирањето, употребата и транспортот на потенцијално опасни хемикалии од кои зависи и широк спектар на други сектори на критична инфраструктура.
Комерцијални објекти: Секретаријат за внатрешна безбедност	Секторот за комерцијални објекти вклучува локации кои привлекуваат големи групи на луѓе во целите на нивно сместување, деловна активност, забава и купување. Овие објекти се карактеризираат со отворен пристап до пошироката јавност и во огромно мнозинство се наоѓаат во приватна сопственост.

Комуникации: Секретаријат за внатрешна безбедност	Комуникацискиот сектор обезбедува функционалост во сите сектори на критична инфраструктура. Вклучува копнена, сателитска и безжична комуникација.
Критично производство: Секретаријат за внатрешна безбедност	Во секторот на критично производство се вбројуваат оние производствени капацитети кои поддржуваат многу делови од другите сектори на критична инфраструктура. Тие вклучуваат производство на основни метали, производство на машини, електрична опрема, производство на компоненти и уреди и производство на транспортни средства.
Брани: Секретаријат за внатрешна безбедност	Секторот за брани овозможува задржување и контрола на критичните води што вклучува производство на хидроелектрична енергија, земјоделско наводнување, контрола на наслагите и поплавите, движење по реките и управување со индустриски отпад.
Одбранбено-индустриска база: Секретаријат за одбрана	Секторот за одбранбено-индустриската база го сочинуваат домашни и странски компании кои обезбедуваат материјални и други услуги потребни за операциите и градењето, одржувањето, мобилизирањето, распоредувањето и одржувањето на воените сили на САД.
Служби за прва помош: Секретаријат за внатрешна безбедност	Секторот за служби за прва помош обезбедува секојдневни, како и услуги за реакција и спасување при итни случаи. Организирана е првенствено на сојузно, државно, локално, племенско и територијално ниво на власт и вклучува полиција, противпожарна служба и организации за обезбедување итна медицинска помош оспособени за реакција при опасности од секаков карактер.
Енергетика: Секретаријат за енергетика	Енергетскиот сектор ја опфаќа инфраструктурата што ги обезбедува енергетските ресурси што ги поддржуваат сите сектори на критичната инфраструктура. 80 проценти од енергетската инфраструктура на земјата се во приватна сопственост.
Финансиски услуги: Секретаријат за финансии	Секторот за финансиски услуги вклучува депозитарни институции, инвестициски институции, осигурителни компании и други организации за кредитирање и финансирање кои овозможуваат трансфер на финансиски производи и услуги.

Храна и земјоделство: Секретаријат за земјоделство и Секретаријат за здравство и услуги за човекот на САД	Секторот за храна и земјоделство го обезбедува производството и складирањето на резервите храна и земјоделски производи на земјата.
Објекти на државната управа: Секретаријат за внатрешна безбедност и Управа за општи услуги	Секторот за објекти на државната управа врши надзор врз зградите кои се наоѓаат во САД и во странство, а се во сопственост или се изнајмени од американската влада и во кои се наоѓаат амбасади, воени постројки, судови, национални лаборатории, критична опрема и системи.
Здравствена заштита и јавно здравје: Секретаријат за здравство и услуги за човекот	Секторот за здравствена заштита и јавно здравје ги штити сите сектори од тероризам, заразни болести и природни непогоди. Тој е одговорен за превенција, реакција, отпорност и закрепнување во проблемите поврзани со јавното здравство.
Информациска технологија: Секретаријат за внатрешна безбедност	Секторот за информатичка технологија ги опфаќа луѓето, како и хардверот и софтверот потребни за функционирањето на државниот апарат, академската заедница, деловните организации во приватниот сектор и пошироката јавност. Во координација со секторот за комуникации, одговорен е и за Интернетот.
Нуклеарни реактори, материјали и отпад: Секретаријат за внатрешна безбедност	Секторот за нуклеарни реактори, материјали и отпад го опфаќа производството на нуклеарна енергија, медицински изотопи и нуклеарни и радиолошки истражувања. Исто така, го надгледува движењето на радиолошки пратки во координација со транспортниот сектор.
Транспортни системи: Секретаријат за внатрешна безбедност и Секретаријат за транспорт	Транспортниот сектор се занимава со транспортот на луѓето и стоките. Вклучува воздухопловство, патишта и автопати, поморски транспорт, патничка и железница за масовен транспорт, гасоводни системи, товарна железница и пошта и достава на пратки.
Системи за вода и отпадни води: Агенција за заштита на животната средина	Секторот за системи за вода и отпадни води е одговорен за снабдувањето со чиста вода на земјата. Исто така, тој зазема клучна улога во управувањето со канализацијата и прочистувањето на отпадните води.

За да се изврши подобра приоретизација и фокусирање на ресурсите, како и да се потпомогне брзото закрепнување од сите опасности, Националниот план за заштита на инфраструктурата ги посочува комуникациите, енергијата, транспортот и управувањето со водите како највитални функции за спасување. (Секретаријат за државна безбедност на САД, 2013:17). Идентификувањето на овие функции во рамките на еден сектор на критична инфраструктура им овозможува на засегнатите страни подобро да се подготват преку приоретизирање на размислувањата за овие функции и преку согледување на меѓузависностите меѓу различните сектори. Ваквите меѓузависности се однесуваат на влијанието што определен инцидент кој настанал во еден сектор може да го има врз друг. На пример, во случај на прекин на електрична енергија од голем обем, како таквиот прекин на електричната мрежа би се одразил врз транспортот, управувањето со отпадни води и сл. Меѓузависностите и потребата за меѓусекторска соработка ќе бидат подетално разгледани во друг дел од ова поглавје.

Идентификацијата на највиталните функции е клучна во разработката на државните, локалните, племенските и територијалните (ДЛПТ) планови за реакција и спасување. Анализата на заканите и проценките на ранливоста мора да го земат предвид влијанието врз секоја од функциите во рамките на еден сектор за да се утврди приоретизацијата на средствата за реакција и спасување. Сеопфатната анализа на загубата на електрична енергија за време на пандемиска криза ќе ја нагласи потребата за генерирање резервна електрична енергија во клучните медицински установи, на пример. Исто така, ќе им помогне на разработувачите на плановите да го согледаат ефектот врз комуникацијата и водоснабдувањето што резултира со планови за ублажување на негативните ефекти од губењето на способноста во оваа витална функција. Фокусирањето на највиталните функции помага да се создаде основа за заштита на критичната инфраструктура, како и да се разграничат надлежностите на сите засегнати страни.

Заканите по клучната инфраструктура на земјата спаѓаат во пет категории: директен непријателски напад, сајбер-закани, случајни или технички падови на инфраструктурата и екстремни временски услови и пандемии (Секретаријат за државна безбедност, 2013: 8). Особено важен сектор е енергетиката. Важноста на електричната енергија во секојдневниот живот е очигледна и често се зема здраво за готово. Настаните или активностите во која било категорија на закана може да резултираат со значително нарушување на системот за дистрибуција на електрична енергија. Комбинираните напади во повеќе категории на закани би можеле да резултираат со катастрофална и долгорочна загуба на електрична енергија. Непријателите на САД би можеле да имаат за цел или да овозможат прекини во мрежата на широко ниво и да го искористат влошувањето на комуникациите, како и насоченоста на безбедносните ресурси кон возобновување на електроснабдувањето за домаќинствата, нарушувањето на снабдувањето со храна, водоснабдувањето и здравствените услуги и да нападнат кога САД е ослабната.

Тоа што ја влошува ранливоста на критичната инфраструктура на САД е податокот дека ниту една организација поединечно нема надлежност врз тоа

прашање. Без оглед на тоа колку се вредни сопствениците на критичните инфраструктури, оформувањето на единствен и усогласен напор за заштита на огромниот број меѓусебно зависни делови најверојатно нема да се постигне во целост. Оспособувањето на поединечни граѓани кои сакаат да преземат поголема контрола таму каде што објективно можат да помогнат ќе го зајакне целокупниот напор. Се проценува дека приближно 85% од критичната инфраструктура се во приватна сопственост. Заштитата на националната инфраструктура во која се вбројува и електричната мрежа бара соработка и комуникација меѓу сите засегнати страни, властите, приватната индустрија и локалните заедници. Иако властите регулираат многу аспекти на производството и дистрибуцијата на електрична енергија, приватната индустрија, јавните комисии и кооперативите, тие мора да соработуваат заедно со просечниот граѓанин за да ги воспостават клучните елементи на отпорноста и безбедноста. Во следниот дел ќе разговараме за односот меѓу властите на сојузно, државно, локално, племенско и територијално ниво од една страна и сопствениците на критична инфраструктура од приватниот сектор од друга.

4.2. Јавно-приватни партнерства, улогите и одговорностите на клучните засегнати страни

Заштитата на критичната инфраструктура во Соединетите Американски Држави е одговорност која ја споделуваат приватните сопственици во секој сектор и институциите на власта на сојузно, државно, локално, племенско и територијално ниво. Канцеларијата за отчетност на Владата на САД (ГАО) проценува дека 85% од клучната инфраструктура на ниво на САД се во сопственост на приватниот сектор (Канцеларија за отчетност на Владата на САД, ГАО, 2009). Владата на САД, во координација и соработка со клучните засегнати страни, изработи неколку документи за стандардизација кои им даваат структура на програмите за заштита низ сите 16 сектори.

Планот за заштита на националната инфраструктура на САД од 2013 година ја задржува задачата содржана во претходните верзии на Националниот план која предвидува Секретаријатот за внатрешна безбедност да ги одржува секторските планови за сите клучни инфраструктурни сектори кои претставуваат пресек на секторските политики, мерки и активности на сите инволвирани секторски фактори. Првите такви секторски планови беа усвоени во 2010 година, за потоа да бидат ревидирани во 2015 година. Секој од нив е дополнително поврзан со конкретни документи за стратешка безбедносна политика. Секторски специфичните политики може да се спроведуваат само преку доброволна соработка со сопствениците и операторите од приватниот сектор и нивните партнери меѓу јавните институции. Државниот и приватниот сектор на поединечна основа поседуваат особени одговорности и гледиштата на секој од нив имаат подеднаква важност. Секторски специфичните планови се спроведуваат преку употреба на секторски координативни совети, владини координативни совети и регионални конзорциуми. Овие тела за соработка се расчленуваат уште понатаму со цел да се овозможи нивно фокусирање на конкретни области во рамките на еден сектор. На пример, во секторот Финан-

Слика 2:
Планот и пристапот на САД кон градење и одржување единство во напорите

Извор: НПЗИ, 2013

сиски услуги, Центарот за размена на информации и анализи во финансиските услуги - (ЦРИА-ФУ) дејствува како главен ресурс на финансиската индустрија за анализа и размена на разузнавачки информации за сајбер и физички закани. Ова е организација која се состои од членови кои доаѓаат од приватниот сектор, како и од владините и непрофитните организации, заедно со одбраните партнери на засегнатите актери. Вакви ЦРИА се основани и во други сектори. Националниот совет на ЦРИА (НСЦРИА) претставува координативно тело кое ја олеснува соработката со ЦРИА во поединечните сектори. Целосниот список на сите поединечни секторски ЦРИА кои се во функција може да се најде на интернет-страницата на НСЦРИА: https://www.nationalisacs.org. Членовите на ЦРИА придонесуваат со специфични информации и разузнавачки податоци во секторот, во обид да се здобијат со знаења и искуства од целокупниот сектор. Оваа доброволна соработка меѓу засегнатите страни во секторот е клучен елемент во севкупниот план за заштита на националните критични инфраструктури и е од суштинско значење за успешноста на напорите за заштита на критичната инфраструктура.

Општиот водич за заштита во секторот Енергетика е Националниот план за заштита на инфраструктурата на САД (НПЗИ). Како дел од Националниот план за заштита на инфраструктурата, партнерите од јавниот и приватниот сектор во секој од 16-те клучни инфраструктурни сектори и властите на ниво на државната, локалната, племенската и територијалната заедница развија Секторски специфичен план кој се фокусира на единствените работни услови и спектарот на ризици во посочениот сектор. Развивани во тесна соработка со сојузните институции и партнерите од приватниот сектор, Секторски

специфичните планови се ажурираат на секои четири години со цел да му се овозможи на секој поединечен сектор да се приспособи кон спомнатиот спектар на ризици кој постојано се менува. Во 2015 година, ажурирањата на секторски специфичните планови се однесуваа на врската меѓу сајбер и физичката безбедност, меѓузависноста на секторите, ризиците по инфраструктурата поврзани со стареењето на истата, застарената технологија и климатските промени, како и на промените во работната сила кои се потребни за да продолжи да се спроведува Националниот план.

Преглед на плановите во највиталните сектори

Енергетика

Во 2013 година, ПДСП-21 го идентификуваше енергетскиот сектор како сектор од исклучителна важност бидејќи обезбедува суштински функции во речиси сите сектори на критичната инфраструктура. Најновиот Секторски специфичен план за енергетскиот сектор е тој од 2015 година (Секретаријат за државна безбедност на САД 2015). Водечката институција која има надлежност врз Планот за енергетскиот сектор е Секретаријатот за енергетика на САД (СзЕ). Ажурирањето на енергетскиот сектор беше заеднички напор помеѓу СзЕ, координативните совети во енергетскиот сектор и владините партнери. Меѓусебно поврзаните поделементи на енергетскиот сектор се електричната енергија, нафтата и природниот гас. Ова вклучува производство, рафинирање, складирање и дистрибуција на електрична енергија, гас и нафта. Не вклучува производство на хидроелектрична или нуклеарна енергија. Овие конкретни извори спаѓаат во одделни потсектори. Секторот за енергетика ја поддржува транспортната индустрија, ги снабдува дејностите и домаќинствата со електрична енергија и обезбедува енергија за индустриското и земјоделското производство ширум САД. За возврат, тој опстојува во однос на зависност со информатичката технологија, комуникациите, водата и финансиите, како и со други аспекти на секторите на критичната инфраструктура.

Клучна компонента на Секторски специфичниот план во енергетиката е проценката на закани и ризици. Планот за енергетскиот сектор ги идентификува ризиците и заканите во секој потсектор. За потсекторот за електрична енергија, Планот за 2015 година ги нагласува како основни закани и ризици сајбер и физичките закани, природните катастрофи и екстремните временски услови, способноста на работната сила и човечките грешки, опремата која затајува и старее, развојот на регулаторните барања за животната средина, економијата и сигурноста, но и промените во техничкото и оперативното опкружување. Слично на ова, во потсекторите за нафта и гас, како примарни области на закана и ризик се посочени природните катастрофи и екстремните временски услови, регулаторните и законодавните промени - вклучувајќи ја и состојбата на животната средина, побарувачката на испарлива нафта и гас, оперативните опасности, политичките и граѓанските немири и терористичката активност, транспортните инфраструктурни ограничувања, несоодветното и недостапно осигурување, стареењето на инфраструктурата и ризиците по работната сила и сајбер-безбедноста, како и заканата од инсајдерски напади.

Комуникации

Природата на комуникациите значително се промени во изминатите 25 години, претворајќи се од средина која беше главно ориентирана кон обезбедувањето гласовни услуги во една меѓусебно поврзана индустрија која користи копнени, безжични и сателитски комуникациски системи. Координативниот совет на Секторот за комуникации и Владиниот координативен совет на Секторот за комуникации работеа заеднички на ажурирањето на Секторски специфичниот план за комуникации за 2010 година. Планот ја препознава важноста на учеството на приватниот сектор, земајќи го истовремено предвид податокот дека повеќето комуникациски инфраструктури кои функционираат во САД се наоѓаат во приватна сопственост. Во Планот за 2015 година, секторот идентификува 3 цели: Заштита и подобрување на севкупната физичка и логичка состојба на комуникациите.

1. Брзо возобновување на критичните услуги во случај на нарушувања и ублажување на каскадните ефекти.
2. Подобрување на подготвеноста на секторот за одржување на националната безбедност и за итни случаи во рамките на сојузните, државните, локалните, племенските, меѓународните и приватните субјекти, а со цел намалување на ризиците. (Секретаријат за државна безбедност на САД 2015).

Ажурираниот Секторски специфичен план ги истакнува целите за соработката меѓу јавните и приватните партнери од редовите на државните институции и приватната индустрија соодветно. Секторот за комуникации обезбедува производи и услуги кои се неопходни за функционирањето на другите сектори на критичната инфраструктура. Тие вклучуваат и физичка инфраструктура, како што се прекинувачи, кули и антени, како и сајбер-инфраструктура, како што се софтверските решенија за пренасочување на сигналот, но и апликациите и архитектурата за оперативна поддршка. Речиси секој аспект на современиот живот зависи од сајбер-инфраструктурата. Банкарството, стоките и услугите, итните комуникации и секојдневната лична интеракција сега зависат од постоењето на отпорна и сигурна сајбер-мрежа. Ваквата зависност ја прави насушно значајна потребата јавно-приватното партнерство во тој поглед да ги опфаќа сите опасни закани по секторот и сите нивни аспекти, како и да опстојува на сите нивоа на одговорност, вклучувајќи ја и таа на поединецот.

Слика 3: Користењето мобилен интернет по секоја минута

Извор: Центар за сајбер-безбедност преку Линкдин

Количината на податоци што се пренесуваат преку интернет секоја минута го истакнува модерното општество кое се потпира на комуникациската инфраструктура не само на САД, туку и на глобално ниво. Според Ериксон,

(2019) користењето на мобилен интернет во Северна Америка е зголемено за 40% во однос на 2015 година. Се предвидува дека овој експоненцијален раст ќе продолжи со зголемувањето на капацитетите кај паметните уреди, како и на флексибилноста на плановите за услуги.

Со континуираниот раст на бројот и видот на уредите и архитектурата за нивната поддршка, расте и потребата за нови политики за заштита на сврзаната инфраструктура и побрзо откривање на заканите и слабостите во тој поглед. Партнерите во секторот мора да продолжат да соработуваат и да се развиваат за да понудат одговор на ваквата зголемена потреба.

Проценката на ризик е клучен дел од Секторски специфичниот план во оваа област. Ажурираниот секторски специфичен план за комуникација за 2015 година ги идентификува следниве како можни области за појава на ризици:

- Природните непогоди и екстремните временски услови - ураганите и пожарите се вбројуваат меѓу непогодите кои зачестија во последниве години. Геомагнетните бури исто така се наоѓаат на листата на природни настани кои би можеле да предизвикаат колапс на електричната мрежа во голем обем и да предизвикаат долгорочни прекини во комуникациите ширум земјата.
- Слабости на синџирот на снабдување - секторот се потпира на хардвер и софтвер и добавувачите кои ја снабдуваат индустријата со истите.
- Глобалните политички и општествени влијанија - геополитичките немири, но и странските и домашните економски околности можат негативно да влијаат врз секторот.
- Сајбер-слабости – зголемувањето на бројот на злонамерни апликации за нарушување или недозволување на пристапот до интернет, пристапот до податоци и интегритетот на истите постојано создава причини за загриженост.

Секторот за комуникации е еден од ретките сектори кои можат да влијаат на сите други сектори. Стабилноста и сигурноста на секторот ја олеснуваат стабилноста и сигурноста на системот како целина.

Транспорт

Ажурираниот план во овој сектор за 2015 година го одразува созревањето на партнерствата во рамките на секторот и го опишува пристапот за управување со безбедноста и отпорноста на транспортните системи во САД. Тој ја доведува во рамнотежа слободата на движење на стоки и луѓе од една страна, со можноста за губење на граѓанските слободи која може да произлезе како последица на прекумерни прописи и ограничувања, од друга. Транспортните системи ги обезбедуваат најнеопходните услуги за движење на стоки и можности за реакција и спасување при катастрофи. Секторски специфичниот план за транспорт (ССП ТС) идентификува 4 цели:

1. Управување со безбедносните ризици за физичките, човечките и сајбер-елементите на критичната транспортна инфраструктура.
2. Ставање во функција на секторските капацитети за реакција, спасување и координација со цел обезбедување поддршка за отпорноста на целата заедница.

3. Да се спроведат процеси за ефективна соработка за да се споделат информации од суштинско значење за зададените задачи низ секторите, областите на надлежност и дисциплините, како и меѓу јавните и приватните засегнати страни.
4. Подобрување на подготвеноста и отпорноста за сите опасности кон глобалниот транспортен систем во целите на заштитување на американските национални интереси. (Секретаријат за државна безбедност на САД, Секторски специфичен план за транспорт, 2015).

ССП ТС го препознава постигнатиот напредок во напорите за надградба на сајбер-безбедноста, и тоа во целите на усогласување со растечката загриженост во врска со сајбер-заканите и влијанијата од нив. Тој применува пристап на согледување на сите опасности во однос на отпорноста и подготвеноста во воздухопловските, поморските, товарно-железничките, автопатните и патните, нафтоводните, поштенските и доставните системи за масовен транспорт и транзитирање во земјата и во странство. Слично како кај другите сектори, како првенствени олеснувачи во транспортот, исто така се јавуваат компаниите од приватниот сектор. Сопствениците и операторите во овој сектор ги оценуваат ризиците и развиваат планови за ублажување на ризиците и реагирање при катастрофи. Овие планови се развиваат заеднички преку бројните совети за координација и партнерските совети и со помошта како на владиниот, така и на институциите од приватниот сектор. Секретаријатот за внатрешна безбедност на САД е основната институција надлежна за разработката на планот и координацијата на секторот и, во рамките на нејзиниот опсег на надлежности, ја дели одговорноста на тој план со Секретаријатот за транспорт на САД, Управата за безбедност во сообраќајот (УБС) и Крајбрежната стража на САД (КС). Владата се координира со индустријата преку регионални совети, стручни и академски организации и неформални конференции и други настани наменети за споделување информации и знаења. Споделувањето на информациите претставува основа на соработката меѓу засегнатите страни. Како план, Шаблонот за споделување информации за безбедноста во транспортот ги набројува повеќенасочното споделување, делотворните и целисходните процеси, доверливите партнерства, безбедносното образование, обуката и свеста, како и заштитата на личните слободи како свои клучни цели. За да се одговори на зголемената загриженост во однос на сајбер-безбедноста во транспортниот сектор, беше формирана Работната група за сајбер-безбедност во транспортниот систем. Таа се состои од претставници на сојузните ДЛПТ-власти и приватната индустрија. Оваа група ја покренува општата свест на индустријата, ги промовира активностите во заедницата и ги поттикнува колаборативните пристапи за зголемување на севкупната сајбер-сигурност низ целата транспортна област.

Ризиците за транспортната критична инфраструктура вклучуваат вештачки и природни закани. Во вештачки закани се вбројува и тероризмот, како физичкиот, така и компјутерскиот. Стареењето на инфраструктурата резултира со поголема веројатност за разорно уништување на физичката инфраструктура поради тешки временски услови, вандализам, саботажа и затајување на

технологијата. Природните непогоди, климатските промени и екстремните временски појави можат да ги уништат или влошат транспортните системи. Поплавите, пожарите, силните невремиња, ураганите, торнадата и сушите влијаат врз транспортните услуги. Во пролетта 2019 година, сушите во Средна Америка резултираа со намален водостој во Панамскиот Канал. Намалениот водостој ја ограничува големината на бродовите кои можат да се движат низ каналот. Ова резултираше со загуба на приходи кај операторите на каналот, намалување на количествата на товар кои може да се пренесат низ каналот и, при екстремни услови, ограничување на видовите на пловила кои можат да се движат низ него. (Zamorano and Franco, 2019).

Постојаната соработка меѓу сите засегнати страни и продолжувањето на обемната размена на информации и разузнавачки податоци преку советите и работните групи во рамките на секторот и во рамките на меѓусекторските настани е од клучно значење за изнаоѓање одговори за заканите кои непрестано се менуваат.

Вода и отпадни води

Целта на Секторски специфичниот план за вода и отпадни води (ССП Вода) е обезбедување и зајакнување на отпорноста на инфраструктурата во секторот (Сектор за државна безбедност на САД, 2015). Едноставно кажано, секторот за вода и отпадни води се однесува на одржување на безбедни и сигурни системи за вода за пиење кои се потребни за одржување на јавното здравје и за спречување болести. Со инфраструктурата која обезбедува свежа вода за пиење и безбедно пренесува и прочистува отпадни води управуваат субјекти во сопственост на сојузните, државните, локалните, територијалните и племенските власти, како и на засегнатите страни од приватниот сектор. ССП Вода го користи моделот на партнерство наведен во НПЗИ со цел да ги вклучи лидерите во приватниот и јавниот сектор во планирањето и спроведувањето на активностите насочени кон заштитата на секторот. Владината институција која е носител на главната надлежност за овој сектор е Агенцијата за заштита на животната средина на САД (АЗЖС).

Безбедноста и сигурноста на системите за вода за пиење во САД се од клучно значење за здравствената, стопанската, психолошката и еколошката состојба низ целата земја. Инцидентите како што се загадувањето на мрежите за вода за пиење, каков што беше контаминацијата на системот за водоснабдување во Флинт, Мичиген, ги истакнуваат драстичните проблеми поврзани со здравјето на луѓето кои ги предизвикува небрежноста во справувањето со можната контаминација (Национален совет за одбрана на природните ресурси, NRDC.org. 2018). Во обид да заштедат пари, градските власти одлучија да го прекинат користењето на свежа вода за пиење која доаѓаше од Детроит и наместо тоа, да користат вода од реката Флинт сè додека не се изгради нов водовод кој влече вода од езерото Хјурон. Градот не успеа правилно да ја деконтаминира и прочисти оваа вода, што резултираше со значително зголемување на нивото на олово во крвта кај децата, осипи на кожата и бројни други заболувања. Желбата да се заштедат пари доведе до значителни дополнителни трошоци не само за чистење

на системите за водоснабдување, туку и за исплаќање обештетувања на жителите на Флинт за покривање на нивните медицински трошоци.

ССП Вода е водечки документ чија цел е да помогне да се спречат настаните како тој којшто го искусија жителите на Флинт во Мичиген. Покрај човечкиот елемент, во планот се разгледуваат бројни елементи кои се однесуваат на категоријата вода за пиење. Изворите на водата, преносот, складирањето на непрочистена вода, прочистувањето, дистрибутивните системи за складирање на прочистена вода и системите за нивно следење ги сочинуваат физичките компоненти опфатени со планирањето. Системите за надзор и прибирање податоци (СНКПП), како и оперативните системи за контрола на процесот се области кај кои значењето на сајбер-елементите е потенцирано. Контролата и управувањето со дистрибуцијата и производството на вода сè повеќе се остваруваат со помош на дигиталните системи. Компромитирањето на ваквите системи претставува закана која веќе е препознаена и означена како таква.

Отпадните води се третирани одделно во ССП Вода. Физичкиот елемент во делот на планот кој се однесува на отпадните води се состои од собирањето, складирањето на суровини, првичната преработка, преработката, дезинфекцијата, истекувањето или исцедокот, остатоците, цврстите биолошки остатоци и системите за следење на состојбите. Сајбер-елементот ги опфаќа истите области како што се посочени во деловите за водата, СНКПП и оперативните системи за контрола на процесот. Се разбира, мора да се разгледа и човечкиот елемент. Не само јавните функционери, туку и лабораториските техничари, микробиолозите, хемичарите, вработените во јавниот сектор и специјалистите за животна средина, спаѓаат во многуте професионалци кои се неопходни за управување со овој сложен систем.

Секторските ризици се категоризираат како најзначајни, високи и средни ризици. Најзначајните закани бараат приоритетно внимание и дејствија за ублажување. Тие имаат најголем потенцијал за далекусежно влијание. Високиот ризик бара сериозно внимание, додека настаните со среден ризик би можеле да ескалираат доколку не им се обрати должно внимание. Примери за најзначаен ризик се природните непогоди како што се поплавите, земјотресите и другите природни појави кои негативно влијаат на квалитетот на водата во големи географски области, застарената инфраструктура и со нив поврзаните економски импликации, како и можноста за ескалација на последиците која произлегува од неспособноста за справување со кризи во поширок подрачја. Високи ризици може да бидат злонамерни чинови, неактивност кај засегнатите страни или давателите на комуналните услуги и несоодветна подготовка, реакција и спасување. Средни ризици се недоволното или несоодветното управување со средствата и ресурсите, како и немањето разработени планови за реакција при итни случаи и при обезбедувањето заемна помош. Овие примери кои ја илустрираат категоризацијата на ризиците помагаат да се изврши приоретизација врз основа на препознаените потреби во секторот. Анализата на ризиците зависи од дадените ситуации, а контекстуализацијата на таквата анализа каква што е понудена во ССП помага да се согледаат околностите кои се поврзани со процесот кој е неопходен за проценување на невообичаените ситуации.

Секторски специфични планови постојат за сите 16 сектори. Прегледот на секторски специфичните планови нуди општо согледување на подробностите со кои треба да се занимава секоја секторски специфична институција со цел да одговори на сложеноста на секој соодветен сектор. Како што беше посочено во целиот овој дел, неопходноста за соработка меѓу сите засегнати страни во секој сектор заслужува најсилно да се нагласи. Редовната интеракција, како во формален, така и во неформален вид, е потребна за да се одговори на динамичната природа на технологијата, заканите и ранливоста. Плановите мора да бидат флексибилни и енергични и да содржат политики што овозможуваат прилагодување и надзор.

4.3. Националните стандарди и улогата на државната управа во изготвувањето на политиките и нивното спроведување

Американската влада почна да ги формализира напорите за развој на сеопфатна национална политика за критична инфраструктура во средината на 1990-тите. *Извршната наредба (ИН) 13010 - Заштита на критичната инфраструктура* од 1996 година вели дека „одредени национални инфраструктури се од толку суштинско значење што нивното онеспособување или уништување би довело до ослабување на одбраната или стопанската безбедност на САД". Заканите за критичните инфраструктури првенствено се определуваат како физички и сајбер-закани (Белата куќа, 1996). ИН понатаму пропишува воспоставување на тела и придружни механизми со цел да се оформи нормативна рамка за заштита на критичната инфраструктура во САД. Меѓу другото, со неа беше пропишано и формирањето на Претседателската комисија за заштита на критичната инфраструктура (ПКЗКИ) составена од претставници од јавниот и приватниот сектор, кои беа задолжени да ги проценат заканите и слабостите на инфраструктурата во САД и да препорачаат национална политика и стратегија за заштита во поглед на истата. Во јули 1996 година, претседателот Клинтон ја формираше Комисијата за заштита на критичната инфраструктура (ПКЗКИ), со задача да ги означи критичните инфраструктури, да ги процени нивните пропусти, да препорача сеопфатна национална политика и стратегија за спроведување на заштитата на тие инфраструктури од физички и сајбер-закани и да предложи законски или регулаторни активности кои ќе влијаат врз препорачаните правни лекови[4]. Критичната инфраструктура беше дефинирана во *Директивата за претседателска одлука НСЦ-63* од 1998 година – *Заштита на критичната инфраструктура (Белата куќа, 1998)* како „физички и сајбер-системи од суштинско значење за најосновното делување на стопанството и државната управа. Тие ги вклучуваат, но не се ограничени на телекомуникациите, енергијата, банкарството и финансиите, транспортот, системите за вода и службите за итни случаи, како државни така и приватни".

4 ПКЗКИ го поднесе својот извештај *Критички основи: Заштита на инфраструктурите на Америка* во октомври 1997 година. Извештајот на ПКЗКИ претставуваше основа за Директивата за претседателска одлука бр. 63 (од 22 мај 1998*) - Заштита на критичната инфраструктура* која утврдува дека националната политика и организациската структура за воспоставување јавно-приватно партнерство и за постигнување на функциите за посебна заштита кои се во законска надлежност на државната управа (Секретаријат за одбрана, 1998).

Понатаму, се истакнува дека „многу или сите од критичните инфраструктури на САД, од историска, физичка и логичка гледна точка претставуваа одделни системи кои само во мала мера опстојуваа во меѓусебно зависен однос. Меѓутоа, како резултат на напредокот во информатичката технологија и потребата од подобрување на ефикасноста, овие инфраструктури станаа се повеќе автоматизирани и меѓусебно поврзани. Ваквиот напредок создаде нови пропусти во однос на затајувањето на опремата, човечките грешки, временските и другите природни непогоди, како и физичките и сајбер-нападите. Справувањето со овие слабости нужно ќе бара флексибилни и еволутивни пристапи кои ќе го опфаќаат како јавниот, така и приватниот сектор и ќе ја штитат домашната и меѓународната безбедност" (Белата куќа, 1998).

Претседателската директива за спроведување политики бр. 21 (ПДСП-21) ги артикулира основните надлежности на Сојузната влада на САД во улогата која таа ја игра во зајакнувањето на безбедноста и отпорноста на американската критична инфраструктура од физички и сајбер-закани. ПДСП 21 ја нагласува потребата од партнерство со приватниот сектор и меѓународните засегнати страни и ја препознава меѓузависноста во системот на критични инфраструктури како целина (Белата куќа (2013:2). Сојузната влада го олеснува усогласувањето со регулативата преку одржување редовна комуникација, спроведување програми за инспекција, разгледување на барања за лиценцирање и издавање финансиски казни за непочитување на обврските.

За да им помогне на сојузните држави и на локалните власти во спроведувањето на Националната програма за заштита на инфраструктурата (НПЗИ), Секретаријатот за државна безбедност спроведе програма која користи „советници за заштита на безбедноста". Според канцелариите за отчетност на Владата на Соединетите Американски Држави (ГАО-18-62 - Заштита на критичната инфраструктура), програмата за СЗБ на СВБ е основана во 2004 година за да им помогне на тековните напори на сојузните држави и на локалните власти до ниво за безбедност на критичната инфраструкура преку воспоставување и одржување односи со советниците за внатрешна безбедност на ниво на сојузните држави, со засегнатите страни во заштитата на критичната инфраструктура во сојузните држави и со други државни, локални, племенски, територијални и приватни организации. СЗБ треба да го поддржат развојот на националните активности во областа на справувањето со ризиците преку спроведување проценки за ранливоста и безбедноста за да се идентификуваат недостатоците во безбедноста и потенцијалните слабости во најкритичните инфраструктури во земјата (дополнителен акцент). (Канцеларија за отчетност на Владата на САД, 2017).

Имајќи ја предвид нивната корисност и фактот дека претставуваат големо подобрување во однос на претходните, неусогласени или неконзистентни напори за спроведување на програма на национално ниво, преку добивање информации на локално ниво, улогата на СЗБ пред сè, сепак, се остварува на национално ниво, но истовремено тие ги помагаат и поддржуваат државните, локалните, племенските и територијалните напори. СЗБ се од огромна помош во поврзувањето на властите и сопствениците или операторите на критични инфраструктури на локално ниво. Тие служат како стручни познавачи на НПЗИ

- најзастапениот претставник на напорите во рамките на ПЗКИ на СВБ со кој се најдобро запознаени сојузните држави и локалните власти.

По објавувањето на ПДСП-21 и Извршната наредба (ИН) 13636: *Подобрување на сајбер-безбедноста на критичната инфраструктура*[5], Комитетот за меѓуинституционална безбедност (КМАБ) формираше работна група за преразгледување на Процесот на управување со ризици во објектите во сојузна сопственост: Стандардот на Комитетот за меѓуагенциска безбедност и да ја оцени неговата ефикасност во однос на зајакнувањето на безбедноста и издржливоста на Сојузната критична инфраструктура. ИН 13636 понатаму му наложи на Националниот институт за стандарди и технологија (НИСТ) да го предводи разработувањето на рамката за намалување на сајбер-безбедносните ризици по критичната инфраструктура[6]. Во февруари 2014 година, НИСТ ја објави *Рамката за подобрување на сајбер-безбедноста на критичната инфраструктура*. Рамката беше дополнително ревидирана и во 2018 година беше објавена верзијата 1.1 на документот[7]. Примарната цел на овој документ е да обезбеди заедничка рамка за компаниите и властите преку користење на заеднички јазик кој ги идентификува ризиците по сајбер-безбедноста и го олеснува спроведувањето на практиките и политиките за откривање на слабостите и намалување на ризиците што истите ги носат. Исто така, тој ги опишува методологиите за категоризирање на ризиците и отпорноста кон истите. Едноставноста на Рамката и користењето на светски признати стандарди во истата овозможува таа да се смета за модел за меѓународна соработка во сите сектори.

Во 2017 година, Белата куќа издаде Извршна наредба која се фокусираше на продолжување на зајакнување на напорите за ЗКИ - особено за сајбер-безбедноста на сојузните мрежи и поддршката на сопствениците или операторите на критични инфраструктури. Извршната наредба им даде инструкција на сите сојузни секретаријати да „ја користат Рамката за подобрување на сајбер-безбедноста на критичната инфраструктура (Рамката) разработена од Националниот институт за стандарди и технологија или секаков документ кој би се сметал за наследник на истата, со цел управување со ризиците по сајбер-безбедноста во институцијата". (Белата куќа, 2017).

Директивата понатаму им наложува на клучните секретаријати и институции да „ги идентификуваат властите и капацитетите кои институциите би можеле да ги искористат за поддршка на сајбер-безбедносните напори на критичните инфраструктурни субјекти" (Белата куќа, 2017). Од ова е очигледно дека САД продолжува да ја гледа заштитата на критичната инфраструктура како клучен елемент на националната безбедност.

Во текот на целава оваа дискусија беше нагласена важноста на вклученоста на приватниот сектор во политиките и активностите за ЗКИ. При вр-

5 Извршна наредба 13636 *Подобрување на сајбер-безбедноста на критичната инфраструктура* од 12 февруари 2013. Вашингтон. Сојузен регистар/Том 78, Бр. 33/вторник, 19 февруари 2013/ Претседателски списи

6 Истото, стр.11741

7 Национален институт за стандарди и технологија (2018). *Рамка за подобрување на сајбер-безбедноста на критичната инфраструктура*. Вашингтон: Национален институт за стандарди и технологија, стр.1-48.

шењето надзор во оваа област, Владата на САД се потпира на вклученоста и придонесот на индустријата. Преку многуте координативни совети и секторски специфични организации за размена на информации, заинтересираните страни во секторите развиваат стандарди и најдобри оперативни практики за кои во општа мера полагаат отчетност. Ова не значи дека сојузните, државните, локалните, територијалните и племенските власти не ги применуваат законите, правилата и прописите со кои се уредува спроведувањето на активностите поврзани со критичната инфраструктура. На сите нивоа на власта во САД, институциите спроведуваат законска регулатива која ги води и насочува операциите на сопствениците или операторите во сите 16 сектори. Да се обезбеди сеопфатен список на сите регулаторни документи претставува неблагодарна задача и истото е, впрочем, и непотребно за целите на овој текст. Сепак, за подобро да се илустрира како регулативата ги обликува активностите поврзани со ЗКИ, може да се опише суштината на неколку такви документи.

Националниот план за заштита на инфраструктурата (НПЗИ) од 2013 година го претставува главниот документ во кој се прикажани визијата, мисијата, целите и основните концепти на кои треба да се придржуваат јавните и јавно-приватните сопственици или оператори на критична инфраструктура. Тој ги дава мерилата според кои се вреднуваат партнерствата во однос на остварувањето на поставените цели и сврзаните параметри. Секторски специфичните планови, како што претходно беше посочено, дополнително ги прочистуваат и стеснуваат целите и задачите, како и информациите кои што се релевантни и актуелни за одредени сектори. Организациите за стандарди како што е НИСТ навлегуваат во уште поситни подробности преку разработување на конкретни оперативни практики. Иако НИСТ не е регулаторно тело, стандардите кои тој ги развива произведуваат одредници според кои организациите ја мерат нивната способност да обезбедуваат стоки и услуги на безбеден начин. Сојузната влада на САД ги користи овие стандарди во доделувањето на договори за користење услуги од страна на државниот сектор. Организации од приватниот сектор кои не покажуваат усогласеност со НИСТ во засегнатите области како што е сајбер-безбедноста не ги исполнуваат основните барања кои се јавуваат како неопходни при склучувањето на договори. Овој концепт се применува и во однос на бројни други организациски и индустриски стандарди. Подробен список на организации и индустриите кои тие ги опслужуваат може да се најде на веб-страницата на американскиот Национален институт за стандарди (НИСТ)[8]. Подолу е, пак, краток список на неколку поголеми организации чија работа се однесува на повеќе сектори на критичната инфраструктура истовремено:

1. НСФ Интернешенел. НСФ е невладина, непрофитна организација која е меѓународно призната во областа на јавното здравство и безбедност. Оваа

8 НИСТ обезбедува информации за организациите за разработка на стандарди кои работат да ги усогласат најдобрите практики ширум бројните индустрии кои функционираат во рамките на 16-те сектори на критичната инфраструктура. Иако не се непосредно поврзани со Националниот план, многу стандарди и организации играат клучна улога за овозможување највисоките стандарди на квалитет и сигурност да се одржуваат во јавниот, како и во приватниот сектор https://www.standardsportal.org/usa_en/resources/sdo.aspx

организација обезбедува обука и сертификација во широк спектар на дисциплини поврзани со јавното здравје и безбедност[9].

2. АЗМИ (Американско здружение на механички инженери). АЗМИ е непрофитабилно професионално здружение кое ги промовира механичките и мултидисциплинарните инженерски практики низ целиот свет. Повеќе од 500 технички стандарди на АЗМИ се признаени во светски рамки кои се однесуваат на нуклеарните компоненти, цевководните системи, вентилите, дигалките и садовите со материи под притисок, меѓу останатите области[10].
3. ИСО (Меѓународната организација за стандарди). ИСО е непрофитна организација која развива и објавува стандарди од речиси секаква природа. Таа е со седиште во Женева, Швајцарија и во нејзин состав влегуваат претставници на по едно признаено национално тело за стандардизација од нејзините 164 земји-членки. ИСО е најголемиот разработувач и изработувач на стандарди во светот[11].
4. РТФИ (Регулаторно тело за финансиска индустрија). РТФИ е непрофитна организација овластена од Конгресот на САД да ги заштити инвеститорите со тоа што обезбедува правилна и чесна работа на финансискиот пазар од страна на брокерите-посредници. РТФИ е организација за соработка која изготвува правила кои ги регулираат инвестициите, спроведува проверки на почитувањето на обврските кај фирмите и обезбедува образование за инвеститорите. Дилерите или брокерите лиценцирани од страна на FINRA мора да се придржуваат до ригорозни стандарди за заштита на американските финансиски пазари на инвестиции[12].
5. Стандарди на Секретаријатот за транспорт (СзТ) на САД. СзТ на САД е надлежен за копнените и водните патишта во САД. Оваа институција обезбедува сеопфатна програма која вклучува регулирање, стандарди за производство, оперативни стандарди и создавање општи правила во пошироките рамки на транспортниот сектор. СзТ соработува со невладини организации за стандардизација во бројни области за да обезбеди безбедност и ефикасност на транспортот во земјата. Во областите од интерес се вбројуваат автомобилите, авијацијата, велосипедите и пешаците, јавниот транзит, цевководите и опасните материјали, камионскиот и автобускиот транспорт, поморските и водните патишта и копнените патишта и мостови[13].
6. ЗПЗОО (Законот за преносливост на здравствено осигурување и одговорност). ЗПЗОО од 1996 година утврди стандарди за заштита на поединечните здравствени досиеја и другите лични здравствени информации. Барањата по ЗПЗОО се применуваат во сектори кои го вклучуваат јавното здравје и преносот на лични здравствени информации[14].

9 Подетални податоци за меѓународните стандарди и програми на НСФ може да се најдат на http://www.nsf.org/

10 Подетални податоци за АЗМИ и стандардите на АЗМИ може да се најдат на http://www.asme.org/

11 Подетални податоци за ИСО и нејзините програми може да се најдат на https://www.iso.org

12 РТФИ обезбедува широка палета на алатки и услуги во финансискиот сектор. Сеопфатен опис на нивната регулаторна активност и лиценци е достапен на https://www.finra.org

13 Целосен список на надлежности, активности и постапки е достапен на интернет страницата на Секретаријатот за транспорт https://transportation.gov

14 Правилата за приватност според ЗПЗОО и како тие се применуваат во различите индустрии може да се најдат на интернет-страницата на Секретаријатот за здравство и услуги за човекот. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

7. Северноамериканска корпорација за сигурност на снабдувањето со електрична енергија (НЕРК). Стандардите на НЕРК се однесуваат на производителите на енергија за потрошувачка на големо во Северна Америка. Тие се фокусираат на перформансите, управувањето со ризиците и капацитетите на субјектите[15]. Стандардите на НЕРК ги дефинираат барањата за сигурност на активните системи за снабдување со електрична енергија за потрошувачка на големо. НЕРК развива стандарди преку својот Комитет за стандарди кој е составен од претставници на сите елементи во системот за производство и дистрибуција на електрична енергија и на приватниот и јавниот сектор. НЕРК овозможува усогласување со и спроведување на стандардите и ја регулира електричната мрежа во Северна Америка и сопствениците оператори кои го сочинуваат системот за производство и дистрибуција на електрична енергија.

Ова се неколку од организациите од висок профил кои воспоставуваат и спроведуваат стандарди кои ги опфаќаат сите аспекти на националниот систем на критични инфраструктури. Тоа претставува соработка која вклучува владини институции, непрофитни организации, професионалци од индустриите и академски институции. Само преку земањето учество во овој процес од страна на сите актери во него може да се одлучува за широката и динамична природа на критичната инфраструктура во земјата, како и да се одржува и обезбедува истата.

4.4. Меѓузависноста на секторите на критична инфраструктура

16-те сектори на критичната инфраструктура не може да се разгледуваат независно еден од друг. Секој поединечен сектор се наоѓа во зависен сооднос со другите сектори. Согледувањето на односите меѓу секторите и нивните поделементи, но и како тие меѓусебно ги поддржуваат другите сектори овозможува преземање сеопфатен пристап кон идентификувањето на ризиците и задолженијата во активностите за намалување на истите.

Постои делумна загриженост дека националните и меѓународните енергетски и информатички инфраструктури достигнале ниво на сложеност и меѓусебна поврзаност кое ги прави особено ранливи на каскадни прекини во напојувањето предизвикани од материјално затајување, природни непогоди, намерни напади или човечки грешки. Потенцијалните последици од падовите на мрежите никогаш не биле поголеми бидејќи транспортот, телекомуникациите, нафтата и гасот, банкарството и финансиите, како и останатите инфраструктури зависат од континенталната електрична мрежа за да ги спроведуваат и контролираат нивните дејности.

Секој од претходно споменатите сектори може да се гледа како одредена типична критична инфраструктура „над просечното ниво" во смисла на важноста на услугата или функцијата која истата ја обезбедува. Степенот до кој нашето современо општество се потпира на овие специфични сектори го потврдува нивното означување како „најважни сектори" за критичната инфраструктура.

15 Стандарди, NERC.com 2019. https://www.nerc.com/pa/Stand/Pages/default.aspx

Сè поголем дел од дејностите во светот, индустријата, уметноста и науката, забавата, па дури и криминалот се спроведуваат преку светската мрежа, т.е. преку Интернетот. Но, користењето на овие електронски информациски системи зависи, како и во повеќе поделикатни активности од секојдневниот живот, од многу други комплексни инфраструктури, како што се кабелските и безжичните телекомуникации, банкарството и финансиите, земјиштето, водата и воздушниот сообраќај, гасот, водата и нафтоводите и електричната мрежа.

Земени поединечно, но и во целина, сите овие системи се тесно поврзани со стопанската благосостојба, безбедноста и општествениот состав на заедниците на кои им служат. Разгледувањето на критичната инфраструктура преку согледување на подмножеството на највитални сектори помага да се разјаснат карактеристиките кои се заеднички за основните системи за поддршка и дава увид во инженерските предизвици во напорите за подобрување на ефикасноста на големите мрежи.

Највиталните системи се меѓусебно зависни, првенствено врз основа на објективната близина и оперативната интеракција. Сите највитални системи си влијаат еден на друг. Електричните мрежи, на пример, обезбедуваат енергија за пумпните станици, објектите за складирање и опремата за контрола на преносните и дистрибутивните системи за нафта и природен гас. Нафтата обезбедува гориво и мазива за генератори, додека природниот гас обезбедува енергија за станици за производство, компресори и складишни устројства кои се неопходни за работа на електричните мрежи. Ваквиот реципроцитет може да се воочи меѓу сите највитални системи (O'Rourke, 2007).

Најважната директива за тековната заштита на критичната инфраструктура во политиката на САД е Претседателската директива за спроведување политики бр. 21 (ПДСП-21). По препораките пропишани со ПДСП-21, НПЗИ за 2013 година потврдува дека „ефективното управување со ризиците бара согледување на критичноста на средствата, системите и мрежите, како и поврзаните зависности и меѓузависностите на критичната инфраструктура" (Секретаријат за државна безбедност, 2013).

Проценката на критичните инфраструктурни зависности и меѓузависности е една од седумте основни принципи дефинирани во НПЗИ за 2013 година. Според планот, „согледувањето и справувањето со ризиците од меѓусекторските зависности и меѓузависности е од суштинско значење за подобрување на безбедноста и отпорноста на критичната инфраструктура"[16] (СВБ, 2013). Овие стратешки директиви ја откриваат важноста на анализирањето на зависностите во инфраструктурата, меѓузависностите и поврзаните каскадни ефекти од прекините во функционирањето на критичната инфраструктура за подобрувањето на националната безбедност и отпорност.

Директивата, исто така, ја истакнува важноста на зависностите меѓу највиталните критични инфраструктури, истакнувајќи ја потребата да се разгледаат „зависностите на секторите од енергетските и комуникациските системи и да се утврдат мерките за спречување и ублажување на настани или алтернативните капацитети за време на прекините на тие системи" (Белата куќа, 2013).

16 исто

Теориите кои се развиваат во врска со заштитата на инфраструктурата подразбираат согледување на инфраструктурните системи како сложени интерактивни мрежи (Amin, 2000). Се случува зголемена интеракција меѓу оваа инфраструктура и електричната мрежа, додека обемот и сложеноста продолжуваат да се зголемуваат со брз чекор. Појавата на неколку каскадни падови на мрежата во минатото помогна вниманието да се насочи кон потребата да се разберат комплексните појави кои се доведуваат во однос со овие меѓусебно поврзани системи.

Многу од клучните инфраструктури на нашата земја претставуваат сложени меѓузависни мрежни системи. Најдобрите примери за тоа се силно меѓусебно поврзаните и интерактивни индустрии кои ја сочинуваат една национална или меѓународна инфраструктура, вклучувајќи ги телекомуникациите, транспортот, гасот, водата и нафтоводите, електричната мрежа и множеството сателити во орбитата на Земјата. Интеракциите помеѓу ваквите мрежи ја зголемуваат сложеноста на дејствијата и нивната контрола. Безбедното и сигурно функционирање на овие системи е од основно значење за нашето стопанство, како и за нашата безбедност и квалитет на живот. Овие големи мрежи се карактеризираат со многу точки на интеракција меѓу различните учесници сопственици, оператори, продавачи и купувачи. Поврзаната природа на мрежите ги прави ранливи на каскадни падови со далекусежни последици.

Енергијата, телекомуникациите, транспортот и финансиската инфраструктура стануваат сè поповрзани меѓусебно, со што се поставуваат нови предизвици за нивното безбедно, сигурно и ефикасно функционирање (Amin, 2002). Речиси секоја клучна стопанска и општествена функција зависи од безбедното и сигурно функционирање на инфраструктурата.

Бидејќи овие инфраструктури станаа посложени, со што се оспособија да се справуваат со различни барања, тие со истото станаа и меѓусебно зависни. Интернетот, компјутерските мрежи и нашата дигитална економија ја зголемија побарувачката за сигурен доток на електрична енергија и без никакви нарушувања, додека, пак, банкарството и финансиските системи зависат од стабилноста на електричната енергија, како и на кабелските и безжичните телекомуникации. Транспортните системи, вклучувајќи ги и воените и комерцијалните авиони и копнените и поморските возила, зависат од комуникациските и енергетските мрежи. Врските меѓу електричната мрежа и телекомуникациите, како и меѓу електричната енергија и нафтата, водата и гасоводот продолжуваат да претставуваат основен составен елемент на мрежите за снабдување со енергија. Оваа силна меѓузависност значи дека дејството во еден дел од една инфраструктурна мрежа може брзо да создаде каскадни ефекти на глобално ниво во рамките на истата мрежа, па дури да се прелее и на други мрежи.

Меѓусекторски мерки и соработка

Еволуцијата на меѓусекторската соработка и соработката во заштитата на критичната инфраструктура во САД го вклучува развојот на Меѓусекторскиот совет за критична инфраструктура. Меѓусекторскиот совет за критична инфраструктура претставува меѓусекторски совет за критична инфраструктура

кој е составен и управуван од страна на претставници на приватниот сектор. Основан во 2015 година, Меѓусекторскиот совет за критична инфраструктура ги олеснува консултациите, размената на информации и координираните напори во клучните инфраструктурни сектори и потсектори, како и со Сојузната влада и со Координативниот совет на ниво на државните, локалните, племенските и територијалните власти (КСДЛПТВ), Регионалниот конзорциумски координативен совет (РККС) и Националниот совет за центри за размена на информации и анализи (НСЦРИА) (Секретаријат за државна безбедност, 2015).

Меѓусекторскиот совет за критична инфраструктура беше формиран со цел да се обезбеди можност за влегување во активности со сојузните владини претставници кои би довеле до постигнување на консензус за заедничките приоритети и активности за унапредување на безбедноста, заштитата и отпорноста на критичната инфраструктура, но и одржување заеднички состаноци меѓу Меѓусекторскиот совет за критична инфраструктура и претставници на сојузните секретаријати и институции. Меѓусекторскиот совет за критична инфраструктура е организиран и раководен од, но и одговора пред раководителите и назначените претставници на секторските координативни совети (СКС) кои го сочинуваат неговото членство. Меѓусекторскиот совет за критична инфраструктура им го обезбедува на своите членови неопходниот претставнички форум за консултации, координација и соработка во врска со прашања кои се однесуваат на безбедноста, заштитата и отпорноста на инфраструктурата.

Дополнително, во август 2017 година, Националниот советодавен совет за инфраструктура (НССИ), кој го советува претседателот на САД, препорача да се спроведат натамошни проучувања во насока на зголемување на соработката и зајакнување на меѓусекторските мерки.

НССИ му препорача на претседателот на САД дека Советот може да помогне во оформувањето на активностите за намалување на ризици преку натамошно проучување на следните седум области:

1. Вметнување на отпорноста во планирањето на сојузниот капитал и инвестициите за обновување.
2. Користење на осигурувањето за препознавање и наградување на инвестирањето во отпорноста.
3. Јавно-приватна, меѓусекторска и регионална размена на информации.
4. Ризици предизвикани од меѓусекторската меѓузависност при долготрајни прекини на дотокот на енергија.
5. Безбедност и отпорност на инфраструктурата на пристаништата.
6. Трендови кај работната сила кои влијаат на безбедноста и отпорноста на критичната инфраструктура.
7. Безбедност и отпорност на преносот на нафта и природен гас преку гасоводи и железници (Секретаријат за државна безбедност, 2017).

Бидејќи нашиот свет станува сè поповрзан, а нашиот современ пазар развива побрзи и поинтелигентни системи за да обезбеди контрола и управување со критичната инфраструктура, станува сè поголем предизвик податокот дека ќе бидеме принудени да ги откриваме и ублажуваме ризиците предизвикани од овие зголемени меѓузависни и поврзани системи.

4.5. Идната слика на критичната инфраструктура во Соединетите Американски Држави

Критичната инфраструктура на земјата и фокусот во идентификувањето и заштитата на истата постојано се менува. Од крајот на Втората светска војна до периодот пред 11 септември 2001 година (нападите врз Светскиот трговски центар во Њујорк, САД), фокусот беше ставен врз воено-индустриската база и физичките закани што ги претставуваат чинители надвор од САД и првенствено тие кои доаѓаат од различни странски држави. По нападите на Светскиот трговски центар, кој секако беше настан кој наликуваше на нападот врз Перл Харбор, вниманието на национално ниво се префрли и ранливоста од терористички напади врз инфраструктурата на земјата стана поочигледна. Во периодот до 2007 година, фокусот беше ставен на идентификација и каталогизација на критичните инфраструктурни капацитети на земјата. Во периодот од 2007 до 2013 година, вниманието веќе се сврте кон идентификување и приоретизирање на највиталните сектори и на севкупната меѓузависност на системот на критична инфраструктура како целина. Распространувањето на дигиталната размена на информации и поврзаните дејности доведе до тоа фокусот во овој момент да го ставиме врз градењето на отпорноста и сајбер-безбедноста.

Распространувањето на поврзаните уреди неспоредливо ќе ја зголеми сложеноста на заштитата на критичната инфраструктура. Автоматизацијата и автономните системи претставуваат полиња за нови можни напади во сите сектори. Меѓусебно сè поповрзаната и меѓузависна природа на системите на критична инфраструктура ќе ја направи неопходно потребна меѓусекторската соработка.

Заштитата на критичната инфраструктура низ целата земја и на сите нивоа на власта и на засегнатите страни од заедницата останува приоритет и предизвик. Наодите од Националниот извештај за подготвеност (НИП) од 2017 година покажуваат дека „партнерите од јавниот и приватниот сектор продолжуваат да се фокусираат на подобрување на инфраструктурните системи за решавање на слабостите предизвикани од влошената критична инфраструктура" (стр. 89).

ПЗКИ продолжува да биде висок приоритет, а сепак постојано и сè уште претставува предизвик за американските сојузни држави и локални власти. Сумирајќи го статусот на подготвеност и безбедност во САД, во делот кој зборува за инфраструктурните системи, Националниот извештај за подготвеност од 2017 година ја оценува состојбата изразувајќи загриженост.

Фокусот кај инфраструктурните системи паѓа врз стабилизирањето на функциите на клучната инфраструктура, минимизирањето на заканите по здравјето и безбедноста и ефикасното возобновување и ревитализација на системите и услугите кои треба да поддржуваат една одржлива и отпорна заедница. Додека сојузните секретаријати и институции преземаа чекори во насока на решавање на предизвиците за овој основен капацитет како што е објаснето на страна 89, постои мал број на аргументи кои докажуваат дека земјата постигнала значителен напредок во оваа област. Застарената инфраструктура во многу сектори претставува зголемен ризик, а ја намалува и

отпорноста ... Сојузните држави и територии утврдија дека овој основен капацитет покажува потпросечни нивоа на ефикасност во 2016 година (стр.14).

Без разлика на пристапот кој бил применет, треба да се има основно разбирање за елементите што го сочинуваат системот. Предизвик за идните истражувачи, без разлика дали станува збор за тие во академскиот, приватниот или државниот сектор, ќе биде да развијат „модел на зрелост" за оценување на локалните активности за заштита на критичната инфраструктура, како и водич кон еден поцелосен и позрел модел за намалување на ризиците и одржување на отпорноста. Заштитата на критичната инфраструктура мора да продолжи да се развива за да се задоволи динамичната природа на зрелите општества, променливите потреби на народите кои живеат во нивни рамки и развојот на нови и досега непознати технологии. Располагањето со една подвижна, прилагодлива и интегрирана методологија која ги употребува силите на сите засегнати страни во системот е единствениот начин да се обезбеди отпорна и безбедна архитектура на критичната инфраструктура.

Заклучок

Во ова поглавје се разгледуваат пет аспекти на заштитата на критичната инфраструктура. Во делот еден, беше наведена општата структура на заштитата на критичната инфраструктура во САД. Во овој дел се зборува за шеснаесетте сектори на критична инфраструктура и истиот ги посочи институциите на државната управа со примарна надлежност во развојот на политиките, надзорот, стратешкото планирање, соработката во безбедноста и спроведувањето на сè од наведеното. Во вториот дел се разгледува јавно-приватниот карактер на сопственоста и надзорот врз критичната инфраструктура и се идентификувани некои од формалните групи за соработка кои се создадени со цел да ги здружат заинтересираните страни за, преку предизвиците со кои се соочува земјата, заедно да работат за да ја обезбедат нејзината критична инфраструктура. Третиот дел ја разгледува структурата на националните стандарди кои создаваат рамки што се користат за воспоставување конзистентност меѓу секторите и создавање на заеднички јазик за сите засегнати страни во сите сектори. Четвртиот дел се надоврзува на третиот и отвора дискусија за меѓусебната зависност на шеснаесетте критични инфраструктурни сектори, сочејќи на натамошното означување на највиталните сектори. Имајќи предвид дека секторите не можат да се согледуваат независно еден од друг, структурата на националните стандарди и националните рамки, како што е Рамката на сајбер-безбедност на НИСТ, обезбедува меѓусекторска стандардизација и помага да се обликува природата на потенцијалните каскадни ефекти од настаните кои произлегуваат од еден или повеќе сектори. Конечно, поглавјето го разгледуваше идниот лик на заштитата на критичната инфраструктура, понудувајќи кратка дискусија за влијанието на сајбер-инцидентите, зголемувањето на бројот на поврзани уреди и леснотијата за предизвикување нарушувања од страна на недржавни актери на геополитичката сцена која се менува и еволуира.

Начинот за придвижување напред во заштитата на критичната инфраструктура и за практичарите во областа е сложен и непрекинато се менува. Потребата за соработка и партнерство меѓу секторите и меѓу засегнатите страни од приватниот и од јавниот сектор ќе станува сè поголем императив во иднина. Знаејќи дека секојдневниот живот станува сè поповрзан и обичниот човек станува сè позависен од автономни услуги и меѓусебно поврзани уреди, улогата на поединецот во заштитата на критичната инфраструктура исто така ќе расте во важност. Секој систем е само онолку безбеден колку што е и неговата најслаба точка. Силниот план за заштита на критичната инфраструктура ги опфаќа сите можни ранливости и слабости и во себе го вклучува и човечкото суштество како такво.

ГЛАВА 5

ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО ХРВАТСКА

Глава 5

ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО ХРВАТСКА[17]

Доц. д-р Роберт Микац
Факултет за политички науки при универзитетот во Загреб

Ова поглавје дава увид во тековниот развој на оваа област во Република Хрватска. Република Хрватска, до нејзиното членство во Европската унија во 2013 година, донекаде посвети внимание на стратешките и нормативните документи кои се однесуваат на критичната инфраструктура, но не воспостави заокружена законска и подзаконска рамка со која би започнала процес на развивање на систем за заштита на критичната инфраструктура. Непосредно пред влезот во полноправно членство во ЕУ, Хрватска го усвои *Законот за критична инфраструктура* и ја постави неопходната начелна нормативна рамка за започнување на плански развој на оваа област (Влада на Република Хрватска, 2013а). Ваквата системска уредба претставуваше основа за понатамошниот развој на оваа област, како и првичен чекор кон градење на систем за заштита на критичната инфраструктура.

Оттогаш, воспоставувањето на стратегиската и нормативната рамка за заштита на критичната инфраструктура се одвиваше во три фази, што е значајно да се истакне, имајќи предвид дека реализираните документи, процеси и настани во секоја фаза го овозможија постепеното градење и развој на посакуваниот систем на заштита на критичната инфраструктура во Република Хрватска. Исто така, важно е да се нагласи дека Хрватска во моментов не располага со систем за заштита на критичната инфраструктура кој би можел да се смета за целосно воспоставен како таков. Контурите на системот се поставени, а вложени се и значајни напори за негово спроведување. Нормативната основа е поставена, клучните актери се познати, процесите се воспоставени, но она што претставува клучен предизвик во таа насока во овој момент е недостатокот на координација.

Овој преглед и анализа ги претставува клучните активности што ги спроведува Република Хрватска, разгледувајќи ги ваквите тековни процеси и идните можности во таа насока, а со цел да се извлечат конкретни поуки кои можат да бидат корисни од планска гледна точка при разработката на стратегиската, нормативната и оперативната рамка за заштита на критичната инфраструктура во Република Северна Македонија, за чии потреби оваа анализа и беше спроведена. Временскиот период на анализата е од 2008 до крајот на

17 Начелното истражување во оваа област чија цел беше да се истакне целокупната слика и да се анализираат активностите кои се преземаат во тој поглед во Република Хрватска беше изготвено за потребите на книгата Микац, Р.; Цезарец, И и Ларкин. Р. (2018), Критична инфраструктура: Платформа за успешна национална безбедност, Загреб: Јесенски и Турк
За потребите на ова истражување, текстот на наведеното начелно истражување беше преработен и дополнет.

2018 година, при што сите настани се хронолошки подредени и анализирани во целите на следење на различните развојни фази, нивно надополнување и изнаоѓање нови решенија.

Структурата на поглавјето е поделена на следните четири дела: 1. Периодот до влегувањето на Република Хрватска во Европската унија во 2013 година; 2. Воспоставувањето на регулаторната и стратегиската рамка за заштита на критичната инфраструктура, кое го покрива периодот од 2013 до крајот на 2018 година; 3. Структурните предизвици во воспоставувањето на систем за заштита на критичната инфраструктура; и 4. Заклучок. Редоследот по кој истите се изложени се движи од поопшти кон посложени, а со цел да се покаже широчината на областите и предизвиците во воспоставувањето на систем за заштита на критичната инфраструктура.

5.1. Периодот до влегувањето во членство во Европската унија

Во последните десет до петнаесет години, Република Хрватска работи на нормативно и стратегиско уредување на областа за зајакнување на отпорноста и заштитата на критичните инфраструктури. До влегувањето во Европската унија, Република Хрватска ја подвлекуваше важноста на идентификувањето и заштитата на критичните инфраструктури во редица од нејзините стратегиски документи, како и во одредени национални закони. Овде тие ќе бидат хронолошки анализирани при што внимание ќе се обрне на нивните најзначајни делови.

Во *Националната стратегија за заштита од и борба против тероризмот* од 2008 година, концептот на критични инфраструктури се согледуваше од аспект на заштитата од терористички закани. Како што е наведено во стратегијата: „Начелно, терористичката закана може да варира меѓу поединечни напади врз високо симболични вредности, напади насочени кон предизвикување што е можно повеќе жртви, ширење посериозен страв и поголем степен на уништување и напаѓање на државната критична инфраструктура. Државната критична инфраструктура се состои од средства, услуги и системи (сообраќајни, енергетски, комуникациски, индустриски, финансиски и административни) кои го поддржуваат економскиот, политичкиот и општествениот живот во Република Хрватска, а чијашто важност е таква што нејзината целосна или делумна загуба или целосната или делумна опасност по неа предизвикуваат големи човечки загуби, имаат сериозно влијание врз државната безбедност и стопанството и имаат други сериозни последици за заедницата во целост или за делови од истата“ (Влада на Република Хрватска, 2008: т. 8). Во сегментот за заштита од тероризам, Стратегијата укажува дека Република Хрватска треба да изгради национални капацитети за заштита на критичната инфраструктура.

Како најважен документ за планирање на операциите за заштита и спасување на оперативните сили и организацијата на системот на цивилна заштита во одговор на големи несреќи и катастрофи, *Планот за заштита и спасување* на Република Хрватска од 2010 година, ја спомнува критичната инфраструктура во контекстот на вршење преглед на обврските што ги имаат учесниците

вклучени во спроведувањето на мерките за заштита и спасување. Според тоа, Планот не дава дефиниција за критична инфраструктура, иако концептот се појавува при објаснувањето на обврските (во преземањето мерки за заштита и спасување) на учесниците во системот на цивилна заштита преку истакнување на детерминантите за заштита на ранливите (загрозени) критични инфраструктурни објекти (во случај на поплави) и враќањето во функција на објектите кои спаѓаат во критична инфраструктура (во случај на земјотреси). Во врска со спроведувањето на Планот, еден од важните аспекти при неговата примена е „планирањето на процедурите, носителите, изворите на финансирање и координацијата на реконструкцијата на оштетените и уништените основни ресурси и инфраструктурни објекти кои припаѓаат на критичната инфраструктура, како и утврдувањето на концептот на целосно обновување на заедницата погодена од катастрофа и несреќа од големи размери" (Влада на Република Хрватска, 2010: точка 6).

Законот за приватна заштита од 2010 година ја дефинира критичната инфраструктура како „активности, мрежи, услуги и стоки кои спаѓаат во материјални и информатички технологии, а чие затајување или уништување би имало значително влијание врз здравјето и безбедноста на граѓаните или ефикасното функционирање на државната власт" (Хрватски сабор, 2010). Во својата нормативна рамка, државата предвидува дека треба да се заштитат критичните инфраструктурни објекти, но сопственикот или управителот е тој кој одлучува на каков начин истото ќе се спроведе. Со оглед на тоа што приватните агенции за обезбедување располагаат со значителни капацитети за заштита на средствата (не само во поглед на човечките ресурси, туку и на техничките решенија со кои располагаат), за да се обезбеди високо ниво на системска безбедност, а пред сè во однос на мерките за превенција, за таа цел се ангажираат токму такви агенции.

Проценатa на ризиците за Република Хрватска од природни и технички-технолошки катастрофи и големи несреќи (2013), ја става критичната инфраструктура во поширокиот контекст на заштитата од природни и антропогени извори на закана. Во рамките на овој документ се спомнува концептот на заштита на критичната инфраструктура како „заеднички назив за мрежите и системите кои се клучни за функционирањето и животот на заедницата, а чие оштетување или уништување може да предизвика привремени или долгорочни нарушувања и кризи, и коишто се од особен интерес и значење за Република Хрватска како целина, но делумно и за единиците на локалната и регионалната самоуправа" (Влада на Република Хрватска, 2013б: 72). Проценатa на ризиците наведува дека „критичната инфраструктура во Република Хрватска не е дефинирана, ниту пак воопшто е проценета потребата од заштита и обезбедување континуирано функционирање на истата во Република Хрватска, а особено при итни состојби, па затоа е изготвен предлог-закон за критична инфраструктура кој ги зема предвид деловите од законодавството на Европската унија содржани во *Директивата 2008/114/ЕЗ на Советот од 8 декември 2008 година за идентификација и означување на европската критична инфраструктура и процена на потребата за подобрување на нивната заштита* (Службен весник на Европската унија L345 / 75, 23.12.2008) и го усогласува

националното законодавство со таа регулатива на Европската унија“ (Влада на Република Хрватска, 2013б: 73). Проценета на ризикот ја подвлекува потребата од подигнување на нивото на безбедноста на критичната инфраструктура што ќе ја овозможи идната нормативна рамка и одредбите кои би требало со истата да се пропишат.

Националната стратегија и Акцискиот план за непролиферација на оружје за масовно уништување (2013) ја споменуваат како конкретна цел заштитата на критичната инфраструктура и населението од криза предизвикана од масовно уништување (Влада на Република Хрватска, 2013в). Покрај оваа одредба, предметот не е разработен во натамошни подробности.

Иако постои јасен интерес за нормативно обликување на концептите сврзани со критичната инфраструктура, ниту еден од документите не обезбеди целосно решение за управување со ризиците по функционирањето на критичната инфраструктура, како и рамка за нејзина заштита, пред сè поради податокот дека ова не беше посочено како главна цел во наведените документи (Микац и Цезарец, 2019). Во периодот до пристапувањето кон Европската унија, интересот на законодавците и разните експерти во оваа област беше значителен. Сите се согласија дека постои потреба да се воспостави конкретна област посветена на развојот на критичната инфраструктура, бидејќи критичните инфраструктури во тоа време беа разгледувани како дел од областите заштита и спасување, заштита од тероризам и заштита од оружје за масовно уништување и во својство на (дополнителен) инструмент во спроведувањето на соодветните политики, при што, во однос на начинот на кој се разгледува и артикулира, не беше воопшто оформена како целина.

5.2. Воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура

Процесите поврзани со изградбата на системот за заштита на критичната инфраструктура се одвиваа во три временски периоди или циклуси. Првиот, кој го одбележуваше обврската да се регулира заштитата на европските, а потоа и на националните критични инфраструктури на национално ниво, при што клучниот момент претставуваше донесувањето на *Законот за критична инфраструктура* во текот на 2013 година. Вториот временски период од 2014 до 2015 година го одбележа усвојувањето на ажурираната *Национална стратегија за спречување и борба против тероризмот* и на *Националната стратегија за сајбер-безбедноста*, при што двете стратегии, а особено втората, ја нагласија важноста од продолжување на активностите во областа на заштитата на критичната инфраструктура во насока на воспоставување на сеопфатен систем за заштита на истата. Третиот, кој се одвиваше во периодот од 2016 до 2018 година, кога беа донесени следните документи: новата *Стратегија за национална безбедност на Република Хрватска*, *Законот за систем за внатрешна безбедност* и *Законот за сајбер-безбедност на спроведувачите на клучни услуги и давателите на дигитални услуги*. Секоја нова стратегија и закон поттикнаа нови процеси кои беа повеќе конкретизирани и ги насочуваа сите фактори во градењето на еден систем за заштита на критичната

инфраструктура кон заедничката и конечна цел, а тоа беше воспоставувањето на самиот систем како таков.

Прв циклус – 2013 година

Значителните чекори за решавање на критичната инфраструктура во Република Хрватска започнаа под влијание на *Директивата 2008/114/ЕЗ на Советот од 8 декември 2008 година за идентификација и означување на европската критична инфраструктура и процена на потребата за подобрување на нејзината заштита (Директива 2008/114/ЕЗ)* во 2011 година со која се регулира прашањето за Европските критични инфраструктури, при што наведената Директива 2008/114/ЕЗ утврдува дека земјите-членки се одговорни за воспоставување на нормативна рамка за заштита на европските критични инфраструктури (Совет на Европската унија, 2008), што за многу земји исто така претставуваше јасна покана за дефинирање на начините за заштита на нивната национална критична инфраструктура. По ова, засегнатата професионална и научна јавност во Република Хрватска го зголеми интересот за предметната област преку организирање бројни семинари, работилници и конференции за критичната инфраструктура.

Како дел од процесот на постигнување на полноправно членство во Европската унија, Република Хрватска се обврза нормативно да ги подреди и уреди прашањата за идентификација, означување и заштита на европските критични инфраструктури преку транспонирање на *Директивата 2008/114/ЕЗ* во нејзиното законодавство и нејзино применување до моментот на стапување во полноправно членство. Покрај наведената *Директива 2008/114/ЕЗ*, намерите на Република Хрватска беа да ја регулира областа на управување со ризици во работењето и заштитата на националните критични инфраструктури со закон и подзаконски уредби кои се однесуваат на следново:

- Критичната инфраструктура како темел на националната и јавната безбедност, како и на одржливиот развој и напредокот од клучен интерес, не само за населението/поединците, туку и за целокупното стопанство, општествената активност и државата како целина.
- Изложеноста на опасности, како на тие од природно потекло, така и на оние предизвикани од технички или технолошки процеси - вклучувајќи ја и изложеноста на терористички активности во реалниот и во сајбер-просторот.
- Ставањето акцент на ранливоста на критичните инфраструктури, имајќи предвид дека ресурсите на Република Хрватска не дозволуваат целосно развивање на алтернативни или излишни системи, но и податокот дека чувствителноста се зголемува со меѓусебната поврзаност и меѓузависноста на бројните сектори, како на национално ниво, така и со клучните инфраструктурни сектори на соседните и другите земји.
- Недостатокот на интегриран, единствен и сеопфатен систем за управување со кризи.

Во целите на имплементација на *Директивата 2008/114/ЕЗ* и уредување на предметната област, Владата на Република Хрватска на 25 ноември 2010 го-

дина донесе *Одлука за основање на Меѓуресорска работна група за подготовка на активностите потребни за дефинирање и утврдување на Националната критична инфраструктура на Република Хрватска*, која ги засили своите напори за изготвување на Законот за критична инфраструктура во септември 2012 година. Со анализа на националните законодавства на земјите-членки на Европската унија, Работната група одлучи дека прашањето за критичната инфраструктура во Република Хрватска треба да биде соодветно уредено со усвојување на соодветен закон (Чемерин, 2013).

Од анализите на актуелните согледани практики, утврдено е дека тие во голема мера се разликуваат во одделните земји во Европската унија. На пример, Република Италија одлучи единствено да ја регулира идентификацијата и означувањето на европските критични инфраструктури, изоставувајќи ја нормативната активност во врска со прашањата на националните критични инфраструктури. Најголемиот број земји избраа прагматичен пристап и со единствена нормативна рамка ги заокружија активностите поврзани со идентификување, означување и заштита на европската, како и на националната критична инфраструктура. Некои земји, како што се Чешка и Полска, направија „чекор понатаму" и, како дел од нужната интеграција на различните процеси, активностите поврзани со заштитата на критичните инфраструктури ги инкорпорираа во националните уредби за управување со кризи. Република Хрватска одлучи преку своето законодавство да ја регулира областа на идентификација, означување и заштита на европската инфраструктура во исто време со националната критична инфраструктура, што, пак, претставува сеопфатен одговор на барањата на Европската комисија.

По јавната расправа, предлог-законот беше доставен на усвојување во Саборот, кој го изгласа кон крајот на април, за истиот потоа да биде и прогласен во мај 2013 година. Законот ги уредува правата, овластувањата и обврските на Владата на Република Хрватска и централните органи на државната управа, како и овластувањата, правата и обврските на сопственикот или управителот на критични инфраструктури во идентификувањето, означувањето и заштитата на националната критична инфраструктура и обезбедување на нивно непречено функционирање. Исто така, Законот ги утврдува дефинициите за национална и европска критична инфраструктура, сектори на критична инфраструктура, управување со критичната инфраструктура, начинот на изработка на анализите на ризик, плановите за безбедност на сопственикот или управителот, позицијата и улогата на офицерите за врска за безбедноста за критичната инфраструктура, но и потврдува дека европската критична инфраструктура е заштитена со истите мерки кои важат и за националната критична инфраструктура. Покрај тоа, размената на чувствителни и класифицирани информации во таквите цели е регулирана со поистоветување на истата со надзор врз спроведувањето на Законот (Влада на Република Хрватска, 2013а).

Законот ги постави основите за започнување на повеќересорска соработка во идентификувањето, означувањето и заштитата на националната критична инфраструктура и соработката со соседните земји и телата на Европската унија во означувањето и заштитата на критичните европски инфраструктури на територијата на Република Хрватска и другите земји. По усвојувањето на

нормативната рамка, се создадоа предуслови за отпочнување на процес на спроведување сеопфатни дејства за заштита, зајакнување на отпорноста и намалување на негативните влијанија во случај на закани по критичната инфраструктура. Во наведената нормативна рамка, Република Хрватска ги постави предусловите за воспоставување на систем кој ќе биде задолжен за заштита на критичните инфраструктури, како на домашните, така и на европските, доколку некои се означени како такви на територијата на Република Хрватска.

Во согласност со *Законот за критична инфраструктура*, усвоени се уште две уредби кои заедно ја обликуваат нормативната рамка во областа на постигнување безбедност и зајакнување на отпорноста на критичните инфраструктури. Првиот документ е *Одлука за означување на областите во кои органите на државната управа на централно ниво ги идентификуваат националните критични инфраструктури и списоците со редоследот на областите со критични инфраструктури* кои препознаваат единаесет области во кои органите на државната управа на централно ниво (девет надлежни министерства) можат да идентификуваат национални критични инфраструктури, а тоа се следниве области: 1. Енергетика; 2. Комуникациска и информатичка технологија; 3. Транспорт; 4. Здравствена заштита; 5. Водостопанство; 6. Храна; 7. Финансии; 8. Производство, складирање и транспорт на опасни стоки; 9. Јавен сектор; 10. Национални споменици и вредности; 11. Наука и образование. (Влада на Република Хрватска, 2013г.). Вториот нормативен документ е *Правилникот за методологијата за изработка на деловна анализа на ризици за критичната инфраструктура* која ги утврдува насоките, критериумите и одредниците за идентификување на критичните инфраструктури и анализите на ризиците за функционирањето на критичните инфраструктури, како и обврските на давателите на услугата на изработка на деловна анализа на ризик за критичната инфраструктура (Државна управа за заштита и спасување, 2013). Со цел усогласување со меѓународните стандарди, во 2016 година беше усвоен и влезе во сила новиот *Правилник за методологијата за изработка на деловна анализа на ризици за критичната инфраструктура* која се заснова на меѓународниот стандард ISO 31000:2009 Управување со ризик: Начела и насоки (Државна управа за заштита и спасување, 2016) година), со што престана важноста на претходната уредба од 2013 година.

Во фазата на неговото усвојување и веднаш по неговото донесување, *Законот за критична инфраструктура* предизвика многу коментари во однос на она што требало да се направи или што било пропуштено при воспоставувањето на нормативната рамка. Крунослав Антолиш (2013) смета дека дефиницијата за критична инфраструктура во Законот е недоволна, бидејќи концептот не го вклучува поимот „сопственост", при што интелектуалниот капитал е особено важен како клучен фактор во поддршката на развојот на Република Хрватска, што претставува многу интересно согледување, имајќи предвид дека интелектуалниот капитал е значајна вредност за секое општество и би било од големо значење да се вметне во дефиницијата, но се поставува прашањето како истиот да се објасни и вреднува. Ксенија Буторак (2013) анализира неколку различни методологии за процена на деловни ризици за критични инфраструктури и обезбедува преглед на најзастапените такви процени на глобално ниво.

Иако таквата нејзина анализа обезбеди голема (додадена) вредност, за жал таа не најде примена во тој период. Иван Показ (2013) ја нагласува важноста на разузнавачката поддршка за сопствениците или управителите на критичните инфраструктури. Ова е исклучително важно, бидејќи, доколку законодавецот им наложува обврска и одговорност на сопствениците или управителите да ја заштитат критичната инфраструктура и не им обезбедува поддршка во форма на размена на податоци и информации што им се неопходни и до кои самите не можат да дојдат, тогаш тие не можат да ја постигнат својата основна задача да го заштитат сопствениот имот што спаѓа во национална критична инфраструктура.

Важноста на овој закон се состои од податокот дека истиот претставува системска уредба за критичната инфраструктура и главна нормативна точка за следење и спроведување на сите активности во оваа област. Ова исто така важи и за прашањето на дефинирањето на самиот концепт на заштита на критичната инфраструктура и обврските кои произлегуваат од истиот. Во тој период беше воочливо користењето на различни дефиниции на наведениот концепт од страна на многу хрватски автори и практичари, кои пак споменуваа и различни фактори во процесот на идентификување, означување и заштита на критичните инфраструктури и користеа различни нормативни извори на Република Хрватска кои беа во сила пред усвојувањето на *Законот за критична инфраструктура*. Ова не беше добра практика, па така подигањето на свеста во таа насока значеше претворање на одредбите од Законот во почетна точка за понатамошна дискусија и дејствување. Законодавецот сфати дека при усвојувањето нови стратегиски и нормативни документи, тој спровел само нормативно усогласување и „прескокнување" на критичните инфраструктури при одредувањето на надлежноста на уредбите донесени по влегувањето во сила на Законот за критична инфраструктура. Како пример може да се спомене стратегискиот документ наречен *Процена на ризик од катастрофи за Република Хрватска* усвоен во 2015 година, во кој концептот за критичната инфраструктура се користи само делумно при прикажувањето на последиците од различните ризици за нејзино оштетување или прекин на функционирањето, па така целокупната рамка се потпира врз односниот Закон. Земајќи го сево ова предвид, повикувањето на претходни документи понатаму станува беспредметно.

Во дискусијата за критичната инфраструктура, важно е да се посочат и степените на надлежност. *Законот за критична инфраструктура* и придружните одлуки и уредби, ја пропишаа заштитата на критичната инфраструктура само на национално ниво без да наметнуваат обврски за единиците на локалната и регионалната самоуправа. Ова е важно да се нагласи од три причини. Прво, со тоа, се укинува надлежноста и потребата националната критична инфраструктура да се согледува и на пониските политички нивоа како што беше наведено во некои од поранешните стратешки документи. Второ, единиците на локална и регионална самоуправа може на нивната територија да имаат национална критична инфраструктура, но немаат одговорност за нивна идентификација, додека пак, од друга страна, се одговорни за нивната заштита (заштитата се спроведува во координација со државните институции и сопствениците или

управителите на критичните инфраструктури). Трето, иако е неспорно дека единиците на локална и регионална самоуправа имаат во нивна сопственост и во нивната област локална критична инфраструктура од важност за нивната работа, за безбедноста на луѓето и за функционирањето на деловните субјекти, истата не претставува национална критична инфраструктура.

Државната управа за заштита и спасување (ДУЗС), тело на државната управа на централно ниво надлежно за активностите за цивилна заштита, е назначена како координативно тело за споменатите активности и општо за целиот систем на критична инфраструктура. Ова е разбирливо со оглед на преклопувањето на областите за заштита на критичната инфраструктура и цивилната заштита, а во контекст на идентификација на заканите и ризиците, процена и анализа на ризиците и спроведување мерки за намалување на ризиците. ДУЗС е исто така национална контакт-точка за соработка со земјите-членки на ЕУ и со Европската комисија (Микац и Цезарец, 2016).

По влегувањето во сила на Законот за критична инфраструктура, ДУЗС одржа консултативни состаноци со претставници на органите на државната управа на централно ниво кои подлежат на обврските според Законот, а во врска со следното: Определување на офицер за врски за безбедност и негов заменик за секој сектор на критична инфраструктура во соодветната област и обезбедување на управување со критичните инфраструктурни ризици и нивна заштита, вклучително и поставување на секторски одредници за идентификација и секторска анализа на ризик; идентификација и изготвување на предлози за критична инфраструктура; изработка на секторски планови за обезбедување на функционирањето на критичната инфраструктура со обезбедување испорака на стоки или услуги од неговиот делокруг. Беа организирани неколку работни состаноци каде што се толкуваше принципот, контекстот и „духот" на критичната инфраструктура. Состаноците, исто така се одржуваат на барање и по потреба во министерствата одговорни за одредени клучни инфраструктурни сектори. Различни работилници беа спроведени како дополнителна поддршка за спроведување на планираните активности, но беше воочливо дека основната обврска не беше прифатена подеднакво од страна на сите надлежни тела, имајќи предвид дека некои претставници не реагираа на состаноците и не ги реализираа обврските и заклучоците од заедничката координација на сите засегнати страни.

И покрај напорите и иницијативите на Државната управа за заштита и спасување и одредени засегнати страни од релевантните министерства кои ја признаа важноста на оваа активност, почетните неколку години (од 2013 година наваму) беа обележани со неусогласен пристап и нееднаков одговор од стрна на сите чинители во процесот. Еден од првичните предизвици се состоеше од недостатокот на политичка „тежина и моќ" на координаторот на системот - ДУЗС, која како орган на државната управа претставува тело со пониски надлежности од министерствата чии активности е предвидено таа да ги пропишува и координира. Со *Законот за критична инфраструктура*, на министерствата како секторски носители им се оставени шест месеци по усвојувањето на Законот во 2013 година, за да ја идентификуваат критичната инфраструктура во нивните сектори, да ѝ предложат на Владата истата да ја означи со Одлука, а потоа, за-

едно со сопствениците или управителите на овие инфраструктури, да го воспостави и следи процесот на нејзина заштита. Во предвидениот период, ниту едно министерство (девет министерства се одговорни за единаесет сектори во кои е можно да се идентификуваат и назначат критични инфраструктури) не го остварии пропишаното (иако постојат позитивни примери на преземени напори) и токму од таа причина не е можно да се координира воспоставувањето на внатрешните процеси во рамките на системот, имајќи го предвид непостоењето во тој момент на сите неопходни елементи за поврзување на соработката, практиката и размената на знаења и искуства.

Во анализираниот период, во согласност со *Директивата 2008/114/ЕЗ,* воспоставени се обврски во врска со процесот на идентификување на критичните европски инфраструктури. Преку свикување и одржување билатерални состаноци, Државната управа за заштита и спасување презеде иницијатива за идентификување и утврдување на европските критични инфраструктури на територијата на Република Хрватска или територијата на соседните земји-членки на Европската унија - Словенија и Унгарија (кои се важни за Република Хрватска). За време на билатералниот разговор со претставници на Република Словенија (Министерството за одбрана на Република Словенија е националното тело задолжено за координација на критичната инфраструктура во Република Словенија) се утврди дека на територијата на Хрватска или на Словенија не постојат критични инфраструктури кои би биле значајни и за двете земји. При разгледувањето на европската критична инфраструктура со Унгарија, претставниците на двете земји (Министерството за внатрешни работи на Унгарија - Управата за управување со катастрофи е надлежна за критичната инфраструктура во Унгарија), како свој главен приоритет, ја утврдија идентификацијата и означувањето на нивните национални критични инфраструктури, и само потоа тие беа подготвени да дискутираат за прекуграничните влијанија. Беше договорено дека, по спроведувањето на процесот на национално ниво, Унгарија ќе воспостави контакт со Хрватска за спроведување на анализата на овие влијанија (Цезарец, 2017, Микац и Цезарец, 2019 година).

2013 година беше исклучително значајна во однос на различните содржински активности поврзани со прашањата од критичната инфраструктура, но и покрај сите од горенаведените, изостанува конечниот исход во првата фаза од процесот на воспоставување на систем за критична инфраструктура, а тоа е идентификацијата на поединечни објекти, мрежи или системи како национална критична инфраструктура. Практиката покажа (и покрај постојната нормативна рамка, не е направен почетниот чекор за идентификација и не е означена националната критична инфраструктура) дека е потребен подолг период и интензивиран процес за воспоставување на таков систем. Гледајќи од позитивна перспектива, иако 2013 година не даде конкретни резултати, таа постави многу нешта кои претставуваа основа за процесите кои се одвиваа во наредните години. Без разлика дали станува збор за воспоставување соработка помеѓу засегнатите страни, или, пак, согледување на одредени пропусти, идентификување на таквите како неуспеси и преземање чекори и мерки за да се исправат, сето тоа претставува капитал за иднината. Во 2013 година постоеја примери за спомнатото.

Втор циклус – 2014 до 2015 година

Продолжувањето на развојот на целиот процес на заштита на системот на критична инфраструктура и неговото воспоставување беа поттикнати преку изготвување на две стратегии: *Националната стратегија за спречување и борба против тероризмот* и *Националната стратегија за сајбер-безбедноста*, заедно со придружните а кциски планови. Пред да разгледаме зошто овие стратегии се значајни, неопходно е да им обрнеме внимание на трите трудови (анализи) на националните експерти кои ги посочија суштинските работи во воспоставувањето на систем за заштита на критичната инфраструктура.

Анита Перешин и Александар Клаиќ (2012: 336) дадоа навистина добар исказ дека „заштитата на системот (на критичната инфраструктура) не подразбира само физичка заштита, туку и заштита на податоци и информатички системи, односно електронски услуги поврзани со одредена критична инфраструктура, целосна примена на соодветни политики за безбедност на информации, како и заштита на сајбер-просторот каде се генерираат и пренесуваат различни видови податоци. Според тоа, критичната информатичка инфраструктура го претставува електронскиот проток на информации и во таа смисла самиот сајбер-простор претставува критична информатичка инфраструктура, што резултира со потребата за согледување на тесната врска помеѓу концептите за заштита на критичната инфраструктура и заштитата на сајбер-просторот". Ова гледиште не беше земено предвид во текот на изготвувањето на *Законот за критична инфраструктура,* кој во основа е изработен следејќи ја филозофијата дека заштитата на критичната инфраструктура претставува заштита само на физички предмети, мрежи и системи. Авторите потоа велат: „За воспоставување на систем на заштита (на критични инфраструктури), многу е важно да се утврди национална политика за безбедност на информациите" (Перешин и Клаиќ, 2012: 336). Ова беше применето при изготвувањето на *Националната стратегија за сајбер-безбедност*, која беше прв документ од ваков вид во Република Хрватска. Овој процес е многу важен бидејќи „безбедноста на сајбер-просторот е од клучно значење за безбедноста на критичната инфраструктура како целина" (Перешин и Клаиќ, 2012: 338). Авторите заклучуваат дека „заштитата на националната критична инфраструктура не може да се постигне без соодветна заштита на сајбер-просторот во кој се пренесуваат и складираат податоците поврзани со работата на критичната инфраструктура" (Перешин и Клаиќ, 2012: 352). Презентираниот труд ја покажува неразделната врска меѓу елементите на критичната инфраструктура и нејзините физички и информатички делови, на кои секако треба да се додаде третата компонента - луѓето. Го споменавме овој труд бидејќи, иако беше напишан во 2012 година, ги отвори прашањата кои всушност беа решени во анализираниот период од 2014 до 2015 година.

Вториот важен документ на кој сакаме да се осврнеме е поврзан со значењето на поддршката на разузнавачката заедница во воспоставувањето на ефикасен систем за заштита на критичната инфраструктура и поддршката од истата за сите засегнати страни во таквата заштита. Дарио Малнар и Никола Млинац, вработени во Агенцијата за безбедност и разузнавање на Република Хрватска, ги утврдија одредбите на *Законот за критична инфраструктура*

чија имплементација бара ангажирање на безбедносниот и разузнавачкиот систем - станува збор за анализа на ризиците за критичната инфраструктура, разработување сценарија за можни закани, развивање на секторски насоки кои вклучуваат процена на ризик и развивање на план за безбедност за сопствениците или управителите на критичните инфраструктури (Малнар и Млинац, 2014). Ова е многу важно ако се знае потребата за соработка помеѓу Државната управа за заштита и спасување и разузнавачката заедница, што беше и истакнато од страна на вработените во Агенцијата за безбедност и разузнавање во рамките на академските кругови (како на пр. во нивните трудови), имајќи предвид дека вистинска соработка не се воспостави во потребната мера во текот на годините во кои се изготвуваше *Законот за критична инфраструктура*. Авторите потоа ги набројуваат активностите кои ги спроведува разузнавачкиот систем и се поврзани со процесите од интерес за ова истражување. Тие наведуваат дека „безбедносниот разузнавачки систем функционира преку собирање на податоци и, стратешки и аналитички, преку евалуација и обработка на расположливите податоци, како во областа на подготовка на стратегиските документи, така и во проценатa на ризици и закани, но и во анализата на процесите од суштинско значење за заштитата на критичната инфраструктура". Сè што е посочено е навистина неопходно, но останува прашањето колку од тоа се спроведува во практиката. Самите автори ги поставуваат истите прашања: „Клучни прашања се начините на кои компонентата на безбедносно разузнавање може најделотворно да се користи во заштитата на критичната национална инфраструктура, а тоа се прашања поврзани со процесите на дефинирање на барањата за заштита на критичната инфраструктура од страна на безбедносните разузнавачки служби и соодносот меѓу безбедносните потреби на клучните инфраструктурни системи од една страна и можностите со кои располага разузнавачката заедница во тој поглед од друга" (Малнар и Млинац, 2014: 1013). Сево од наведеново покажува дека во рамките на разни организации во безбедносниот сектор постои свесност за потребата од поголема соработка и координација, но истите се градат пребавно во споредба со брзината на развојот на актуелните состојби. Авторите истакнуваат дека „заштитата на критичната инфраструктура, и покрај изградбата на националниот систем за заштита и напорите за централизирање на активностите, сè уште е во голема мера фрагментирана активност, која е секторски уредена преку домените на надлежност на различните министерства и другите државни органи. Таквата дисперзија на заштитата, како и специфичноста на објектите, го отежнуваат концентрирањето на разузнавачките активности и ја намалуваат целисходноста на дејствијата" (Малнар и Млинац, 2014: 1013).

Како трет труд, треба да се истакне мислењето на Иван Показ и Ута Перчиќ, кои забележаа неколку клучни работи околу прашањето зошто системот не е ставен во употреба и што треба да се промени во таа насока. Тие правилно ја поставуваат претпоставката дека проблемот се состои во отсуството на формализиран систем на национална безбедност, како и во начинот на разгледување на области и активности во рамките на концептот на критична инфраструктура што отвора многу неизвесности. Забележуваат и дека *Законот за критична инфраструктура* не дава приоритет на заканите од тероризам,

а според нивното мислење, истото требало да се направи (Показ и Перчиќ, 2014: 1137). Авторите на Законот не го споменуваат тероризмот директно, тие се одлучиле да употребат понеутрален израз (поим) во членот 6: „Органот на државна управа во чија надлежност се задачи за заштита и спасување, во соработка со органите на државната управа во чија надлежност е и одредена критична инфраструктура, редовно ги следи и ги проценува заканите и предлага оперативни и други мерки за процена на критичноста и потребата за предлагање мерки за управување и заштита на критичната инфраструктура" (Влада на Република Хрватска, 2013а). Оваа формулација оддава двосмисленост бидејќи „не е јасно на кои закани поточно се мисли", додела ДУЗС „има приоритетна задача за заштита и спасување во случај на големи несреќи и катастрофи, но не и задача да врши процена на закани предизвикани од намерни и непријателски дејствија кои ги преземаат луѓе или субјекти создадени од луѓето (тероризам, организиран криминал, компјутерски криминал, активности на странски разузнавачки агенции и други" (Показ и Перчиќ, 2014: 1138). Замислата е дека креаторите на таквите поими во текстот на Законот се раководеле од претпоставката дека ДУЗС до тој момент не успеала да воспостави соодветно ниво на соработка со агенциите од безбедносниот сектор (првенствено со разузнавачката заедница) за да ги искористи нивните знаења и производи во проценатa на заканите и координацијата на другите актери во системот. Пологично објаснување е дека при изготвувањето на Законот не било посветено доволно внимание на деталите, додека општата идеја дека тоа претставува структурно прашање ја потврдуваат и Показ и Перчиќ (2014: 1137), наведувајќи дека Законот претставува „доказ за недоволното разбирање на прашањата и терминологијата во управувањето со безбедносните ризици во таа област". Затоа е потребно да се вклучат сите прогресивни сили од државата, вклучувајќи ги и граѓанскиот и приватниот сектор, како и академскиот свет, во сите општествени активности насочени кон заедничко развивање на подобри решенија во тој поглед, а за доброто на сите нас.

Во 2015 година беа усвоени две значајни, погореспомнати безбедносни стратегии - *Националната стратегија за спречување и борба против тероризмот* и *Националната стратегија за сајбер-безбедноста*, заедно со придружните акциски планови. И двете се значајни бидејќи во нив областа на критичната инфраструктура е силно препознаена и застапена. Ова во голема мера е резултат на интензивното застапување на Државната управа за заштита и спасување (без да се намалува вредноста на придонесите на некои колеги од други органи на државната управа кои постојано се присутни, активни и помагаат процесот да стане повидлив) за време на учеството на вработените во неа во работните групи за развивање на спомнатите стратегии, имајќи предвид дека токму тие беа првите кои ја увидоа можноста да ја актуелизираат оваа област и да ја направат видлива за сите засегнати страни во политичкиот и безбедносниот сектор (бидејќи тие се тие кои располагаат со можности да го рестартираат процесот на највисоко ниво).

Националната стратегија за спречување и борба против тероризмот ја препознава терористичката закана и потенцијалниот напад врз националната критична инфраструктура чиј прекин во работењето или испораката на

стоки и услуги може да има сериозни последици врз националната безбедност, здравјето и животот на луѓето, имотот и животната средина, безбедноста и економската стабилност и континуираното функционирање на државниот апарат. Активностите потребни за заштита на критичната инфраструктура од тероризам се наведени преку следните мерки: „а. развој и зајакнување на националните капацитети за заштита на луѓето и имотот; б. означување и навремено активирање на посебен режим за заштита на локации и објекти од особено значење за одбраната на земјата; в. заштита на дипломатските, конзуларните и другите претставништва на Република Хрватска во странство; г. информирање на хрватските граѓани и правни лица за нивото на терористички закани во земјите во кои патуваат или работат; д. заштита на дипломатските, конзуларните и другите странски претставништва на територијата на Република Хрватска; ѓ. прилагодување на постојните концепти во областа на националната безбедност и правната рамка за воспоставување на системи за управување со вонредни состојби и кризни ситуации, а со тоа и во случај на терористички активности; е. зајакнување на системот за заштита и надзор на државната граница; ж. зајакнување на контролата на вооружувањето и разоружувањето, како и складирањето на оружје, експлозиви и други средства што може да се искористат за извршување на терористички напади; з. зајакнување на надзорот врз превозот и употребата на стоки со двојна намена; ѕ. воспоставување на систем за заштита на критичната инфраструктура, со почитување и примена на постојните секторски мерки, планови и надлежности за заштита; и. воспоставување на систем за продолжување на критичните операции на деловната инфраструктура; ј. зајакнување на системот за цивилна заштита; к. зајакнување на надзорот во однос на можните сајбер-напади“ (Влада на Република Хрватска, 2015б: став 23). Јасно е дека авторите на Стратегијата го опишуваат концептот на критични инфраструктури заедно со сите потребни активности и развојот на функциите за нивна поддршка како многу поширок од непосредната заштита, надевајќи се дека тоа ќе наиде на позитивна реакција и поголемо внимание кон организацијата на системот на критична инфраструктура. Но, тоа не се случи како што се очекуваше.

Националната стратегија за сајбер-безбедност и *Акцискиот план за имплементација на Националната стратегија за сајбер-безбедност* обрнуваат внимание на критичната инфраструктура во многу посилна мера отколку сите други национални стратегии, процени и планови до нејзиното усвојување. Ова првенствено се согледува преку опишувањето на критичните комуникациски и информатички инфраструктури кои се дефинирани како комуникациски и информатички системи чие нарушување на функционирањето значително ќе го наруши работењето на означените поединечни или групни национални критични инфраструктури. Стратегијата посветува многу простор на критичната комуникациска и информатичка инфраструктура доведена во врска со управувањето со сајбер-кризите. Општо земено, Стратегијата силно ја нагласува важноста на *Законот за критична инфраструктура* и потребата истиот да почне да се применува. Поточно, Стратегијата истакнува вкупно пет цели кои треба да се реализираат за да се заштити критичната комуникациска и информатичка инфраструктура и делотворно да се управува со сајбер-кризите:

1. Утврдување на критериуми за препознавање на критичната комуникациска и информатичка инфраструктура.
2. Утврдување на задолжителни безбедносни мерки што ги применуваат сопствениците или управителите на означената критичната комуникациска и информатичка инфраструктура.
3. Зајакнување на превенцијата и заштитата преку управување со ризици.
4. Зајакнување на јавно-приватните партнерства и техничката координација во обработката на инциденти поврзани со компјутерската безбедност.
5. Воспоставување на капацитети за ефективна реакција кон закана што може да предизвика сајбер-криза (Влада на Република Хрватска 2015а: точка 5.2.).

Стратегијата ја наведува потребата да се идентификува критичната комуникациска и информатичка инфраструктура и сите оние постапки што две години пред тоа беа пропишани со *Законот за критична инфраструктура*, а не беа имплементирани. Проблемот е во тоа што државните органи се тие кои се задолжени да го спроведат тој процес, но тие тоа не го сторија, што го поставува прашањето за тоа каква слика за себе им испраќа државата на приватните сопственици или управителите на критичните инфраструктури, како и на поширокатa јавност и Европската комисија. Сите пет мерки даваат одлични насоки за тоа што треба да се направи, а важно е поконкретно да се потцрта Целта 3 „Зајакнување на превенцијата и заштитата преку управување со ризици" и предложената структура за тоа што во себе вклучува секторската процена на ризиците, т.е. идентификацијата на критичните функции (услуги, податоци, мрежи , итн.); идентификацијата на заканите, опасностите, пропустите и последиците; анализата на ризик и приоретизацијата; одредувањето прифатлив ризик и управувањето со ризик. Горенаведеното (ако веќе знаеме дека безбедносниот разузнавачки систем има капацитет и способност да помага во правењето вакви процени) нè води кон заклучокот дека сите елементи и засегнати страни треба првично да направат секторска процена, проследена со секторски план за обезбедување на функционирањето на критичната инфраструктура, а кои заедно ќе дадат рамка за формирање секторски политики и започнување конструктивна соработка со клучните засегнати страни во секторските процеси.

Исто така, треба да се забележи дека не постои специјализирана и сеопфатна програма во високообразовните институции во Република Хрватска во чии рамки сите што се вклучени во активности поврзани со критичната инфраструктура можат да се едуцираат и да ги стекнат основните знаења потребни за подобро спроведување на задачите и одговорностите во областа на идентификацијата, заштитата и зајакнувањето на отпорноста на критичната инфраструктура. Во потрага по ад-хок решение за обезбедување на основно и еднакво разбирање од страна на сите актери (од претставници на ДУЗС, до офицерите за врска за безбедност и нивните заменици од девет министерства) и усогласување на очекувањата и знаењата на овие експерти, во 2014 година беше спроведен начелен курс наречен „Деловна анализа на ризик за критичната инфраструктура". Во 2015 година, исто така, беше спроведен

напреден курс насловен како „Евалуација на проценатa на ризик и оптимално управување со ризик во согласност со ISO 31000 и IEC 31010". Двата семинари беа наречани и финансирани од страна на ДУЗС, а ги спроведе Универзитетот за применети науки во Велика Горица заедно со неколку надворешни соработници. По овие курсеви, не беше спроведена никаква едукација ниту обука и ниедна од високообразовните институции не отвори специјализирана програма наменета за едукација на вработените кои работат на заштита на критичните инфраструктури.

Затоа, во иднина е неопходно да се планира професионална (стручна) обука, како и едукација за сопствениците и управителите на критичните инфраструктури, така што сите засегнати страни ќе се здобијат со едно првично и подеднакво знаење за важноста, меѓузависноста и начините на функционирање на концептот на заштита на критичната инфраструктура. За да се постигне тоа, неопходно е да се обезбедат финансиски ресурси, планови и програми за обука на засегнатите страни во системот за управување со ризици по критичната инфраструктура, да се зголемат знаењата и вештините и колку што е можно повеќе да се вклучи научната заедница во истото, но и законски да се пропише обврската за спроведување едукација. Во сите земји каде што системот за заштита на критичната инфраструктура е високо развиен се посветува големо внимание на образованието, така што Република Хрватска исто така треба да развие модел за обука на сите клучни актери кои имаат свои улоги и одговорности во системот на заштита на критичната инфраструктура.

Трет циклус – 2016 до 2018 година

Имајќи го предвид фактот дека создавањето на соодветен систем на заштита на критичната инфраструктура бара континуирана работа и инвестирање во развојот на областа, неопходно е да се утврдат претпоставките за изготвување силна нормативна рамка проследено со координирано спроведување на активности, а со цел да се обезбеди усогласено спроведување на прописите, мерките и постапките во заштитата на критичните инфраструктури. Според тоа, во 2016 година, како надлежен орган, Државната управа за заштита и спасување достави *Правилник за методологијата за изработка на деловна анализа на ризици за критичната инфраструктура* (Државна управа за заштита и спасување, 2016), како и подзаконски акт за *Правилата за методологијата за изработка на деловна анализа на ризици за критичната инфраструктура* (Државна управа за заштита и спасување, 2017) во 2017 година, а во 2018 година започна со преразгледување и на самиот *Закон за критична инфраструктура*. Ова може да обезбеди добра основа за воспоставување на систем кој ќе обезбеди реализација на сите досегашни неуспешни активности на национално ниво, што, пак, од своја страна, сигурно ќе ја зајакне позицијата на Република Хрватска на меѓународен план во контекстот на целите и задачите кои Европската унија им ги постави на своите земји-членки на тој план.

Севкупните досегашни предизвици се актуелизираа повторно во 2017 година со изготвувањето на два важни документи во областа на националната безбедност кои ја стават критичната инфраструктура во списокот на

размислувања и приоритети, а тоа се *Стратегијата за национална безбедност на Република Хрватска* и *Законот за систем на внатрешна безбедност*. Стратегијата, меѓу другото, носи девет стратегиски цели за Република Хрватска кои подразбираат конкретно спроведување на националната безбедносна политика. Стратегиската цел за „Постигнување на највисоко ниво на безбедност и заштита на населението и критичната инфраструктура" е поврзана и произлегува од националниот интерес (еден од четирите основни национални интереси) дефиниран како „Безбедност на населението, територијалниот интегритет и суверенитетот на Република Хрватска". Во рамките на таа стратегиска цел, големо внимание се посветува на критичната инфраструктура со првичната определба дека, за безбедно општество, потребно е да се заштити животот, да се спасат луѓето и да се заштитат критичните инфраструктури. Потоа, неколку важни делови се посветени на активностите што се очекуваат од сите фактори во формулирањето на безбедносните политики. „Заштитата на критичната инфраструктура ќе се фокусира на спречување, отстранување или ублажување на ризиците кои можат да предизвикаат слабости на критичната инфраструктура и да ја зголемат нејзината отпорност. Системот за управување и контрола на некои критични инфраструктури треба постојано да се надградува и подобрува, со примена на најдобрите искуства од оваа област кои се достапни во други земји. Ќе се развиваат модели за размена на податоци меѓу државните органи и институциите, од една страна, и управителите на критичните инфраструктури во јавна и приватна сопственост, од друга, со цел навремено препознавање на потенцијалните безбедносни закани и ризици" (Хрватски сабор, 2017а: Национален интерес од А-категорија).

„Со развојот на документите кои ја уредуваат политиката и методологиите за управување со критичната инфраструктура и ограничените државни стоковни ресурси, Република Хрватска јасно ќе утврди кои делови од истите треба да останат во мнозинска сопственост на државата, со што се спречува загрозување на виталните функции важни за државата и населението во случаи на деловна нестабилност. Зајакнувањето на отпорноста на националната критична инфраструктура во однос на современите безбедносни предизвици и ризици бара истовремено одржување и заштита на националните критични граѓански капацитети кои ќе ги поддржат севкупните капацитети на еден координиран и сеопфатен јавен и приватен сектор, а пред сè, на приватниот сектор за безбедност. Овие напори исто така ќе бидат усогласени со сојузниците, меѓународните организации и партнерите. Цивилната подготвеност, која целосно претставува одговорност на државата, е столб на националната отпорност" (Хрватски сабор, 2017а: Национален интерес од А-категорија).

Повеќето од горенаведените одредби се утврдени порано, а се и многу пати истакнувани од страна на стручната и академската заедница во бројни дискусии за прашања поврзани со критичната инфраструктура. Она што е важно да се нагласи, иако истото не претставува апсолутна новина, е извонредната значајност на податокот дека во еден документ на вакво рамниште е наведена потребата да се утврди кои делови од критичната инфраструктура мора да останат во мнозинска сопственост на државата, со што ќе се спречи вложените максимални напори за спречување и заштита на некоја критична

инфраструктура потоа да бидат легитимно купени на берзата со преземање на мнозинскиот удел во компанијата од страна на некој кој е потенцијално несоодветен да управува со истата.

Стратегијата за национална безбедност на Република Хрватска е основен стратешки документ кој ги истакнува политиките и инструментите за остварување на националните визии и интереси, како и постигнување на безбедносни услови што ќе овозможат урамнотежен и континуиран развој на државата и општеството. Нешто што е особено важно за дискурсот во рамките на ова истражување е податокот дека концептот на критична инфраструктура е силно застапен во оваа Стратегија. Со цел Стратегијата да биде навистина применета во пракса во однос на воспоставувањето на Системот за внатрешна безбедност и со него поврзаното управување со безбедносните ризици, кризи и критичната инфраструктурата, беше усвоен и *Законот за систем на внатрешна безбедност*.

Законот за систем на внатрешна безбедност не ги менува надлежностите на државните органи или нивните одговорности според други закони, туку ги доведува во врска со координативната акција поврзана со управувањето со безбедносните ризици и дејствијата кои се преземаат во кризни состојби. Ова е закон за кој постоеше итна потреба во Република Хрватска и кој е од исклучителна важност, при што, исто така е многу значајно да се напомене и дека, во него, критичната инфраструктура е силно застапена. Меѓу шесте клучни одредби од воведниот дел од Законот, исто така е наведена намерата истиот да обезбеди усогласено спроведување на прописите со кои се утврдуваат безбедносните мерки и постапки од значење за националната безбедност, а особено заштитата на критичните инфраструктури. Врз основа на Законот, Координативното тело за Системот за внатрешна безбедност е формирано како меѓуресорко тело одговорно за усогласување и координирање на работата на Системот за внатрешна безбедност (Хрватски сабор, 2017б). По воспоставувањето на Координативното тело, истото потоа пристапи кон усвојување на Годишниот работен план за координација на Системот за внатрешна безбедност на Република Хрватска за 2018 и 2019 година, каде што беше повторно истакната потребата да се идентификуваат и посочат националните критични инфраструктури, а беа препознаени и измените и дополнувањата на *Законот за критична инфраструктура*.

Во однос на воспоставувањето на сајбер-безбедноста, во 2018 година беше усвоен *Законот за сајбер-безбедност на спроведувачите на клучни услуги и давателите на дигитални услуги* кој се засноваше на Националната стратегија за сајбер-безбедност од 2015 година и со кој се регулираат правата и обврските на засегнатите страни во односниот систем, а во согласност со критериумите неведени во Анекс 1 - *Список на клучни услуги со критериуми и прагови за утврдување на важноста на негативното влијание на еден инцидент* (Хрватски сабор, 2018 година). Со овој закон, *Директивата 2016/1148 на Европскиот парламент и на Советот во врска со мерките за постигнување на високо заедничко ниво на безбедност на мрежните и информативните системи ширум Унијата (Директивата НИС)* беше транспонирана во националното законодавство. По донесувањето на Законот, во Република Хрватска

беа воспоставени постапките за идентификација и беа пропишани мерките за заштита на комуникациската и информатичката инфраструктура, а во законскиот рок беа утврдени и одредени Спроведувачи на клучни услуги и Даватели на дигитални услуги. Споменатиот закон и процесите кои се спроведуваат во рамките на истиот, во оваа почетна фаза, претставуваат позитивен пример за добра практика. Искуствата од процесите што се одвиваа под закрила на *Законот за критична инфраструктура* секако придонесоа за тоа. Во периодот што претстои (при што истиот на краток рок ги опфаќа само следните година или две), останува да видиме како ќе се усогласат процесите кои се одвиваат во рамките на овие две законодавни рамки, при што се очекуваат предизвици во однос на преклопувањата и како истите ќе бидат решени.

Да заклучиме, кога станува збор за овој дел, треба да се забележи дека, во набљудуваниот и анализираниот период, севкупните напори во изминатите години, од донесувањето на *Законот за критични инфраструктури*, подзаконските акти и новите стратегии, до бројните активности и работилници, резултираа со идентификација на голем број критични инфраструктури во одредени сектори, иако во само некои од нив, наспроти во сите како целина. Ова претставува значаен исчекор во однос на натамошните активности насочени кон воспоставувањето на систем за критична инфраструктура. Точниот број на идентификувани национални критични инфраструктури е доверлив. Од друга страна, постојат јавно достапни информации во согласност со *Законот за сајбер-безбедност на спроведувачите на клучни услуги и давателите на дигитални услуги* што нè наведоа до тоа да бидеме во состојба во моментов да препознаеме и означиме 98 спроведувачи на клучни услуги и даватели на дигитални услуги во Република Хрватска.

5.3. Структурни предизвици при воспоставувањето систем за заштита на критичната инфраструктура

Доколку се има предвид дека областа на критичната инфраструктура претставува мошне динамична сцена во која своја улога играат најразлични чинители и нивните политики, потреби и начини на согледување на нештата, како и дека истата претставува дел од националната безбедност, зазема главен дел од вниманието при многу настани и случувања низ целиот свет и е средство за реализација на разни проекти, тогаш мора да се заклучи дека процесот на воспоставување на систем за заштита на критичната инфраструктура во Република Хрватска не беше спроведен во првите години по донесувањето на *Законот за критична инфраструктура*. Иако до пишувањето на оваа анализа системот сè уште не е воспоставен, на овој план навистина се преземени многу позитивни чекори, но и понатаму останува жалењето за пропуштеното време и можности.

Тоа покажува дека целокупниот процес на пренесување на европското законодавство во областа на критичната инфраструктура не е доволно добро подготвен и имплементиран во Република Хрватска, иако целта беше исполнување на стандардите потребни за пристапување кон полноправно членство на Унијата. Главната причина за ова е недостатокот на стратешка визија

на највисокото политичко ниво за спроведување на овој процес, како и за давање „дозвола" на пониско поставените кадри да ги исполнат своите обврски според Законот. Како резултат на тоа, направени се бројни негативни коментари на сметка на Државната управа за заштита и спасување во кои се тврди дека таа не ја врши својата работа како тело назначено да го координира процесот поврзан со критичната инфраструктура во Република Хрватска. Иако ДУЗС имаше одредени пропусти во однос на сè од погоре спомнатото, негативните коментари беа главно неосновани, бидејќи ДУЗС не можеше да започне да воспоставува и да гради систем на заштита на критичната инфраструктура во состојба во која министерствата кои требаше да се координираат „одбиваа" да бидат координирани. Уште од своето основање, Државната управа за заштита и спасување исто така ја следи и имиџот на нереализирана организација во своите законски овластувања и капацитети, делумно поради тоа што не ѝ беше овозможено тоа да го постигне (што поради недоволните финансии и персонал, немањето јасни насоки, проблемите со спротивставените надлежности за што најочигледен пример е во сегментот на управување со пожари, така и како последица на непочитувањето со кое се соочуваше од страна на различни министерства при остварувањето на нејзините законските обврски и задачи, а делумно и на нејзините сопствени погрешни политики и практики). Според тоа, ДУЗС стана „омилена цел за критики" кај многу од засегнатите страни.

За да не се добие впечатокот кај секој читател дека значајни предмети, мрежи или системи во Република Хрватска се незаштитени или уживаат низок степен на заштита, од особена важност е да се истакнат неколку работи. Критичната инфраструктура е заштитена дури и без постоење на систем. Постојат многу комплементарни процеси кои се спроведуваат во согласност со други правни основи во Република Хрватска, додека најважната критична инфраструктура во земјата е заштитена со висок степен на заштита. Единствениот проблем е тоа што тие не се нарекуваат „национални критични инфраструктури" (т.е. не се службено именувани како такви) како што предвидува *Законот за критична инфраструктура*.

Првиот таков процес започна во 1999 година со усвојувањето на *Уредбата за критериуми за одредување и заштита на објекти од посебна важност за одбраната на земјата во согласност со Законот за одбрана* (Службен весник на Република Хрватска 74/93, 57/96). Преку овој процес беа развиени критериуми за означување на воени и други објекти од особено значење за одбраната на земјата, изработена е методологија за процена на заканите и план за заштита на воени и други објекти, таквите објекти беа утврдени и попишани, пропишани беа и општи и посебни мерки за нивната заштита, а беа спроведени и редица други активности во таа насока. Процесот е воспоставен, објективно функционира добро и е делотворен. Кај оваа Уредба постои голема сличност, а кај некои нејзини одредби дури и целосна идентичност со одредбите од *Законот за критична инфраструктура* и поврзаниот подзаконски акт. Тука треба да се одбележи дека, иако овие процеси беа комплементарни, не дојде до нивно усогласување и заземање заеднички пристап кон сопствениците или управителите на одредени објекти од особено значење за одбраната на

земјата. Овој податок особено го нагласуваат стручните лица кои работат во овие установи – имајќи предвид дека во голем број случаи станува збор за истите објекти (бидејќи нема други) кои, преку систем координиран од страна на Министерството за одбрана на Република Хрватска, се означени како објекти од особено значење за одбраната на земјата и кои најверојатно ќе бидат именувани како национална критична инфраструктура во рамките на идниот систем кој ќе биде координиран од Државната управа за заштита и спасување. Она што е важно да се забележи е податокот дека, кога станува збор за усогласување на процесите, неопходното ниво на координација помеѓу Министерството за одбрана на Република Хрватска и Државната управа за заштита и спасување, всушност, не постои.

Следниот пример се однесува на усогласувањето и обезбедувањето комплементарност на Република Хрватска со НАТО во областа на управување со кризи. Во февруари 2014 година, Владата на Република Хрватска ја усвои *Одлуката за утврдување на национални координатори за спроведување на мерките за одговор на кризи на Организацијата на Северноатлантскиот договор во Република Хрватска и нивните надлежности* (Влада на Република Хрватска, 2014). Во согласност со Одлуката, како оперативен документ за спроведување на мерките за одговор на кризи е определен *Прирачникот за систем за одговор на кризи на НАТО*. Овде, значајно е тоа што во Прирачникот, меѓу другите, се пропишани и активностите поврзани со заштитата на критичната инфраструктура, а како координатор на целиот процес се јавува Министерството за одбрана. По Одлуката на Владата, следеше процесот на означување на носителите на дејноста за секоја од мерките за заштита на критичната инфраструктура наведени во Прирачникот. По означувањето на носителите на дејностите, беа изработени сценарија за секоја од мерките, истите беа споени со документот подготвен од Министерството за одбрана, па како такви беа доставени до Владата на Република Хрватска. Тука наидуваме на сосема поинаква ситуација во однос на соработката помеѓу Министерството за одбрана и Државната управа за заштита и спасување. Во процесот поврзан со користењето на *Прирачникот за системот за одговор на кризи на НАТО*, Министерството за одбрана и Државната управа за заштита и спасување соработуваат многу добро и координирано, а со тоа се наметнува и логичното прашање зошто ова не функционира во претходно опишаниот случај.

Овие примери ги илустрираат различните практики и решенија, т.е. несоодветната координација во првиот процес наспроти заемната соработка во вториот. По овој преглед, праведно е да се праша - зошто државата не ги координира своите клучни безбедносни процеси? Понатаму, доколку Министерството за одбрана и Државната управа за заштита и спасување не можат да се усогласат, тогаш се поставува прашањето кој е тој кој ги координира таквите процеси и со каков квалитет? Ваквите состојби се показател дека во Република Хрватска има многу простор за подобрување на управувањето со безбедносниот сектор, како и за координација на клучните процеси и фактори, но и за поголемо искористување на научноистражувачката и научната дејност во сите овие активности.

Најчестата дискусија за причините поради кои не е воспоставен системот на заштита на критичната инфраструктура во Република Хрватска е насочена кон сето она што ДУЗС досега го сторила или требало да го направи. Овде не станува збор за влегување во некаква одбрана на Државната управа за заштита и спасување поради нејзините ограничувања и пропусти кои всушност произлегуваат од проблемот со распределбата на моќта во рамките на системот на државната администрација, означувањето на стратегиските приоритети (и на државно ниво и на рамниште на ДУЗС) и малиот број на персонал кој ѝ е доделен да се занимава со оваа тема (како и неговите надлежности). Во овој дел треба да се нагласат некои предизвици кои го спречуваат воспоставувањето, а потоа и делотворниот развој на системот за заштита на критичната инфраструктура. Истите треба да се посочат за да се истакнат работите кои треба да се променат од корен.

Една од карактеристиките на дискусијата е, условно речено, преголемата посветеност на заштитата на критичната инфраструктура и запоставувањето на другите составни делови кои ги прават самиот систем и сите негови компоненти функционални на долг рок. Постојат интересни групи кои првенствено се фокусираат на заштитата на критичната инфраструктура, што е разбирливо затоа што тие работат врз основа на пазарните начела и имаат сопствен интерес. Но, интерес на државата е да посвети поголемо внимание на целокупниот концепт и јасно да ја утврди политиката за комуникацијата по ова прашање. Во рамките на ваквата политика, неопходно е јасно и недвосмислено да се објасни како државата го гледа управувањето во оваа област преку примена на сите мерки и активности за сеопфатно дејствување. Во обид да одговориме на прашањето како да се заштити националната критична инфраструктура од извори на закани, треба да почнеме од толкувањето на потенцијалните извори на загрозеност, т.е. оние од природен, техничко-технолошки карактер, како и делата извршени и поттикнати од луѓе. При анализата на можните закани треба да ги согледаме сите ризици во просторот, почнувајќи од тоа каде определен објект, мрежа или систем се лоцирани и што е тоа што би можело да ги загрози во смисла на закани предизвикани од човекот, без разлика дали станува збор за таквите кои се предизвикани од страна на внатрешни вработени кои поради каква било причина сакаат да нанесат штета или, пак, за заканите кои доаѓаат од надворешни напаѓачи. Критичната инфраструктура, но и целата земја, соодветно ќе ги заштитиме преку што е можно поголема диверзификација на изворите, областите и секторите од кои сериозно зависиме. Критичната инфраструктура ќе биде најдобро заштитена доколку е изградена во подрачја во кои постои што е можно помал ризик за поплава и земјотрес и во согласност со професионалните стандарди, како и со користење на квалитетни материјали и системи и почитувајќи ги сите стандарди за градење и одржување. Следниот чекор е да се подготви целосната придружна документација и да се стекнат сознанија за самите процеси, а со цел да се избегнат одложувања и можни каскадни ефекти доколку определен систем не функционира или се појави дефект во некој објект или клучна инфраструктура. Понатаму, доаѓаме до отпорноста на самиот систем, неговата цврстина и оптимална функционалност. Потоа, прашањето е дали компанијата ги направила сите неопходни

процени, анализи и планови кои се бараат во согласност со други уредби, бидејќи прашањето за критичната инфраструктура претставува само прашање на надградба на сè што било направено претходно. Секако, би било добро за една компанија доколку таа ја усогласи или подобри својата дејност преку применување на еден од меѓународните стандарди за деловност, управување со квалитет, управување со кризи или управување со вонредни состојби. Исто така е важно дали таа има план за кризи, план за комуникација во услови на криза, дали спроведува внатрешни вежби, дали е поврзана со услуги за итна помош и слично. Според тоа, постои цела низа неопходни активности кои треба да се преземат пред да почнеме да зборуваме за техничката и физичката заштита, при што соработката, координацијата и размената на знаења и искуства се од суштинско значење (Микац, 2017).

Кога станува збор за спроведувањето на *Директивата 2008/114/ЕЗ* на Европската унија во рамките на хрватското законодавство, времето покажа дека е преоптимистички да се очекува идентификување и означување на критични инфраструктури во единаесет сектори. Од друга страна, откако *Законот за критична инфраструктура* и придружните документи, веќе беа изработени и областа беше нашироко разгледана, вклучувањето на сите главни сектори во нив најверојатно претставуваше прагматично решение. *Директивата 2008/114/ЕЗ* ги обврзува сите земји-членки да земат предвид два сектора - енергија и транспорт. Со текот на времето, стана јасно дека првичниот концепт, како и обликувањето и структурата на идниот систем во Република Хрватска во тој поглед, се преоптимистички устроени. Сепак, постои сè уште простор одредени активности да се насочат кон изнаоѓање на прифатливо решение во согласност со тоа што го нудат можностите. Потребен е само доволен капацитет за стратегиско управување. Во дадените околности, корисно е постојните активности да се прилагодат кон сегашниот контекст и, при идентификацијата и означувањето на првите критични национални инфраструктури, акцентот да се фрли врз транспортниот и енергетскиот сектор, со цел да се остане во тек со сето она што претставуваат прашања од најголем интерес за Европската комисија. Откако ова ќе се реализира, би можеле да соработуваме со други земји на ЕУ кои стасаа подалеку од нас во овој процес. Паралелно со тоа, треба да работиме на други сектори за да ја добиеме целокупната слика за состојбите и да го изградиме системот. Нивото на заштита ќе зависи од приоретизацијата на секој сектор според секторски и меѓусекторски критериуми, т.е. преку проценување „што е повеќе, а што помалку важно за нас". Постапките ќе се утврдуваат со помошта на безбедносни планови кои, исто така, ќе треба да се изработат. Доколку добиеме голем број на секторски одлуки за идентификувани критични инфраструктури, ќе се случи блокада на функционирањето на системот дури и пред истиот да почне да функционира како таков. Кога станува збор за бројот на специфични секторски критични инфраструктури, се спомнуваа сто објекти кои секторите би можеле да ги посочат како можна критична инфраструктура. Следствено, прашањето кое се поставува е што е тоа што е навистина од критично значење и тоа без кое не можеме да функционираме во Република Хрватска, имајќи предвид дека сето она за кое има алтернатива не е од критичен интерес. За споредба можеме да ја земеме Република Словенија,

која успешно го заврши процесот на идентификација и откри вкупно осум сектори во кои идентификуваше барем по една критична инфраструктура, со што низ целата земја идентификуваше помалку од 60 такви.

Потоа се поставува прашањето како некои министерства имаат потреба од неколку години да ги исполнат своите обврски, при што некои дури и по пет години не успеале да идентификуваат барем една критична инфраструктура во рамките на секторот во нивна надлежност. При таквите случаи, разумно и апсолутно легитимно би било да се верува дека навистина не постоела инфраструктура која можела да се смета за критична во дадениот сектор, но дури и тоа да е така, засегнатите министерства не донеле соодветни одлуки кои тоа би го потврдиле на формално ниво. Не постои конкретен одговор зошто ваквата состојба е таква каква што е бидејќи истата е последица на неколку различни фактори. Може да се каже и дека овој процес не е многу интересен за највисокото ниво на власта, па затоа и не е означена клучната инфраструктура во некои сектори, ако не и во сите нив. Друга работа е дека досега многу е направено за развој на секторски мерки и вршење „анализа на моменталната состојба" во рамките на секторите, но недостасува „последниот чекор", кој се состои од поднесување предлог до Владата на Република Хрватска да ги означи како национална критична инфраструктура идентификуваните објекти, мрежи или системи. Дел од одговорот лежи и во фактот што во системот на државната управа нема утврдено работно место за офицер за врска за безбедност, што е клучна точка и позиција која треба, т.е. мора да го „поттикне процесот" во насока на исполнување на обврските во овој контекст. Дали е неопходно да се пропише таква работна позиција е прашање на различни гледишта, но непобитен факт е дека постоењето на истата ќе ги олесни процесите кои мора да се спроведат. Во исто време, доаѓаме до прашањето дали сегашните офицери за врска за безбедност се соодветно позиционирани во рамките на нивните сопствени сектори и дали тие можат да ги запознаат своите претпоставени со важноста на овој процес и да им го привлечат вниманието кон него. Истите проблеми се детектирани и кога станува збор за хиерархиската поставеност на советниците за информатичка безбедност (предвидени според *Законот за информатичка безбедност*) во некои од државните органи. Бидејќи овие две позиции се преклопуваат во своите задачи и одговорности, би било неопходно тие да се обединат, да се пропишат нивните точни надлежности и да се формира оддел во кој одреден персонал задолжен за предметните области во поголемите тела би работел заедно, додека во помалите тела или органите со помал опсег на надлежностите (како што е Министерството за култура) тоа би му било доделено како задача на едно исто лице.

По ова, доаѓаме до непостоењето на структурно подготвена основа за делување во оваа област во Република Хрватска. Зошто е тоа важно? Бидејќи сите високо развиени земји инвестираат многу време, енергија и финансиски ресурси во развојот на концепти, системи и знаење за критичните инфраструктури. Европската комисија посвети многу внимание на оваа област, а финансира и бројни активности и проекти во таа насока. Големите компании сè повеќе бараат специфични знаења и услуги за зајакнување на издржливоста и заштита на нивната критична инфраструктура. Ако сакаме да останеме во чекор со сите нив, треба да инвестираме повеќе. Структурно, целата државна

управа не успеа да ги подготви основните претпоставки за спроведување на заштитата на критичната инфраструктура - нема доволен број на персонал способен да го координира целиот процес, изостанува неопходната рамка и програми за обука на персонал кој треба да работи на проблеми со критичната инфраструктура, нема пропишани квалификации за лицата кои треба да бидат вработени на овие работни места и не постои работна позиција офицер за врска за безбедност на критичната инфраструктура, па одговорноста за тоа се дава без спроведување на соодветниот процес на селекција и само на повремена основа, иако ова претставува позиција со полно работно време. Исто така, нема едукација на инспектори кои треба да го надгледуваат спроведувањето, а тие понатаму и не се целосно во тек со содржината на задачите. Освен тоа, од гледна точка на правото, хрватскиот модел на јавно-приватно партнерство е ограничен на инвестиции за изградба и одржување на објекти и не е ни малку прилагоден на потребите на критичната инфраструктура. Промени се исто така неопходни и во однос на ова прашање.

Друга важна работа што не може да се пропушти е односот со сопствениците или управителите на критичните инфраструктури. Овде треба да се подвлече дека на тој план не постои партнерство, туку односи во кои државата дејствува од позиција на надреденост, исклучувајќи ги сопствениците или управителите како од дискусијата за моделите на владеење, така и од меѓусебната размена на информации, па на рамниште на државната управа, тие најчесто се оптоварени со нормите и прашањето што е тоа што треба да го исполнат како нивна обврска, при што сето ова се одвива без да им се обезбеди соодветно ниво на поддршка. Прашањето е зошто приватните сопственици би ја прифатиле одлуката дека нивните субјекти се означени како национална критична инфраструктура? Најчесто тие ја добиваат таквата одлука без претходно да бидат консултирани и таквиот пристап не е добар. Неопходно е да се разговара со сите сопственици или управители за придобивките и недостатоците во поглед на тоа, но и доколку државата пропишува повисоко ниво на заштита кое бара од нив инвестирање на средства кои треба да ги извлечат од нивната сопствена добивка, потребно е тие да бидат информирана за начинот на кој може да се здобијат со одредени придобивки при воспоставувањето на такво партнерство или однос. Државата треба да понуди соодветни придобивки за тие компании, а за најдобрите од нив треба да користи економска дипломатија и да им помогне да се пробијат на нови пазари. Исто така, државата може да ги стави на список на компании за кои државата нуди гаранции во поглед на водењето деловни односи со нив, како на пример во целите на воспоставување и водење деловни односи со НАТО, имајќи предвид дека без поддршка од нивната држава, компаниите не можат деловно да соработуваат со НАТО на своја рака. Државата би можела, врз основа на постојните примери (од други земји), да формира фонд за инвестиции наменети за заштита на критичната инфраструктура, при што би постоеле различни начини на прибирање финансиски средства, како и за да обезбеди инвестиции наменети за повисоките нивоа на заштита што државата ги пропишува за одредени инфраструктури. Постојат бројни примери на позитивни практики на меѓународно рамниште во овој поглед, па некои од таквите кои содржат квалитет треба да се применат и во Република Хрватска.

Заклучок

Сите предизвици поврзани со развојот на системот за заштита на критичната инфраструктура во Република Хрватска кои беа идентификувани врз основа на минатите искуства може да се преточат во неколку клучни точки, а тоа се следните: недоволна и несоодветна комуникација и соработка на офицерите за врска за безбедност на критична инфраструктура, од една страна, со носителите на одлуки во органите на државната управа на сите нивоа, од друга, недоволна соработка на органите на државната управа на централно ниво со надлежните агенции и професионални здруженија, недоволно образование на засегнатите страни, недостаток на регулатива, одговорните државни органи не располагаат со неопходните алатки (софтвер) во областа на управување со ризици за критичните инфраструктури и недостаток на научно-истражувачки активности во оваа област.

Сите овие предизвици се претвораат во очигледни потреби кога станува збор за активностите кои треба да се преземат за да се создаде соодветен систем на заштита на критичната инфраструктура на национално ниво. Според анализите на потребите за воспоставување висококвалитетен систем за заштита на критичната инфраструктура кои се направени досега, одредени пропраки може навистина да се понудат во тој поглед. Во фазата на означување на критичната инфраструктура која следува по идентификацијата, треба да се посвети големо внимание на критериумот критичност и на националното значење на конкретната инфраструктура, а на начин на кој стремежот за прегласување на сопствената важност кој присуствува кај одредени сектори нема административно да го оптовари системот преку тоа што ќе се спречи идентификувањето преголем број на инфраструктури кои всушност поседуваат помал степен на критичност. Ова, исто така, го забавува процесот на одредување на критичната инфраструктура што го спроведува Владата, а се остварува преку носењето Одлука за доделување статус на критична инфраструктура. По означувањето, потребно е да се спроведе приоретизација, имајќи во вид дека целокупната критична инфраструктура (ниту, пак, сите одделни компоненти во нејзини рамки) не бара еднакво ниво на заштита, ниту, пак, сите критични инфраструктури поседуваат иста важност. Во врска со натамошните активности и фази во реализацијата на заштитата на критичната инфраструктура, неопходно е во системот да се воведат и соодветни меѓународно признати стандарди (како што се Меѓународниот стандард ISO 31000: 2009 Управување со ризик: Начела и насоки) кои се во функција на процена на ризиците и одржување континуитет во делувањето на критичната инфраструктура.

Во поглед на соработката меѓу заинтересираните страни, клучен елемент е постоењето на јавно-приватните партнерства и воспоставувањето квалитетна соработка. Приватниот сектор, од кој произлегуваат повеќето сопственици или управители на критична инфраструктура (како што е хрватскиот „Телеком" во информатичкиот и телекомуникацискиот сектор) има одговорност да ја заштити инфраструктурата што е важна за функционирањето на целото општество, а тоа не може да се направи ефикасно и без поголеми трошоци ако не постои соработка со јавните институции. Таквиот сооднос создава голем

број отворени прашања во тој поглед, како што се оние во врска со следново: развивањето на заеднички постапки, размената на претходно спомнатите чувствителни податоци кое, пак, бара градење доверба, како и размена на знаења и искуства. Затоа, во Република Хрватска неопходно е да се воспостави прифатлив заеднички модел на соработка во оваа област со јасно утврдени заемни права и обврски.

Развојот на моделот и воопшто на сите компоненти кои се однесуваат на системот за заштита на критичната инфраструктура треба да бидат насочени кон воспоставувањето посебно тело кое во исполнувањето на неговите задачи ќе има институционални овластувања и влијание врз сите заинтересирани страни во системот. Во многу земји постојат добри примери (како што се САД, Велика Британија, Романија) за успешно формирање такви тела кои се наречени *Центри за заштита на критичната инфраструктура*. Со анализирање на нивните активности, можно е истите да се прилагодат и соодветно да се формира таков центар и во Република Хрватска.

Освен тоа, треба да се вложат напори за подобрување на системот и за развивање на методи за зголемување на свеста за важноста на критичните инфраструктури (како за благосостојбата на населението, така и за функционирањето на економијата и на јавната и национална безбедност), но и за подигнување на свеста за нивната меѓузависност, важноста на нивната заштита и управувањето со ризиците за нив, како и за самата природа на ризиците кои потенцијално можат да ги загрозат. Заштитата на критичната инфраструктура е одговорност и обврска на целото општество, така што е потребен консензус на национално ниво во однос на националната програма за заштита на критичната инфраструктура, кој е тешко да се постигне без неопходната политичка поддршка која треба да обезбеди развој и напредок на процесот. Во 2017 година беа усвоени *Националната стратегија за безбедност* и *Законот за внатрешна безбедност*, коешто во рамките на заштитата на критичните инфраструктури беше посочено како една од стратешките цели на Република Хрватска и кое ја смени состојбата во поглед на препознавањето на важноста на концептот на заштита на критичната инфраструктура. Со тоа, можноста за реализирање на сите напори кои сме ги направиле досега се зголемува до таму што веќе имаме воспоставено еден поквалитетен систем од оној кој всушност порано сметавме дека сме во состојба да го воспоставиме.

ГЛАВА 6

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА И ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Глава 6

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА И ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Проф. д-р Марина Митревска
Проф. д-р Тони Милески
Универзитет Св. Кирил и Методиј - Скопје
Филозофски факултет, Институт за безбедност, одбрана и мир

Современите безбедносни закани попримаат нова „иновативна" димензија која налага да се прошири опфатот и поимањето на одредени безбедносни закани кои можат негативно да се одразат на функционирањето на критичната инфраструктура. Притоа, стануваат пософистицирани и подеструктивни во својата манифестна форма. Таквата состојба еминентно ја потенцира потребата од развој на современ концепт за национална отпорност и современ концепт за заштита на критична инфраструктура.

Во ова поглавје, авторите се осврнуваат на актуелните состојбите во Република Северна Македонија поврзани со градењето ефикасен систем за заштита на критичната инфраструктура. Идентификувани се приоритетните сектори, како што се енергетиката, информатичките технологии, водните системи и воздушниот сообраќај. Во секој од посочените сектори, како резултат на реформските зафати на државата, постојат определени законски и подзаконски акти кои можат да овозможат ефикасно регулирање на заштитата на критичната инфраструктура. Консеквентно на тоа, авторите нудат соодветни мерки и препораки кои би биле најцелисходни во организацијата на заштитата на критичната инфраструктура. Така на пример, понуден е пример за креирање ефикасна стратегија за заштита на енергетската критична инфраструктура. Стратегијата, после идентификација на постоечките ризици, треба да даде вистинска насока за надминување на состојбите околу немањето позитивно законодавство за енергетската критична инфраструктура. Сепак, идентификувани се парцијални решенија во различни сектори на критичната инфраструктура, кои не се погрешни, но многу веројатно можат да придонесат кон „задушување" на целиот процес за креирање и ефикасно функционирање на оптималниот систем за заштита на критичната инфраструктура. Како резултат на таквите состојби, на крајот од поглавјето, дадени се препораки за преземање практични чекори во насока на изградба на систем за заштита на критичната инфраструктура.

6.1. Состојби во Република Северна Македонија на полето на заштитата на критичната инфраструктура

Како резултат на евроатлантските определби, Република Северна Македонија презема и реализира голем дел реформи кои неодминливо го зафаќаат и спектарот на прашања поврзани со заштитата на критичната инфраструктура.

Република Северна Македонија по осамостојувањето започна да води своја автономна политика во сите домени на општественото живеење како рамноправен меѓународен правен субјект. Во таа насока, таа гради свои принципи на надворешна политика, а во тие рамки и принципи за безбедносна политика, како неделив дел од остварувањето на своите национални интереси. Во редот на најважните активности, врз чија основа понатаму се надоврзува безбедносната политика, спаѓа и заштитата на критичната инфраструктура.

Во редот на најважните активности, врз чија основа понатаму се надоврзува и заштитата на критичната инфраструктура, спаѓаат:

- дефинирање на објекти како критична инфраструктура;
- дефинирање на мерки за нивна заштита и безбедност; и
- дефинирање на задолженија и одговорности.

Од овој аспект, особено е значајно да се забележи дека детерминирањето на критичната инфраструктура во Република Северна Македонија не е во согласност со насоките на Европската унија. Во таа насока, недостасува јасно конкретизирање на поимот критична инфраструктура. Токму затоа, општоприфатен е ставот дека во конкретизирање на објектите како критична инфраструктура треба да се тргне од анализа на неколку одлуки, и тоа:

- Одлуката за определување на личности и објекти за заштита. Оваа Одлука е донесена врз база на Законот за внатрешни работи. Во Одлуката прецизно се наведени објектите од интерес за безбедноста на Република Северна Македонија, и тоа: електростопанството, ПТТ сообраќајот, железниците, аеродромите, водоводите и др.
- Одлуката за определување на правните лица кои се должни да имаат приватно обезбедување.[18] Во Одлуката таксативно е наведено обезбедувањето на правни лица, чија дејност е поврзана со ракување, и тоа:
  - со радиоактивни материи или пак, други по луѓе и околината опасни материи;
  - правни субјекти регистрирани за производство и промет на големо со лекови и медицински помагала;
  - правни субјекти регистрирани за производство и промет на запалливи течности и гасови;
  - правни субјекти регистрирани за вршење на превоз на опасни материи;
  - правни субјекти регистрирани за ракување со предмети и објекти од особено културно и историско значење.[19]

За да може оперативно, стручно и ефикасно да се заштити критичната инфраструктура во Република Северна Македонија, во делот IV на оваа Одлука дефинирано е задолжително приватно обезбедување на правните лица и тоа кога е интерес остварување на безбедноста на Република Северна Македонија. Конкретно, дефинирани се неколку дејности, и тоа:

18 Оваа Одлука е донесена од страна на Владата на Република Северна Македонија, во 2013 година, а потребата за носење произлегува од Законот за приватно обезбедување од 2012 година и од Законот за изменување и дополнување на Законот за приватно обезбедување, донесен во 2013 година.

19 Одлука за определување на правните лица кои се должни да имаат приватно обезбедување, „Службен весник на Република Македонија", бр.106/2013, член 2

- енергетиката (производство, пренос и дистрибуција на енергија);
- водоснабдувањето;
- животната средина;
- Македонската радиотелевизија, електронските и печатените медиуми;
- Народната банка на Република Северна Македонија и други правни лица регистрирани за вршење на банкарски работи.[20]

6.2. Заштита и обезбедување на критичната инфраструктура во Република Северна Македонија

Заштитата и обезбедувањето на критичната инфраструктура во Република Северна Македонија треба да бидат насочени кон неколку клучни дејности, и тоа кон:

- енергетскиот сектор;
- информатичките технологии;
- водните системи; и
- воздушниот сообраќај.

Енергетскиот сектор во Република Северна Македонија е регулиран во согласност со Законот за енергетика. Тука, како приоритетни би ги издвоиле стратегиски најважните компании, и тоа: ЕЛЕМ (Електрани на Македонија) и АД МЕПСО (Македонски електропреносен систем, оператор), кои со целокупните капацитети претставуваат стожер на енергетскиот систем. Додека пак, од нафтената инфраструктура, приоритет во заштитата има АД ОКТА, затоа што има значајна улога во продажбата, снабдувањето и дистрибуцијата на нафтени деривати во Република Севрна Македонија.

Информатички технологии. Во овој сектор посебен акцент треба да биде ставен на широкиот спектар на мерки за обезбедување и заштита на комуникациската инфраструктура. Како приоритетни би ги издвоиле стратегиски најважната критична инфраструктура, и тоа: „Македонски телеком" и ВИП. Ова се компании кои со целокупните капацитети, претставуваат стожер на фиксната и на мобилната мрежа и на најсовремените информатички технологии.

Водните системи во Република Северна Македонија се регулирани во согласност со Законот за води. Во овој сектор, посебен акцент треба да биде ставен на широкиот спектар на мерки за обезбедување и заштита на површинските води, езерата, акумулациите и изворите, водостопанските објекти и др. За таа цел, потребно е да се обезбедат:

- достапност на доволни количини здравствено исправна и чиста вода за пиење;
- снабдување со здравствено исправна вода за пиење;
- во случај на нејзино контаминирање, забрана или ограничување на користењето;

20 Исто

- преземање на мерки за континуирано обезбедување на квалитет на водата за пиење.

Воздушниот сообраќај во Република Северна Македонија е регулиран во согласност со Законот за воздухопловство. Според него, организации кои се вклучени во безбедноста на цивилниот воздушен сообраќај на национално ниво се:

- Агенцијата за цивилно воздухопловство;
- Министерството за внатрешни работи;
- аеродромските оператори; и
- авиопревозниците. (Закон за воздухопловство, 2015).

Ефикасна безбедност на оваа критична инфраструктура може да се постигне само доколку се исполнат неколку предуслови, и тоа:

- континуиран развој;
- примена на законски прописи;
- континуирано преземање на мерки, програми и процедури.

Оттука, можеме да заклучиме дека за да се постигне стандардизирано рамниште на безбедност на воздушната пловидба, треба преку телото кое е задолжено за безбедност (обично преку Агенцијата за цивилно воздухопловство) да се усвои:

- сеопфатна политика, поддржана со законски прописи, која ќе ја спроведуваат сите субјекти вклучени во која било безбедносна структура на цивилното воздухопловство;
- секој од спомнатите субјекти, полициските служби, авиооператорите, разузнавачките служби и др. мораат да имаат јасно дефинирана политика, процедури, стандарди за делување и методи за примена во согласност со насоките на државата;
- предлог за формирање на Национален комитет за безбедност и Комитет за аеродромска безбедност;
- други ефикасни тела со кои координирано ќе се спроведуваат политиката и стандардите за спроведување на мерките за безбедност. (Алчески, Ѓ., 2016: 213-2014).

6.3. Пример за креирање ефикасна стратегија за заштита на енергетската критична инфраструктура

Под претпоставка дека во доменот на заштитата на критичната инфраструктура, секторот на енергетика и транспорт ќе биде приоритет за Република Северна Македонија во процесот на интеграција во ЕУ, во оваа прилика ќе на-правиме пресек и анализа на состојбите во сферата на енергетскиот сектор.

Прецизното дефинирање на енергетската инфраструктура на Република Северна Македонија е дел од потенцираните реформски зафати. Како еден од структурните елементи и составен дел на критичната инфраструктура,

енергетската инфраструктура подлежи на бројни мерки и активности за нејзина заштита. Она што мораме да го предочиме е фактот што активностите кои се преземаат за обезбедување на енергетската инфраструктура претставуваат посебен концепт, различен од концептот на енергетска безбедност кој првенствено се фокусира на политички и економски мотивираните прекини на снабдувањето со соодветните енергетски ресурси. Современиот концепт за заштита на енергетската инфраструктура на развиените држави е релативно нов и поразличен од традиционалниот – одбранбено фокусиран – начин на обезбедување на енергетската инфраструктура. Тој е сеопфатен и интегриран во концептот за заштита на критичната инфраструктура и има нераскинлива врска со националната безбедност. Тоа значи, дека покрај државните институции вклучени се сите релевантни структури од приватниот сектор кои стопанисуваат со енергетската инфраструктура. Како резултат на тоа, современиот концепт има сериозен потенцијал да се развие во ***систем*** кој драстично ќе го редуцира ризикот од современите безбедносни закани.

Гернерално гледано, и покрај фактот што во нашата држава нема позитивно законодавство за критична инфраструктура, сепак постои своевидна заштита на објектите и системите кои спаѓаат во категоријата критична инфраструктура. За жал, таквите парцијални решенија, кои најчесто се и неконсолидирани, не се преточени во систем, па во пракса може да се случи одредени институции да се преклопуваат во надлежностите или паралелно, а различно да постапуваат. Оттука се гледа важноста оваа област која сама по себе е и важно безбедносно прашање, да биде соодветно регулирана. Со донесување на соодветно законодавство (закон, подзаконски акти) прво, конечно би се воспоставил јасен систем според кој би биле дефинирани клучните поими во оваа област, би се утврдиле основните сектори или области од сферата на критичната инфраструктура, би била јасно детерминирана и доделена улогата на централно тело за координација и др., со што ќе дојде до креирање на оптимален ***систем*** во кој адекватно би биле лоцирани и соодветно искористени сите потребни, особено човечки ресурси, затоа што заштитата на критичната инфраструктура нужно бара планирање и спроведување на безбедносни мерки и брза и соодветна реакција на опасностите и можните штети. Во нив треба да се вклучени не само државните капацитети, кои се сепак ограничени, туку и огромните ресурси кои ги нуди приватниот безбедносен сектор.

Но, се додека држават не го воспостави конкретниот систем за заштита на критичната инфраструктура, државните авторитети мора да прифатат она што е актуелна состојба, односно парцијално нормативно регулирање на оваа проблематика. Како пример, потенцираме дека ќе биде анализирана сферата на енергетиката и заштитата на енергетската инфраструктура.

Ако се направи анализа на повеќе националните стратегии за заштита на критичната инфраструктура на држави членки на ЕУ и НАТО, ќе се увиди дека интересот за заштита на енергетската инфраструктура од асиметрични закани или природни катастрофи, претставува еден од клучните императиви на современите демократски држави. Затоа, современите држави и нивните енергетски сектори преземаат соодветни мерки, но и одговорност да ја гарантираат достапноста на потребните количини енергетски ресурси во секое време

и без прекин кој би имплицирал дополнителни безбедносни или економски проблеми. Во тој контекст, Република Северна Македонија не треба и не смее да претставува исклучок. Како земја со исклучително важна геополитичка и геостратегиска положба во Европа и дефинирани стратегиски определби за интеграција во ЕУ и НАТО, енергетската инфраструктура на Република Северна Македонија не е имуна на глобалните асиметрични закани. Во поновата историја, Република Северна Македонија сè уште се нема соочено со конкретни безбедносни закани и оштетувања на енергетската инфраструктура кои би имале сериозни последици по нејзината економска и безбедносна состојба. Меѓутоа, недостатокот од оперативни национални и правни регулативи за превенција, како и соодветен одговор во случај на закани по безбедноста на енергетската инфраструктура – како резултат на асиметрични закани – има потенцијал да предизвика сериозни последици по Република Северна Македонија и нејзините граѓани. Бидејќи тоа претставува национален безбедносен проблем, очигледно е дека безбедноста на енергетската инфраструктура, е задача за која Владата на Република Северна Македонија има примарна, но не и единствена одговорност. Во голема мера, тоа е затоа што многу потенцијални терористички или други субверзивни цели – како хидроелектраните, термоелектраните, рафинеријата Окта, нафтоводот Солун-Скопје, магистралниот гасовод Деве Баир-Скопје и сл. се во сопственост или се управуваат од приватни или мешовити компании во кои значен удел има и државата. Токму поради тоа Владата и енергетскиот сектор, покрај подеднакво важните и меѓусебно поврзани обврски, имаат и правна одговорност за заштита на енергетската инфраструктура на Република Северна Македонија.

Со цел детерминирање на клучните фактори за донесување ефективна стратегија за заштита на енергетската инфраструктура на Република Северна Македонија, во оваа точка ќе извршиме анализа на релевантните законски и подзаконски акти кои делумно ја регулираат заштитата и безбедноста на енергетската инфраструктура.

6.4. Правни норми и недостатоци за донесување на стратегија за заштита на енергетската инфраструктура на Република Северна Македонија

Соодветните стратегиски и законски решенија претставуваат предуслов за отпочнување изградба на ефикасен систем за заштита на критична инфраструктура. Врз основа на примерите на поголемиот дел од земјите членки на ЕУ и НАТО, во потрагата по правните основи за заштита на енергетската инфраструктура на Република Северна Македонија, треба да се анализираат:

- Стратегијата за одбрана на Република Македонија;
- Законот за енергетика;
- Законот за управување со кризи и
- Законот за заштита и спасување.

Ваквиот пристап е еден од можните, кои се темели на претпоставката дека секој сектор на критичната инфраструктура ќе има соодветно стратегиско и

законско решение кое ќе овозможи ефикасна заштита на критичната инфраструктура. Како резултат на анализата ќе издвоиме неколку клучни сознанија кои имаа големо значење од аспект на детерминирањето на правните недостатоци, на кои Република Северна Македонија во иднина ќе треба да ги насочи напорите во функција на креирање поволни услови за донесување на стратегија за заштита на енергетската инфраструктура.

6.4.1. Стратегија за одбрана на Република Северна Македонија

Безбедноста и заштитата на граѓаните претставува примарна и основна одговорност на Владата на Република Северна Македонија. Според Стратегијата за одбрана, „развојот и одржувањето на системот за безбедност и одбрана е една од основните задачи на Владата на Република Северна Македонија во интерес на граѓаните". (Стратегија за одбрана на Република Македонија, 2010). Оваа обврска кон националната безбедност на Република Северна Македонија, Владата не може да ја исполни без соодветна заштита на енергетската инфраструктура. Електроенергетскиот сектор, секторот за нафта и нафтени продукти, како и останатите сегменти од енергетската инфраструктура се интегрален дел од безбедноста и добросостојбата на македонските граѓани. Слично на државата, граѓаните на Република Северна Македонија имаат потреба од функционална и стабилна енергетска инфраструктура – отпорна на асиметрични закани, природни или технолошки катастрофи – која на време и во потребните количини ќе ги доставува енергетските ресурси неопходни за одржување и унапредување на безбедноста и добросостојбата на македонските граѓани.

Затоа, покрај органите на државната власт посебни задачи од областа на одбраната, а особено во функција на безбедноста на енергетската инфраструктура, можат да извршуваат и трговските друштва, јавните претпријатија, установите, службите и единиците на локалната самоуправа. Ова особено важи за енергетските оператори, кои водени од целта за безбедно, навремено и квалитетно снабдување на потрошувачите – меѓу кои граѓаните и органите на државната власт – се обврзани да преземаат соодветни превентивно-безбедносни мерки опфатени во останатите законски и подзаконски акти анализирани во оваа точка. За да може да одговори на комплексните барања кои произлегуваат од стратегиските определби за целосна интеграција во ЕУ и НАТО, системот за одбрана на Република Северна Македонија се гради и развива врз основа на неколку фактори кои индиректно ја тангираат и националната енергетска инфраструктура. Проценката на современите безбедносни закани, ризици и предизвици на национално, на регионално и на глобално ниво, геополитичките детерминанти, како и националните ресурси и проектираните економски можности на државата се клучните фактори кои треба да се земат во предвид при планирањето, организацијата и реализацијата на заштитата на националната енергетска, односно критична инфраструктура. Како еден од столбовите на системот за одбрана, Стратегијата го нагласува развојот на оперативните способности на Армијата на Република Северна Македонија, и тоа во две насоки поврзани со безбедноста на енергетската инфраструктура.

Првата насока е поддршка на полицијата и на другите државни институции при заштитата на критичната инфраструктура и поддршка во справувањето со последиците во случај на терористички напад, додека втората е поддршка на државните институции во случај на природни катастрофи и епидемии, техничко-технолошки и други опасни и кризни состојби. (Чаминski, Б. 2017: 168).

6.4.2. Закон за управување со кризи

Водечката улога на Владата во процесот на заштита на критичната, односно енергетската инфраструктура, е дефинирана и во Законот за управување со кризи кој го уредува системот за управување со кризи во Република Северна Македонија. (Закон за управување со кризи, 2005). Покрај Владата и останатите органи на државната управа и државната власт, АРМ и силите за заштита и спасување, во превенцијата, раното предупредување и справувањето со кризи можат да учествуваат и јавните претпријатија, јавните установи и служби, како и трговските друштва. Истите имаат обврска за заштита и спасување на вработените, лицата кои се затекнале кај нив и материјалните добра како и отстранување на последиците од кризната состојба. Иако недостасува експлицитно нагласување на поимот, сепак – кога станува збор за енергетските оператори - се подразбира дека „материјалните добра" ја претставуваат енергетската инфраструктура со која тие стопанисуваат. Исто така, министерствата и останатите органи од државната управа и општините, јавните установи и служби, како и трговските друштва од посебно значење за работа во кризна состојба, имаат обврска во своите акти за организација и систематизација да утврдат работни места за подготвување и извршување на работни задачи во врска со превенција и спасување во кризна состојба. Според членот 12 од Законот, во системот за управување со кризи се формираат Управувачки комитет, Група за проценки и Дирекција/Центарот за управување со кризи. Покрај мерките и активностите кои Управувачкиот комитет ги презема во кризна состојба, истиот има обврска да обезбеди навремена, квалитетна и реална проценка на загрозеноста на безбедноста на Републиката од ризици и опасности. Со оглед на фактот дека го сочинуваат министрите за внатрешни работи, за здравство, за транспорт и врски, за одбрана и за надворешни работи, тогаш без никакво сомнение може да се констатира дека лидерската функција на Владата во заштитата на критичната инфраструктура воопшто не е спорна. Покрај Управувачкиот комитет и Групата за процена е тело на Владата во чиј состав влегуваат директорите на Бирото за јавна безбедност, на Управата за безбедност и контраразузнавање, на Агенцијата за разузнавање, директорите и замениците на директорите на Центарот за управување со кризи и Дирекцијата за заштита и спасување, заменикот на началникот на Генералштабот на АРМ и раководителот на Службата за безбедност и разузнавање во Министерството за одбрана. Како тело чиј лидер го определува Владата на Република Северна Македонија, Групата за процена има перманентна задача – не само во случај на криза – да врши процена на ризиците и опасностите по безбедноста на државата и да предлага мерки и активности за нивна превенција, за рано предупредување и на крај за справување со кризна состојба. Резултатите и заклучоците Групата за процена ги доставува до Управувачкиот комитет, Претседателот на Владата, Претседателот

на Републиката и Претседателот на Собранието. Центарот за управување со кризи е самостоен орган и носител на вкупната поддршка на Управувачкиот комитет и Групата за процени кој обезбедува континуитет во меѓуресорската и меѓународната соработка во управувањето со кризи, изработува и ажурира единствена процена на ризиците и опасностите по безбедноста на Република Северна Македонија. Како оперативно стручно тело, кое раководи со активностите за превенција и справување со кризни ситуации, во рамките на Центарот се формира Главен штаб кој го сочинуваат претставници на органите инволвирани во работата на Управувачкиот комитет. Врз основа на претходно наведеното може да се констатира дека Законот им делегира одговорност на секоја од институциите вклучени во органите и телата во системот за управување со кризи, да преземат мерки и активности за собирање информации и идентификување на безбедносните ризици и опасности, вклучувајќи ги оние кои ја загрозуваат безбедноста на енергетската инфраструктура. Во рамки на законската легислатива и овластувањата, институциите опфатени во системот за управување со кризи, врз основа на нивните проценки ги утврдуваат целите, задачите и спроведувањето на потребните дејства за превенција, рано предупредување и справување со кризи. Меѓу другото, учесниците во системот за управување со кризи се должни меѓусебно да комуницираат, координираат и соработуваат со Центарот при извршувањето на должностите утврдени со законот. Со цел планско, навремено, целесообразно и координирано донесување на одлуки, насоки и препораки за преземање на мерки за превенција, како и за најоптимално справување со кризна состојба, се изработува процена на загрозеност на безбедноста на Република Северна Македонија од сите ризици и опасности која ја донесува Владата. Што се однесува до имплементацијата, односно применувањето на одредбите од овој Законот, Центарот за управување со кризи пропишува инспекциски надзор во органите на државната управа, општините и останатите елементи од јавниот и приватниот сектор и предвидува соодветни казнени одредби во случај на непочитување на одлуките и останатите мерки пропишани со Законот за управување со кризи. (Чаминski, Б. 2017: 168-171)

6.4.3. Закон за заштита и спасување

Заштитата и спасувањето, кое го организираат и спроведуваат не само државните и органите на управата туку и сите јавни установи, трговски друштва меѓу кои и енергетските оператори, претставува работа од јавен интерес за Република Северна Македонија. Согласно соодветниот закон, системот за заштита и спасување се остварува преку поголем број на мерки и активности, меѓу кои: набљудување, откривање, следење и проучување на можните опасности од природни непогоди и други несреќи; преземање превентивни мерки, известување и предупредување; одредување и спроведување на заштитните мерки; надзор на спроведувањето на заштитата и спасувањето; идентификација и процена на опасностите; изработка на процена на загрозеност од природни непогоди и други несреќи и планови за заштита и спасување и ажурирање на истите, итн. Покрај природните, наведените мерки и активности се преземаат и за проценка и спречување на други несреќи, кои Законот ги дефинира како

настани кои се резултат на одредени превиди и грешки во извршувањето на секојдневните стопански и други активности, како и невнимание при ракување со опасни материи и средства при производство, складирање и транспорт на истите (пожари, големи несреќи во патниот, железничкиот и воздушниот сообраќај, несреќи во рудници, индустриски несреќи предизвикани од експлозии и други техничко-технолошки причини, паѓање на радиоактивни врнежи, прашини и талози, излевање на нафта и нафтени деривати и други отровни хемикалии, експлозии на гасови, запаливи течности и гасови, како и други горливи материи кои со воздухот создаваат експлозивни смеси и други експлозивни материјали од поголем размер). Иако асиметричните закани експлицитно не се наведени во Законот, сепак постои голема веројатност од „намерни превиди или грешки" (саботажа или диверзија) при ракувањето со наведените опасни материи, од кои дел спаѓаат во примарните или финалните продукти на енергетскиот сектор на Република Македонија. Од вкупно осумте начела на кои се засновува заштитата и спасувањето во Република Македонија, од аспект на енергетската инфраструктура најзначајни се следните: секој има право на заштита и спасување од природни непогоди и други несреќи; Република Северна Македонија, општините, јавните претпријатија, установи и служби и трговските друштва се должни, навремено да ги организираат и преземаат превентивните и оперативните мерки за заштита и спасување од природни непогоди и други несреќи; секое физичко и правно лице, во согласност со Законот, одговара за неспроведување на предвидените мерки за заштита и спасување, итн. Од особено значење за заштитата на енергетската инфраструктура е начелото кое ги обврзува институциите на системот за безбедност, и компаниите од јавниот и приватниот сектор (каде спаѓаат и енергетските оператори) да организираат и преземаат, пред сè оперативни мерки, на кои стратегиите за заштита на критичната инфраструктура на современите демократски држави им даваат клучна улога во процесот на постигнување на целите на соодветните национални стратегии. Планирањето на заштитата и спасувањето се реализира врз основа на Националната стратегија за заштита и спасување која ја донесува Собранието по предлог на Владата на Република Северна Македонија. Со цел организирано спроведување на заштитата и спасувањето, сите учесници во системот донесуваат План за заштита и спасување од природни и други несреќи. Планот за заштита и спасување се изработува врз основа на Проценатa на загрозеност од природни и други несреќи на територијата на Република Северна Македонија, додека за потребите на приватниот сектор, вклучувајќи ги и енергетските оператори, проценатa ја донесува органот кој управува со истите. Според тоа, може да се констатира дека проценатa на загрозеност на енергетските оператори кои се во приватна сопственост – согласно расположливите информации – ја донесува менаџментот, врз основа на која го донесува и планот за заштита и спасување по кој ги презема натамошните мерки и активности за обезбедување на инфраструктурата од природни катастрофи и други закани. (Закон за заштита и спасување, 2012).

6.4.4. Закон за енергетика

Законот за енергетика е уште еден правен акт кој се совпаѓа со примарната одговорност на Владата на Република Северна Македонија – безбедност и заштита на граѓаните. Сигурното, безбедно и квалитетно снабдување на потрошувачите со енергија и енергенти, создавање на ефикасен, конкурентен и финансиски одржлив енергетски сектор, и заштитата на животната средина од негативни влијанија при вршењето на одделни дејности од областа на енергетиката, се дел од главните цели на овој закон. (Закон за енергетика, 2018).

Законот за енергетика е единствен закон во кој се опфатени поимите: безбедност, заштита, енергија (видовите на енергенти) и инфраструктура. Под поимот „безбедност", Законот за енергетика ја дефинира способноста за обезбедување на заштитата на здравјето и животот на луѓето, заштита на животната средина и имотот со преземање на технички и други видови безбедносни мерки при производство, пренос и дистрибуција на енергија или енергенти. Покрај разните видови на енергенси, Законот ги дефинира и најголемиот дел од компонентите на енергетската инфраструктура, како гасовод, нафтовод, дистрибутивна мрежа за електрична енергија, електроенергетски систем, енергетски објект, енергетски сектор, оператор, производител на електрична енергија итн. Исто така, со законот се регулираат бројни права и обврски кои енергетските оператори треба да ги преземаат во функција на заштита на енергетската инфраструктура и сигурност во снабдувањето не само на граѓаните туку и на институциите од системот за национална безбедност. Согласно Законот за управување со кризи, операторите на системите за пренос и дистрибуција на соодветен вид енергија или енергенс, се должни да изготват планови за постапување во кризни состојби и да ги достават за одобрување до Министерството за економија. Понатаму, операторите на дистрибутивните системи се должни да донесат и објават правила за дистрибуција со кои, меѓу другото, се уредуваат: техничките и другите услови за сигурно и безбедно функционирање на дистрибутивните системи; мерки, активности и постапки во случај на нарушувања и хаварии; пропишаните мерки за безбедност итн. Исто така, Законот предвидува строги безбедносни мерки кои потенцијалните инвеститори во енергетскиот сектор мора да ги преземат како предуслов за добивање на овластување за изградба на енергетски објекти. Тие мерки се однесуваат на безбедноста и сигурноста на енергетскиот систем, објектите и соодветната опрема, заштитата на јавното здравје и сигурноста, и заштитата на животната средина. Иако постојат соодветни законски основи и обврски за заштита на енергетската, односно критичната инфраструктура во која главната улога ја има централната власт, Република Северна Македонија значително заостанува во однос на видот и ефективноста на правните регулативи за заштита на критичната инфраструктура на земјите членки на ЕУ и НАТО, анализирани во претходната глава. Како земја кандидат за полноправно членство во ЕУ, Република Македонија треба да ги следи чекорите кои Унијата и нејзините членки ги преземаат во функција на заштитата на критичната инфраструктура. Затоа Владата на Република Северна Македонија најпрво мора да ја дефинира критичната инфраструктура, а потоа да пристапи кон изработка и донесување на Програма за заштита на националната критична инфраструктура како ос-

нова за развој на ефективна стратегија за заштита на истата. Програмата треба да биде резултат на конструктивна соработка која мора да се воспостави и одржува помеѓу приватниот сектор – вклучувајќи ги и енергетските оператори – и надлежните владини институции на државно и локално ниво, не само во кризна состојба туку и во мирновремени услови. Основната цел на таа соработка е создавање оперативна и ефективна национална рамка за заедничко дејствување и изградба на еластична и стабилна критична инфраструктура, по примерот на организацијата на органите и телата во системот за управување со кризи. Изработката на предлог-стратегија за заштита на критичната инфраструктура, во која ќе учествуваат надлежните владини институции, оператори и компании од приватниот сектор, како и искусни експерти од областа на безбедноста на критичната инфраструктура, претставува следен чекор во процесот на донесување на ефективна стратегија за заштита на енергетската, односно критичната инфраструктура. Намената на предлог-стратегијата е изработка и дефинирање на централизирана, интегрирана и прогресивна стратегија која ќе вклучува доброволно учество на индустриските, енергетските и останатите оператори од приватниот сектор, како и надлежните институции од централната и локалната власт. Посакуваниот исход од стратегијата е доволно еластична и имуна - на безбедносни ризици и закани - критична инфраструктура која на граѓаните ќе им овозможи континуиран и гарантиран пристап до основните сервиси, меѓу кои и снабдувањето со потребните енергетски ресурси. Еден од водечките принципи на стратегијата претставува подигање на свеста кај енергетските и индустриските оператори и централната и локалната власт од потребата за заштита на националната критична инфраструктура, како и потребата од целосно и перманентно интегрирање на разузнавачките и безбедносните проценки во плановите за справување со кризна состојба.

Доколку се направи компарација меѓу Законот за управување со кризи, Законот за заштита и спасување и Законот за енергетика, може да се заклучи дека јавните претпријатија, трговски друштва, индустриски капацитети и енергетските оператори, доброволно или договорно може да учествуваат во превенцијата, раното предупредување и справување со природните и безбедносните ризици и опасности. Меѓутоа, без оперативна рамка за соработка, институциите од системот за национална безбедност и менаџментот на енергетските оператори не се во можност ефективно да ги имплементираат и координираат мерките и активностите за заштита на енергетската инфраструктура. Решавањето на овој проблем не треба да се перципира единствено како национален проблем, туку претставува обврска која државата ја има како аспирант за полноправно членство во ЕУ и НАТО. Енергетските оператори мора да имаат доволно информации неопходни за релевантни безбедносни проценки врз основа на кои ќе ги планираат и реализираат потребните мерки за заштита на инфраструктурата. Ова особено се однесува на асиметричните закани за кои енергетските оператори немаат ниту капацитет ниту законски овластувања за собирање на разузнавачки информации од таков карактер. Затоа креирањето на заеднички интегриран пристап во функција на безбедноста на енергетската инфраструктура треба да биде подеднакво важен и законски императив, како за Владата така и за енергетските оператори. (Чаминski, Б. 2017:172-175).

6.5. Елементи и модел на стратегија за заштита на енергетската инфраструктура

Современиот концепт за заштита на енергетската инфраструктура, како интегрален дел од националните стратегии за заштита на критичната инфраструктура, се состои од низа последователни и меѓусебно поврзани елементи кои ја регулираат безбедноста на енергетскиот сектор како основен двигател на економската и развојната политика на современите демократски држави. Денес, речиси и да нема дел од приватниот и јавниот сектор кој не зависи од инфраструктурата која ги обезбедува потребните енергетски ресурси за нивно непречено и безбедно функционирање. Затоа, во фокусот на заштитата на критичната инфраструктура се токму енергетските објекти кои се неопходни за функционирање на политичките, социјалните, економските и безбедносните процеси во општеството. При планирањето на елементите од стратегија за заштита на енергетската инфраструктура, без разлика дали ќе биде самостојна или составен дел од стратегијата за заштита на критичната инфраструктура, треба да се земе предвид дека секој сегмент од енергетскиот сектор во Република Северна Македонија се состои од сложена физичка, компјутерска, институционална, функционална и персонална структура чие функционирање е невозможно без употреба на современите комуникациски системи и интернетот. Најголемиот дел од објектите за производство, пренос и дистрибуција на електрична енергија се наоѓаат на површината на земјата и се видливи. Исклучувајќи го железничкиот и патниот транспорт, како и контролните станици, инфраструктурата за пренос и дистрибуција на природен гас и нафта се наоѓа под површината на земјата и истата (со одредени исклучоци) не е видлива, но е означена. Оттука, треба да се развие единствена методологија за идентификување на енергетските објекти, системи и функции кои имаат критично значење за државата и приоритет во однос на нивната заштита. За таа цел, неопходно е креирање на сеопфатна, просторно и временски ажурирана база на податоци за прецизно одредување на критичните објекти, системи и функции, како и конкретна поделба на одговорностите меѓу приватниот и државниот сектор. Ризикот од напад врз енергетската инфраструктура варира во однос на вредноста и важноста на капацитетот (производство, преработка, складирање, транспорт – нафтовод, гасовод, далекувод – дистрибуција и сл.). Неодамна, енергетската инфраструктура стана легитимна цел и на глобалните терористички организации. Забрзаниот процес на глобализација и неизбежната меѓународна трговија со енергетски ресурси, дополнително го зголеми ризикот од терористички напади врз енергетската инфраструктура. Иако Република Северна Македонија и поширокиот регион на ЈИЕ не се соочија со директни терористички напади, сепак нападот и онеспособувањето на енергетската инфраструктура на земјите од кои потекнуваат или преку кои транзитираат енергетските ресурси, може да има сериозно влијание по националната енергетска безбедност и економскиот развој на државата. Покрај финансирањето на сопствените активности, терористичките организации настојуваат да предизвикаат сериозни оштетување на енергетската инфраструктура со вооружен или сајбер-напад од далечина со цел создавање паника во општеството, прекин на индустриското производство и пред сè прекин на

преносот на електрична енергија, нафта и нафтени деривати. Од аспект на заканите, различните елементите на енергетската инфраструктура на Република Северна Македонија се карактеризираат со различен степен на ранливост. Загрозувањето на безбедноста на одредени енергетски капацитети може да резултира со сериозна еколошка катастрофа, иако се лоцирани на релативно мал простор кој физички лесно може да се обезбеди. Секторот за производство на нафта и нафтени продукти, како и секторот за приреден гас се карактеризираат со просторна инфраструктура чие оштетување може да доведе до прекин на снабдувањето, исцрпување на државните резерви и намалување на економските и одбранбените способности. Слична е состојбата и со електроенергетскиот сектор чија главна слабост претставува неговото централизирано автоматско управување и недостатокот од капацитети за акумулација на потребните количини електрична енергија. Со оглед на фактот дека енергетската инфраструктура има огромно значење за економската и безбедносната состојба на Република Северна Македонија, нејзината безбедност е од суштинско значење. Покрај терористичките, енергетската инфраструктура може да биде изложена на разни видови закани кој мора да бидат земени во предвид, како при анализата и проценката на ризикот и заканите, така и при дефинирањето на безбедносните и превентивните мерки. Тука спаѓаат природните катастрофи, технолошките акциденти и човечките грешки кои сериозно можат да загрозат, да предизвикаат големи штети или да уништат одредени сектори од енергетската инфраструктура од витално значење за населението и општеството во целина. Тоа може да предизвика т.н. домино ефект кој има потенцијал да парализира повеќе сектори од критичната инфраструктура на државата, да предизвика огромни штети на националната економија и губење на довербата во политичкото раководство на државата. Во тој контекст, сопствениците на енергетските капацитети и институциите на системот, иако не можат во целост да ја гарантираат безбедноста на енергетската инфраструктура, согласно законските регулативи на Република Северна Македонија, тие се должни да преземат соодветни и навремени мерки за намалување на ризикот од оштетување на инфраструктурата и повторно воспоставување на снабдувањето со потребните енергетски ресурси под поволни услови.

Бидејќи безбедноста на енергетската инфраструктура е заедничка задача на Владата и енергетските оператори на национално и на локално ниво, нивните напори треба да бидат насочени кон подигање на нивото на нејзина заштита на територијата на државата преку преземање на соодветни и меѓусебно координирани мерки. По идентификувањето на критичните делови од енергетската инфраструктура и проценката на ризикот и заканите, превенцијата е основната мерка во функција на заштитата на енергетската инфраструктура. Во случај на оштетување, неопходен е ефективен план за кризен менаџмент и подготвеност на енергетските оператори за навремено враќање на погодениот енергетски капацитет во функционална состојба. За таа цел, согласно ажурираните безбедносни процени и искуствата на земјите од меѓународната заедница, потребно е да се развијат – законски пропишаните – стандарди за заштита кои ќе обезбедат одржлива енергетската инфраструктура, имуна на современите безбедносни закани. Доследната примена на превентивите

мерки, стандардите за заштита и нивното правилно менаџирање во форма на циклус за кризен менаџмент за енергетската инфраструктура, претставуваат основната гаранција за ефективна заштита на енергетската инфраструктура на Република Северна Македонија. Најголемиот услов кој мора да биде исполнет за остварување на наведените стратегиски цели е потребата од постојана размена на информации и соработка меѓу владините институции и енергетските оператори. Без овој услов, реално не може да се очекува имплементација на стратегијата за заштита на енергетската инфраструктура, бидејќи истата вклучува збир од планови, програми, мерки и инструменти за координација и унапредување на истите, како од владините институции така и од страна на енергетските оператори.

Врз основа на сознанијата добиени од компаративната анализа на стратегиите за заштита на критичната инфраструктура на дел од земјите-членки на ЕУ и НАТО и актуелната законска регулатива за заштита на енергетската инфраструктура на Република Северна Македонија, може да се констатира дека моделот на Националната стратегија за заштита на енергетската инфраструктура – одделно или како дел од националната критична инфраструктура – претставува една целина составена од следните меѓусебно поврзани и зависни елементи:

- стратегиски цели и интереси на државата во однос на енергетската инфраструктура, дефинирани во националната стратегија за безбедност;
- усогласена законската легислатива;
- дефинирање на критичните елементи од критичната/енергетската днфраструктура и поделба на одговорноста;
- процена на безбедносните закани, ризикот и ранливоста на елементите од енергетската инфраструктура;
- одредување на стратегиската цел на стратегијата – ефективна заштита на критичната/енергетската инфраструктура;
- соработка, координација и размена на информации помеѓу инволвираните страни и
- имплементација.

Покрај идентификувањето на целите за заштита на енергетската инфраструктура, предложениот модел издвојува две нивоа на одлучување – политичко ниво и ниво на посебни сектори од критичната инфраструктура.

Стратегијата за национална безбедност и Стратегијата за заштита на критичната инфраструктура се артикулирани во рамките на првото ниво, додека во рамките на второто ниво, јавниот и приватниот сектор – заеднички – ги создаваат конкретните цели, мерки и активности за заштита на секторите од критичната инфраструктура, вклучувајќи го и енергетскиот сектор. Според предложениот модел, целите за заштита на критичната инфраструктура се поставени на највисоко стратегиско ниво и истите се дефинирани во рамките на Националната стратегија за безбедност. Покрај целите на заштита, во оваа фаза се дефинирани и сеопфатните принципи за заштита на критичната

инфраструктура. Следниот чекор е создавање стратегии за заштита на критичната инфраструктура во кои се нагласени посебните сектори и потсектори од критичната инфраструктура, а принципите за заштита (како размена на информации, создавање партнерство меѓу приватниот и јавниот сектор и сл.) се имплементирани и дополнително обработени и конкретизирани. Овој чекор води кон процес на трансфер на стратегијата од политичко, на ниво на посебни сектори. Со други зборови, доаѓа до примена на целите и принципите за заштита на критичната инфраструктура – развиени на политичко ново – во посебните/одделните сектори, каде државниот сектор и операторите од приватниот сектор меѓусебно комуницираат и разменуваат информации и искуства во функција на безбедноста на секторите и потсекторите од идентификуваната критична инфраструктура. Во нивото на посебни сектори, целите и принципите за заштита се прилагодуваат согласно посебните потреби на идентификуваниот и означен секторот или потсекторот од критичната инфраструктура. Тоа резултира во создавање на планови за заштита на секој посебен сектор од критичната инфраструктура, вклучувајќи го и енергетскиот сектор. Во оваа фаза, улогата на енергетските или индустриските оператори од приватниот сектор е да управуваат со секторите од критичната инфраструктура, да соработуваат со јавниот сектор и да артикулираат цели и мерки за да го достигнат потребното ниво на заштита на инфраструктурата. Во рамките на јавниот сектор, наменските агенции (како Центарот за управување со кризи, Дирекцијата за заштита и спасување и сл.) им ги пренесуваат националните законски обврски на операторите од критичната инфраструктура и создаваат платформи за размена на информации и партнерства.

Покрај опишаниот модел за заштита на критичната инфраструктура, кој се базира на традиционалниот принцип „од горе кон долу", постои и принцип „од долу кон горе" кој со повратни информации го информира политичкото ниво за ефективноста на целите, принципите и мерките за заштита на секторите од критичната инфраструктура. И во двете нивоа, поширокатa информираност овозможува увид и влијание врз идентификуваните, цели, принципи, мерки и средства за заштита на секторите од критичната инфраструктура, како од страна на институциите од јавниот сектор и националните/локалните агенции така и од страна на операторите од приватниот сектор и академската заедница. Според тоа, може да се констатира дека наведениот предлог-модел претставува пример за динамичен, интерактивен, и пред сè ефективен процес во кој се инволвирани сите страни кои имаат улога во процесот на дефинирање, унапредување и имплементација на целите, принципите и мерките за заштита на енергетската инфраструктура како клучен сектор од критичната инфраструктура на Република Северна Македонија. (Чаминski, Б. 2017:175-181).

Заклучоци и препораки

Како што веќе напоменавме, критичната инфраструктура претставува платформа за одржување на развојот на секое општество и држава. Оттука, Владата треба да биде вклучена во системот на заштита на критичната инфраструктура како предлагач на закони и подзаконски акти и има задача да им

даде овластување на одредени министерства да бидат координатори на целиот систем.

Владата обезбедува стратегиска рамка која е од суштинско значење за успешно функционирање на системот, соработката, комуникацијата и координацијата на сите вклучени актери. Владата, исто така ги одредува (со посебна одлука) секторите од одредени критични инфраструктури со цел да обезбедат холистички пристап за заштита и намалување на негативните влијанија во случај на закана за критичната инфраструктура.

После Владата, следниот најважен актер е координаторот (одредено министерство) на целиот систем за заштита на критичната инфраструктура. Постојат различни примери и практики за тоа кое тело е соодветно за оваа улога. Во повеќе европски земји функцијата е доделена на министерствата за внатрешни работи. Оттука, постојат различни решенија и практики, но секоја земја треба сама да го препознае најсоодветниот модел. Од сеопфатна анализа предлагаме Министерството за внатрешни работи на Република Северна Македонија да биде координатор на целиот систем за заштита на критичната инфраструктура.

Доколку МВР е координатор на системот, тој ке ја има улогата да комуницира директно со сите актери на системот, со меѓународни актери и да доставува извештаи до Владата.

Организациски пристап кон имплементацијата на заштитата на критичната инфраструктура во Европската унија и земјите кои се стремат кон полноправно членство (како Република Северна Македонија) е даден во Директивата 2008/114/ЕК за идентификација и утврдување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита – главен документ на Европската Унија за критичната инфраструктура.

За да можеме одлучно да зачекориме кон имплементација на горенаведеното, даваме неколку почетни препораки:

1. Во изградбата на системот за заштита на критичната инфраструктура потребно е да се тргне од стратегиската рамка. Неопходно е јакнењето на отпорноста и заштитата на критичната инфраструктура да се вгради во една од стратегиите на Република Северна Македонија. Притоа има неколку можности:

   А. Доколку се утврди потребата од ревизија на постоечката или изготвување на нова стратегија за национална безбедност потребно е да се посвети протстор за критичната инфраструктура во стратегијата. Неспорно е дека во Стратегијата за национална безбедност треба да се наведе дел за критичната инфраструктура.

   Б. Доколку постои или е во фаза на изготвување Стратегија за сајбе- безбедност, критичната инфраструктура може да се спомне во неа. Ваква стратегјиа е изготвена во 2018 година и во неа има делови кои се насочени кон заштитата на критичната информатичка инфраструктура како дел од севкупната критична инфраструктура. Исто така, донесен е и Акциски план за заштита на критичната информатичка инфраструктура. (Национална стратегија за сајбер-безбедност на Република Северна Македонија, 2018-2022).

В. Третото решение е предлог за изработка на Стратегија за заштита на критичната инфраструктура.

2. Нормативно, може да се предложи изработка на закон за заштита на критична инфраструктура. Додека истиот не ги помине сите предвидени фази за негово донесување, тематиката за критичната инфраструктура може привремено да се уреди во рамките на некој друг закон или подзаконски акт. (претпоставка е дека процедурите за тоа се пократки и побрзо може привремено да се уреди проблематиката).
3. При изработката на нормативната регулатива за критичната инфраструктура препораката е да се регулираат првенствено подрачјата на енергетиката и транспортот – овие два сегмента ги бара Европската унија од своите земји членки и оние кои имаат намера да ѝ пристапат. Доколку се вклучат и останатите сектори од критичната инфраструктура може да се повтори искуството на Хрватска веднаш на почеток за го успори и усложни процесот. Затоа препорака е да се тргне со секторите енергетика и транспорт.
4. Во претстојните нормативни решенија (закон и подзаконски акти), секако дека треба да се предвидат можностите за регулирање на европската критична инфраструктура.
5. Во законот или подзаконските акти мора да биде спомнат безбедносниот координатор кој претставува клучна фигура која во сите тела и органи ќе биде задолжена за работите околку критичната инфраструктура.
6. Во законот или подзаконските акти да се нагласи местото и улогата на јавното-приватно партнерство.
7. Во законот или подзаконските акти да се нагласи школувањето, едукацијата и тренингот.
8. Местото и улогата на новоформираниот Центар за заштита на критичната инфраструктура е исклучително значајно. Од тие причини, можеби Министерството за внатрешни работи е добар избор да биде државно координативно тело за овој процес. Затоа што во Центарот би требало да се собираат податоци и да се координираат активности. Исто така, во законот или подзаконските акти важно е да се наведе дека работите околу заштитата на критичната инфраструктура ќе се одвиваат преку Центарот за заштита на критична инфраструктура.
9. Што се однесува до ознаката на тајност, на почеток треба да се стави најниската можна за да не се доведеме во ситуација да се блокира процесот уште на самиот почеток.
10. Во креирањето на стратегиските решенија и законското решение треба да се формира меѓуресорска група која ќе вклучи поширок круг на стручни лица, од универзитетите, министерствата, коморите, приватниот сектор.
11. После донесување на законот, понатаму потребно е со подзаконски акти да се регулираат и уредат поединечните процеси.

После стратегијата и законот потребно е да се започне со изградбата на СИСТЕМОТ за заштита на критична инфраструктура. СИСТЕМОТ се гради со едукација, работилници и запознавање на сите фактори во тој процес. Потребно е да се направи петтогодишен акциски план за дејствување.

Литература

[1] Алчески, Ѓ., (2016), Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија (со осврт на аеродромската безбедност), Филозофски факултет, Скопје;

[2] Amin, M. (2000), National Infrastructures as Complex Interactive Networks, in: Samad, T. i Weyrauch, J. (ed.) Automation, Control, and Complexity: An Integrated Approach, New York: John Wiley and Sons, pp. 263-286;

[3] Amin, M. (2002), Modeling and Control of Complex Interactive Networks, IEEE Control Systems magazine http://massoud-amin.umn.edu/publications/Amin_IEEE_CSM_Feb_02.pdf;

[4] Antoliš, K. (2013), *Intellectual Capital and National Critical Infrastructure*, New security threats and national critical infrastructure. Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pages 7-14;

[5] Babos T. (2016) *The First Critical Infrastructure Protection Research Project in Hungary*. In: L. Nádai and J. Padányi (eds.), Critical Infrastructure Protection Research, Topics in Intelligent Engineering and Informatics 12, Springer International Publishing Switzerland;

[6] Bell, G.R., (2009) NATO's Grapple with Energy Security. In: Luft, G., Korin, A. (eds.) (2009) Energy Security Challenges for the 21st Century: a Reference Handbook. Santa Barbara: ABC-CLIO;

[7] Benjamin K. Sovacool (2010) *A Critical Evaluation of Nuclear Power and Renewable Electricity in Asia,* http://dx.doi.org/10.1080/00472331003798350;

[8] Bognar, B. 2009. The process of critical infrastructure protection, AARMS, Budapest;

[9] Braubach, A., Lauwe, P. and John-Koch, M. (2014), *CIP in Germany: Cooperation and recommendations as main driving forces,* Global Security 2014, pg. 5-14;

[10] Brian Wilson, (2012), Maritime Energy Security. NATO Centre of Excellence Defence Against Terrorism (COEDAT) in November 2012;

[11] Butorac, K. (2013), Risk Assessment Methodologies in Critical Infrastructure Protection, New security threats and national critical infrastructure. Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pages 46-58;

[12] Čemerin, D. (2013), Croatian Critical Infrastructure, Opatija: Fifth Adriatic City Security Conference, http://zastita.info/hr/sigg_2013/program0/;

[13] Cesarec, I. (2017), An overview of former and present activities of regulating Critical Infrastructure System in the Republic of Croatia, Opatija: Ninth Adriatic City Security Conferencehttp://www.zastita.info/UserFiles/file/zastita/SIGG/SIGG%202017/Prezentacije/06.%20Ivana%20Cesarec.pdf;

[14] Cesarec, I. (2019), The Civil Protection Directorate of the Republic Croatia, National Contact Point for Critical Infrastructure (electronic correspondence of authors);

[15] Чаминski, Б. (2017) Геополитичко значење и заштита на енергетската инфра¬структура на Република Македонија од асиметрични закани. Докторска дисертација. Одбранета на Филозофскиот факултет, под менторство на проф. д-р Тони Милески. Март. 2017;

[16] Dawson M., Omar M., 2015. NewThreats and Countermeasures in Digital Crime and Cyber Terrorism Information Science Reference;

[17] Deutscher Bundestag (2015), *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)* http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf (Accessed August 14 2017.);

[18] Ducamin, I. 2016. State and Operators Cooperations for Critical Infrastructure Protection;Buliding Trust for Common Interest;

[19] Engdahl, E-M. (2016), *The European Programme for Critical Infrastructure Protection,* Gas Infrastructure Europe, http://www.gie.eu/index.php/publications/doc_download/26303-critical-infrastructure-protection-in-europe;

[20] Ericsson (2019), Future mobile data usage and traffic growth, https://www.ericsson.com/en/mobility-report/future-mobile-data-usage-and-traffic-growth;

[21] Ford, N. (2015), *New German cyber security law to protect critical infrastructure,* IT Governance Ltd, https://www.itgovernance.eu/blog/en/new-german-cyber-security-law-to-protect-critical-infrastructure/;

[22] Haemmerli, B. and Renda, A. (2010), *Protecting Critical Infrastructure in the EU,* Brussels: Centre for European Policy Studies, https://www.ceps.eu/system/files/book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf;

[23] Johansson, J. (2010), *Risk and Vulnerability Analysis of Interdependent Technical Infrastructure: Addressing Socio-Technical Systems,* Lund University, Sweden;

[24] John-Koch, M. (2017), Head of Division II.3 – Critical Infrastructure Protection (CIP) Strategy, Cyber Security CIP, Federal Ministry of the Interior of the Republic of Germany (electronic correspondence of authors);

[25] Kandek, W. (2015.), Germany's approach to securing critical infrastructure - a benchmark for others?, SC Magazine, https://www.scmagazineuk.com/germanys-approach-to-securing-critical-infrastructure--a-benchmark-for-others/article/534852/;

[26] Keković, Z. 2013. National Critical Infrastructure protection regional perspective, Belgrade;

[27] Lars K. Kristian (2015) Unfolding Green Defense. Linking green technologies and strategies to current security challenges in NATO and the NATO member states. Copenhage: CENTER FOR MILITÆRE STUDIER KØBENHAVNS UNIVERSITET;

[28] Lazari, A. (2014) European Critical Infrastructure Protection. Springer International Publishing, Switzerland;

[29] Lazari, A. (2014), *European Critical Infrastructure Protection,* Springer International Publishing Switzerland;

[30] Lazari, A. and Simoncini, M. (2014), *Beyond compliance: An analysis of the experiences that maximise the implementation of the Directive 114/08/EC on European Critical Infrastructures,*International Juornal of Critical Infrastructure, https://www.dropbox.com/s/gvs5jhivvhqd3on/IJCIP-S-14-00008.pdf;

[31] Levis, G., 2006. Critical Infrastructure in Homelend Security-Defending a Net-worked National, John Wiley&Sons Inc.Hoboken, New Jersey (USA);

[32] Lopez, J., Setola, R. and Wolthusen, S. D. (2012), Overview of Critical Information Infrastructure Protection, LNCS 7130, pp. 1-14, Springer-Verlag Berlin Heidelberg;

[33] Malnar, D. and Mlinac, N. (2014), *Security-Intelligence Component for the Protection of the Critical National Energy Infrastructure of the Republic of Croatia,* University of Applied Sciences Velika Gorica: Book of Proceedings of the Seventh International Conference "Crisis Management Days", page 1007-1020, http://dku.hr/wp-content/uploads/2016/09/DKU-zbornik-radova-2014.pdf;

[34] Mark r. Chhasin and Jerod m. Loeb. High-Reliability Health CareL Getting There fromHere. TheMilbank Quarterly, Vol.91, No.3, 2013, p.459-491;

[35] Mikac R., Cesarec I.&Larkin R. 2018. Kritična infrastruktura-platforma uspješnog razvoja sigurnosti nacija. Naklada Jesenski I Turk, Zagreb;

[36] Mikac, R. (2017), *What's more, and the less important?,* Zagreb: Zaštita Journal, Number 3;

[37] Mikac, R. and Cesarec, I. (2016), *Critical Infrastructure Security and Resilience of the Republic of Croatia*, The CIP Report International Issue, August 2016, Washington: George Mason University – Center for Infrastructure Protection & Homeland Security, https://cip.gmu.

edu/2016/08/18/critical-infrastructure-security-resilience-republic-croatia/;

[38] Mikac, R. and Cesarec, I. (2019), *Current state of play of the Republic of Croatia regarding Critical infrastructure security and resilience*, accepted publication work as a chapter in a book to be published by Springer International;

[39] Милески, Т. (2014) Енергетска безбедност. Скопје: Филозофски факултет;

[40] Mitrevska M., Mikac R., 2017: Handbook on Critical Infrastructure protection, Chamber of Republic of Macedonia for Private security, Skopje, Macedonia;

[41] Monaghan, A. (2008) Energy Security: NATO's Limited, Complementary Role;

[42] Moteff J., Parfomak P., 2004. Critical infrastructure and Key Assetc: Definition and Identification, Congressional Research Service, the Library of Congress;

[43] O'Rourke, T. D. (2007), Critical infrastructure, interdependencies, and resilience, BRIDGE-Washington-National Academy of Engineering, 37(1), pp. 21-29, https://pdfs.semanticscholar.org/6c17/b35ec7555a9f27d5ccb6ca1d357a20b5ce0a.pdf;

[44] Perešin, A. and Klaić, A. (2012), The role of cyber security in critical infrastructure protection, University of Applied Sciences Velika Gorica: Book of Proceedings of the Fifth International Conference "Crisis Management Days", page 335-355, http://dku.hr/wp-content/uploads/2016/09/zbornik2012.pdf;

[45] Pokaz, I. (2013), The importance of intelligence support to critical infrastructure owners / managers, New security threats and national critical infrastructure. Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pages 279-289;

[46] Pokaz, I. and Perčić, U. (2014), Critical Infrastructure and Crisis Management, University of Applied Sciences, Book of Proceedings of the Seventh International Conference "Crisis Management Days", pages 1129-1144, http://dku.hr/wp-content/uploads/2016/09/DKU-zbornik-radova-2014.pdf;

[47] Popovski V;, 2019. Contemporary Macedonian Defence, Ministry of defence Republic of Macedonia, No.36/2019, p.61;

[48] Poustourli, Aikaterini & Kourti, Naouma. (2014). STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP) -THE CONTRIBUTION OF ERNCIP. https://www.researchgate.net/publication/304777853_STANDARDS_FOR_CRITICAL_INFRASTRUCTURE_PROTECTION_CIP_-THE_CONTRIBUTION_OF_ERNCIP (пристапено на 17.06.2019);

[49] Radoman, J. Securitization of Energy as a Prelude to Energy Security Dilemma. Western Balkans Observer, Issue: 4/2007;

[50] Roberts, K.H., 1990. Some characteristics of highreliability organizations. Organization Science, 1, 160-177;

[51] Santillan, M. (2015), Germany Introduces New Law to Strengthen Critical Infrastructure Protection, Tripwire, https://www.tripwire.com/state-of-security/latest-security-news/germany-introduces-new-law-to-strengthen-critical-infrastructure-protection/;

[52] Setola, R., Luiijf, E. and Theoharidou, M. (2016), Critical Infrastructures, Protection and Resilience, pp. 1-18, in: Managing the Complexity of Critical Infrastructures - A Modelling and Simulation Approach, Springer Open;

[53] Thomas Noonnan and Edmund Archuleta (2008) The Insider Threat to Critical Infrastructures, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf;

[54] Varwick, J. (2008) NATO's Role in Energy Security. NATO at a Crossroads. IP Summer 2008;

[55] Weick, K.E. 1990. The vulnerable system:An analysis of the Tenerife airdisaster. Journal of Management, 16/3, p.571-593;

[56] Zamorano, J. and Franco, A. (2019), Drought hits Panama Canal shipping, highlights climate fears, The Washington Post, 30 April 2019, https://www.washingtonpost.com/business/drought-hits-panama-canal-shipping-highlights-climate-fears/2019/04/30/f8dc5be0-6afc-11e9-bbe7-1c798fb80536_story.html?utm_term=.95741bb41126.

Извештаи и директиви

[1] Association of Old Crows, CACI International Inc, and the Center for Security Policy (2014), *Countering Asymmetric Threats: Cyber, Electronic Warfare and Critical Infrastructure*, Asymmetric Threat Symposium Eight, https://www.asymmetricthreat.net/pdf/symposium8_report.pdf;

[2] Aviation Law, "Official Gazette of the Republic of Macedonia", Skopje, no.63/2015;

[3] Brookings Doha Center Analysis (2016) *Risky Routes: Energy Transit in the Middle East*, https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transit-security-mills-2.pdf;

[4] Brussels Summit Declaration. 11 July 2018. www.nato.int;

[5] Bucharest Summit Declaration, NATO Press Release (2008/049) 3 April 2008. www.nato.int;

[6] Cabinet Office of the *Government of the United Kingdom* (2008), *The National Security Strategy of the United Kingdom*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf;

[7] Cabinet Office of the *Government of the United Kingdom* (2008), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61934/national_risk_register.pdf;

[8] Cabinet Office of the *Government of the United Kingdom* (2009), *The National Security Strategy of the United Kingdom*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229001/7590.pdf;

[9] Cabinet Office of the *Government of the United Kingdom* (2010), *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf;

[10] Cabinet Office of the *Government of the United Kingdom* (2010), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211853/nationalriskregister-2010.pdf;

[11] Cabinet Office of the *Government of the United Kingdom* (2012), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211858/CO_NationalRiskRegister_2012_acc.pdf;

[12] Cabinet Office of the *Government of the United Kingdom* (2013), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf;

[13] Cabinet Office of the *Government of the United Kingdom* (2015), *National Security Strategy and Strategic Defence and Security Review 2015,* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf;

[14] Cabinet Office of the *Government of the United Kingdom* (2015), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf;

[15] Cabinet Office of the *Government of the United Kingdom* (2017), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf;

[16] Canadian Security Intelligence Service (2017) *Cybersecurity and Critical Infrastructure Protection*, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php;

[17] Centre for the Protection of National Infrastructure (2017), *About CPNI*, https://www.cpni.gov.uk/about-cpni;

[18] Chicago Summit Declaration. 20 May, 2012. www.nato.int;

[19] Commitments in the field of Disaster Risk Reduction, http://www.osce.org/secretariat/123189;

[1] Communication from Commission to the Council and the European Parliament-Critical Infrastructure Protection in the fight against terrorism, 2004.

[2] Communication from the Commission on a European Programme for Critical Infrastructure Protection, 2006;

[20] Council of the European Union (2007), *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*, EUR-Lex, Official Journal, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0124;

[21] Council of the European Union (2008) *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Brussels, 2008/114/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:18:03:32008L0114:HR:PDF;

[22] Council of the European Union (2008), *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***,** Brussels, 2008/114/EC, EUR-Lex, Official Journal, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF;

[23] Council of the European Union (2008), *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*, Brussels, 2008/114/EC, EUR-Lex, Official Journal, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF;

[24] Council of the European Union 2008. *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Brussels,2008/114/EC,http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:18:03:32008L0114:HR:PDF;

[25] Croatian Parliament (2010), *Private Protection Act,* Official Gazette, number 68/2003, 31/2010, 139/2010, https://www.zakon.hr/z/291/Zakon-o-privatnoj-za%C5%A1titi;

[26] Croatian Parliament (2017a), *National Security Strategy of the Republic of Croatia,* Official Gazette, number 73/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2017_07_73_1772.html ;

[27] Croatian Parliament (2017b), *Homeland Security System Act,* Official Gazette, number 108/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_11_108_2489.html;

[28] Croatian Parliament (2018), *The Cyber Security Act of the Key Service Operators and Digital Service Providers,* Official Gazette, number 64/2018, https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html;

[29] CTED Trends Reports (2017), https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-March-2017-Final.pdf (accessed on 03.05.2019);

[3] DCSINT Handbook, 2006, Critical infrastructure threats and terrorism, Kansas, No.1.02, p. 1;

[30] Defense Strategy of the Republic of Macedonia, "Official Gazette of the Republic of Macedonia", 30/2010. p.6 http://www.slvesnik.com.mk/Issues/2EDC3A5EF4DD1747A803A4D1FF418F11.pdf (accessed on 20.06.2019);

[31] Department of Defense (1998), *Critical Infrastructure Protection Plan*, https://fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm;

[32] Department of Homeland Security (2003), *Homeland Security Presidential Directive 7,* Washington, D.C., https://www.dhs.gov/homeland-security-presidential-directive-7#;

[33] Department of Homeland Security (2013), *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf;

[34] Department of Homeland Security (2015a), *Energy Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf;

[35] Department of Homeland Security (2015b), *Communications Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf;

[36] Department of Homeland Security (2015c), *Transportation Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf;

[37] Department of Homeland Security (2015d), *Water and wastewater Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf;

[38] Department of Homeland Security (2015e), Critical Infrastructure Cross Sector Council Charter, Washington, D.C., https://www.dhs.gov/sites/default/files/publications/cipac-cross-sector-council-charter-2015-508.pdf;

[39] Department of Homeland Security (2017a), *National Infrastructure Advisory Council, Future Focus Study: Strengthening the NIAC Study Process*, https://www.dhs.gov/sites/default/files/publications/niac-future-focus-study-strengthening-the-niac-study-process-final-508.PDF;

[40] Department of Homeland Security (2017b), *2017 National Preparedness Report,* Washington, D.C., https://www.fema.gov/media-library/assets/documents/134253;

[41] Department of Homeland Security (2019), *Homeland Security Presidential Directive 21,* https://www.dhs.gov/homeland-security-presidential-directive-21#;

[42] European Commission (2002), *Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection*, https://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf;

[43] European Commission (2004), *Communication on Critical Infrastructure Protection in the fight against terrorism,* EUR-Lex, Official Journal, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702;

[44] European Commission (2005), Green Paper on a European Programme for Critical Infrastructure Protection, EUR-Lex, Official Journal, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576;

[45] European Commission (2006), European Programme for Critical Infrastructure Protection, EUR-Lex, Official Journal, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786;

[46] European Commission (2013), *Commission staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*, EUR-Lex, Official Journal, https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf;

[47] European Commission (2014) *ECHO Factsheet – Disaster RiskManagement – 2014,*http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf, p.1;

[48] European Commission (2014) The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience, http://ec.europa.eu/echo/files/news/post_hyogo_managing_risks_en.pdf;

[49] European Commission (2017), *Commission staff working document on assessment of the EU 2013 Cybersecurity Strategy*, EUR-Lex, Official Journal, http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF;

[50] European Commission (2019), Cybersecurity, https://ec.europa.eu/digital-single-market/en/cyber-security;

[51] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EUR-Lex, Official Journal, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf;

[52] European Environment Agency (2011) *Mapping the impacts of natural hazards and technological accidents in Europe* (Technical report No 13/2010), http://www.eea.europa.eu/publications/mapping-the-impacts-ofnatural/at_download/file;

[53] European Parliament and of the Council of the European Union (2016), *Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union,* EUR-Lex, Official Journal, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN;

[4] European Union Council Directive 2008, On the identification and designation of European Critical I nfrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23/12/2008;

[54] Federal Ministry of the Interior (2007), Critical Infrastructure Protection Implementation Plan, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile;

[55] Federal Ministry of the Interior (2008), Protection of Critical Infrastructures Baseline Protection Concept, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/Baseline%20Protection%20Concept.pdf?__blob=publicationFile;

[56] Federal Ministry of the Interior (2009), National Strategy for Critical Infrastructure Protection, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile;

[57] Federal Ministry of the Interior (2011a), *Cyber Security Strategy for Germany,* Federal Republic of Germany, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/cyber%20security%20strategy.pdf?__blob=publicationFile;

[58] Federal Ministry of the Interior (2011b), *National Plan for Information Infrastructure Protection,* Federal Republic of Germany, http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf;

[59] Federal Ministry of the Interior (2016), *Cyber-Sicherheitsstrategie für Deutschland,* https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Cyber_Sicherheitsstrategie2016.pdf?__blob=publicationFile;

[5] FOCUS D5, 2012, Problem space report: Critical Infrastructure&Supply Chain Protection, Cross Border Research Association (CBRA);

[60] Government of the Republic of Croatia (2008), *National Strategy for the Prevention and Suppression of Terrorism,* Official Gazette, number 138/2008, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_139_3896.html;

[61] Government of the Republic of Croatia (2009) Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća;

[62] Government of the Republic of Croatia (2010), *Protection and Rescue Plan for the Republic of Croatia,* Official Gazette, number 96/2010, https://narodne-novine.nn.hr/clanci/sluzbeni/2010_08_96_2707.html;

[63] Government of the Republic of Croatia (2013a), *Critical Infrastructure Act,* Official Gazette, number 56/13, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html;

[64] Government of the Republic of Croatia (2013b), *Risk Assessment for Republic of Croatia from Natural and Technical – Technological Disasters and Major Accidents,* http://stari.duzs.hr/download.aspx?f=dokumenti/Clanci/PROCJENA_web_20.03.2013..pdf;

[65] Government of the Republic of Croatia (2013c), *The National Strategy and Action plan for the* Non-Proliferation of Weapons of Mass Destruction, https://vlada.gov.hr/UserDocsImages//Sjednice/Arhiva//71.%20-%206.pdf;

[66] Government of the Republic of Croatia (2013d), Decision on Designation the Sectors from which the Central State Administrative Bodies Identify National Critical Infrastructure and Lists of the Order of the Sectors of Critical Infrastructures, Official Gazette, number 108/2013, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html;

[67] Government of the Republic of Croatia (2014), *Statement from the closed part of the 140th session of the Government of the Republic of Croatia,* published on 6th February 2014, https://vlada.gov.hr/vijesti/priopcenje-sa-zatvorenog-dijela-140-sjednice-vlade-republike-hrvatske/14530;

[68] Government of the Republic of Croatia (2015a), *National Cyber Security Strategy,* Official Gazette, number 108/2015, https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html;

[69] Government of the Republic of Croatia (2015b), *National Strategy for the Prevention and Suppression of Terrorism,* Official Gazette, number 108/2015, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2015_10_108_2105.html;

[6] Green Paper on a European Programme for critical infrastructure protection, 2005, Brussels, Annex II;

[70] Home Office of the *Government of the United Kingdom* (2009), *National Counterterrorism Strategy*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf;

[71] Home Office of the Government of the United Kingdom (2011), The United Kingdom's Strategy for Countering Terrorism, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf;

[72] Joint Research Centre of the European Commission (2008), *Non-Binding Guidelines for application of the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection,* http://publications.jrc.ec.europa.eu/repository/bitstream/JRC48985/guidelines%20document%20final.pdf;

[73] Joint Research Centre of the European Commission (2017), *The ERNCIP Project Platform,* https://erncip-project.jrc.ec.europa.eu/;

[74] Law on Crisis Management, 2005. "Official Gazette of the Republic of Macedonia", 29/2005. http://www.macefdrr.gov.mk/files/dokumenti/pzrdo/Zakon%20za%20upravuvanje%20so%20krizi%202005.pdf (accessed on 21.06.2019);

[75] Law on Energy, 2018, "Official Gazette of the Republic of Macedonia", Skopje, no.96 from 28.5.2018 http://www.erc.org.mk/odluki/2%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%B7%D0%B0%20%D0%B5%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D0%BA%D0%B0_96_18.pdf (accessed on 21.06.2019);

[76] Law on Protection and Rescue, "Official Gazette of the Republic of Macedonia", 93/2012. http://www.slvesnik.com.mk/Issues/1F2D347B699C764F9E65C717889E74B2.pdf (accessed on 21.06.2019);

[77] Lisbon Summit Declaration. 20 November, 2010. www.nato.int;

[78] Military Doctrine of the Russian Federation. https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf (accessed on 10.06,2019);

[7] National Guidelines for Protection Critical infrastrukture from terrorism, 2011;

[79] National Institute of Standards and Technology (2018), *Framework for Improving Critical Infrastructure Cybersecurity,* Washington, D.C., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf;

[80] National Protection and Rescue Directorate (2013), *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure,* Official Gazette, number 128/2013, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_10_128_2792.html;

[81] National Protection and Rescue Directorate (2016), *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure*, Official Gazette, number 47/2016, https://narodne-novine.nn.hr/clanci/sluzbeni/2016_05_47_1221.html;

[82] National Protection and Rescue Directorate (2017), *Amendments to the Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure,* Official Gazette, number 93/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_09_93_2167.html;

[83] National Stategy for Cyber Security of the Republic of Macedonia 2018-2022. http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf (accessed on 26.06.2019);

[84] National Strategy for Critical Infrastructure Protection (CIP Strategy) of Federal Republic of Germany, 2013;

[85] NATO ENSEC COE. https://enseccoe.org/en/ (accessed on 10.06.2019);

[86] NRDC.org (2018), *Flint Water Crisis: Everything You Need to Know*, https://www.nrdc.org/stories/flint-water-crisis-everything-you-need-know;\

[8] Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012: 1-2-3;

[9] Patriot Act, 2001.

[87] Prague Summit Declaration (2002); https://www.nato.int/cps/en/natohq/official_texts_19552.htm (accessed on 23.04.2019);

[88] Research Division - NATO Defense College, Rome - No. 36 – May 2008;

[89] Review of the implementation of OSCE Commitments in the field of Disaster Risk Reduction, http://www.osce.org/secretariat/123189, p.20;

[90] Riga Summit Declaration http://www.nato.int;

[91] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. p.p 11-17. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (accessed on 05.04.2019);

[92] Strategic Concept For the Defence and Security of The Members of the North Atlantic

[93] Swedish Civil Contingencies Agency (2011), *A functioning society in a changing world: The MSB's report on a unified national strategy for the protection of vital societal functions,* https://www.msb.se/RibData/Filer/pdf/26084.pdf;

[94] Swedish Civil Contingencies Agency (2014), *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure,* https://www.msb.se/RibData/Filer/pdf/27412.pdf;

[95] Swedish Civil Contingencies Agency (2016), *Protection of vital societal functions & critical infrastructure,* https://www.msb.se/RibData/Filer/pdf/27956.pdf;

[96] Swedish Civil Contingencies Agency (2019), About MSB, https://www.msb.se/en/About-MSB/;

[97] The Alliance's New Strategic Concept https://www.nato.int/cps/en/natohq/official_texts_23847.htm (accessed on 02.04.2019);

[98] The Alliance's Strategic Concept https://www.nato.int/cps/en/natohq/official_texts_27433.htm?mode=pressrelease;

[99] The North Atlantic Treaty. https://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed on 10.06.2019);

[100] United Nations Development Programme (2014) *Review of the implementation of OSCE Commitments in the field of Disaster Risk Reduction*, http://www.osce.org/secretariat/123189, p.8;

[101] United Nations Development Programme (2014) Review of the implementation of OSCE;

[102] United Nations Security Council (2016) *Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/92;

[103] United Nations Security Council Counter-Terrorism Committee (2017) Physical Protection of Critical Infrastructure against Terrorist Attacks, https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf;

[104] United States Government Accountability Office (2009), *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts by Sectors' Characteristics*, GAO-07-39, Washington, D.C., https://www.hsdl.org/?view&did=469089;

[105] United States Government Accountability Office (2017), *Critical Infrastructure Protection: DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning, GAO-18-62,* Report to Congressional Requesters, October 2017, https://www.gao.gov/assets/690/688879.pdf;

[106] Wales Summit Declaration, 05 September 2014. www.nato.int;

[107] Warsaw Summit Communiqué. 09 July 2016. www.nato.int;

[108] White House (1996), *Executive Order 13010 Critical Infrastructure Protection,* Washington, D.C., https://fas.org/irp/offdocs/eo13010.htm;

[109] White House (1998), *Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998.* Washington, D.C., https://fas.org/irp/offdocs/pdd/pdd-63.pdf;

[110] White House (2013), *Presidential Policy Directive 21 / PPD-21 Critical Infrastructure Security and Resilience,* Washington, D.C., https://fas.org/irp/offdocs/ppd/ppd-21.pdf;

[111] White House (2017), *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/;

Индекс

За авторите

Марина Митревска е редовен професор на Институтот за безбедност, одбрана и мир при Филозофскиот факултет, Универзитет „Св.Кирил и Методиј" во Скопје, Република Северна Македонија. Раководител е на трет циклус докторски студии по безбедност, одбрана и мир. Член е на Одборот за акредитација и евалуација на високото образование во Република Северна Македонија. Главен и одговорен уредник е на меѓународното научно списание „Современа македонска одбрана". Научно-истражувачко подрачје е безбедност, дипломатија, мировни операции и кризен менаџмент. Интензивно се занимава со истражување и објавување на научно-стручни написи и книги и тоа од областа на безбедност. Автор е на единаесет книги и повеќе од сто научни труда.

E-mail: marinamitrevska@yahoo.com

Тони Милески е редовен професор и истражувач во областа на политичката географија и геополитика, еколошката безбедност, енергетската безбедност и миграциите и конфликтите. Вработен е на Универзитетот „Св. Кирил и Методиј", Филозофски факултет – Институт за безбедност, одбрана и мир. Професорот Милески учествувал во повеќе научни и истражувачки проекти. Во октомври 2012 година, бил дел од меѓународната програма за лидерство, организирана од Амбасадата на САД, Програма што се одржала во Вашингтон, Њујорк и Бостон, САД. Тој е втора година, последователно, програмски координатор на два научно-истражувачки проекти изработени заедно со Брандербуршкиот технолошки универзитет во Котбус - Германија и Фондацијата DAAD. Тој е автор на шест книги, неколку поглавја во книги и повеќе од осумдесет научни трудови.

E-mail: toni@fzf.ukim.edu.mk

Роберт Микац е доцент на Факултетот за политички науки на Универзитетот во Загреб од областа на општествените науки, во полето на политичките науки, со под-области меѓународни односи и националната безбедност. Области од неговиот интерес и стручност се: меѓународни односи; меѓународна и национална безбедност; управување со безбедност; управување со кризи и катастрофи; цивилна заштита; Авганистан; приватизација на безбедноста, заштита на критична инфраструктура и еластичност; миграции и безбедност. До денес има издадено три книги (првата за Авганистан, втората за приватизација на безбедноста и третата за заштита на критичната инфраструктура) и околу четириесет научни и стручни трудови. На претходното работно место во Дирекцијата за национална заштита и спасување беше надлежен за работи поврзани со критична инфраструктура, а од 2012 до 2015 година е национален координатор за критична инфраструктура.

E-mail: robert.mikac@yahoo.com

Ричард Ларкин е поранешен директор за управување со вонредни состојби во градот Сент Пол, Минесота, САД. Тој има над 30 години искуство во јавната безбедност како итен медицински техничар/болничар, пожарникар и експерт за управување со итни случаи во шеснаесеттото по големина градско подрачје во САД. Вклучен е во активности за преглед и поддршка на програмата за управување со итни случаи (цивилна заштита/управување со кризи) во Хонг Конг, Народна Република Кина; Перу, Република Хрватска и во три од британските прекуокеански територии на Карибите. Негови области од интерес и стручност се: управување со итни случаи и администрација на програмата за државна безбедност, управување со кризи и катастрофи; цивилна заштита; заштита на критичната инфраструктурата и еластичност; национални стандарди и акредитација на програми за управување со итни случаи и континуитет на деловно работење, планирање на итни случаи и подготвеност, управување со инциденти и одговор на итни случаи. Тој е член на Меѓународниот институт за безбедносна политика и поранешен претседател на Меѓународната организација за развој на стандарди за управување со вонредни состојби (EMAP). Тој, исто така, е автор на три рецензирани учебници за заштита на критичната инфраструктура и еластичност.

E-mail: rjlarkin103@gmail.com

Метју Ватер е пензиониран висок армиски офицер од Националната гарда на Минесота. За време на службувањето во Националната гарда на Минесота, тој имал бројни лидерски позиции, меѓу кои и како директор за стратешки планови и политика. Тој ја предводеше програмата за операции на вонредни состојби на Националната гарда, која се фокусираше на воената поддршка на цивилните власти за време на националните вонредни состојби и националните катастрофи. Неговиот тим ги напиша и ги спроведе плановите што обезбедуваат воени ресурси за цивилните власти и воспостави команден орган и развој на односите помеѓу локалните, државните и племенските агенции за одговор при итни случаи. Тој ја надгледуваше програмата за државно партнерство со Хрватска и помагаше во развојот на разни национални програми за безбедност и политики за вклучување во одговор на кризи, заштита на критичната инфраструктура и обука за компјутерска одбрана, заедно со традиционалната воена меѓусебна операбилност. Дипломирал на Воениот колеџ на американската армија и универзитетите во Минесота и Висконсин. Тој завршил додипломски студии за наука за земјата и е магитер по статегија и безбедносни технологии. Тој е коавтор на академски текстови за заштита на критичната инфраструктурата и на научни трудови за енергетска еластичност. Тој во моментов работи во државата Минесота како помошник комесар за Одделот за трговија каде води тим од 58 агенти за потрошувачки услуги и професионални истражители. Тој честопати држи предавања за компјутерска безбедност за мали бизниси и за заедничка одговорност на владата и приватниот сектор за безбедност и еластичност.

E-mail: mattvatter@gmail.com

Professor Roberto Setola

Univertsita Capmus Bio-Medico di Roma, Italy

После 25 години од формирањето на американската Комисија за заштита на критичната инфраструктура, формирана при претседателот на 15 јули, 1996 година, вниманието се свртува кон заштитата на критичната инфраструктура, а оваа книга дава преглед на различните иницијативи промовирани на национално и меѓународно ниво за да се подобри стабилноста, еластичноста и способноста за континуитетот на услугите на ваквите витални системи. Книгата му овозможува на читателот да ја долови комплексноста на овој конкретен проблем, нагласувајќи ја од една страна потребата за посилна координација и споделување информации помеѓу различните заинтересирани страни и власти, а од друга страна го нагласува присуството на „иновативна“ димензија на безбедноста каде природните настани и нападите предизвикани од човекот треба да се управуваат во една холистичка рамка. Ваквата перспектива за сите опасности е основата на современиот концепт на заштитата на критичната инфраструктура.

Associate Professor Jonas Johansson

Director of Centre for Critical Infrastructure Protection Research, Lund University, Sweden

Ова е книга која е зрела и изобилува со важни поенти и научени лекции при поставувањето и имплементирањето на национални системи за заштита на критичната инфраструктура, засновани на сеопфатен преглед на историјата на заштитата на критичната инфраструктура и клучни насоки за иднината од аспект на ЕУ, НАТО, САД и, со посебен акцент, на перспективата на балканските земји. Таа ги доловува и ги отсликува предизвиците од мултидисциплинарна перспектива, но сепак останува заснована во својата перспектива на политиките. Важноста на сигурноста, безбедноста и еластичноста на нашите динамични и развојни критични инфраструктури ќе станува сè повеќе нагласена во иднина, а нивната меѓусебна поврзаност повикува на меѓусекторска политика и соработка на највисоко ниво.