МАРИНА МИТРЕВСКА, РОБЕРТ МИКАЦ

ПРИРАЧНИК
ЗА ОБЕЗБЕДУВАЊЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

проф. д-р. Марина Митревска,
доц. д-р. Роберт Микац

ПРИРАЧНИК
ЗА ОБЕЗБЕДУВАЊЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Резензент:
Проф. д-р *Зоран* КЕКОВИЌ

Издавач:
КОМОРА НА РЕПУБЛИКА МАКЕДОНИЈА
ЗА ПРИВАТНО ОБЕЗБЕДУВАЊЕ
ул. „50-та дивизија“, бр.34
1000 Скопје, Република Македонија
www.obezbeduvanje.org.mk
info@obezbeduvanje.org.mk

За издавачот:
м-р *Верица* МИЛЕСКА СТЕФАНОВСКА,
претседател
на Комората на Република Македонија за приватно обезбедување

Јазична редакција:
Жанет РИСТОСКА

Корица:
Александар АТАНАСОВ

Компјутерска подготовка:
Александар АТАНАСОВ

Тираж:
300 примероци

Печати:
„Попе Компани“ ДОО, Скопје

МАРИНА МИТРЕВСКА

РОБЕРТ МИКАЦ

ПРИРАЧНИК
ЗА ОБЕЗБЕДУВАЊЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Скопје, 2017

КОМОРА НА РЕПУБЛИКА МАКЕДОНИЈА
ЗА ПРИВАТНО ОБЕЗБЕДУВАЊЕ
ул. „50-та дивизија“, бр.34
1000 Скопје, Република Македонија
www.obezbeduvanje.org.mk
info@obezbeduvanje.org.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека «Св. Климент Охридски», Скопје
355.45(035)

МИТРЕВСКА, Марина
Прирачник за обезбедување на критичната инфраструктура / Марина Митревска, Роберт Микац. - Скопје : Комора на Република Македонија за приватно обезбедување, 2017. - 63, 55 стр. ; 25 см

Насловна страна на припечатениот текст: Handbook on critical infrastructure protection / Marina Mitrevska, Robert Mikac. - Обата текста меѓусебно печатени во спротивни насоки. - Текст на мак. и англ. јазик. - Фусноти кон текстот. - Библиографија: стр. 55-59 ; Bibliography: стр. 50-54

ISBN 978-608-65990-5-8
1. Микац, Роберт [автор]
а) Критична инфраструктура - Државна безбедност - Прирачници
COBISS.MK-ID 103781898

СОДРЖИНА

ПРЕДГОВОР

Поаѓајќи од концептот за критична инфраструктура како воопштен збир на вредности и добра кои се од суштествено 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, јасно е препознатлива потребата од градење на координиран пристап при креирање на современ концепт за заштита на критичната инфраструктура. Дотолку повеќе таа треба да претставува врвен приоритет за институциите на системот, но и за сите засегнати страни во општеството.

Комората на Република Македонија за приватно обезбедување како клучен предизвик во тенденцијата за континуирано унапредување на секторот приватно обезбедување ја има препознаено заштитата, односно обезбедувањето на критичната инфраструктура и истата доследно ја има вградено во развојната визија за дејноста.

Преку претходно утврдени конкретни мерки и насоки за идни вложувања на капацитети и ресурси, токму обезбедувањето на критичната инфраструктура претставува една од идентификуваните стратегиски цели за развој на дејноста приватно обезбедување во Република Македонија. Нашиот систематски пристап вклучува примарно содавање на предуслови за надградување на легислативната рамка за обезбедување на критичната инфраструктура и втора фаза, креирање на практични решенија како директен одговор на потребите.

Имено, Комората на Република Македонија за приватно обезбедување практикува конзистентна практика на континуирано унапредување, преку надградба на знаењата, вештините и компетенциите, така што портфолиото на стручни обуки и семинари вбројува повеќекратни активности во сферата на обезбедувањето на критичната инфраструктура. Додадена вредност претставува издавачката активност на Комората, манифестирајќи ја определбата дека за професионалното надградување е неопходна стручна литература, наменета за непосредните вршители на дејноста.

Во контекст на сето изложено, овој прирачник ја илустрира посветеноста на Комората на Република Македонија за приватно обезбедување за натамошно вложување во обезбедувањето на критичната инфраструктура. Истовремено, прирачникот претставува реализација на потребите на непосредните вршители на дејноста, чија развиена свест отворено побарува практични механизми за подобрување на работењето, во функција на поголема професионализација и темелна гаранција за општата безбедност на граѓаните.

Искрено се надеваме дека содржините претставени во овој прирачник ќе ги задоволат апетитите на вршителите на приватното обезбедување, но воедно искрено очекуваме дека оваа публикација ќе претставува и провокација за анимирање на интересите на сите партиципиенти во процесот на обезбедување на критичната инфраструктура во Република Македонија, па и пошироко, заради фактот што само со препознавање и прифаќање на општата одговорност, директно вклучување, соработка и заедничко дејствување може да се гарантира општата безбедност на глобално ниво.

Претседател
м-р Верица Милеска Стефановска

ВОВЕД

Критичната инфраструктура претставува поим и концепт кој често се користи во современиот свет. Додека пак, потребата да се обезбедат виталните функции на државата го одредува значењето на критичност на одредена инфраструктура. Во тој контекст треба да се потенцира дека „критичната инфраструктура“ опфаќа ресурси кои се неопходни за функционирање на општествата, и тоа: енергетски капацитети, информатичка и комуникациска технологија, вода, транспорт и улогата на приватниот сектор.

Предизвиците за заштита на критичната инфраструктура се бројни. За оние земји кои само што започнуваат со формирањето на концептот на заштита на критичната инфраструктура, предизвиците се манифестираат во разбирање на нејзината важност, развивање на нормативната рамка, идентификација, означување на секторот и индивидуалната критична инфраструктура, воспоставување соодветни и квалитетни мерки за заштита. Во Југоисточна Европа, посебно во земјите кои го поминаа процесот на распаѓање на Југославија и сè уште не се дел од ЕУ и НАТО, а сè уште се борат и со други приоритети, концептуалното и нормативното поле на заштита на критичната инфраструктура е сè уште неразвиено. Во тие услови, како легитимно прашање и предуслов за успешно остварување на безбедноста, обезбедувањето на критичната инфраструктура треба да стане дел и од агендата на Република Македонија. За таа цел, во рамките на Прирачникот се нуди анализа на клучните аспекти на критичната инфраструктура, која треба да послужи на Република Македонија во процесот на формирање на концептот за заштита на критичната инфраструктура.

Проблематиката за обезбедување на критичната инфраструктура во Прирачникот е систематизирана во седум дела.

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 соработката 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 проценка на потребата да се подобри нивната заштита.

Во рамките на **Т**ретиот дел „ Критични инфраструктурни објекти и функции од посебен интерес" акцентот е ставен на анализа на различните пристапи кон зајакнување на отпорот и заштита на критичната инфраструктура. Овој дел на аналитичко сондирање на критични инфраструктурни објекти и функции од посебен интерес е посветен на анализата на енергетскиот сектор, транспортниот сектор, информацискатa и комуникацискатa технологија, водата и местото и улогата на приватниот сектор.

Во рамките на Четвртиот дел ***„Ризици и закани за критичната инфраструктура"*** акцентот е ставен на анализа на природните закани и ризици за критичната инфраструктура. Во него е содржана и анализа на техничко-технолошките опасности и антропогените закани и ризици по критичната инфраструктура.

Во рамките на Петтиот дел „Обезбедување на критичната инфраструктура" се разработени четири клучни прашања. Најнапред се анализира организацијата на заштитата

на критичната инфраструктура. Второто прашање опфаќа анализа на институциите кои се компетентни за заштита на критичната инфраструктура. Во следното прашање акцентот е ставен на заштитата на критичната инфраструктура, односно јавно-приватното партнерство. Последното прашање претставува преглед на неколку програми и процедури за работа.

Шестиот дел „Заштита на критичната инфраструктура во Република Македонија" е посветен на анализа на заштитата и обезбедување на критичната инфраструктура во Република Македонија.

Во Седмиот дел „Примери за досегашни терористички напади врз критична инфраструктура" вниманието е посветено на примери за досегашни терористички напади врз критичната инфраструктура. Во него е содржана анализа на терористичките напади во САД, во Мадрид и во Лондон.

1 ГЛАВА ПОИМНО ОПРЕДЕЛУВАЊЕ НА ТЕРМИНОТ КРИТИЧНА ИНФРАСТРУКТУРА

1. УТВРДУВАЊЕ НА ИНФРАСТРУКТУРА ЗА КРИТИЧНА

Поимот „критична инфраструктура“ не е универзално дефиниран. Потребата да се обезбедат виталните функции на државата го одредува значењето на критичност на одредена инфраструктура. Се смета дека поимот „критична инфраструктура“ датира уште од средината на деведесеттите години и е тесно поврзан со енергетската безбедност, телекомуникациите, енергетските системи, гасоводите и нафтоводите, економијата, транспортот, водоводот и сл.[1] 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.[2] 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.[3] 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. Високата меѓузависност на овие системи со останатите системи од социјалниот живот, налага потреба да се обрне поголемо внимание на нивната заштита.[4] Да разгледаме некои од нив.

1. Во САД, критичната инфраструктура се определува како „системи и средства, физички или виртуелни, витални за значењето на една држава каде што нивното онеспособување или уништување ќе има негативен ефект врз националната, економската и социеталната безбедност“. [5]
2. 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.[6]
3. Во Германија, под поимот „критична инфраструктура се подразбира организациската структура и објектите од витално значење за општеството, така што нивната деградација

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

[2] Commision of the EU,(2004), p. 4

[3] Levis, G., (2006), Critical Infrastructure in Homelend Security-Defending a Net-worked National, John Wiley&Sons Inc.Hoboken, New Jersey (USA), p.1

[4] Keković, Z., (2013), National Critical Infrastructure protection regional perspective, Belgrade, p.203

[5] Patriot Act, 2001

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

или дефицит ќе резултира со недостатоци, ќе предизвика значително намалување во снабдувањето, нарушување на јавниот ред или други последици“. [7]

4. 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“. [8]
5. 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. [9]
6. 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. [10]
7. Во ЕУ, критичната инфраструктура се дефинира како „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“. [11]

Имајќи го предвид досега кажаното, може да се констатира дека сè уште не постои универзално прифатена дефиниција за поимот критична инфраструктура. Анализата покажува дека при дефинирањето постојат мали разлики и тоа кога се работи за земји-членки на НАТО или пак, земји-членки на ЕУ. Од тие причини, ќе се обидеме да извлечеме неколку заеднички елементи, и тоа:

Првиот елемент се однесува на фактот дека критичната инфраструктура претставува систем, средства, имот, услуги и сл., кои се клучни за нормално функционирање на државата во поглед на економските, здравствените, социјалните и безбедносните потреби.

Вториот елемент се однесува на фактот дека 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.

Третиот елемент произлегува од потребата за контролирање и развивање на критичните инфраструктури. Притоа, акцентот се става на целта да се промовира институционален пристап. Конкретно, пристапот треба да биде насочен кон креирање на стратегиска рамка за критичната инфраструктура.

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

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

[9] Исто.

[10] Bognar, B., (2009), The process of critical infrastructure protection, AARMS, Budapest, p.552

[11] 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.

2. ЗАКАНИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

Заканите за критичната инфраструктура, за разлика од минатото, денес се проширија во многу сектори, и тоа:

- во економијата (со посебен акцент на банкарството и финансиите);
- во транспортот (аеродромите и железниците) и во дистрибуцијата;
- во енергетиката;
- во здравството;
- во комуникациите;
- во комуналните услуги;
- во снабдувањето со храна;
- во владините услуги и др.

Оттука, не е лесно да се констатира дека некои од критичните елементи во наведените сектори не се конкретно „инфраструктура“, туку се мрежа или пак, снабдувачки синџири, поврзани со суштински производи или услуги. Ова го поткрепува и фактот дека се зголемуваат факторите кои им се закануваат на различни елементи од инфраструктурата.

Заканите врз критичната инфраструктура можат да бидат поделени во неколку групи и подгрупи, и тоа:

- вештачки;
- природни; и
- закани од технолошка природа. [12]

Во вештачки или организирани акции со штетни намери спаѓаат: тероризам, злоупотреба за политичка корист, злоупотреба за економска корист, поттикнување на вооружени конфликти, немири и протести.

Додека пак, во закани од природни сили спаѓаат: поплави, пожари, земјотреси, лизгање на земјиштето и сл.

Заканите од технолошка природа можат да бидат предизвикани од знаење или незнаење, намерно или ненамерно 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. [13]

Во теоријата се застапени повеќе методологии кои директно помагаат во идентификацијата на посебните закани, и тоа:

- идентификација на основната инфраструктура;
- евалуација на заканите;
- евалуација на загрозувањето на критичната инфраструктура;
- процена на ризикот.[14]

[12] Bognar, B., (2009), The process of critical infrastructure protection, AARMS, Budapest, p.500

[13] Bognar, B., (2009), The process of critical infrastructure protection, AARMS, Budapest, p.500

[14] Marjanović, M. and Nađ, I. (2013) National critical infrastructure protection –regional perspective: Assesment of threats to critical infrastructure facilities from serious and organized crime, Belgrade, p.78-79

3. ПОТРЕБА ОД ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Потребата од заштита на критичната инфраструктура, во основа, произлегува од процесот на глобализацијата и експанзијата на тероризмот. Ваквата состојба и потреба укажуваат на тоа дека: прво, постои директна врска помеѓу заканата од тероризмот и заштитата на критичната инфраструктура; второ, постои потреба секоја држава да има систематизиран пристап кон постојната инфраструктура; трето, потребно е инфраструктурата да се дефинира како критична, заради можноста да биде потенцијална цел и тоа подеднакво од трите вида закани.

Во таа насока, се наметнува потребата за една соодветна анализа на потребата од заштита на критичната инфраструктура. Всушност, изборот нема за цел поединечната анализа да биде обемна, ниту пак неминовно репрезентативна, туку изборот е направен:

- ❖ од аспект на меѓународниот статус, каде што ЕУ значи најатрактивен, релативно нов, економски, политички и безбедносен актер и меѓународен феномен;
- ❖ од аспект на меѓународниот систем, каде што НАТО значи политичка рамка за еден меѓународен сојуз моделиран да спречи агресија или да ја одврати истата, или помош во случај на катастрофи и несреќи од поширок размери.

Затоа, основна задача на оваа анализа е преку пример како ЕУ и една земја-членка на НАТО ја регулираат заштитата на критичната инфраструктура.

ЕУ својата безбедност ја насочува кон земјите-членки, но и кон соседите бидејќи негативните последици од уништување или онеспособување на критичната инфраструктура може да бидат заемни и од тие причини потребно е да се постигне стандардизирано ниво на безбедност на критичните инфраструктури кои ќе го минимизираат ризикот од дестабилизирање на нормалните функции на државите-членки на Унијата. Генерално гледано, тоа се остварува преку соработка во различни форми и концепти на надворешната соработка на примарно фокусирано ниво, поради глобалната поврзаност на одредени сектори, кои бараат поразличен пристап, дијалог и размена на најдобрите практики.[15]

Додека пак, САД како водечка земја-членка на НАТО, потребата од заштита на критичната инфраструктура ја регулираат преку интегрален пристап, и тоа:

- преку идентификување, спречување и подготовка за справување со заканите врз критичната инфраструктура;
- преку намалување на ранливоста на критичната инфраструктура;
- преку ублажување на последиците врз критичната инфраструктура.[16]

Во таа насока, посебно место има и Директивата на САД за заштита на критичната инфраструктура, затоа што ги идентификува енергетиката и комуникациските системи како значајни критични инфраструктури. Овде, пред сè, се работи за поврзаноста со функциите кои се обезбедуваат во рамките на сите критични сектори.[17] Оттука, пристапот на САД се води низ три стратегиски императиви, и тоа:

Прво, јасни функционални односи, со цел унапредување на националното единство и

[15] Алчевски, 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), Скопје, стр.36-37

[16] National Infrastructure Protection Plan (NIPP), (2013) Partnering for Critical Infrastructure Security and Resilience, Homeland security, USA, p.7

[17] Presidentiali Policy Directive, (2013) Critical Infrastructure Security and Resilience The White House Office of the Press Secretary , USA.

зајакнување на безбедноста на критичната инфраструктура.

Второ, создавање на услови за ефикасна размена на информации.

Трето, имплементација и интеграција на анализите од досегашните операции поврзани со заштитата на критичната инфраструктура, во интерес на квалитетни одлуки.[18]

Без оглед на мотивите за различните ставови во однос на заканите врз критичната инфраструктура, ЕУ и САД успеаја да формираат заедничко определување на две нивоа со кои се дефинира:

- кои ресурси претставуваат критична инфраструктура; и
- кои мерки се потребни за нивна заштита.[19]

На ова треба да се надоврзе и фактот дека за заштита на критичната инфраструктура се потребни и значителни човечки потенцијали. Токму оттаму произлегува и потребата од надминување на многу предизвици, од кои би ги издвоиле:

- 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;
- меѓузависноста на секторите од критичната инфраструктура и др.[20]

Затоа, паралелно со определување на стратегиските императиви, неопходно е да се обезбеди и добра процена на заканите, на ранливоста 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.

4. ИНДИКАТИВНА ЛИСТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Во рамките на ЕУ и на повеќето држави-членки на НАТО 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.[21] Додека пак, во рамките на земјите-членки на НАТО, Индикативната листа ги вклучува, и тоа:

- во Германија: 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.;

[18] Presidentiali Policy Directive, (2013) Critical Infrastructure Security and Resilience The White House Office of the Press Secretary , USA.

[19] Škero, M., Zaštita kritične infrastructure I osnovni elementi uskladivanja sa direktivom Saveta Evrope 2008/114/ES

[20] Prezelj., I., (2008) Konceptualna opredelitev kritične infrastructure, Fakultet društvene vede, Ljubljana, p.13

[21] Green paper on a European Programme for critical infrastructure protection, (2005), Brussels, Annex II

- во Велика Британија: енергијата, телекомуникациите, владините институции, здравството, финансиите, транспортот, итните служби, водата и одводните системи и др.;
- во САД: енергијата, информациите, телекомуникациите, јавното здравство, храната, водата, финансиите, итната помош, владините институции, основната одбранбена индустрија, хемиската индустрија и опасните материи и др.[22]

Анализата покажува дека сите пристапи се исти или слични, разликата е само во надополнувањето со одделни специфични сектори.

[22] Види пошироко, Алчевски., Ѓ., (2016), стр.40-41

2 ГЛАВА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО ЕВРОПСКАТА УНИЈА

Доменот на заштита на критичната инфраструктура во Европската унија се развиваше во неколку различни паралелни процеси. Постојат две главни насоки: првата е одбележана со индивидуален развој на овој домен, односно индивидуално, од земјите членки, без контакт и координација со Европската унија, а другата насока се базира на политиките и процесите кои Унијата ги има иницирано и истите се труди да ги координира. Првата насока има подолга временска рамка и земјите како Велика Британија, Шведска, Швајцарија, Холандија, Германија и Франција почнаа да ја развиваат главно во последната четвртина од XX век, обидувајќи се да ја зајакнат сопствената структура од која зависи нивното функционирање. Европската унија почна институционално да се занимава со критичната инфраструктура на почетокот на XXI век, под влијание на САД и после терористичкиот напад на 11 септември 2001 година. После тоа, развојот на овој домен од аспект на Европската унија се карактеризира со три процеси кои се случуваат паралелно и истите се поврзани. Ова е потребно да се земе предвид заради разбирањето на овој домен. Прво, Унијата првенствено се обидува да остави свој печат во полето на заштитата на критичната инфраструктура; второ, таа се обидува да развие соработка со оние земји-членки кои имаат најразвиени национални политики; трето, Унијата се обидува да го стандардизира полето, да ја изедначи насоката и брзината на развој и да го сподели заедничкиот пристап на сите земји-членки. Многу напор беше вложен во овие процеси, затоа што беше неопходно да се усогласат различните гледишта и размислувања за критичната инфраструктура, посебно помеѓу развиените и постари земји-членки и поновите членки кои се запознаа со заштитата на критичната инфраструктура непосредно после стекнувањето полноправно членство во Европската унија. Фокусот на овој дел 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 соработката со приватниот сектор.

1. ЗАЕДНИЧКА РАМКА ЗА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Европската унија го започна овој процес под силно влијание на терористичкиот напад на САД во 2001 година, Глобалната војна против тероризмот која следеше и големите терористички напади во Европа во 2004 година во Мадрид и во 2005 година во Лондон, и го имаше првичниот дискурс на набљудување и заштита на критичната инфраструктура, поврзан со одбраната од тероризмот. Овој дискурс беше доминантен во раните години од развојот на овој домен на ниво на Европската унија.

Критичната инфраструктура и тероризмот претставуваат два поими и концепти кои често се користат во современиот свет. Нивната интеракција е всушност во тоа што многу од оние кои работат во областа на критичната инфраструктура се обидуваат истата да ја заштитат од тероризам. Многу автори го сметаат тероризмот за водечка закана за критичната инфраструктура, додека Елза Ли оди чекор понатаму и верува дека главните цели на терористите во Соедине-

тите Американски Држави (САД) и повеќето западни земји се критичната инфраструктура.[23] Официјалните политики на многу земји и организации во полето на заштитата на критичната инфраструктура се формирани на истиот начин. Но, споменатиот пристап има одредени недоследности, започнувајќи од неадекватната терминолошка дистинкција, концептуална неразвиеност на системот за заштита на критичната инфраструктура, па се до несоодветна национална и меѓународна соработка во поглед на заштитата на критичната инфраструктура. Споменатите феномени се посебно видливи во земјите кај кои недостасува нормативна рамка за заштита на критичната инфраструктура, им недостасуваат главните стратешки документи во областа на националната безбедност или пак истите не се ажурирани, или се во некоја мера нестабилни, било заради внатрешни или надворешни причини.[24]

Предизвиците за заштита на критичната инфраструктура се бројни. За оние земји кои само што започнуваат со формирањето на концептот на заштита на критичната инфраструктура, предизвиците се манифестираат во разбирање на важноста на гореспоменатото, развивање на нормативната рамка, идентификација, означување на секторот и индивидуалната критична инфраструктура, воспоставување соодветни и квалитетни мерки за заштита. Во Југоисточна Европа, посебно во земјите кои го поминаа процесот на распаѓање на Југославија и сè уште не се дел од ЕУ и НАТО, а сè уште се борат и со други приоритети, концептуалното и нормативното поле на заштита на критичната инфраструктура е сè уште неразвиено.

Од организациски аспект, за заштита на критичната инфраструктура Работната група за заштита на критичната инфраструктура на Центарот за студии за европска политика, предизвиците ги гледа во: врската помеѓу јавниот и приватниот сектор; неограниченост, посебно во случајот на критични информациски инфраструктури, не постојат физички бариери или политички граници; поголема вмреженост, сложеност; зависност од одлуките кои ги носат луѓето и ранливост.[25]

После првите неколку години на разгледување на овој домен, Европската унија започна со негово нормативно уредување. Така, во 2004 година Европската комисија донесе Комуникација на заштитата на критичната инфраструктура во борбата против тероризмот, каде беа изложени препораките што треба да прави Европа за да спречи терористички напади на критичната инфраструктура, да ја зголеми својата издржливост и да ја развие способноста да одговори на нападот.[26] Една година подоцна Комисијата донесе „Зелена книга“ за Европската програма за заштита на критичната инфраструктура во која беа предложени решенијата за воспоставување програма за заштита на критичната инфраструктура и креирање на мрежа за информирање во случај на закани по критичната инфраструктура.[27] Потоа, во 2006 година, Комисијата донесе Европска програма за заштита на критичната инфраструктура во која беа наведени сите опасности по критичната инфраструктура, но тероризмот останува примарен фокус и грижа.[28] Во 2007 година, Советот на Европската унија донесе одлука за воспоставување

[23] Lee, E. (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

[24] Perinić, J. and Mikac, R. (2014) *Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia*, in: Comprehensive Approach as"Sine Qua Non" for Critical Infrastructure Protection, NATO Science for Peace and Security Series: Information and Communication Security.

[25] Heammerli, 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(цитирано 5 мај 2017).

[26] European Commission (2004) *Communication on Critical Infrastructure Protection in the fight against terrorism,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702(цитирано 6 мај 2017).

[27] European Commission (2005)*Green Paper on the European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576(цитирано 6 мај 2017).

[28] European Commission (2006) *European program of Critical Infrastructure Protection,*http://eur-lex.europa.

на специјална програма, Превенција, подготвеност и управување со последици од тероризам и други ризици поврзани со безбедноста, како дел од Генералната програма за безбедност и заштита за периодот од 2007 до 2013 година. Програмата препознава бројни ризици поврзани со безбедноста, а во средината има дел посветен на поддршка на напорите на земјите-членки за спречување терористички напади, подготовка за заштита и заштита на луѓето и критичната инфраструктура од ризици поврзани со терористички напади.[29]Како што може да се види, Унијата го фокусираше својот првичен дискурс првенствено на одбрана од тероризам. Со текот на времето, другите ризици беа сè повеќе признавани и разгледувани, но тероризмот, сепак, останува најголема закана.

2. ДИРЕКТИВА 2008/114/ЕК ЗА ИДЕНТИФИКАЦИЈА И ОДРЕДУВАЊЕ НА ЕВРОПСКИТЕ КРИТИЧНИ ИНФРАСТРУКТУРИ И ПРОЦЕНА НА ПОТРЕБАТА ДА СЕ ПОДОБРИ НИВНАТА ЗАШТИТА

Претходно споменатиот дискурс преовладуваше до 2008 година кога беше донесена Директивата 2008/114/ЕК за идентификација и утврдување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита, која сега претставува главен документ за критична инфраструктура во Европа, кој повеќе не е главно фокусиран на заканата од тероризмот, туку се обидува процесот на заштита на критичната инфраструктура целосно да го постави на ниво на земјите-членки, како и на Унијата во целина.[30]

Според Директивата, критична инфраструктура значи „имот, систем или дел од него кој се наоѓа во земјите-членки и е од суштинско значење за одржувањето 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 значи „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 на инфраструктура.“[31]

Прашањето е како да се одреди критичната инфраструктура од аспект на критичност и национално значење. Постојат два критериуми кои се поважни од другите. Прво, атрибутот критична треба да се смета за нешто од посебно значење и без кое не е возможно да се функционира. Второ, ако одредиме премногу атрибути кои се критични, самата критичност се намалува. За таа цел, вреди да се укаже на ризикот дека државите кои се неискусни во овие прашања и оние кои се вклучени за прв пат во процесот на идентификување и утврдување на критичната инфраструктура, ќе ја преценат важноста на некои инфраструктури и ќе одредат премногу инфраструктура во категоријата критична. Дополнителен предизвик се јавува поради

eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786(цитирано 6 мај 2017).

[29] Council of the European Union (2007) *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0124(цитирано 6 мај 2017).

[30] 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(цитирано 1 мај 2017).

[31] Ibid, стр.174.

ограничените институционални капацитети кои се на располагање за оваа активност, што во голема мера попречува сеопфатен пристап кон заштитата на критичната инфраструктура. Дефинирањето на националното значење е варијабилен и експанзивен концепт и претставува рамка за набљудување на материјални, нематеријални, виртуелни и интелектуални објекти, системи и вредности за кои, според одредени критериуми, може да се претпостави дека нивниот прекин со работа, нарушување на работата или пак оттуѓување, би имале значителни последици за националната безбедност, здравјето и животот на луѓето, имотот и животната средина, економската стабилност и континуираното функционирање на владата. Таквиот широко прифатен концепт нè доведува до предизвиците на рационалната визуелизација, затоа што во зависност од контекстот на просторот и времето, многу од горенаведеното може да се смета како критична инфраструктура.

Во енергетскиот и транспортниот сектор Директивата 2008/114/ЕК се применува од страна на земјите-членки на ЕУ од 12 јануари 2011 година, со перспектива нејзината примена да се прошири и на други сектори на критичната инфраструктура. Пред пристапување кон полноправно членство во Европската унија, сите нови членки на Унијата се обврзани да ја имплементираат оваа Директива во нивното национално законодавство. Документот е замислен како прва мерка за идентификување, утврдување и процена на потребната заштита на критичната инфраструктура и оваа обврска и одговорност им се доделува на државите и на сопствениците на критичната инфраструктура. Директивата бара единствен пристап за заштита на критичната инфраструктура со имплементација во три фази: 1) Идентификување на потенцијалната критична инфраструктура; 2) Одредување на критичната инфраструктура; 3) Заштита на критичната инфраструктура. Притоа, дефинирањето на критичната инфраструктура треба да се спроведе преку секторски и меѓусекторски мерки со анализирање на ризикот за непрекинатост на работењето, каде меѓусекторските мерки вклучуваат три критериуми: човечки загуби; економски загуби; влијание врз јавноста. Директивата многу јасно истакнува дека е неопходно да се направи анализа на деловниот ризик и сигурносните планови за заштита на критичната инфраструктура и да се идентификуваат безбедносни координатори и национални контакт-точки за комуникација со Комисијата и други земји. Иако Директивата е фокусирана на енергетскиот и транспортниот сектор, земјите-членки имаат можност во рамките на националната рамка да идентификуваат дополнителни сектори каде е можно да се идентификува и утврди критична инфраструктура. Меѓу другото, Директивата става акцент на вклучувањето на приватниот сектор во заштитата на критичните инфраструктури (супервизија, управување со ризик, планирање на континуитет во работењето, закрепнување од катастрофи).[32]

3. УЛОГАТА НА ПРИВАТНИОТ СЕКТОР ВО ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Јавното-приватно партнерство е клучната врска во имплементацијата на политиките за заштита на критичната инфраструктура бидејќи поголемиот дел од таквата инфраструктура е во приватна сопственост, сите зависат од неа, и ниедна компанија во светот не може сама да ја заштити својата сопственост од сите можни ризици кои потенцијално ѝ се закануваат, без соработката со јавниот сектор. Развиените земји со развиени политики за заштита на критичната инфраструктура го гледаат јавното-приватно партнерство како неопходен и исклучително важен елемент на целокупните активности во областа на заштитата на критичната инфраструктура. Од друга страна, земјите во транзиција за време на процесот – освен недостатокот на стратегиска рамка за јавно-приватно партнерство во заштитата на критичната инфраструктура – се среќаваат

[32] Ibid.

со отворени прашања за идентификување, утврдување, начини и модели на заштита, но исто така и со сопственоста на критичната инфраструктура.[33]

Како што веќе беше споменато, во развиените индустриски земји од западната хемисфера, сопственик и управител на повеќето важни национални критични инфраструктури е приватниот сектор. Затоа, дополнително се потенцира предизвикот за заштита на критичната инфраструктура. Националната стратегија за внатрешна безбедност на САД од 2002 година, потенцира дека приватниот сектор е главниот снабдувач на стоки и услуги на државата и поседува 85 проценти од националната критична инфраструктура и со тоа, тој е клучен партнер за постигнување на националната безбедност.[34] Британската национална критична инфраструктура е претежно во приватна сопственост. Исполнувањето на националните цели зависи од тесната соработка помеѓу јавниот и приватниот сектор, а приватниот сектор е клучен за заштита на интересите на Велика Британија.[35] Понатаму, приватниот сектор кој има функција на управување со критичната инфраструктура исто така има одговорност да обезбеди негова заштита. Со оглед на тоа, приватниот сектор е главен инвеститор во критичната инфраструктура. Пропорционалноста на инвестициите е видлива преку примерот на компанијата „National Grid“, која планира да инвестира 35 милијарди фунти во критична инфраструктура на пазарите на Обединетото Кралство и САД во периодот од 2013 до 2021 година. Политиките за заштита на критичната инфраструктура на Обединетото Кралство и САД се доста слични затоа што тие ја следат истата логика која потекнува од стратегиското партнерство, силните врски помеѓу британската и американската економија, заеднички вредности и цели.

Земјите во транзиција, на кои им недостасуваат стратегиски документи во областа на националната безбедност, имаат потешкотии затоа што тие не дефинирале теоретски што претставува критичната инфраструктура и немаат јасен концепт за јавно-приватно партнерство во однос на управувањето и заштитата на критичната инфраструктура. Вредно е да се истакне мислењето на група автори од Србија кои ја набљудуваат комплексноста на проблемот преку три призми: случаи на тежок економски криминал во компаниите кои претставуваат потенцијална критична инфраструктура, недостаток на јавно-приватно партнерство во заштита на критичната инфраструктура, високо ниво на исполитизиран менаџмент во таквите компании.[36]

Јавното-приватно партнерство е клучната врска во имплементирањето на политики за заштита на критичната инфраструктура бидејќи најголем дел од таквата инфраструктура е во приватна сопственост, сите засегнати страни зависат од тоа и нема компанија која може без соработка со јавниот сектор, односно независно да го заштити сопствениот имот од сите можни ризици кои потенцијално го загрозуваат.

Додека сите консултирани извори укажаа на важноста на јавното-приватно партнерство во заштита на критичната инфраструктура, овој однос е обременет со многу предизвици кои Ли ги поставува на генерално ниво како: заемна недоверба; непознавање на процедурите, овластувања и обврски; страв од размена на информации поради случаите на „протекување“

[33] Perinić, J. and Mikac, R. (2014) *Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia*, in: Comprehensive Approach as"Sine Qua Non" for Critical Infrastructure Protection, NATO Science for Peace and Security Series: Information and Communication Security.

[34] Office of Homeland Security (2002), *National Strategy for Homeland Security*, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (цитирано 12 мај 2017), стр.viii.

[35] Home Office (2009), *National Counterterrorism Strategy*, *Government of the United Kingdom,* http://tna.europarchive.org/20100419081706/http:/security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy-2009?view=Binary(цитирано 12 мај 2017).

[36] Davidović, D., Kešetović, Ž. iPavičević, O. (2012), *National Critical Infrastructure Protection in Serbia: The Role of Private Security,* Journal of Physical Security; 6(1), 59-72, Argonne National Laboratory, http://jps.anl.gov/Volume6_iss1/Davidovic.pdf(цитирано 14 мај 2017).

на двете страни.[37]Поради таа причина, Конфедерацијата на европските безбедносни служби (КоЕБС) изработи Бела книга и насоки насловени Јавно-приватна можност. КоЕБС како претставник на европските приватни безбеносни служби, силно верува дека нејзините членки и нивните придружни компании за приватна безбедност треба да играат многу поголема улога во обезбедувањето и заштитата на критичната инфраструктура на начин кој носи придобивки за сите – надлежните органи, сопствениците и операторите на инфраструктурата, крајните корисници на критичната инфраструктура, компаниите за приватна безбедност и општата јавност во целост. Во споменатиот документ, КоЕБС потенцира некои примери каде функционира јавно-приватната соработка во корист на сите инволвирани страни. Тој исто така содржи предлози за тоа како овие примери би можеле да се искористат како најдобри практики и да се следат и имплементираат на друго место. На крај, овој документ исто така дава насоки за сите вклучени страни за тоа како најдобро да се обезбеди и заштити критичната инфраструктура.[38]

Соработката помеѓу јавниот и приватниот сектор е неизбежна во доменот на заштитата на критичната инфраструктура. Во современиот свет кој е оптоварен со зголемен број на асиметрични закани и ризици, соработката на сите елементи на општествената моќ едноставно е предуслов кој не може да се избегне. Државите и општествата кои го земаат тоа предвид се понапредни и имаат повеќе шанси за успех отколку оние кои не го користат моделот на јавно-приватно партнерство како концепт за имплементација.

4. РЕВИДИРАЊЕ НА ДИРЕКТИВАТА 2008/114ЕК ЗА ИДЕНТИФИКАЦИЈА И УТВРДУВАЊЕ НА ЕВРОПСКИТЕ КРИТИЧНИ ИНФРАСТРУКТУРИ И ПРОЦЕНА НА ПОТРЕБАТА ЗА ПОДОБРУВАЊЕ НА НИВНАТА ЗАШТИТА

Со усвојувањето на Директивата, земјите-членки се соочија со предизвикот на прилагодување на националните рамки или, за прв пат, воспоставувајќи цела низа на програми поврзани со заштитата на критичните инфраструктури. Некои консултирани извори (Хемерли и Ренда, Лазари и Симончини) сметаат дека по усвојувањето на Директивата недостасуваа понатамошни потребни чекори од страна на Комисијата за развојот на полето, и се создаде вакуум во кој земјите-членки беа повеќе или помалку оставени да дејствуваат сами. Поконкретно, иако Директивата дава јасни одредби, недостасува следење на нејзиното спроведување во националното законодавство. Алесандро Лазари и Марта Симончини истакнаа дека Директивата е инкорпорирана во секој од 28-те национални закони на Унијата, имено преку: амандмани 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); декларации и извршни наредби (8 држави), но не сите држави ја донесоа нормативата за Директивата на потребниот начин.[39] Уште од усвојувањето

[37] Lee, E. (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

[38] The Confederation of European Security Services (CoESS),*The Public – Private Opportunity*, http://www.naftso.org/language/en/uploads/files/home__0/home__b12b429e50767e06715e1294ce238774.pdf(цитирано 16 мај 2017).

[39] 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,*InternationalJuornal of Critical Infrastructure, https://www.dropbox.com/s/gvs5jhivvhqd3on/IJCIP-S-14-00008.pdf(cited 8 May 2017).

на Директивата, Комисијата немаше јасна цел како да го води и моделира процесот.[40]

Иако Директивата се стреми да ги охрабри земјите-членки тесно да соработуваат, да разменуваат информации и добри практики и да воспостават заеднички европски критични инфраструктури (во моментов се одредени нешто повеќе од педесет европски инфраструктури), државите многу тешко се одлучуваат за таква соработка и ги задржуваат политиките на заштита на критичната инфраструктура претежно во рамките на националните граници. Работната група за заштита на критичната инфраструктура на Центарот за студии за европска политика, смета дека, иако Комисијата донесе многу политички иницијативи во оваа област, сè уште постојат четири главни проблеми: „Прво, земјите-членки се со различен степен на зрелост во однос на развојот на сеопфатна и ефикасна политика за заштита на критичната инфраструктура. Второ, постојат делови на соработка во земјите-членки на ЕУ, но нема целосен концепт на работење на ниво на ЕУ. Трето, партнерствата и односите се распространети низ земјите (секоја поединечна земја има и ќе одржи уникатни односи со сопствениците од приватниот сектор и глобалните компании кои тоа им го овозможуваат). Четврто, критичната инфраструктура на ЕУ е исто така распространета низ многу различни земји.“[41]Комисијата го препозна застојот во процесот и ја ревидира Директивата во 2012 година и во обид да направи пробив во заштитата на критичната инфраструктура во рамките на Унијата, во средината на 2013 година презентираше работен документ на персоналот на Комисијата за нов пристап кон Европската програма за заштита на критичната инфраструктура: Обезбедување поголема сигурност на европската критична инфраструктура, првично усвоен во 2006 година. Работниот документ има нова перспектива за попрактична имплементација на Европската програма за критична инфраструктура, обезбедува анализа на елементите на тековната програма и предлага редефинирање на пристапот на заштита на критичната инфраструктура на Европската унија, врз основа на практичната имплементација на активностите во областа на превенција, подготвеност и одговор. Дел од новиот пристап е да се согледаат зависностите помеѓу критичната инфраструктура, индустријата и државните ентитети бидејќи е забележано дека досегашната меѓузависност не е доволно разгледана. За пилот-проект за анализа на меѓузависноста помеѓу различни критични инфраструктури важни за Европа, беше избран: „Евроконтрол, Галилео“, мрежа за пренос на електрична енергија и дистрибутивна мрежа за гас. Бидејќи голем дел од критичната инфраструктура е во приватна сопственост, се потврдува ставот дека е потребна подобра соработка со приватниот сектор, како и развој на структуриран дијалог на јавно-приватно партнерство. Дополнително, идентификувани се четири приоритетни области на европскиот модел за заштита на критичната инфраструктура: 1) процедури за идентификување и утврдување на критичните европски инфраструктури и процена на потребата за подобрување на нивната заштита (детално објаснети во Директивата 2008/114/ЕК на Советот); 2) мерки дизајнирани да помогнат во имплементацијата на Европската програма за критична инфраструктура, вклучувајќи Акционен план, Информативна мрежа за предупредување за критичната инфраструктура (CIWIN), употребата на експертски групи за заштита на критичната инфраструктура на ниво на ЕУ, размена на информации, идентификација и анализа на меѓузависности; 3) финансирање на мерки поврзани со заштитата на критичните инфраструктури и проекти поврзани со посебна програма за Превенција, подготвеност и управување со последици од тероризам и други ризици поврзани со безбедноста; 4) развој на надворешна димензија на Европската програма за критична инфраструктура.[42] **Со овој нов**

[40] Heammerli, 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(цитирано 5 мај 2017).

[41] Ibid, стр.3.

[42] 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*, https://ec.europa.

пристап, Комисијата има цел да ја подобри заштитата на критичната инфраструктура низ целата Унија, да го подигне целиот процес на повисоко ниво и да креира платформа за споделување на информации и најдобри практики со формирање на експертски групи за секој сектор.

eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf(цитирано 21 мај 2017).

3 ГЛАВА КРИТИЧНИ ИНФРАСТРУКТУРНИ ОБЈЕКТИ И ФУНКЦИИ ОД ПОСЕБЕН ИНТЕРЕС

Секоја нација ги определува и ги набљудува објектите кои се од посебен интерес за функционирањето и одбраната на земјата. Постојат разни примери за да се разгледаат и да се искористи најдобрата практика. Во кралството Шведска поимот критична инфраструктура се однесува на активностите, објектите, мрежите, инфраструктурата и услугите кои ги одржуваат виталните општествени функции. На тој начин витални општествени функции е термин за активности кои одржуваат одредена функционалност. Секоја таква функција е вклучена во еден или во повеќе општествени сектори. Во Шведска примарниот фокус не е на дискусијата за критичните инфраструктурни објекти, туку на функциите што ја обезбедуваат нивната оперативност. Националната инфраструктура на Шведска во моментов е категоризирана во 11 критични сектори кои обезбедуваат множество на критични општествени функции.[43] Во кралството Шпанија фокусот е поставен поинаку, од цели до одржување на витални општествени функции. А законот за ЗКИ дава официјална дефиниција за тоа што се подразбира под критична инфраструктура: „Стратешките инфраструктури (односно оние кои обезбедуваат основни услуги) чие функционирање е неопходно и не дозволува алтернативни решенија, се причината зошто нивното нарушување или уништување ќе има сериозно влијание на основните услуги.“ Националната инфраструктура на Шпанија во моментот е категоризирана во 12 критични сектори. Инфраструктурите никогаш не биле толку важни и влијателни за нормалното функционирање на услугите кои се од суштинско значење за населението и главните системи за производство, како што се денес.[44] Во САД, според „Патриотскиот акт“, критичната инфраструктура се дефинира како „Системи и средства, физички или виртуелни, кои се толку важни за САД што онеспособувањето или уништувањето на таквите системи и средства би имало ослабнувачки ефект на безбедноста, националната економска сигурност, националното јавно здравство или сигурност, или која било комбинација од претходно наведените,“[45] при што фокусот на набљудување и заштита е подеднакво ставен и на критичните инфраструктурни објекти и на нивните функции кои се неопходни за нивно ефикасно работење. САД имаат 16 сектори на критична инфраструктура.

Како што е прикажано во овие 3 примери, постојат различни пристапи кон зајакнување на отпорот и заштита на критичната инфраструктура, во зависност од одлуката на секоја земја на што ќе биде фокусот. Некои држави се фокусираат на физичката форма, други на функциите, а трети на набљудување на целокупната ситуациона слика.

Како што покажува практиката, не сите сектори, објекти и функции на критичната инфраструктура се подеднакво важни за функционирањето на државата и општеството, а

[43] 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(цитирано 15 мај 2017).

[44] For more information see: Spanish Parliament (2011) *Law 8/2011 by which measures for the Protection of Critical Infrastructure Protection*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf(цитирано 16 мај 2017), Ministry of Interior (2011) *Regulation for the Protection of Critical Infrastructure*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf(цитирано 16 мај 2017).

[45] United States Congress (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA PATRIOT Act),*стр.401, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf(cited 15 May 2017).

одредени држави како САД одлучија да дадат приоритет на начинот на кој ќе се разликуваат одредени функции кои се од суштинско значење за работењето на повеќето сектори на критичната инфраструктура. Овие витални функции вклучуваат комуникации, енергија, транспорт и вода.[46] Во меѓувреме, Шпанија идентификуваше 12 сектори каде може да се идентификува критична инфраструктура и во секој сектор утврди барем една или повеќе инфраструктури. Специфичноста е во тоа што Шпанците прават разлика помеѓу стратегиски инфраструктури и критични инфраструктури. Тие имаат околу 4000 стратегиски инфраструктури и околу 400 критични инфраструктури, при што критичните се поважни отколку стратегиските.

Во дискусија која се однесува на оваа тема, важно е да се споменат и обработат оние сектори и примери кои се позначајни од другите, дали преку посредување на Директивата 2008/114/ЕК за идентификување и утврдување на европските критични инфраструктури и проценатa од потребата за подобрување на нивната заштита, или пак одредени сектори за енергија и транспорт кои се задолжителни да се согледаат и анализираат или како во примерот за САД, да се земат предвид виталните функции (комуникации, енергија, транспорт и вода) кои имаат предност пред другите. Во анализата на сите пристапи на различни организации и држави, важно е да се истакнат оние клучни политики и процеси кои се од суштинско значење за функционирање било на физичките објекти на критичната инфраструктура или виталните функции на кои тие придонесуваат. Затоа тука ќе бидат разработени примери за: енергија, транспорт, информациска и комуникациска технологија и вода.

1. ЕНЕРГЕТСКИ СЕКТОР

Енергетската инфраструктура е предмет на европското и националното законодавство и процена на ризик за да се одреди нејзината критичност, одразувајќи ја нејзината стратегиска важност. Основната филозофија на заштитата на европската критична енергија ги опфаќа следните три точки: А) верување во заеднички и холистички пристап за заштита на инфраструктурата од стратегиска прекугранична важност во Европа. Б) сите држави-членки се соочија со постојано зголемување на бројот на напади врз нивната критична енергетска инфраструктура, главно во форма на кражби, вандализам и сајбер-напади. В) сопствениците и операторите ја делат истата цел (обезбедување „ефикасно и сигурно работење во секое време и низ цела Европа“) без исклучоци. Ова бара отвореност и еднаква размена на информации помеѓу операторите, сопствениците и државните органи.[47] Европската комисија се фокусира на поврзување на земјите-членки во ова поле, преку финансирање на одредени проекти, како и објавување на студии и извештаи кои можат да придонесат за подобрување на самото поле.[48]

Како и Европската унија и НАТО, исто така, го разгледува значењето и важноста на енергетскиот сектор. Енергетскиот сектор се потпира на голем број различни категории на инфраструктура, кои ги сочинуваат сите различни компоненети на енергетскиот синџир. Тие вклучуваат инфраструктури за екстракција, производство или генерирање на енергија,

[46] Department of the Homeland Security (2013) *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (цитирано 17 мај 2017).

[47] European Commission (2012) *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 (цитирано 17 мај 2017).

[48] For more information see webpage of Directorate-General Migration and Home Affairs https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en, and webpage about Energy https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure(цитирано 16 мај 2017).

инфраструктури за копнен и поморски транспорт, за преработка и рафинирање, за складирање, дистрибуција итн. Енергетскиот сектор, исто така вклучува неколку потсектори – гас, нафта, јаглен и електрична енергија, секој со свои посебни инфраструктури. На пример, инфраструктурите за производство на електрична енергија вклучуваат објекти базирани на гас, нафта, јаглен, хидроенергија, нуклеарна енергија, ветар и други извори. Во однос на потребите за заштита, електричната енергија генерално се смета за поразновидна и според тоа, помалку привлечен потсектор за терористите, додека нафтениот сектор е попривлечен поради високата зависност на развиените земји од странската нафта, главно за транспорт.[49]

Привлечноста на енергетската инфраструктура за терористите е резултат на горенаведените карактеристики – меѓузависност на енергетските инфраструктури, зависност од енергија на други витални услуги и сектори, зависност на западните економии од енергетската инфраструктура лоцирана во нестабилни региони. Иако напад на голема енергетска инфраструктура можеби нема да предизвика многу жртви – иако ова очигледно зависи од целта, економските трошоци и нарушувањата најверојатно ќе бидат огромни. Всушност, неговото влијание може да се засили неколку пати нарушувајќи ја целната инфраструктура; предизвикувајќи каскадни ефекти на други инфраструктури, како и на други сектори на економијата; предизвикувајќи психолошко влијание засилено од медиумите; и потенцијално предизвикувајќи претерана реакција на финансиските пазари. Терористите исто така ја демонстрираа својата способност да нападнат енергетски инфраструктури ширум светот, иако не сите заговори беа успешни.[50]

Како што е прикажано во Воведот и сега во оваа глава, државите и мултинационалните организации се свесни за важноста на енергетскиот сектор за одржување на постојното ниво на развој, потребите на јавната и национална безбедност и просперитетот на граѓаните. Денес е непрактично да се запре постојниот напредок бидејќи како поединци, општества и држави ние сме ориентирани кон нови извори на енергија и одржување на постојните. Во оваа активност значаен партнер е секако приватниот сектор на кој посебно внимание ќе биде посветено во оваа глава.

2. ТРАНСПОРТЕН СЕКТОР

Транспортните системи се еден сектор кој опфаќа: воздухопловство, автопатна инфраструктура и моторни превозни средства, поморски транспортен систем, масовен транзит и патничка железница, гасоводен систем, товарна железница и поштенски пратки. Транспортот е клучен економски сектор, кој го олеснува движењето на луѓе, храна, вода, лекови, гориво и други артикли. Тој се соочува со повеќе закани, почнувајќи од несреќи, неуспеси или човечки грешки до злонамерни акции, како саботажа, внатрешни закани или терористички напади. Примери за последното се настаните во Њујорк и Вашингтон (2001), Мадрид (2004) и Лондон (2005). Заеднички елемент на овие инциденти е употребата на компоненти на транспортната инфраструктура. Во неколку случаи, беа употребени транспортни компоненети како главни средства за нападот; во други случаи, тие беа користени како цел, што исто така вклучуваше и сајбер-напади. Потенцијалните закани вклучуваат нарушување на главната точка на транспортната мрежа, употреба на транспортна компонента како метод на напад и ослободување на биолошки агенс во патнички објект (железничка станица, ферибот терминал, аеродромски

[49] NATO Parliamentary Assembly (2008) *Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures,* **http://www.nato-pa.int/Default.asp?SHORTCUT=1478**(цитирано 18 мај 2017).

[50] Ibid.

центар).[51]

Ние секојдневно зависиме од транспортот, но транспортот треба да се смета како и секоја друга развојна платформа (исто како и во претходниот дел за енергетскиот сектор) во неговата меѓузависност со други сектори. Енергетскиот сектор зависи од транспортот во однос на обезбедување сообраќајни правци, технологии и техники за транспорт на енергетски извори од нивниот извор до дестинацијата. Од друга страна, транспортниот сектор во голема мера е зависен од изворите на енергија за да ги изврши своите неопходни активности. А сите тие зависат и се меѓусебно поврзани со ИТ и комуникациските технологии без кои денес не е можно да се оствари одржлив високоефикасен бизнис.

Значењето на транспортниот сектор одлично го опишува американскиот пример во кој се вклучени и актерите и податоците кои треба да се земат предвид за да се согледа целата ширина на предметното поле. Секторот на транспортните системи – сектор кој ги опфаќа сите видови транспорт е огромен, отворен, меѓусебно поврзан мрежен систем кој пренесува милиони патници и милиони тони на стоки. Транспортната мрежа е од клучно значење за начинот на живот на САД и економската виталност. Обезбедувањето на неговата безбедност е мисија доделена на сите партнери во секторот, вклучувајќи ги владините (федерални, државни, регионални, локални и племенски) и заинтересираните страни од приватната индустрија. Транспортната мрежа секојдневно ги поврзува градовите, производителите и трговците, пренесувајќи големи количини на стоки и поединци преку комплексна мрежа од околу 6,5 милиони километри на патишта и автопати, 160.000 километри железнички пруги, 600.000 мостови, повеќе од 300 тунели и бројни поморски пристаништа, над 3 милиони километри нафтовод, 500.000 железнички станици и 500 јавни аеродроми.[52] Во овој пример потребно е да се обрне внимание на специфичноста во разгледувањето и заштитата на критичните инфраструктури. Кога гледаме колку се големи бројките во случајот на САД, иако како земја тие имаат големи ресурси (но тие не се неограничени), неопходно е да се посвети посебно внимание на вредностите и големините кои ќе бидат утврдени како критични инфраструктури. Бидејќи не е можно сите да бидат заштитени, односно не можат да бидат заштитени со истиот пристап. Затоа, кога се дефинираат критичните инфраструктури, треба да се направи дополнителна приоритизација за да се утврди на што ќе биде посветено повеќе внимание во однос на другите инфраструктури. И во овој случај, улогата на приватниот сектор е незаменлива, кога се работи за напредните нации.

3. ИНФОРМАЦИСКА И КОМУНИКАЦИСКА ТЕХНОЛОГИЈА

Со технолошкиот развој низ годините, информатичката и комуникациската технологија станаа интегрален дел од многу елементи на критичната инфраструктура во сите организациски сектори, како јвни така и приватни. Денешниот свет и неговиот понатамошен развој се незамисливи без информациска и комуникациска технологија. Ние сме толку приврзани и се потпираме на овој сектор што може да се заклучи дека сме зависни од него во таков обем и во таква мера како од ниеден друг сектор. Тука исто така се гледа и меѓусебна поврзаност, а можеме дури и да кажеме – зависност од приватниот сектор кој главно развива, произведува,

[51] Theoharidou, Marianthi; Kandias,Miltiadis and Gritzalis, Dimitris (2012) *Securing Transportation-Critical Infrastructures: Trends and Perspectives*, https://pdfs.semanticscholar.org/5441/f94eb1dbb98f9fa4031c52ef3e476f71050b.pdf (цитирано 19 мај 2017).

[52] Department of the Homeland Security (2007) *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, https://www.hsdl.org/?view&did=474328(цитирано 17 мај 2017).

одржува и надградува современи системи што ние ги земаме здраво за готово и секојдневно ги користиме. Тоа е друг показател дека јавното-приватно партнерство е платформа за успешен развој на сите нивоа на општеството.

Иако користењето на ИКТ инфраструктурата има позитивен ефект врз развојот на функционалните способности на системите, големиот пораст на меѓусебно поврзани уреди и производи на информации исто така ја зголемува ранливоста на објектот и други критични инфраструктури меѓусебно поврзани првенствено преку изложеност на сајбер- закани и дефекти на ИКТ инфраструктурата. Системите и инфраструктурите стануваат многу кревки и подложни на ризик што може да предизвика дисфункционалност и понатаму може да резултира со голем технолошки колапс. Претходно споменатата „Зелена книга“ на Европската комисија за критични инфраструктури содржи Листа на примери на критични сектори, производи и услуги. За критичниот сектор на информациски и комуникациски технологии се наведени седум производи и услуги: информациски систем и мрежна заштита; инструментација, системи за автоматика и контрола (SCADA и др.), интернет; обезбедување фиксни телекомуникации; обезбедување мобилни телекомуникации; радиокомуникација и навигација; сателитска комуникација и радиодифузија. Нации како што е Холандија, кои ги опишаа нивните критички телекомуникации или секторот за информациска и комуникациска технологија како критични услуги и производи, ги препознаваат фиксните телекомуникациски услуги, мобилните телекомунокациски услуги, пристапот до интернет, сателитската комуникација и медиумите/радиодифузијата како услуги на критичната инфраструктура за нивните нации. Други држави само го дефинираат нивниот сет на критични сектори или ги дефинираат услугите и производите на високо ниво. Швајцарија, на пример, ги препознава следните три ИКТ потсектори: информатички технологии (ИТ), медиуми и телекомуникации. САД во своите сектори на критична инфраструктура исто така ги вклучуваат и комуникацискиот сектор и ИТ секторот. Критичниот комуникациски сектор опфаќа жичани, безжични, сателитски, кабелски и радиодифузни инфраструктури; критичниот ИТ сектор се состои од обезбедување на ИТ производи и услуги, способности за управување со инциденти, услуги за решавање на име на домен, управување со идентитет и придружни услуги за поддршка на доверба, интернет содржини, информациски и комуникациски услуги и интернет рутирање, услуги за пристап и поврзување.[53]

4. ВОДА

Водата е клучен сегмент од животот, додека инфраструктурата за вода се смета за една од најважните критични инфраструктури на глобално ниво.[54] Луѓето користат вода за најосновните човечки потреби. Виталните мрежи и бизниси, индустриите, болниците, други комунални претпријатија, земјоделството и производтствените индустрии се зависни од системите за вода. Системите за вода се исто така од суштинско значење за напорите за обновување што следат после секоја природна катастрофа и за одржување на животниот стандард во секојдневниот живот.[55] Како што вкупното светско население расте, сè повеќе ќе има поголема потреба и

[53] Luiijf, Eric and Klaver, Marieke (2015) *Governing Critical ICT: Elements that Require Attention*, http://societalsecurity.net/sites/default/files/document-database/files/2016-03/pdf/3018787-governing-critical-ict-elements-require-attention.pdf(цитирано 21 мај 2017).

[54] Birkett, D.M. (2017) *Water Critical Infrastructure Security and Its Dependencies*. Journal of Terrorism Research. 8(2), pp.1–21. DOI: http://doi.org/10.15664/jtr.1289 (цитирано 24 мај 2017).

[55] Van Leuven, Laurie (2011) *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, https://www.researchgate.net/publication/226050430_WaterWastewater_Infrastructure_Security_Threats_and_Vulnerabilities(цитирано 24 мај 2017).

притисок врз системите за вода. Многу луѓе денес немаат пристап до чиста вода и поради тоа луѓето страдаат. Како резултат на глобалните климатски промени се зголемува загадувањето на животната средина и се намалува обработливото земјиште, голем број на луѓе се принудени на постојана миграција што ја зголемува побарувачката за посилни системи за вода кои ќе ги задоволат постојано растечките потреби. Постојат многу конфликти околу водата, на пример на Блискиот Исток, и повеќе внимание се посветува на заштита на системите за вода отколку на заканите од тероризам. Како и секој друг сектор на критичната инфраструктура, секторот за вода исто така ги има некои од најважните сегменти кои треба да се земат предвид за да се добие појасна слика за компонентите за кои дискутираме како целина, како и за објектите кои треба да се заштитат. Четири компоненти во дизајнот на јавен водоводен систем се однесуваат на безбедноста и сигурноста на водата за пиење. Тие се: снабдување со сирова вода, вклучувајќи ги и придружните цевководи; системи за пречистување; дистрибутивни системи; оперативни и контролни системи.[56]

Критичната инфраструктура за вода е силно поврзана и зависна од некои други претходно дискутирани сектори, како информатичката и комуникациската технологија, исто како и од електричната енергија. Еднакво како и другите сектори на критична инфраструктура, критичната инфраструктура за вода е подложна на различни природни и човечки закани. Луѓето може да ја доведуваат во прашање потребата да се обезбедат пумпни станици, капацитети за складирање вода, постројки за пречистување или цевководи. Едноставниот одговор на ова размислување е дека негативните последици од намерен напад се премногу големи за да се игнорираат. Значаен напад на системот за вода може да резултира со широко распространета болест или жртви. Сценарио за одбивање на услуга може да влијае на критичните услуги како што се противпожарната и здравствената заштита и може да ги наруши другите зависни сектори како што се енергетскиот, транспортниот, храната и земјоделството.[57]

5. МЕСТОТО И УЛОГАТА НА ПРИВАТНИОТ СЕКТОР

Со текот на времето се зголемува свеста за потребата од синергија помеѓу јавниот и приватниот сектор во изградбата, одржувањето и заштитата на критичната инфраструктура. Уште од почетокот на развојот на ова поле, Европската комисија беше многу јасна за потребата од заедничка соработка на јавниот и приватниот сектор. Така, во 2004 година, Европската комисија укажа на тоа како Европејците очекуваат критичните инфраструктури да продолжат да функционираат, без оглед на тоа кои организации ги поседуваат или управуваат со составните делови. Тие очекуваат владите на земјите-членки и ЕУ да играат водечка улога во обезбедувањето тоа да се случи. Тие очекуваат сите нивоа на сопственици и оператори од владиниот и приватниот сектор да соработуваат за да се обезбеди континуитетот на услугите од кои зависат Европејците. Каде што ќе има успех, меѓу другите показатели, тој исто така ќе се мери со: Европската заедница решава да воспостави заеднички пристап за справување со безбедноста на критичните инфраструктури преку соработка на сите јавни и приватни актери.[58]

[56] Public Safety and Emergency Preparedness Canada (2003) *Water, Critical Infrastructure Protection and EmergencyManagement*, http://publications.gc.ca/collections/collection_2008/ps-sp/PS4-7-2004E.pdf(цитирано 19 мај 2017).

[57] Van Leuven, Laurie (2011) *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, https://www.researchgate.net/publication/226050430_WaterWastewater_Infrastructure_Security_Threats_and_Vulnerabilities(цитирано 24 мај 2017).

[58] European Commission (2004) *Communication on Critical Infrastructure Protection in the fight against terrorism,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702 (цитирано 6 мај 2017).

Во следниот значаен документ Европска програма за заштита на критичната инфраструктура, Европската комисија не беше толку експлицитна во однос на соработката на јавниот и приватниот сектор која е спомената во јавниот-приватен дијалог во врска со заштитата на критичната инфраструктура, како и учество во експертските групи кои би ја советувале Комисијата за суштински прашања.[59] Меѓутоа, во најважниот документ во оваа област, Директивата за идентификација и утврдување на европските критични инфраструктури и проценатa на потребата за подобрување на нивната заштита (Директива 2008/114/ЕК), Комисијата накратко, но одлучно ја истакна важноста и улогата на приватниот сектор. Со оглед на многу значајното вклучување на приватниот сектор во надгледување и управување со ризици, планираање на континуитетот во работата и обновување после катастрофи, пристапот на Заедницата треба да поттикне целосно вклучување на приватниот сектор.[60]

Поединечни институции и автори кои беа консултирани силно веруваат во потребата од ова партнерство. На пример, некои автори веруваат дека вклучувањето на приватниот сектор е императив. Тие нагласуваат дека приближно 90 проценти од националните критични инфраструктури се всушност во рацете на приватниот сектор. Освен тоа, тие веруваат дека компаниите во приватниот сектор се најдобро лоцирани за да проценат кои системи и потсистеми во рамките на нивниот сопствен бизнис или сектор бараат посебна заштита.[61] Центарот за европски политички студии нагласува дека не постои начин да се организира значајна политика за заштита на критичната инфраструктура без да биде вклучен приватниот сектор бидејќи критичните инфраструктури во Европа се главно во сопственост на приватни ентитети, од кои многу се компании кои оперираат на светско ниво.[62] Што се однесува до имплементациската страна на заштита на критичната инфаструктура, КОЕБС нагласува дека обезбедувањето и заштитата на критичната инфраструктура е една од најпогодните области за јавно-приватни партнерства, со оглед на нивниот честопати јавен (национален или локален) карактер, кој се преведува во јавна сопственост или јавен менаџмент или јавна цел. Сè поголем број на безбедносни функции, кои претходно беа вршени директно од јавните власти, сега ги преземаат компаниите за приватна безбедност и стануваат сè повеќе вклучени во обезбедување јавна безбедност, вклучително и на критичната инфраструктура.[63]

[59] European Commission (2006) *European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (цитирано 6 мај 2017).

[60] 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 (цитирано 1 мај 2017).

[61] Brömmelhörster, Jörn; Fabry, Sandra and Wirtz, Nico (2004) *Critical Infrastructure Protection: Survey of World-Wide Activities*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.html (цитирано 17 мај 2017).

[62] Heammerli, 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(цитирано 5 мај 2017).

[63] The Confederation of European Security Services (CoESS),*The Public – Private Opportunity*, http://www.naftso.org/language/en/uploads/files/home__0/home__b12b429e50767e06715e1294ce238774.pdf(цитирано 16 мај 2017).

4 ГЛАВА ЗАКАНИ И РИЗИЦИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

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. За да се заштитат на најдобар начин, потребно е да се земат предвид најзначајните закани и ризици категоризирани во горенаведените групи. Освен тоа, 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. 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. 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. 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. Понатаму, каде што има емпириски докази, ќе бидат користени примери од регионот на Југоисточна Европа и повремено поширокиот контекст.

1. ПРИРОДНИ ЗАКАНИ И РИЗИЦИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

Програмата за развој на Обединетите нации во своето истражување наведува дека регионот на земјите-членки на Организацијата за безбедност и соработка во Европа е многу подложна на природни непогоди – како што се земјотреси, поплави, суши, бури, топлотни бранови, шумски пожари – кои влијаат на повеќе од 76 милиони луѓе во последните 25 години. Според анализите од 1990 до 2014 година, бурите (34%) и поплавите (31%) се најчести природни непогоди. Поплавите (35%), бурите (29%) и сушите (19%) влијаат врз повеќето луѓе во наведената област. Најголем број луѓе останаа без своите домови 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.[64] Маргарета Валстром, специјален претставник на Генералниот секретар на ООН за намалување на ризиците од катастрофи наведе дека според проценката глобалните годишни економски загуби предизвикани од природни непогоди се поголеми од 100 милијарди УСД и трендовите покажуваат дека тие ќе продолжат да растат. Кристијан Фриз Бах, генерален секретар на ООН на Економската комисија за Европа приложи податоци за загубите од 100 милијарди евра во

[64] 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, стр.8 (цитирано 21 мај 2017).

ЕУ во изминатите 10 години кои беа предизвикани од природни катастрофи. За истиот период, Европската комисија проценува дека природните катастрофи во Европската унија меѓу 2002 и 2014 година предизвикале повеќе од 80 илјади смртни случаи и повеќе од 100 милијарди евра економски штети.[65] 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. Според извештајот на Европската агенција за животна средина, од 1998 до 2009 година биле пријавени 213 поплави во Европа, предизвикувајќи 1126 смртни случаи и економски загуби од повеќе од 52 милијарди евра.[66] Некои области во Европа се повеќе подложни на поплави отколку други, што може да се види во историски записи, но и од неодамнешните настани. Во изминатите неколку години поплавите доминираа во областа на Централна и Југоисточна Европа. Го забележуваме историскиот максимум на водата во големите европски реки како што се Дунав, Тиса, Драва, Мура, Сава и други реки и нивните притоки. Поплавите предизвикаа пробивање на повеќе насипи, поплавување на голема заштитена област, човечки жртви и масовно оштетување на имот во десетици држави. Според Европската комисија, Централна Европа во 2013 година ја доживеа 100-годишната поплава, односно поплавата со веројатност да се случи еднаш на сто години, а се случува по втор пат за само 13 години.[67] Исто така, веќе не е реткост водомерите во многу водотеци во европската област да бележат нивоа на водата кои одговараат на веројатноста на 200 и 500 години големи води. 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.[68] Слична ситуација се случи во Југоисточна Европа, каде што најзначајните последици се манифестираа во 2014 година. Во поплавите во мај, кои беа такви што се појавуваат еднаш на секои 1000 години, 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.[69] 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.

Областа на Југоисточна Европа, како дел од медитеранско-транзициониот појас, се одликува со изразена сеизмичка активност. Карактеристика на просторната распределба на сеизмичката активност е концентрацијата на земјотреси во одредени потесни области или зони. Ова особено важи за крајбрежните области и делови од внатрешноста кои биле погодени од катастрофални земјотреси. Истакнуваме неколку многу силни земјотреси кои ја означуваат оваа

[65] European Commission (2014) *ECHO Factsheet – Disaster RiskManagement – 2014*,http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf, стр.1 (цитирано 21 мај 2017).

[66] 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, (цитирано 22 мај 2017).

[67] European Commission (2014) *ECHO Factsheet – Disaster RiskManagement – 2014*,http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf, стр.1 (цитирано 21 мај 2017).

[68] 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, (цитирано 22 мај 2017).

[69] 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, стр.20 (цитирано 21 мај 2017).

област. На пример, 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.[70] Земјотресот во Скопје во 1963 година 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 уништи 75 до 80 проценти од градот. Земјотресот во 1969 година речиси целосно ја уништи Бања Лука. 15 лица беа мртви, повеќе од 1000 беа потешко или полесно повредени. 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. Во сите горенаведени земјотреси беше причинета голема материјална штета. Од аспект на критичната инфраструктура, значајна штета е забележана на бројни објекти, мрежи и системи на локалната и државната инфраструктура. Големи штети беа причинети во образовните, културните, здравствените, социјалните и објектите на јавната администрација. Значителни штети исто така се појавија во економијата, дури и до степен одредени бизниси целосно да престанат со нивните активности.

Причината за земјотресот во крајбрежниот дел е подвлекувањето на Јадранската плоча под Динаридите како резултат на движењето на Африканската плоча кон Евро-азиската плоча. Во северозападниот континентален дел, причините за земјотресите се процеси на компресија заради промената на Динаридите и Алпите, додека во други области се предизвикани од различни движења на масите на одредени планини. Иако областа на Југоисточна Европа е изложена на реални ризици од земјотреси, таа не е најактивната сеизмичка област во светот. Апенинскиот полуостров се соочува со постојани земјотреси кои резултираат со човечки загуби, материјална штета и прекин на работата и оштетување на критичната инфраструктура. Сеизмички најактивната зона е областа на Тихиот океан. Во земјотресот што се случи во 2004 година во Тихиот океан и како последица предизвика цунами во областа на Индонезија и соседните острови, загинаа повеќе од 227.000 луѓе. Земјотрес со исто сценарио се случи во 2011 година, во којшто беше погодена Јапонија. Нуклеарната централа во Фукушима беше исто така погодена од домино-ефект, а загинаа повеќе од 16.000 лица.

Од аспект на дискусијата за преземање на одредени мерки и активности идентификувани од овие земјотреси, се истакнува потребата од поотпорна конструкција со цел да се минимизира и избегне, колку што е можно, оштетување на домовите, патиштата, локалните, како и критичните инфраструктури. Така, зградите изградени до 1920 година имаа тавани изградени исклучиво од дрво. Тавани од армиран бетон постепено беа градени во периодот од 1920 до 1940 година. Од 1945 до 1964 година преовладуваа армирано-бетонски монолитни тавани од полумонтажен тип или направени на самото место. По 1964 година изградените објекти беа систематски градени со хоризонтални и вертикални греди, а објектите за колективно домување со армирано-бетонски систем за поддршка беа изградени во согласност со одредбите на Сеизмичките прописи од 1964 година (по земјотресот во Скопје), што може да се смета за современ начин на градба во смисла на научното знаење во тоа време.[71] Посебно внимание е посветено на градење на критичната инфраструктура, како на локално така и на државно ниво.

Пожарите од различен вид претставуваат потенцијална опасност за сите нивоа и облици на општеството и економијата. Тие потенцијално загрозуваат голем број на луѓе и средства во сите видови на објекти каде се собираат голем број на луѓе, во различни начини на транспорт, во тунели, во технолошки капацитети и инфраструктури кои складираат опасни

[70] Government of the Republic of Croatia (2009) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*, http://www.duzs.hr/download.aspx?f=dokumenti/Stranice/PROCJENAUGROZENOSTIREPUBLIKEHRVATSKE.pdf, стр.11 (цитирано 23 мај 2017).

[71] Ibid, стр.16.

стоки, исто како и пожарите на голем отворен простор. Во последните десет години посебна опасност во областа на Југоисточна Европа се пожарите на отворен простор. Оваа опасност е нагласена во сушните периоди во лето, особено во крајбрежниот дел. Поради климатските промени и нивното влијание, сè повеќе сме сведоци на големи пожари кои ја погодија Босна и Херцеговина, Србија, Македонија и 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.

2. ТЕХНИЧКО-ТЕХНОЛОШКИ ОПАСНОСТИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

Големите техничко-технолошки несреќи и катастрофи со сериозни последици за луѓето, материјалните и културните добра, како и за критичната инфраструктура можат да настанат поради бројни причини, но и како домино-ефект после првичните несреќи. Најопштата класификација на големите техничко-технолошки несреќи и катастрофи ја покажува целата ширина на потенцијалните сценарија за загрозување на вредностите кои ние настојуваме да ги заштитиме. Гореспоменатите се поделени на: техничко-технолошки катастрофи и големи несреќи во економски објекти; техничко-технолошки катастрофи и големи сообраќајни несреќи; нуклеарен ризик. Ако ова се разгледа, потребно е да се истакне дека во овој случај се прикажани катастрофи и големи несреќи што се јавуваат поради негативните фактори на технолошкиот процес, како и ненамерна човечка грешка.

Во сите земји, 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, додека 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[72] којашто осигурува систематска контрола и следење на потенцијалните извори на опасност од хемиско загадување и штетни ефекти врз животната средина и луѓето, што е исто така транспарентно за општата јавност.[73] 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.

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 и за време на нивната манипулација на штандовите. Можните причини за опасност од неочекувани настани може да се проценат од искуството на несреќи што веќе се случиле, имено: несоодветно ракување на возила во транспортот; неточен 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. Како пример за техничко-технолошка несреќа во сообраќајот, може да споменеме еден пример на турскиот товарен брод „UND Adriyatik“ во 2008 година во близина на западниот брег на Истра, Република Хрватска. Бродот носел голем број камиони до пристаништето во Трст и поради неидентификувани причини се случил пожар. Екипажот не можел да го спречи пожарот што се раширил и го зафатил поголемиот дел од товарот. Тие се евакуирале од бродот и „UND Adriyatik“ со денови бил носен од морските струи во многу тесниот северен дел на Јадранското Море. По неколку дена, пожарот бил угаснат, а бродот бил одвлечен во Италија. Постоела реална опасност дека пожарот ќе резултира со распаѓање на трупот и истекување на големи количества хемикалии во морето. Ова би предизвикало еколошка катастрофа и голема директна штета на туристичкиот сектор како еден од најважните сектори на критичната инфраструктура кога ќе се земе предвид зависноста на Хрватска од пополнување на државниот буџет преку овој сектор. Нуклеарните несреќи се ризик што треба да се разгледа со најголемо внимание. Нуклеарните централи, без оглед на видот на постројки, содржат големи количини на радиоактивни материи, што претставува потенцијална опасност за луѓето, животните, животната средина и нормалниот животен циклус. Поголемиот дел од радиоактивноста е поврзан со продуктите на фисија кои се

[72] 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.

[73] 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 мај 2017).

наоѓаат во јадрото на реакторот. Секое неконтролирано испуштање на радиоактивни материи од нуклеарната централа во животната средина го загрозува здравјето и животот на населението и ја загадува животната средина. На безбедноста на нуклеарните централи ѝ се посветува големо внимание, а постојат обиди ризиците да се сведат на најмала можна мера. Сепак, досегашното искуство покажува дека сè уште се случуваат нерегуларности, инциденти, несреќи, па дури и катастрофи во нуклеарните централи.[74] Примери за сериозни несреќи на нуклеарна централа се нуклеарната катастрофа во Фукушима Даичи (2011 година), катастрофата во Чернобил (1986 година), несреќата на островот Три Милји (1979 година) и несреќата СЛ-еден (1961 година).[75] Од 2014 година се случиле повеќе од 100 сериозни нуклеарни несреќи и инциденти како резултат на користењето на нуклеарна енергија. После катастрофата во Чернобил се случија 57 несреќи, а околу 60 проценти од сите нуклеарни несреќи се случија во САД.[76] Покрај ова, бројни несреќи се случија на советските нуклеарни подморници, како и радиолошки несреќи ширум светот.[77]

3. АНТРОПОГЕНИ ЗАКАНИ И РИЗИЦИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

Како антропогените закани и ризици за критичната инфраструктура генерално се сметаат: дела поврзани со тероризам, саботажа и криминал насочени кон функционирањето на целата или некои делови на критичната инфраструктура.

Критичната инфраструктура претставува огромен, глобален сектор. Поради тоа, не е можно да се обезбеди нејзина целосна заштита во секое време и на сите места. За жал, 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. Ова беше случај на 22 март 2016 година, кога два тима на оперативци на ИСИЛ извршија симултани напади во Брисел на аеродромот „Завентем“ (убиени 11 лица) и во метрото „Мајлбег“ (убиени 20 лица). Околу 300 луѓе беа повредени.[78] „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.[79] Иако

[74] Government of the Republic of Croatia (2009) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*, http://www.duzs.hr/download.aspx?f=dokumenti/Stranice/PROCJENAUGROZENOSTIREPUBLIKEHRVATSKE.pdf, стр.45 (цитирано 23 мај 2017).

[75] TIME (2009) *The Worst Nuclear Disaster*, http://content.time.com/time/photogallery/0,29307,1887705,00.html, (цитирано 22 мај 2017).

[76] Benjamin K. Sovacool (2010) *A Critical Evaluation of Nuclear Power and Renewable Electricity in Asia,* http://dx.doi.org/10.1080/00472331003798350, стр.369-400 (цитирано 24 мај 2017).

[77] За повеќе информации види: the International Atomic Energy Agency webpage, http://www-pub.iaea.org/books/IAEABooks/Publications_on_Accident_Response, (цитирано 23 мај 2017).

[78] 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, стр.3-4 (цитирано 2 јуни 2017).

[79] 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, (цитирано 2

некои автори забележуваат дека енергијата привлекува само мал дел на терористички напади, трендот покажува брз раст на интерес на терористите за нафта и гас.[80] Според бројни студии, повеќе напади во светот се насочени кон критичните инфраструктури.

Следната важна антрополошка закана е чинот на саботажа, што е гранична појава помеѓу терористичкиот акт и кривичното дело, и секој случај треба да се разгледува посебно. Саботажите и терористичките напади се главните закани за критичните инфраструктури. 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. 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. Непријателските сајбер-напади доаѓаат и во државна и во недржавна варијанта: странски разузнавачки агенции, терористи, погрешни активисти или едноставно поединци кои дејствуваат сами. Овие непријателски актери имаат пристап до сè поголем број на алатки и техники за сајбер-напад. Како што технологиите се развиваат и стануваат покомплексни исто така тоа се случува и со предизвиците за откривање и заштита од сајбер-напади. Иако вообичаено се смета дека главните напаѓачи преку интернет се хакери и – или терористи, неопходно е исто така да се привлече вниманието на државните актери во оваа активност. Агенциите за разузнавање сè повеќе користат интернет за да ги спроведат своите операции за шпионажа: тоа е релативно евтин начин со низок ризик за да се добијат класифицирани, сопственички или други чувствителни информации. Главните цели се високотехнолошки 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. Напаѓачите кои се спонзорирани од државата бараат информации кои ќе им дадат конкурентна предност на нивните домашни компании. 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- шпиунажа, сајбер-саботажа и други сајбер-операции се дел од една поширока економска закана за клучните сектори на критичната инфраструктура.[81]

Криминалните активности кон критичната инфраструктура можат да се поделат на внатрешни и надворешни. Внатрешните закани се дел од секоја организација. Во суштина, ова се случува кога доверлив вработен ги издава неговите обврски и лојалност кон работодавецот вршејќи саботажа или шпионажа против нив. Овие „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.[82] Надворешните закани веќе беа делумно опишани и тие претставуваат разновидни обиди за инфилтрирање во системот, било физички или преку интернет, а мотивот може да биде различен, во зависност од мотивацијата на напаѓачот. Физичките упади претставуваат обид за оттуѓување на дел од опрема или добивање важни информации директно преку соработка со вработените во компанијата или со одреден вид

јуни 2017).

[80] 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, (цитирано 2 јуни 2017).

[81] Canadian Security Intelligence Service (2017) *Cybersecurity and Critical Infrastructure Protection,* https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php, (**цитирано** 12 јуни 2017).

[82] 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, (цитирано 6 **јуни** 2017).

измама или изнуда. Но, многу поголеми и посериозни инвазии се обидите да се нападне сајбер-просторот. Такви напади на критичната инфраструктура се случуваат секој ден на глобално ниво и трендот се зголемува. Со оглед на тоа што 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. Оваа силна корелација помеѓу интернетот и критичните инфраструктури доаѓа по цена на зголемена комплексност и како последица на тоа, зголемен ризик на случајни грешки.

5 ГЛАВА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Заштитата на критичната инфраструктура е многу широка и динамична активност што ја извршуваат јавни тела, како што се различни законодавни институции, агенции за спроведување на законот, инспекциски и судски органи, оргазнизации за приватна безбедност, до меѓународни тела како што се Европската унија и НАТО. Секој случај е посебен, па затоа е неопходно да се посвети посебно внимание и да се согледа фактот дека многу актери учествуваат во нејзина заштита во различни фази и процеси. 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. Како што е очигледно, 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. Може 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. Така, кога зборуваме за заштита на критичната инфраструктура, важно е да се има предвид дека тие се комплексни системи за кои е потребен холистички пристап во разгледувањето на нивното функционирање, 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, како и нивна заштита.

Клучно разбирање на целокупната заштита на државата и општеството од аспект на зачувување на функционирањето на критичната инфраструктура се заснова на „пакетот за заштита“ на сите инфраструктури, како и на секој поединец. Секоја инфраструктура и целата земја ќе бидат најдобро заштитени ако се преиначат патиштата за снабдување и испорака колку што е можно, се создадат и зајакнат алтернативи за критичната инфраструктура и се зајакне нивната отпорност. Потоа, таквите објекти ќе ги заштитиме ако тие се изградат во области каде што постои најмал ризик од поплави, пожари и земјотреси. Исто така, ако се изградат според правилата на професијата и со користење на квалитетни материјали, почитувајќи ги сите стандарди за градба и одржување. Следниот чекор е да се креира комплетна придружна документација и познавање на процесите за да се избегнат застои и домино-ефекти. Исто така, постои и отпор на самиот систем, неговата робусност и висока функционалност кои треба да се земат предвид. Потоа, се поставува прашањето дали критичната инфраструктура ги направила сите потребни процени, анализи и планови кои се бараат со други закони, бидејќи националните закони кои се директно поврзани со прашањето на критичната инфраструктура се само надградба на сè што е претходно направено. Секако дека би било добро ако сопственикот

или менаџерот на критичната инфраструктура ги усогласи и/или подобри неговите бизниси според меѓународните стандарди за бизнис, управување со квалитет, управување со кризи и/или управување со вонредни состојби. Важно е и прашањето дали тие имаат кризен план, план за комуникации во време на криза, дали спроведуваат внатрешни вежби, дали се поврзани со итни служби и слично. Значи, постои цел спектар на потребни и претходно преземени активности преку кои со структурни мерки ние ја избегнуваме и намалуваме ранливоста на критичната инфраструктура. Бидејќи тоа е многу широк спектар на работни места и области на одговорност, приватниот сектор има значајно место во овој опсег.

1. ОРГАНИЗАЦИЈА НА ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Пристапот кон заштитата на критичната инфраструктура треба првенствено да се заснова на анализа на ризик, која треба да утврди кои ризици го загрозуваат работењето на критичната инфраструктура и како да се одговори на нив. Ризикот е функција на веројатноста за даден извор на закани кој покажува одредена потенцијална ранливост и резултатот од влијанието на тој несакан настан. Анализата на ризикот 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. Процесот на процена на ризикот, исто така служи како алатка за донесување одлуки, со тоа што неговите резултати 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.[83] Во рамките на приватниот сектор постојат специјализирани компании кои успешно работат на ова поле, па така постојната соработка помеѓу јавниот и приватниот сектор треба дополнително да се развие за да се овозможи знаењето и вештините од приватниот сектор да бидат достапни за заштита на критичната инфраструктура.

Организацискиот пристап кон имплементацијата на заштитата на критичната инфраструктура во Европската унија и земјите кои се стремат кон полноправно членство е даден во Директивата 2008/114/ЕК за идентификација и утврдување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита (во понатамошниот текст Директива).[84] Воведот во Директивата јасно покажува дека примарната и клучната одговорност за заштита на европските критични инфраструктури паѓа на земјите-членки и сопствениците/операторите на таквите инфраструктури.[85] Овој принцип, исто така, важи и за заштитата на националната критична инфраструктура. Од аспект на соработка помеѓу јавниот и приватниот сектор, уште една одредба од Воведот на Директивата е многу значајна, во која 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 поттикнат целосно вклучување на

[83] Myriam Dunn(2006) *Understanding Critical Information Infrastructures: An Elusive Quest* in: Myriam Dunn and Victor Mauer (eds.) INTERNATIONAL CIIP HANDBOOK 2006, VOL. II, Analyzing issues, Challenges, and Prospects, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf(цитирано 28 мај 2017).

[84] 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 (цитирано 1 мај 2017).

[85] Ibid, Introduction, paragraph 6.

приватниот сектор.[86]

Директивата, исто така наведува дека во организирањето на заштитата на критичната инфраструктура неопходно е 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 релевантни 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.[87] 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 се осигура 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.[88] Ефикасната заштита на критичните инфраструктури бара комуникација, координација и соработка на национално ниво и на ниво на заедницата. 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.[89] 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,

[86] Ibid, Introduction, paragraph 8.

[87] Ibid, Introduction, paragraph 11.

[88] Ibid, Introduction, paragraph 13.

[89] Ibid, Introduction, paragraph 17.

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. Приватниот сектоер е неоспорен актер на овие процеси и на самиот систем во сите негови делови.

2. ИНСТИТУЦИИ КОИ СЕ КОМПЕТЕНТНИ ЗА ЗАШТИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

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

Бидејќи критичната инфраструктура претставува платформа за одржување на развојот на секое општество и држава, соодветно е дека нивото на вклученост на институциите е исто така конзистентно со тоа. Владата на државата е вклучена во системот на заштита на критичната инфраструктура како законодавец кој носи закони и подзаконски акти и има задача да им даде овластување на одредени министерства и/или централни владини тела да бидат координатори на целиот систем и носители на секторските процеси. 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 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.

После владата, следниот најважен актер е координаторот на целиот систем за заштита на критичната инфраструктура. Постојат различни примери и практики за тоа кое тело е соодветно за оваа улога. Во САД оваа функција ја врши Министерството за внатрешна безбедност, во повеќето европски земји функцијата е доделена на министерствата за внатрешни работи. Меѓутоа постојат примери, како оној на Република Словенија, каде Министерството за одбрана ја има таа должност и Република Хрватска, каде таа е доделена на Дирекцијата за национална заштита и спасување (независно тело на централно државно ниво под министерствата). Постојат многу различни решенија и практики, но секоја земја треба сама да го препознае најсоодветниот модел. Координаторот на системот комуницира директно со сите актери на системот, со меѓународните актери, 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 проценка на критичноста и потребата од предложените мерки за управување и заштита на критичната инфраструктура.

Централните органи на државната управа назначени од владата (најчесто релевантните министерства) се оние 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, ние 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 областа 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 енергетски субјекти во вршење на енергетски 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 – одредување 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.

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 заедно со агенциите за спроведување на законот, исто така 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 препозна гореспоменатото и

изјави 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.

3. ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ЈАВНО-ПРИВАТНО ПАРТНЕРСТВО

Во поширока смисла, јавното-приватно партнерство често се дефинира како заедничка иницијатива на јавниот и приватниот сектор каде секој субјект придонесува за специфичните ресурси на системот и учествува во планирањето и донесувањето одлуки.[90] Тоа е токму она кон што треба да се стремат системите на јавно-приватно партнерство на полето на јакнење на отпорноста и заштитата на критичната инфраструктура. Приватниот сектор во западните земји е сопственик (менаџер) на повеќе од 85% на националните критични инфраструктури, па затоа е разбирливо дека приватниот сектор е најдобро запознаен со барањата за критичната инфраструктура – слабости и предности, и мора да биде дел од јакнење на отпорноста и заштитата на критичната инфраструктура. Се зголемува свеста за важноста на заштитата на критичната инфраструктура за секојдневно функционирање на сите современи субјекти, националната безбедност и меѓународната соработка, како и размената на знаење, искуства и најдобри практики помеѓу засегнатите страни (и приватниот и јавниот сектор), затоа што јакнењето на отпорноста и заштитата на системот на критична инфраструктура треба да биде дури и вообичаена практика. Живееме во општество каде зависноста од нормалното функционирање на критичната инфраструктура е дел од нашиот секојдневен живот, но за жал, повеќето граѓани, па и експерти кои не се вклучени директно во оваа и слични теми, не се дури ни свесни за нејзиното постоење. Поради овие факти, неопходно е поголемо инвестирање во сите сегменти на овој клучен процес.

Создавањето соодветен систем за заштита на критичната инфраструктура е многу тешка задача за која било земја, во кој било степен на развој. Заканите стануваат посложени и го загрозуваат функционирањето на инфраструктурите, што е голем предизвик за државата, нејзините тела и оператори. Општо земено, постојат ограничени финансиски и организациски ресурси, а заштитата на критичната инфраструктура обично е еден од последните приоритети за компаниите кои управуваат со критичните инфраструктури. 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. На европско ниво, станува тешко да се најдат и утврдат активности на полето на заштитата на европската критична инфраструктура токму заради таа разлика на пристапи и специфичната организација на државите и правниот поредок. На пример, земјите во Западна Европа повеќе се склони на

[90] За повеќе информации види: White House (1998) *Presidential Decision Directive/NSC-63,* Washington, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm; 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; Heammerli, 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.

пазарните принципи во обезбедување заштита на критичната инфраструктура отколку земјите од Источна и Јужна Европа, каде што, заради поранешниот социјалистички систем, организација на заштитата на сите важни сегменти на државата и општеството се базира на улогата на државата. Во овој контекст, иако во сите споменати држави имаше транзиција, промена во структурата и начините на извршување на безбедносна активност, државата сè уште претставува многу важно и централно место за регулирање на врските во однос на властите и должностите на институциите за регулирање на индивидуалните општествени процеси. Управувањето и обезбедувањето континуитет на критичната инфраструктура, секако, спаѓа меѓу нив. Ќе биде потребно да помине извесно време, пред земјите од Источна и Јужна Европа 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. Воспоставувањето на соодветен систем на јавно-приватно партнерство во областа на заштитата на критичната инфраструктура е тековен процес, кој практично никогаш не завршува. Потребно е да се обезбеди најшироко можно учество на предлози, па ќе биде потребно, покрај обезбедување на соодветно ниво на свест, јасно да се дефинираат надлежностите и одговорностите, исто така на ниво на самите оператори на критичната инфраструктура. Значаен дел од ефикасен систем е заемната доверба помеѓу засегнатите страни, како и размената на информации. Обично постојат две клучни категории 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. Тоа посебно ќе дојде до израз во случаите кога сопственоста поминува во приватни раце и ќе се појават неколку компании во одредена област кои ќе бидат конкурентски во логиката на пазарната економија. Кога станува збор за компании кои се во мнозинска сопственост на државата, тие се првенствено фокусирани на задоволување на тесните политички и економски цели, кои често не се базираат на добро владеење и грижа за континуирано работење на критичната инфраструктура. Исто така, приватните сопственици ја следат главната цел, што се одразува во профитот, а инвестициите во одржувањето и безбедното функционирање на критичната инфраструктура не се една од нивните важни стратегиски цели. Сето ова мора да се земе предвид кога зборуваме за изградба на ефикасен систем за заштита на критичната инфраструктура. Како еден од моделите на соработка помеѓу јавниот и приватниот сектор и потребата за размена на информации, ние може да ги посочиме американскиот пример за Центрите за фузија.[91]

Исто така, неопходено е јавното-приватно 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 – јавното-приватно 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 – насочено кон намалување на критичноста и/или зголемена флексибилност на инфраструктурите, заинтересираните страни од јавното-приватно партнерство треба да ги вклучат ресурсите кои им се на располагање (пр. капитал), како што веќе е наведено во националниот Акт за јавно-приватно партнерство, а

[91] Department of the Homeland Security (2013) *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (цитирано 17 мај 2017).

тоа треба да биде дел од релевантни договори. 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 – ако се појави потреба за институционални промени во процесот на управување со ризик на критичните инфраструктури на ниво на давателот на услуги или тела.
- Реални очекувања – краткорочните планови со ограничени временски рамки резултираат со решенија кои тешко се применуваат. Позначајни институционални промени кои гарантираат квалитет бараат време. Исто така, 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.[92]

4. ПРОГРАМИ И ПРОЦЕДУРИ ЗА РАБОТА

Според наше мислење, приватниот сектор има една од главните улоги за заштита на критичната инфраструктура, која се базира на јавно-приватно партнерство и високо ниво на квалитет и услуга. Приватниот сектор треба да биде признаен како доверлив партнер од страна на надлежен јавен орган и од сопственикот/менаџерот на критичната инфраструктура. Иако на ниво на ЕУ сè уште не постои сеопфатен сет на мерки за регулирање на активностите за заштита на критичната инфраструктура од приватниот сектор, надлежноста, секако, 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. На пример, ISO 22300:2012 содржи поими и дефиниции кои се применуваат во општествената безбедност за да се воспостави заедничко разбирање, така што ќе се користат конзистентни термини. ISO 28000:2007 ги специфицира условите за системот за управување со безбедноста, вклучувајќи ги и оние аспекти кои се од клучно значење за сигурносно обезбедување на синџирот на снабдување. Управувањето со безбедноста е поврзано со многу други аспекти од управувањето на бизнисот. Аспектите ги вклучуваат сите активности контролирани или под влијание на организации кои влијаат на безбедноста на синџирот за снабдување. Овие други аспекти треба да се земат предвид директно, односно каде и кога тие имаат влијание врз управувањето со безбедноста, вклучувајќи го и транспортот на овие стоки долж синџирот на снабдување. ISO 18788:2015 обезбедува рамка за воспоставување, имплементирање, работење, следење, прегледување, одржување и подобрување на управувањето со безбедносни операции. ISO/PAS 28007:2012, бродови и поморска технологија-упатства за приватни компании за поморска безбедност (ПКПБ) кои обезбедуваат вооружен безбедносен персонал во приватна сопственост (ВБППС) на бродовите.

Покрај тоа, постои уште еден документ со многу висок квалитет кој треба да го привлече вниманието на приватниот сектор, но и на јавните институции и на сопствениците на критичните инфраструктури. Тоа е прирачникот „Купување квалитетни приватни безбедносни услуги“, креиран од Конфедерацијата на европски безбедносни служби (КоЕБС) и UNI - Europa[93] со

[92] EU funded project RECIPE (2015) *NATIONAL STANDPOINTS Project - Resilience of Critical Infrastructure Protection in Europe (RECIPE)*, www.recipe2015.eu, (цитирано 23 мај 2017).

[93] UNI – Europa е европска федерација на синдикати за 7 милиони службеници во секторите кои го сочинуваат столбот на економскиот и општествениот живот во Европа.

финансиска поддршка на Европската унија.[94] Овој прирачник се обидува да му ги обезбеди на купувачот неопходните аргументи зошто приватните безбедносни услуги треба да се засноваат на најдобрата вредност, вклучувајќи ги и социјалните критериуми релевантни за секторот. Тој ја покажува клучната важност за дефинирање, идентификување, пребарување и избор на најдобра вредност за приватните безбедносни услуги. Во оваа смисла, прирачникот ги опфаќа сите аспекти на тендерскиот процес. Тој им помага на купувачите да го дефинираат она што го сметаат за квалитет; изготвување на тендерска документација каде се отсликани тие елементи за квалитет; споредување на тендерските поднесоци со практичната алатка развиена како дел од овој прирачник, каде различни понуди можат да бидат оценети во однос на изворно избраните критериуми за квалитет; и конечно евалуација на понудите со користење на избраните критериуми за квалитет и избор на понудата со највисок квалитет до потпишувањето на договорот.

Заштитата на критичната инфраструктура од страна на приватниот сектор е активност која опфаќа заштита на предмети, објекти и различни облици на имот што се врши со физичка и/или техничка заштита. Приватното обезбедување може да го вршат лица и компании кои имаат одобрение од полициската администрација за извршување на овие задачи. Основната функција на заштитата на критичната инфраструктура од страна на приватниот сектор е превентивно дејствување. Приватната заштита претставува најмасивна и најефикасна форма на организација на општеството и поединците во смисла на самоодбрана и во превентивна смисла. Приватниот сектор обезбедува услуги и врши задачи за заштита кои ги покриваат оние области кои не се обезбедени од страна на надлежните државни органи или како дополнување на безбедносните активности што ги вршат државните органи.

Физичката заштита се дефинира како непосредно заштитување и обезбедување на објекти и различни облици на имот на критичната инфраструктура. Според ООН, кога се разгледува физичката заштита на критичната инфраструктура од терористички закани, физичката заштита значи комплексен процес кој треба да го опфати целиот циклус на можен терористички напад. Потребна е соработка во земјата и надвор од неа. Физичката заштита на критичната инфраструктура може да го спречи извршувањето на терористички напади со големо влијание. Неизбежно, некои терористички заговори ќе успеат. Непосредниот одговор може да ги спречи „каскадните“ ефекти што таквите напади честопати ги наметнуваат, вклучувајќи и понатамошни жртви.[95] Важно е да се согледа и разбере дека не постои апсолутна безбедност во заштитата на критичната инфраструктура. Ова не треба да се користи како алиби и однапред утврдено оправдување, туку како разбирање на сложеноста на задачите кои треба да се направат и постојаната потреба за надградба на системот за заштита.

Техничката заштита е збир на акции кои директно или индиректно ја заштитуваат критичната инфраструктура. Таа се врши со технички средства и уреди и системи, со примарна цел за спречување на нелегални дејства насочени кон критичната инфраструктура. Најчесто применети мерки во техничката заштита се: техниките против кражби и фалсификати; заштита од неовластен пристап до заштитени подрачја; заштита од пренесување на експлозивни, јонизирачки и други опасни материи во објекти; заштита од отстранување или оттуѓување на заштитени објекти.

[94] Confederation of European Security Services (CoESS) and UNI - Europa (2014) *Buying quality private security services*, http://www.securebestvalue.org/wp-content/uploads/2014/11/Best-Value-Manual_Final.pdf (cited 13 May 2017).

[95] 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, стр.11 (цитирано 2 јуни 2017).

Техничката заштита се врши во областа на заштитениот објект или во самите заштитени простории. Техничките средства и уреди може да се поврзат на системите за техничка заштита. Системите за техничка заштита треба да се имплементираат, одржуваат и сервисираат во согласност со прописите за условите и начинот на имплементација на техничката заштита. Средствата и уредите за техничка заштита се средства и уреди за физичко спречување на неовластен влез на лица во објект под заштита, од кои некои се: специјални огради; специјални рампи и барикади; врати против кражба; сите видови брави со сериски број или код; посебна градежна конструкција; непробојно стакло и слични конструкции; опрема за складирање, чување и трансфер на вредни објекти и документи (каси, сефови, безбедносни контејнери, итн.); уреди за детекција на метални објекти; рендгентски уреди за контрола на багаж.

Со техничката заштита, како сензорни и алармни системи и видеонадзор, чуварите ја зголемуваат безбедноста на предметите, лицата и имотот. Безбедносните системи може да се поврзат со диспечерски центри, кои добиваат директни информации за можна кражба и испраќаат мобилен безбедносен тим на местото на случување.

6 ГЛАВА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО РЕПУБЛИКА МАКЕДОНИЈА

Република 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 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 Македонија, и тоа: електростопанството, ПТТ сообраќајот, железниците, аеродромите, водоводите и др.
- Одлуката за определување на правните лица кои се должни да имаат приватно обезбедување.[96] 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 запаливи 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.[97]

За да може оперативно, стручно и ефикасно да се заштити критичната инфраструктура

[96] Оваа Одлука е донесена од страна на Владата на Република 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.

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

во Република 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 Македонија. Конкретно, дефинирани се неколку дејности, и тоа:

- енергетиката (производство, пренос и дистрибуција на енергија);
- водоснабдувањето;
- животната средина;
- Македонската радиотелевизија, електронските и печатените медиуми;
- Народната банка на Република Македонија и други правни лица регистрирани за вршење на банкарски работи.[98]

1. ЗАШТИТА И ОБЕЗБЕДУВАЊЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО РЕПУБЛИКА МАКЕДОНИЈА

Заштитата и обезбедувањето на критичната инфраструктура во Република 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 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 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 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;

98 Исто

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

Воздушниот сообраќај во Република 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.[99]

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.[100]

[99] Закон за воздухопловство, „Службен весник на Република Македонија“, Скопје, бр.63/2015

[100] 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, стр.213-214

7 ГЛАВА ПРИМЕРИ ЗА ДОСЕГАШНИ ТЕРОРИСТИЧКИ НАПАДИ ВРЗ КРИТИЧНАТА ИНФРАСТРУКТУРА

Новата ера на тероризмот започна со терористичките напади во САД, продолжи со терористички напади во Мадрид, во Лондон, во Брисел, во Париз, во Манчестер и на други места. Според оценките на експертите, досегашната тактика на војување т.н. „modus operandi" на „Ал каеда" е сменета. Новина е новиот правец на „изборот на целта". Без оглед на мотивите за ваквата промена, секако, значајно е да се нагласи дека целта е насочена кон уништување на одредени делови од критичната инфраструктура или т.н. „меки цели" и да се нанесе голем удар.

Потврда за ова е терористичкиот напад во САД, кога на 11 септември 2001 година припадниците на „Ал каеда" киднапираа 4 комерцијални авиони, со кои ги пренасочија летовите кон нивните цели, и тоа: кон Светскиот трговски центар и кон Пентагон. На ова ќе се надоврзе и фактот што билансот на загинати во Светскиот трговски центар изнесува 2.603 лица, додека пак, бројот на загинати патници во четирите авиони бил 246, а во зградата на Пентагон загинале 125 и уште 24 лица се исчезнати и се сметаат за загинати.[101]

Според оценката на американските стручњаци, во моментот на нападите 16.000 луѓе биле во опасната зона во Светскиот трговски центар. Оттука, позитивен придонес, пред сè се состоел во овозможувањето услови за навремена евакуација и тоа на 92% од нив. Секако, од посебно значење е тоа што овој процент на евакуирани граѓани, влијаеше билансот на загинати да биде помал.

Истовремено, терористичките напади во Њујорк, покрај голем број жртви, предизвикаа и пад на економијата. Според податоците, растот на БДП бил на ниско ниво, односно падот на економијата довел до целосна рецесија.[102]

Имајќи ги предвид општите сознанија од анализата на терористичкиот акт, може да се заклучи дека последователните анализи биле насочени, и тоа:

- кон предизвиците насочени кон цивилите и кон приватниот сектор;
- кон пропустите од непостоење на протокол за спасување од врв на зграда;
- кон планот за заштита од пожар;
- кон службата 911; и
- кон подготвеноста на цивилите за заштита при вакви терористички напади.[103]

Всушност, терористичките напади покажаа отсуство на ефективен владин пристап кон процена на слабостите и подготвеноста за справување со терористичките напади и заштитата на критичната инфраструктура.

Имено, овие терористички напади извршија влијание за брзи промени, и тоа:

Прво, во октомври 2001 година се изготви „ Патриотскиот акт".

Второ, се направи ревизија на Директивата за заштита на критичната инфраструктура во САД, донесена во мај 1998 година.

Трето, се изготви Директива за идентификација, приоретизација и заштита на критичната инфраструктура. Таа се усвои во јуни 2004 година.

[101] Commission Report, 9/11, http://govinfo.library.unt.edu/9/11/report

[102] A Retrospective Assesment, Congressional Research Service: The Ekonomic Effects of 9/11

[103] За овие аспекти пошироко види Commission Report 9/11

Четврто, во 2006 година се донесе Националниот план за заштита на критичната инфраструктура.

Петто, ФЕМА (Federal Emergency Management Agency) претрпе промени и стана дел од Одделот за домашна безбедност (Emergency Preperedness and Response Directorate of Department of Homeland Security).

На 11 март 2004 година е извршен нов терористички напад врз критичната инфраструктура во Мадрид, Шпанија. Според изјавите на официјалните власти, овие напади се извршени од страна на ЕТА и од страна на „Ал каеда".

Овие терористички напади се изведени во серија, и тоа:

- експлозија на два воза на станицата Atocha;
- експлозија на еден воз на станицата El Pozo; и
- експлозија на еден воз на станицата Santa Eugenia.

Според истрагата на власта, се докажа дека не станува збор за самоубиствени напади туку контролирани напади со далечински експлозивни направи.

Конкретно, билансот на загинати е 192 лица, додека пак, бројот на повредени е 1.800 лица, што пак предизвика голема доза на страв, шок и неверување, пред сè поради контроверзностите за вистинските виновници.

На 7 јули 2005 година е извршен нов терористички напад врз критичната инфраструктура во Лондон, Велика Британија.

Овие терористички напади се извршени во три подземни возови и еден двокатен автобус. Билансот на загинати изнесува 56 лица, од кои 4 бомбаши- самоубијци и 700 повредени.

Според оценката на британските стручњаци, при терористичките напади во Лондон се користеле софистицирани средства и експлозивните направи се активирани преку аларм на мобилни телефони, со цел активирањето на експлозиите да се случи во најголемиот сообраќаен метеж и на тој начин да се предизвика максимален број жртви.[104]

Терористичките методи и цели при нападот во Лондон треба да се анализираат од повеќе аспекти.

Според првото стојалиште, планирањето и извршувањето на четирите симултани напади се клучен доказ за идните нови трендови, односно нови „меки цели" во тероризмот.

Според второто стојалиште, тактиката на самоубиствените напади на симултаните повеќекратни напади предизвика дополнителни потешкотии во однос на времето, просторот и ресурсите и тоа во фазата на превенција, во фазата на справувањето и во фазата на посттеристичкото реагирање.

Според третото стојалиште, терористичките напади врз критичната инфраструктура се исклучиво со цел да се постигне шокантен психолошки ефект со голем број цивилни жртви.

Од терористичките напади врз критичната инфраструктура во последните години ќе ги издвоиме терористичките напади во Париз, во Брисел и во Манчестер. На 13 и на 14.11.2015 се изведени терористички напади на шест локации во центарот на Париз, Франција со 129 загинати и 300 повредени. На 22 март 2016 година во Брисел, Белгија е извршен терористички напад врз критичната инфраструктура. Овие терористички напади се извршени на белгискиот аеродром, со активирање на две експлозии. Билансот на загинати е 31 лице и 250 повредени. На 23 мај 2017 година, во Манчестер, Велика Британија и тоа на „Манчестер арена" и на блиската железничка станица се извршени два терористички напади, а билансот на загинати е 19 лица и 59 повредени.

Заклучокот од анализата на некои од досегашните терористички напади врз критичната

[104] US Army Tradoc G2 (2007) Terror Operations: Case Studies in Terrorism, Kansas, p.91-92

инфраструктура може да послужи како пример за појдовна основа во креирање на промени во пристапот за заштита на истата. Новата ера на тероризмот, новата тактика на војување со јасна цел насочена кон уништување на критичната инфраструктура, односно на „меките цели“, бараат и нов пристап кон заштитата на критичната инфраструктура. За таа цел ќе издвоиме неколку приоритети, и тоа:

- креирање на ефективна стратегија за заштита на критичната инфраструктура;
- примена на повеќе модели за рано предупредување;
- успешно превенирање, кое може да придонесе кон намалување на ризиците, што директно ќе влијаат врз зголемувањето на безбедноста на критичната инфраструктура;
- континуирана обука и тренинг на човечките ресурси за справување со напади врз критичната инфраструктура;
- ажурирање или носење на Закон за заштита на критичната инфраструктура, Национална програма за заштита на критичната инфраструктура, Национален план за заштита на критичната инфраструктура и на други документи кои директно или индиректно се поврзани со заштитата на критичната инфраструктура.

ЛИТЕРАТУРА

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.

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

Birkett, D.M., (2017) *Water Critical Infrastructure Security and Its Dependencies*. Journal of Terrorism Research. 8(2), pp.1–21. DOI: http://doi.org/10.15664/jtr.1289 .

Bognar, B., (2009), The process of critical infrastruture protection, AARMS, Budapest.

Brömmelhörster, Jörn; Fabry, Sandra and Wirtz, Nico (2004) *Critical Infrastructure*-Birkett, D.M. (2017) *Water Critical Infrastructure Security and Its Dependencies*. Journal o *Protection: Survey of World-Wide Activities*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.html.

Davidović, D., Kešetović, Ž. Pavičević, O., (2012), *National Critical Infrastructure Protection in Serbia: The Role of Private Security,* Journal of Physical Security; 6(1), 59-72, Argonne National Laboratory, http://jps.anl.gov/Volume6_iss1/Davidovic.pdf.

DCSINT Handbook, (2006), Critical infrastructure threats and terrorism, Kansas, No.1.02, p. 1

Commision of the EU,(2004).

Dunn, Myriam (2006) *Understanding Critical Information Infrastructures: An Elusive Quest* in: Myriam Dunn and Victor Mauer (eds.) INTERNATIONAL CIIP HANDBOOK 2006*,* VOL. II, Analyzing issues, Challenges, and Prospects, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf.

Heammerli, 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.

Keković, Z., (2013), National Critical Infrastructure protection regional perspective, Belgrade.

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 Infr astructures,*InternationalJuornal of Critical Infrastructure, https://www.dropbox.com/s/gvs5jhivvhqd3on/IJCIP-S-14-00008.pdf.

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

Lee, E., (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

Leuven, Van and Laurie, (2011) *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, https://www.researchgate.net/publication/226050430_WaterWastewater_Infrastructure_Security_Threats_and_Vulnerabilities.

Luiijf, Eric and Klaver, Marieke (2015) *Governing Critical ICT: Elements that Require Attention*, http://societalsecurity.net/sites/default/files/document-database/files/2016-03/pdf/3018787-governing-critical-ict-elements-require-attention.pdf.

Marjanović, M. and Nađ, I. (2013) National critical infrastructure protection –regional perspective: Assesment of threats to critical infrastructure facilities from serious and organized crime, Belgrade.

Perinić, J. and Mikac, R., (2014) *Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia*, in: Comprehensive Approach as"Sine Qua Non" for Critical Infrastructure Protection, NATO Science for Peace and Security Series: Information and Communication Security.

Prezelj., I., (2008) Konceptualna opredelitev kritične infrastructure, Fakultet društvene vede, Ljubljana.

Theoharidou, Marianthi; Kandias,Miltiadis and Gritzalis, Dimitris (2012) *Securing Transportation-Critical Infrastructures: Trends and Perspectives*, https://pdfs.semanticscholar.org/5441/f94eb1dbb98f9fa4031c52ef3e476f71050b.pdf .

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.

ИЗВЕШТАИ И ДИРЕКТИВИ

A Retrospective Assessment, Congressional Research Service: The Economic Effects of 9/11

Commission Report 9/11.

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.

Canadian Security Intelligence Service (2017) *Cybersecurity and Critical Infrastructure Protection*, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php, (cited 12 June 2017).

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.

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

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.

Confederation of European Security Services (CoESS) and UNI - Europa (2014) *Buying quality private security services*, http://www.securebestvalue.org/wp-content/uploads/2014/11/Best-Value-Manual_Final.pdf.

Commission Report, 9/11, http://govinfo.library.unt.edu/9/11/report.

Department of the Homeland Security (2007) *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, https://www.hsdl.org/?view&did=474328.

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

European Union Council Directive (2008), On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23/12/2008.

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

European Commission (2005)*Green Paper on the European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576.

European Commission (2006) *European program of Critical Infrastructure Protection,*http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786.

European Commission (2012) *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

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*, https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf.

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

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.

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.

EU funded project RECIPE (2015) *NATIONAL STANDPOINTS Project - Resilience of Critical Infrastructure Protection in Europe (RECIPE)*, www.recipe2015.eu.

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

Green paper on a European Programme for critical infrastructure protection, (2005), Brussels, Annex II.

Government of the Republic of Croatia (2009) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*, http://www.duzs.hr/download.aspx?f=dokumenti/Stranice/PROCJENAUGROZENOSTIREPUBLIKEHRVATSKE.pdf.

Home Office (2009), *National Counterterrorism Strategy*, *Government of the United Kingdom,* http://tna.europarchive.org/20100419081706/http:/security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy-2009?view=Binary.

International Atomic Energy Agency webpage, http://www-pub.iaea.org/books/IAEABooks/Publications_on_Accident_Response.

Ministry of Interior (2011) *Regulation for the Protection of Critical Infrastructure*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf.

National Strategy for Critical Infrastructure Protection (CIP Strategy) of Federal Republic of Germany, 2013

NATO Parliamentary Assembly (2008) *Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures,* **http://www.nato-pa.int/Default.asp?SHORTCUT=1478**.

Office of Homeland Security (2002), *National Strategy for Homeland Security*, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf .

Presidential Policy Directive, (2013) Critical Infrastructure Security and Resilience The White House Office of the Press Secretary, USA.

Public Safety and Emergency Preparedness Canada (2003) *Water, Critical Infrastructure Protection and Emergency Management*, http://publications.gc.ca/collections/collection_2008/ps-sp/PS4-7-2004E.pdf.

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.

Spanish Parliament (2011) *Law 8/2011 by which measures for the Protection of Critical Infrastructure Protection*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf.

TIME (2009) *The Worst Nuclear Disaster*, http://content.time.com/time/photogallery/0,29307,1887705,00.html.

US Army Tradoc G2 (2007) Terror Operations: Case Studies in Terrorism, Kansas.

United States Congress (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA PATRIOT Act),*стр.401, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

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.

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.

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.

White House (1998) *Presidential Decision Directive/NSC-63,* Washington, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm; 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

ЗАКОНИ И ПОДЗАКОНСКИ АКТИ

Закон за воздухопловство, Службен весник на Република Македонија, Скопје, бр.63/2015.

Законот за приватно обезбедување, Службен весник на Република Македонија, Скопје, бр.166/2012.

Законот за изменување и дополнување на Законот за приватно обезбедување, Службен весник на Република Македонија, Скопје, бр.164/2013 .

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