КОН ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА:
СТУДИЈА НА СЛУЧАЈ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

МАРИНА МИТРЕВСКА ▪ ТОНИ МИЛЕСКИ

FRIEDRICH EBERT STIFTUNG

КОН ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА:
СТУДИЈА НА СЛУЧАЈ НА
РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

FRIEDRICH EBERT STIFTUNG

МАРИНА МИТРЕВСКА – ТОНИ МИЛЕСКИ
Редовни професори на Филозофскиот факултет при
Универзитетот „Св. Кирил и Методиј“ во Скопје

КОН ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА:

СТУДИЈА НА СЛУЧАЈ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Скопје, 2022

ЗА ИЗДАВАЧОТ

Фондација „Фридрих Еберт“
Канцеларија Скопје
Бул. „8 Септември“, 2/2-5
1000 Скопје, Северна Македонија

Одговорно лице:
René Schlee, | директор
Тел.: +389 2 3093-181 / -182
www.fes-skopje.org
Контакт:
contact@fes-skopje.org

КОН ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА: СТУДИЈА НА СЛУЧАЈ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Автори:
Проф. д-р Марина Митревска
Проф. д-р Тони Милески

Уредник:
René Schlee

Рецезенти:
Проф. д-р Нано Ружин
Проф. д-р Никола Дујовски

Лектура:
д-р Жанет Ристоска

Компјутерска обработка и печатење:

КОНТУРА
фабрика за дизајн, графички проекти и печатење

Тираж: 150

СОДРЖИНА

3 ГЛАВА

4 ГЛАВА

ЛИСТА НА КРАТЕНКИ

САД – Соединети Американски Држави
АСЕАН – Асоцијација на Југоисточни азиски нации
НАТО – Северноатлантска алијанса
ЕУ – Европска Унија
ЕЕА – акроним од **E**uropean **E**conomic **A**rea, Европска економска заедница
ХЦИ – Хибриден центар за извонредност
NAC – акроним од **N**orth **A**tlantic **C**ouncil, Северноатлантски совет.
5Г – Петта генерација на мобилни телекомуникациски врски
РАНД – акроним од **R**esearch **and D**evelopment, истражување и развој.
CSIS – акроним од **C**enter for **S**trategic and **I**nternational **S**tudies, Центар за стратешки и меѓународни студии
GHG – акроним од **G**reen**h**ouses **G**ases, антропогени емисии на стаклени гасови
ППД – Директива за претседателска политика
ЕУГС – Европска Унија – Глобална стратегија
ООН – Организација на Обединети нации
МИС – Директива за безбедност на мрежите и информациските системи
EADRCC – акроним од **E**uro-**A**tlantic **D**isaster **R**esponse **C**oordination **C**entre, Евроатлантски координативен центар за одговор при катастрофи
РХ – Република Хрватска
СФРЈ – Социјалистичка Федеративна Република Југославија
РС – Република Србија
РЦГ – Република Црна Гора
РСМ – Република Северна Македонија
ИКТ – информациски и комуникациски технологии
КИ – критична инфраструктура
CIP – акроним од Critical Infrastructure Protection, заштита на критична инфраструктура
МО – Министерство за одбрана
МВР – Министерство за внатрешни работи
СОП – Стратегиски одбранбен преглед

PREFACE

During the last decade there is an increased focus on the protection of critical infrastructure. This is simply derived from the understanding that critical infrastructure in any country is at an increased risk.

Coinage of terms like "new wars", "hybrid threats" and "weaponization of everything" illustrate this development, where state and non-state actors alike employ tools to harm civilian infrastructure for profit, influence, or other relative gains over another.

In addition to intentional acts, consequences of climate change, such as the increased frequency of extreme weather events pose additional risks to a state's critical infrastructure that has to be taken into account for its effective protection.

Against this increasingly muddled risk environment, the publication at hand aims to bring clarity to national context of the Republic of North Macedonia for the protection of its critical infrastructure with definitions, concepts, tools, and legislative proposals.

As such, the book is only the latest product of the fruitful cooperation between the Friedrich-Ebert Foundation and the professors from the University of Skopje, Faculty of Philosophy and on-going research of the last three years.

In 2019, just before the Republic of North Macedonia officially became the 30th member of NATO, FES Skopje hosted an international conference on the protection of critical infrastructure[1], where experiences from Western European countries, Croatia and the United States of America were shared and discussed.

1 https://skopje.fes.de/e/critical-infrastructure-concept-and-security-challenges

The fruitful discussions and exchange of experiences there combined with the dedication of professors Marina Mitrevska and Toni Mileski lead to further research that introduced concepts and practices in for the creation of a system for the protection of critical infrastructure in the Republic of North Macedonia. These results were published in "Concepts and Security Challenges of Critical Infrastructure". [2]

Throughout 2021, FES continued to facilitate debate in partnership with the Presidential centre for political education, including multi-disciplinary expert groups that provided a good basis for further development of the policy development to enhance the legislative framework for the protection of critical infrastructure.

"Towards resilience and protection of critical infrastructure: a case study on the Republic of North Macedonia" is a further contribution to the ongoing debate and expert discussion that offers numerous useful ideas and suggestions for a better Macedonian model and a stable system for the protection of critical infrastructure.

Through this publication, the Friedrich-Ebert Foundation is delighted to support this significant contribution to the conceptual definition of the need and possibilities for an effective system for the protection of critical infrastructure, in accordance with international and regional best practices and technical standards, based on requirements and capabilities of the Republic of North Macedonia.

I would like to thank Prof. Mitrevska and Prof.Mileski for their partnership, dedication, persistence and scholarship in shaping the national debate for the protection of critical infrastructure in the Republic of North Macedonia.

René Schlee
Friedrich-Ebert-Stiftung (FES)
Resident Representative for Kosovo and North Macedonia

2 https://library.fes.de/pdf-files/bueros/skopje/15731.pdf

ПРЕДГОВОР

Во последната деценија се забележува зголемен фокус на темата за заштита на критичната инфраструктура. Тоа се случува како последица на зголемениот ризик за критичната инфраструктура во сите земји.

Појавата на термините како "new wars", "hybrid threats" and "weaponization of everything" најдобро го илустрира процесот, каде државните и недржавните чинители користат алатки со кои ѝ нанесуваат штета на цивилната инфраструктура за профит, влијание или други придобивки.

Покрај намерните дејствија, последиците од климатските промени како на пример зголемената фрекфенција на екстремните временски промени, претставуваат дополнителен ризик за критична инфраструктура на државата, кои треба да бидат земени предвид при обезбедување на нејзината ефективна заштита.

Наспроти ова матно и ризично опкружување, оваа публикација има за цел да внесе јасност во националниот контекст на Република Северна Македонија за заштита на нејзината критична инфраструктура со помош на дефиниции, концепти, алатки и законски решенија.

Како таква, оваа публикација е само најнов производ на успешната соработка помеѓу Фондацијата Фридрих Еберт и професорите од Филозофскиот факултет при Универзитот во Скопје и тековните истражувања во последните три години.

Во 2019 година, непосредно пред Република Северна Македонија да стане триесеттата членка на НАТО, ФЕС Скопје ја организираше меѓународната конференција за заштита на

критичната инфраструктура[1], на која беа споделени и дискутирани искуства од западноевропските земји, Хрватска и САД.

Плодната дискусија и размената на искуства во комбинација со посветеноста на професорите Марина Митревска и Тони Милески резултираа со концепти и практики за креирање на систем за заштита на критичната инфраструктура во Република Северна Македонија. Овие резултати беа објавени во книгата " Концепти и безбедносни предизвици на критичната инфраструктура".[2]

Во текот на 2021, ФЕС Скопје продолжи да ја фасцилитира дебатата во соработка со Претседателскиот центар за политичко образование, вклучувајќи мултидисциплинарна експертска група која понуди добра основа за понатамошен развој во креирањето на политики и покрена иницијатива за креирање на законска рамка за заштита на критичната инфраструктура.

"Кон отпорност и заштита на критичната инфраструктура: студија на случај на Република Северна Македонија" на авторите проф.Марина Митревска и проф.Тони Милески претставува дополнителен придонес кон постоечката дебата и експертска дискусија, кој нуди низа корисни идеи и сугестии за подобар модел и стабилен систем за заштита ан критичната инфраструктура во земјата.

Преку оваа публикација, ФЕС Скопје со задоволство го поддржува овој значаен придонес кон концептуалната дефиниција на потребата и можностите за ефективен систем за заштита на критичната инфраструктура во согласност со меѓународните и регионалните добри практики и технички стандарди, основано на потребите и можностите на Република Северна Македонија.

1 https://skopje.fes.de/e/critical-infrastructure-concept-and-security-challenges

2 https://library.fes.de/pdf-files/bueros/skopje/15731.pdf

Би сакале да се заблагодариме на проф. Марина Митревска и проф. Тони Милески за нивната соработка, посветеност и упорност во покренување на националната дебата за заштита на критичната инфраструктура во Република Северна Македонија.

René Schlee

Фондација Фридрих Еберт (ФЕС)

Директор на канцелариите во Северна Македонија и Косово

ВОВЕД

Идејата да напишеме втора книга посветена на критичната инфраструктура насловена *„Кон отпорност и заштита на критичната инфраструктура: студија на случај на Република Северна Македонија“* претставува продолжување на ентузијазмот и научниот предизвик да придонесеме за нашата татковина со еден мал и скромен придонес кон иницирање на потребата од нормативно уредување на оваа област.

Она што на самиот почеток треба да се нагласи е дека зајакнувањето на отпорноста и заштитата на критичната инфраструктура од сите видови закани во последните години влегува во сите сфери на безбедносните политики на бројни држави, акцентирајќи ја важноста на критичната инфраструктура како едно приоритетно безбедносно прашање. Без двоумење, анализата покажува дека критичната инфраструктура најмногу се проучува од аспект на националната безбедност, но во последните години интересот за отпорност и заштита на критичната инфраструктура се шири и од страна на Европската Унија и НАТО Алијансата. Кога на ова ќе се надоврзе и фактот дека поширокатa општествена заедница се соочува со комплексно безбедносно опкружување изложено на бројни закани, станува јасно зошто се иницираат потребни и значителни ангажмани на сите општествени актери, кои индиректно или директно се инволвирани во процесот на заштитата на критичната инфраструктура. Оттаму, оправдано произлегува и потребата од заштитата на критичната инфраструктура, каде што неопходно е да се опфатат активности насочени кон подобрување на општествената отпорност и еластичноста на системите, на објектите и на мрежите, а пред сè, ова прашање е потребно нормативно да се регулира и во нашата држава.

Република Северна Македонија е последната 30-та земја членка која се приклучи на НАТО. Придобивките од членството треба да се гледаат низ призмата на гаранциите за зголемена безбедност, со капацитетите на нашата армија и другите безбедносни актери, кои изградија ресурси, искуство и процедури компатибилни и достојни партнери со другите земји членки на НАТО. Во контекст на анализата, важно е да се напомене дека после Варшавскиот самит во 2016 година, прашањето за критичната инфраструктура и нејзината отпорност е повеќе акцентирано во сите НАТО документи. Конкретно, тоа значи дека се дефинирани клучни области според кои НАТО ќе ја цени отпорноста во секоја земја членка. Или пак, преку документите НАТО се поставува како актер кој е подготвен да придонесе кон континуитет во владеењето и испораката на основните услуги - „continuity of government“, и тоа во широка смисла, од енергија, транспорт, комуникации и др. Од овој аспект, од особено значење е да се посочи дека НАТО и сојузниците, вклучително и ние, мора да ја регулираме отпорноста на критичната инфраструктура.

Додека пак, за членството во Европската Унија, Северна Македонија, по кандидатскиот статус (2005), од 2009 година континуирано добива позитивни извештаи и препораки од Европската комисија за почеток на преговори. Денес, иако прашањето за почеток на преговори е отворено, Северна Македонија продолжува да ја гради државата според европските стандарди, бидејќи Европската Унија е еден од најатрактивните економски, политички и меѓународен феномен и е фундаментален елемент на безбедносната архитектура на европскиот простор. Формирана како мировен проект, денес има изградено специфичен пристап и различити капацитети за справување со предизвиците на 21 век. Досегашните искуства покажуваат дека еден од предизвиците за Европската Унија е и нејзиниот пристап во заштитата на критичната инфраструктура, барајќи го своето место и улога во оваа област, настојувајќи да ја промовира важноста на ова прашање, да обезбеди соработка меѓу земјите членки, да ја забрза размената на знаење и искуства и да ги насочува земјите членки

во нивните напори за развој на критичната инфраструктура. Овој пристап треба да биде иницијален и за земјите кандидати за членство во Европската Унија, како што е случајот со Република Северна Македонија. Секако, тоа треба да биде првиот импетус и бидејќи предизвиците на ниво на Република Северна Македонија во однос на оваа област се повеќеслојни и нивното решавање оди бавно, јасна е потребата од создавање свој идентитет во оваа област, но секако дека притоа ќе биде корисно ако се тргне и од позитивните искуства на некои земји членки на Европската Унија, како на пример Република Хрватска. Или пак, во тој процес да се тргне од искуствата на некои земји, пример Србија и Црна Гора кои се аспиранти за членство во Европската Унија.

Во овој труд ќе ги опишеме актуелните состојби во Северна Македонија поврзани со иницијативата за развивање на систем за заштита на критичната инфраструктура. Во однос на описот на состојбата во Северна Македонија и што треба да се прави, постои основна позиција според која целокупната заштита на државата од аспект на зачувување на функционирањето на критичната инфраструктура мора да се заснова на „пакетот за заштита“ на инфраструктурата. За да се дојде до тоа, потребна е анализа на отворени прашања и предизвици со кои се соочува Северна Македонија. Овој пат, анализата треба да доведе до иницијатива за нормативни решенија. До денес, Северна Македонија презеде и реализира голем дел стратешки и нормативни активности кои ја акцентираат важноста на критичната инфраструктура и потребата од нејзина адекватна заштита. Особено е значајно да се забележи дека детерминирањето на критичната инфраструктура во Северна Македонија не е во согласност со насоките за нормативно регулирање на прашањата од сферата на идентификација, означување и заштита на европската критична инфраструктура, со посебен акцент на обврските произлезени од директивата на Советот на ЕУ 2008/114/ЕК за идентификација и означување на европската критична инфраструктура, како и проценатa од потребата за подобрување на нејзината заштита – Директива на Советот на ЕУ 2008/114/ЕК.

Имајќи го сето ова предвид, книгата е фокусирана на четири главни линии.

Во рамките на првата линија се разгледани прашањата кои произлегуваат од динамиката на современата меѓународна сцена. Драматичните промени во последните години алудираат на алармантност и итност во поглед на подобрување на системите за заштита на критичната инфраструктура. Интензитетот на конвенционалните вооружени судири, природните катастрофи, хибридните закани и хибридното војување, здравствената криза, енергетската криза и климатските промени претставуваат јасни индикатори дека нарушувањето на функционирањето на критичната инфраструктура не е прашање кога евентуално ќе ескалира туку е прашање на време кога тоа ќе се случи.

Овие сознанија предупредуваат и налагаат ургентна реакција на повиканите национални институции да преземат конкретни чекори. Тоа значи во прв ред, дефинирање и јакнење на општествената отпорност, заштитата на критичната инфраструктура преку изградба на систем и евентуална имплементација на концептот на еластичност на системите, мрежите и објектите од критичната инфраструктура. Во оваа глава, авторите, посебно место ќе издвојат за анализа на современите предизвици за критичната инфраструктура од аспект на современите геополитички трендови, заканите од тероризам, хакерските напади и другите хибридните закани, новите и подривачки технологии и климатските промени.

Втората линија на овој труд се фокусира на концептот на општествена отпорност. Сведоци сме дека секојдневните манифестации на природните и човечките опасности може да резултираат со значителна штета и нарушување на заедниците, вклучително и нивните згради, инфраструктурните системи, на економијата и достапноста на социјалните услуги. Тргнувајќи од овие констатации, концептот на отпорност на заедницата, кој вклучува планирање за отпор, апсорбирање и брзо закрепнување од нарушувачките настани, се стекна

со актуелност во последната деценија низ целиот свет. Во тој контекст, пошироко се елаборира местото и улогата на отпорноста во рамките на Европската Унија и стратегиските рамки на НАТО. Односно, како придодадена вредност на веќе воспоставените нормативни рамки олицетворени во постојната Директива од 2008 година, но и предлогот за нејзина ревизија која ќе треба да кооптира нови научени лекции, меѓу другото, и со концептот на отпорност.

Третата линија на овој труд е фокусирана на компаративна анализа на пристапот во креирање на систем за заштита на критичната инфраструктура: случај Хрватска, Србија, Црна Гора и Северна Македонија. Изборот за анализа е направен од аспект на безбедноста, каде што Хрватска, Северна Македонија, Србија и Црна Гора имаат исто безбедносно опкружување, ранливоста на регионот и степенот на порозност. Од аспект на тековниот развој на оваа област во Република Хрватска, во Република Србија и во Република Црна Гора, каде што сите три држави имаат донесено Закон за критична инфраструктура. Од аспект на национален пристап, кон утврдување на критериуми за процена на критичната инфраструктура. Затоа, основна задача на оваа анализа е преку овие примери да го проучи тековниот развој на оваа област, посветено внимание на стратешки и нормативни документи, заокружена законска рамка со која го започнаа процесот на изградба на систем за заштита на критичната инфраструктура. Примери кои треба да ги следи и Северна Македонија бидејќи во моментов не располага со систем за заштита на критичната инфраструктура и усвоен закон за критична инфраструктура, а оваа област се регулира парцијално во неколку законски и стратегиски акти. Токму затоа, овој труд нуди поинаква призма на анализа, создавајќи услови за целисходно решение во креирање на закон и систем за заштита на критичната инфраструктура во нашата држава Северна Македонија.

Четвртата линија на овој труд е фокусирана на националниот пристап во заштитата на критичната инфраструктура во

Република Северна Македонија. Согледувајќи ја реалната состојба преку анализа на стратегиски и нормативни документи, авторите констатираат дека Северна Македонија на патот кон изградбата на системот за заштита на критичната инфраструктура поминува низ две фази. Првата фаза е периодот до влегувањето на државата во НАТО и втората фаза која опфаќа активности насочени кон воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура за подготовка на Закон за критична инфраструктура. Во продолжение се објаснува суштински, преку можен модел, што и како треба да се прави за да се „обликува" сферата на критичната инфраструктура. Притоа, се следат современите пристапи на државите од ЕУ и НАТО и се апострофира општествената отпорност, заштитата на критичната инфраструктура и еластичноста на системите, мрежите, објекти и деловите од објекти. Концептот за еластичност на критичната инфраструктура претставува автентична и оригинална замисла на авторите и се однесува на времето од нарушувањето или прекинувањето на функционирање на системите, мрежите или објектите од критичната инфраструктура до моментот на нивно повторно ставање во функција и опоравување.

Им изразуваме благодарност на рецензентите ***Нано Ружин***, **Professor Emeritus** и *редовен универзитетски професор на Филозофскиот факултет, УКИМ, од 1987 до 2011 година, амбасадор во НАТО од 2001 до 2008 година и ректор на Првиот приватен универзитет ФОН* и ***Никола Дујовски***, *редовен професор и декан на Факултетот за безбедност при Универзитетот „Св. Климент Охридски"*, кои ни укажаа чест со прифаќањето да бидат рецензенти на овој труд, за нивната стручна, академска и искрена поддршка за објавувањето на оваа книга.

Изразуваме голема благодарност на Фондацијата „Фридрих Еберт"-Скопје, за континуираната соработка, за поддршка на овој проект и публикувањето на оваа книга.

Авторите и натаму остануваат благодарни за сите добронамерни сугестии, што ќе ги имаме предвид во следните наши академски чекори.

Скопје, јуни 2022 година Од авторите

1 ГЛАВА

СВЕТСКИ ГЕОПОЛИТИЧКИ ПЕЈЗАЖ: ПРОМЕНЕТАТА ПРИРОДА НА БЕЗБЕДНОСТА

Во Република Северна Македонија, во последните пет години забележан е значителен напредок во придвижувањето на националниот ангажман и пристап кон имплементација на концептот за заштита на критичната инфраструктура. Република Северна Македонија, можеби последна во регионот, има неодложна потреба од нормативно регулирање на сите аспекти од сферата на критичната инфраструктура. Динамичните процеси на меѓународната сцена, со право, даваат сигнали во насока на суштинска потреба од заштита на критичната инфраструктура. Војните, елементарните непогоди, хибридните закани, здравствената криза, енергетската криза, климатските промени и мноштво други неповолни процеси, алудираат на констатацијата дека нарушувањето на функционирањето на критичната инфраструктура не е прашање кога евентуално ќе ескалира туку е прашање на време кога тоа ќе се случи.

Ваквите претпоставки алармираат и налагаат ургентна реакција на повиканите национални институции да преземат конкретни чекори. Тоа, во прв ред значи дефинирање и јакнење на општествената отпорност, заштита на критичната инфраструктура преку изградба на систем и евентуална имплементација на концептот на еластичност на критичната инфраструктура. Во оваа глава, авторите, посебно место ќе издвојат за анализа на современите предизвици за критичната инфраструктура и за Република Северна Македонија од аспект на геополитиката, заканите од тероризам, хакерските напади и другите хибридните закани, новите и подривачки технологии, климатските промени и безбедноста.

1.1. Геополитички аспекти

Слободно можеме да констатираме дека светот доживува пресвртна фаза во втората деценија на 21 век, обележана со геополитичка и економска промена на моќта од Запад кон евро-азиските сили. Сегашниот период на површината носи различни геополитички и геостратешки предизвици, кои секако се поспецифични за справување од оние во 20 век. Овие предизвици се во форма на политичка конфронтација, внатрешни и меѓународно-политички вооружени конфликти, конфликт околу природните ресурси во земјите зафатени од граѓански војни низ регионите на Супсахарска Африка, Латинска Америка, Блискиот Исток, а исто така и во новоистражените стратешки региони како што е Арктикот. Прогресивниот раст на светското население кое брзо се шири се соочува со циклични флуктуации на цените на храната како резултат на климатските промени, економските конфликти, порастот на верскиот фундаментализам, а исто така и фрагментацијата на политичката карта на светот.

Овој последно наведен аспект носи не само пораст на сецесионистичките движења, кршење на територијалниот

интегритет како основен принцип на меѓународната заедница, туку и редефинирање на една од клучните карактеристики на суверената држава, имено меѓународното признавање. Косово, Јужна Осетија, Јужен Судан, Доњецка и Луганска народна република во Украина, се приказни кои можеме да ги наведеме за примери на овој современ тренд што се појавува.

Со право сме исправени пред дилемата дали 21 век ќе биде дефиниран со ривалства меѓу националните (супер) сили, а не со надмоќта на колективните системи или преклопувачките суверенитети, заменувајќи ги суверените држави како што очекуваат теоретичарите и заговарачите на Новиот среден век. Која ќе биде доминантна сила во мултиполарниот свет – САД, кои брзо слабеат, од една страна, или уште посигурната Кина, која се стреми да го врати статусот на најсилната економија во светот (Riegl, M., Landovský, J., 2013).

Повеќе автори, Маркус Корнпробст, Томас Пол, Шамита Гарг, Сушил и други, почнуваат да укажуваат на растечкиот тренд на деглобализацијата. Корнпробст и Пол нагласуваат дека со децении глобализацијата и либералниот меѓународен поредок еволуираат рамо до рамо. Но, констатираат дека од неодамна силите на деглобализацијата се во пораст, а либералниот меѓународен поредок станува сè повеќе изолиран. Во нивниот труд „Глобализацијата, деглобализацијата и либералниот меѓународен поредок“ ги анализираат процесите на глобализацијата и деглобализацијата, нивната испреплетеност со либералниот меѓународен поредок во минатото и сегашноста и констатираат дека разликите веројатно ќе влијаат на иднината на светската политика. Со овие претпоставки, авторите пробиваат нов терен за проучување на иднината на меѓународните односи и најавуваат нови сознанија за епохални промени (Kornprobst, M., Paul T. V., 2021).

Гарг и Сушил констатираат дека светот се движи кон ерата на деглобализацијата, а индустријализираните економии (базирани на активности кои ги комбинираат факторите на производство: објекти, набавки, работа, знаење) го означиле

незјиниот почеток. Авторите потенцираат дека од крајот на 2000-те, силите на деглобализацијата стануваат сè посилни. Одредени автори, од економисти до социолизи, сега дури тврдат дека рамнотежата се навалува повеќе кон деглобализацијата отколку кон глобализацијата – или барем дека тоа ќе се случи наскоро. Се анализира и поставува аналогија помеѓу големата депресија од 1930-тите која ја нерекуваат „деглобализација 1.0“ и големата рецесија од 2007-2009 година наречена „деглобализација 2.0“. Во нивниот труд „Детерминанти на деглобализацијата: хиерархиски модел за истражување на нивните меѓусебни односи како канал на политиката“ издвојуваат дека социолозите го користат терминот деглобализација или на аналитички или на нормативен начин. Деглобализацијата е поткрепена со културни интерпретации на себеси наспроти другите. Исто така, забележлив е позитивен спин на деглобализацијата. Односно, се постулира нова светска економија која е вградена во општеството. Наместо да биде управувана од „логиката на корпоративната профитабилност“, таа обезбедува правична распределба на приходот. Повеќе не постојат транснационални корпорации или глобални организации (Garg, Sh., Sushil., 2021).

Овие глобални трендови го креираат светскиот геополитички пејзаж. Дефинитивно, светот во втората деценија од 21 век бележи редефинирање на геополитичките обрасци и принципи. Очигледно е дека еуфоријата од крајот на Студената војна, наведена во концептот на Френсис Фукујама за крајот на историјата, беше прерана и дека геополитиката на 21 век нема да биде дефинирана со судирот на цивилизациите од 21 век. Европа е таа која, за жал, ги отсликува геополитичките прекршувања на политичката карта. Картата на Европа го дефинира 21 век. Од полињата на Фландрија (Прва светска војна) до плажата Омаха (Втора светска војна), од Берлинскиот ѕид до изгорените села во Босна и Херцеговина, на Косово, Србија и Македонија, од долгата европска војна која траеше од 1914 до 1989, до актуелните крвави воени афтершокови во Украина, Европа е центар на светската геополитика и историја (Riegl, M., 2013).

Геополитичкото преместување на моќта од евроатлантскиот кон азискиот и Азископацифичкиот регион (особено од САД кон Кина) очигледно продолжува и е потврдено од геополитички аналитичари како Нај, Бжежински и Каплан.

Јосеф Нај индентификува пет главни глобални предизвици (вклучително и можните реакции) како одговор на повеќето песимистички проекции на американскиот пад и неизбежниот пораст на економската и геополитичката доминација на Кина.

Предизвиците ги споменува во контекст на промовирањето на американската стратегија за паметна моќ, во неговата книга „Future od Power". Опишувајќи ги силата и ограничувањата на американската моќ, Нај објаснува дека стратегијата за паметна моќ бара надминување на старите разлики помеѓу либералните и реалистичките потреби, овозможувајќи простор за една нова синтеза која може да се нарече либерален реализам. Во контекстот на паметната моќ не е создавање на империја или хегемонија. САД може да влијаат, но не и да ги контролираат сите делови од светот. Моќта зависи од конкретниот контекст и контекстот на транснационалните релации (климатски промени, нелегална трговија со дрога, пандемии и тероризам) и таа е дифузна и хаотично распределена. Воената моќ има мала улога во решавањето и одговорот на новонастанатите закани. Одговорот на овие закани бара повеќе соработка со владини и меѓународни институции. Нај, исто така потенцира дека либерално реалистичката стратегија го нагласува значењето на развојот на интегрирана „голема" стратегија која ќе ја комбинира тврдата моќ со меката моќ во паметна моќ. Во борбата со тероризмот, САД треба да применуваат тврда моќ против тврдокорните терористи, но не може да се очекува победа додека не се победи во срцата и умовите на муслиманите. Понатаму, целта на либерално реалистичката стратегија е да овозможи безбедност на САД и нивните сојузнички, одржувајќи силна домашна и меѓународна економија, одбегнување еколошки катастрофи и јакнење на либералната демократија и човековите права дома и надвор.

Оваа нова стратегија на Нај е предизвикана од пет главни предизвици. Прв предизвик, пресекување на тероризмот со нуклеарни материјали. Ова ќе бара политики за спротивставување на тероризмот, создавање на стабилност на Блискиот Исток, давање соодветно внимание на пропаднатите држави и сл. Втор предизвик, политички ислам. Актуелната борба против радикалниот ислам, според Нај, не е „судир на цивилизации" туку граѓанска војна во рамките на исламот. Поотворена трговија, економски раст, образование, развој на институциите на граѓанското општество и постепено зголемување на политичкото учество. Трет предизвик, подем на непријателски хегемон како што Азија постепено го враќа делот од светската економија. Овој предизвик бара политика која ја поздравува Кина како одговорен и значаен субјект, но штити од можно непријателство од одржување блиски односи со Јапонија, Индија и други земји во Азија кои го поздравуваат американското присуство. Четврт предизвик, економска депресија. Стратегискиот одговор на овој предизвик ќе бара политики кои постепено ќе ја намалуваат американската зависност од нафта, особено од Персискиот Залив каде се наоѓаат 2/3 од светските резерви на нафта. Петти предизвик, еколошки кризи како што се пандемии или негативни климатски промени. Овој предизвик бара внимателни енергетски политики, лидерство во сферата на климатските промени и поголема соработка во рамките на меѓународните институции. (Nye, J.S., 2011: 231-233).

Збигњев Бжежински во неговата книга „Стратешка визија: Америка и кризата на глобалната моќ" се обидува да одговори на четири големи дилеми.

1) Кои се импликациите од променливата распределба на глобалната моќ од Запад кон Исток.

2) Зошто глобалната привлечност на Америка слабее, кои се симптомите на домашното и меѓународното опаѓање на Америка и која геополитичка преориентација е неопходна за ревитализација на светската улога на Америка.

3) Кои би биле веројатните геополитички последици доколку Америка се откаже од својата глобално истакната позиција, кои би биле речиси непосредните геополитички жртви на таквото опаѓање, какви ефекти би имало тоа врз проблемите на глобално ниво во 21 век, и дали Кина може да ја преземе централната улога на Америка во светските работи до 2025 година.

4) Гледајќи по 2025 година, како би требало Америка која воскреснува да ги дефинира своите долгорочни геополитички цели и како може Америка, со своите традиционални европски сојузници, да се обидува да ги ангажира Турција и Русија за да изградат рамномерен поголем и поенергичен Запад?

Бжежински понуди стратешка визија за т.н. „Поголем Запад“, кој се протега од Ванкувер до Владивосток, и кој соработува со Истокот. Поголемиот Запад ќе ги вклучи Турција и Русија кои брзо се развиваат. Двете држави ќе бидат интегрирани во евроатлантскиот институционален дизајн, кој ќе се протега од Ванкувер до Владивосток на Далечниот Исток.

Крајната цел на поголемиот и витален Запад, во тесна соработка со Европа, мора да биде придружена со стратегијата на стабилен и кооперативен Исток. Успехот на оваа стратегија лежи во успешното модерирање на кинеските геополитички грижи, кои се следните:

1) Намалување на опасностите својствени за потенцијалното географско опкружување на Кина, поради: безбедносните врски на САД со Јапонија, Јужна Кореја и Филипините, ранливоста на спречување на поморскиот пристап на Кина во Индискиот Океан преку теснецот Малака и оттаму на Блискиот исток, Африка, Европа...

2) Да воспостави за себе фаворизирана позиција во новоазиската заедница во подем и исто така во веќе постојната АСЕАН.

3) Да го консолидира Пакистан како противтежа на Индија.

4) Да добие значајна предност пред Русија во економското влијание во Централна Азија и Монголија, со што делумно ги задоволува кинеските потреби за природни ресурси, исто така, во области поблиску до Кина отколку Африка или Латинска Америка. Да се реши во корист на Кина преостанатото нерешено наследство од граѓанската војна – Тајван.

5) Да воспостави за себе фаворизирано економско и индиректно политичко присуство во голем број земји од Блискиот Исток, Африка и Латинска Америка (Brzezinski, Z., 2012).

Сепак, геополитичката битка на моќта ќе се води во политички географски простор различен од минатиот век. Европа престана да биде фокус на геополитичко и геостратешко разгледување на клучните актери. Роберт Каплан предвидува дека битката ќе се префрли од европското крајбрежје кон исток.

Според Каплан, големиот Индиски Океан, кој се протега на исток од Рогот на Африка покрај Арапскиот Полуостров, Иранската Висорамнина и Индискиот Потконтинент, сè до Индонезискиот Архипелаг и пошироко, може да биде иконска карта за новиот век како што беше Европа до последниот. Можеме да го лоцираме напнатиот дијалог меѓу западните и исламските цивилизации, ганглиите на глобалните енергетски патишта и тивката, навидум незапирлива доминација на Индија и Кина над копното и морето (Kaplan, R., D. 2010).

Од друга страна, геополитичкиот проект за евроазиство, односно неоевроазиство, претставува процес кој се одвива и пулсира од истокот на светот. Првенствено насочен кон оспорување на американската хегемонија во процесот на одлучување за одредени светски политички процеси. Постојат неколку типови на неоевроазиството. Првиот тип претставува повеќедимензионална идеологија формулирана од одредени политички кругови

на опозицијата во Русија кои се противеле на либералните реформи во периодот од 1990 до 1994 година. Неоевроазиството е засновано на идеите на Савицки, Вернадски, кнезот Трубецки и идеологот на рускиот националболшевизам Николај Устрјалов. Анализата на историските Евроазијци е прифатена како актуелна и апликатибилна во рамките на современите геополитички случувања. Тезата за националната идеократија со империјални континентални размери истовремено парира на западниот либерализам, но и на тесноетничкиот национализам. Русија се набљудува како темел на геополитичкиот „голем простор" и нејзината етничка мисија претставува изградба на Империја. Советскиот период од историјата на Русија се набљудува како модернистички облик на традиционалниот руски национален стремеж кон планетарна експанзија и како што напоменува Александар Дугин, „евроазиски антиатлантистички универзализам". Во рамките на неоевроазиството интензивно и темелно се проучуваат европските континенталистички проекти со што хоризонтите на евроазиското учење се отвораат и кон Европа апсолвирана како потенцијална континентална сила (Дугин, А., 2004: 139).

Втора карактеристика на неоевроазиството е изборот на исламските држави, особено континенталниот Иран за најзначаен стратегиски сојузник. Идејата за континентална руско-исламска алијанса се пронаоѓа во основата на антиатлантистичката стратегија на југозападниот брег од евроазискиот континент. Другите типови на нео-евроазијство претставуваат цел комплекс на идеи со променлива политичка реалност или често пати станува збор само за прагматично економско евроазиство кое се темели на обновување на економската соработка помеѓу поранешните советски простори.

За Александар Дугин и група негови истомисленици, константното акумулирање на моќ по пат на територијално ширење е единственото соодветно однесување во светот во кој вечната борба на геополитичките актери е карактеристика, а особено геополитичката борба на силите кои се ориентирани кон копното и морето (Tsygankov, P., A., 2003: 109)

Каква е суштината на неговите геополитички визии? Интеграцијата на Евроазија или „собирањето на Империјата“ за Дугин претставува мисија во која Русија како земја на Хартленд треба да ја има главната улога. Според Дугин, таквиот тек на настаните е неминовен со оглед на фактот дека контролата над континентот не може да се замисли без контрола над просторот на „географската оска на историјата“. Доколку Русија не успее во оваа мисија, тогаш на површина испливуваат други алтернативни можности како што се: продор на Кина кон север во Казахкстан и источен Сибир или средна Европа ќе тргне кон западните руски земји – Украина, Белорусија. Можни сценарија се и евентуалниот обид на исламскиот свет да ја интегрира Средна Азија, просторот околу реката Волга и Урал, како и одредени територии во јужна Русија. Поврзувањето на Русија, Германија, Јапонија и Иран, Дугин го перцепира како антизападен блок, кој би требало да претставува блок за продорот на Америка кон Европа и Азија (Килибарда, З., 2008: 57). Идејата е создавање мултиполарен свет. Чекори во тој правец се Евроазиската економска унија и Шангајската договорна организација кои треба да бидат опоненти на Европската Унија и НАТО.

Сепак, актуелно на меѓународен план, Москва е повеќе ориентирана на т.н. „стратегиски опортунизам“ во меѓународните односи. Тоа значи преземање на чекори за воспоставување на состојба во која Русија ќе се почитува како респектабилен меѓународен играч, поправање и подобрување на односите со Западот, како и враќање на националната самопочит.

Но, нивните воени интервенции врз позициите на „Исламската држава“ во Сирија, како и воената инвазија во Украина укажуваат и на реалистичкиот приод во решавањето на кризните состојби. Одредени аналитичари потенцираат дека воената интервенција соодветствува на геополитичките теории и концепти од биполарниот светски поредок и постојаниот стремеж на Русија за излез на топли морињa (Медитеран). Сириското пристаниште во градот Тартус е од исклучително значење за Русија (Iglesias L. M., 2014: 137). Овие

состојби се препознаваат после настаните во Грузија од 2008 година кога руската морнарица повторно после Студената војна се враќа во Атлантскиот Океан и Русија покажува посебниот интерес за Сирија, Сомалија, како и за Карипскиот Регион во Куба, Никарагва и Венецуела (De Haas M., 2010: 108).

Настаните во муслиманскиот свет (поддршка од Иран и Сирија) и вооруженият конфликт во Украина, кој во геополитиката е познат и како „мала Русија" (заштита на руското малцинство) се едно од најважните геополитички и безбедносни прашања во врска со ефектуирањето на неоевроазиството. Покрај сите политички, економски и воени последици, тие настани имаат огромна геополитичка важност за идниот глобален геополитички поредок. Можеме да заклучиме дека проектот „изградба на Империјата" најмногу зависи од исходот на тие настани. Евроазиската ориентација е присутна во Русија со векови. Современата ситуација може да ја наведе евроазиската идеја да стане дел од дизајнирањето на големата стратегија на Русија (Mileski, T., 2015).

Сите овие геополитички трендови се испреплетуваат на глобалната геополитичка шаховска табла. Геополитичките играчи настојуваат да го устројат глобалниот геополитички поредок, кој евидентно е дека се наоѓа во транзициски период. Во еден таков период, исполнет со голем набој на конфликтен потенцијал ширум светот, а особено на Блискиот Исток, несомнено, глобалните геополитички трендови ќе ја трансформираат и геополитичката положба на Република Северна Македонија.

1.1.1. Геополитички ризици и сценарија за Република Северна Македонија

На регионално ниво, со дезинтеграцијата на поранешната федерална држава една од стратегиските варијанти и сценарија која може да се препознае заради одржување на долготрајна стабилност на Балканот претставува балансот

на силите на новонастанатите локални политичко-територијални ентитети. Ова, пред сè, подразбира рамнотежа на воените потенцијали со јакнење на слабите и слабеење на големите и нивните просторно површински односи (Tanter, R., Psarouthakis, J., 1999).

Ваквата геостратегиска ориентација овозможува геополитичка трансформација на Балканот, која е актуелна и во моментот на случувањето на мигрантската и бегалска криза. Геополитичката формула за Балканот од периодот на Студената војна беше 2+2+2, односно Грција и Турција – НАТО, Бугарија и Романија – Варшавски договор и Југославија и Албанија – неврзани и неутрални. Денеска таа формула, заснована на тенденцијата за промовирање на теоријата на т.н. „двојни држави" би гласела (1+2) x 6: српскиот народ е конститутивен народ во Србија и Република Српска: хрватскиот народ е конститутивен народ во Хрватска и босанско-херцеговскиот дел од Федерацијата БиХ, албанскиот народ е конститутивен народ во Албанија и Косово, романскиот народ е конститутивен народ во Романија – Молдавија, турскиот народ е конститутивен народ во Турција – Северен Кипар и обидот за туркање на Македонија кон Бугарија. Ова резултира, како што Франциско Веига сугерира, со формирање на една од најкомплексните карти на Балканот во неговата историја (Veiga, F., 2003).

Друга битна геополитичка карактеристика на Балканот може да се осознае преку анализата од аспект на геополитиката на конфликтите и конфликтниот потенцијал. Веќе подолго време за Балканот, како и за постсоветскиот геополитички простор се зборува како за подрачја на „замрзнати конфликти". Подрачја во кое вооруженото насилство е завршено со потпишување на одредени мировни договори (Дејтонски, Охридски, Бриселски) со кои засегнатите страни, од време на време, покажуваат јасно незадоволство (Rhodes, M., Lozancic, D., 2010).

Во една таква геополитичка констелација на Западен Балкан и од перспектива на Северна Македонија, се добива впечаток дека регионот и државата се претворени во

геополитичка лабораторија. Во таа лабораторија геополитичките експерименти наоѓаат апликативна примена креирајќи го геополитичкиот пејзаж во регионот на Западен Балкан. Доколку се осврнеме само на политиките за проширување на ЕУ, последните настани алудираат на тоа дека Северна Македонија мора да прифати сè, најмногу на нејзина штета, за да зачекори на европскиот пат. Нешто што не е предвидено во основните насоки и предуслови за членство во ЕУ. Оттука, ќе посочиме неколку можни сценарија за да донесеме издржани заклучоци и прогнози за тоа што ја чека Северна Македонија на патот на процесот на проширување.

Сценарио 1: Европската Унија се движи од принципот на едногласност кон квалификувано мнозинство во одлучувањето при проширувањето. На овој начин, доколку Северна Македонија почне да се реформира со значителни резултати, тоа ќе биде добар аргумент за земјите членки на ЕУ за капацитетот на земјата да ги исполни барањата предвидени во новата методологија за проширување. Процесот кон ЕУ за Северна Македонија ќе биде отворен, со квалификувано мнозинство.

Сценарио 2: Членство во Европската економска заедница (ЕЕА), заради економска корист, но без политичко единство. Долга пауза во процесот на проширување барем до 2030 година, а во меѓувреме зајакнувањето на европската политика на соседство која не вклучува пристапување, понуди привилегирани партнерства.

Сценарио 3: Без сериозни напори на ЕУ за интегрирање на Западен Балкан, регионот се движи кон кинеска хегемонија и можеби руска дестабилизација. Пандемијата и кризата на американската демократија ни покажаа

дека Западот не се обновува демократски. Различната анализа ја покажува можната транзиција кон барем бинарна американско-кинеска хегемонија и кинеска хегемонија на долг рок.

Сценарио 4: Стагнација на процесот на проширување и ставање на балканските земји во неизвесност, со опција за „мини-шенген" зона.

Сценарио 5: Враќањето на американската дипломатија на Балканот, помогнато од германската дипломатија или враќање на таканаречената „булдожер дипломатија" за затворање на отворените спорови на Балканот, но со можни негативни ефекти, долгорочно, по ЕУ проектот (Mileski, T., Klimoska, K., 2021).

1.2. Хибридни закани

Во 21 век, хибридните закани стануваат доминантен безбедносен предизвик за западните држави. Нивното појавување ја одразува значајната промена во природата на меѓународните односи. Таквата промена, заради сложеноста и двосмисленият карактер на хибридните закани, има тенденција да го зголеми чувството на несигурност и историски гледано, да ги зголеми несогласувањата во општествата. Некои луѓе, за таквата состојба, бараат одговори во минатото, додека други го забораваат минатото. Постојат и трендови кои заговараат прилагодување кон новонастанатите услови и промените, а има и такви кои се обидуваат да го одбранат т.н. статус кво. Сите овие перцепции укажуваат дека сликата за безбедносната средина не е само црна или само бела. Таа е комплексна, повеќеслојна и повеќедимензионална. Оттука, правилната анализа на она што се променило, како се менува и што значи за демократските држави е во сржта на разбирањето на природата на актуелната безбедносна средина во Европа, но и во светот.

Шест големи промени ги доведуваат хибридните закани во прв план. *Првата* е променливата природа на светскиот поредок. Современите случувања укажуваат дека релационата моќ – тоа е моќта да се сменат туѓите верувања, ставови, преференции, мислења, очекувања, емоции и/или предиспозиции за дејствување – денес е поважна од материјалната моќ. Оваа промена, се користи од големите и средните сили за зголемување на сопствениот меѓународен статус и да се стекнат со одредени придобивки.

Второ, светот гледа нов тип на мрежно-базирана акција или темната страна на глобализацијата. Внатрешните и надворешните димензии на безбедноста се меѓусебно посилно поврзани отколку што тоа беа во последните децении. Улогата на националната држава е доведена во прашање, како и улогата на сојузите со бројните норми и правила кои ги ограничуваат одговорите на асиметричните и антагонистички дејства.

Трето, технологиите кои брзо се развиваат, нивната буквална револуција, предизвикуваат нови домени како сајбер-просторот каде допрва треба да се создадат национални и меѓународни правила на игра. Просторот повеќе не е граница, туку оперативно царство, кое, исто така, претставува предизвик за традиционалното безбедносно размислување. Генерално, новата технологија обезбедува нови алатки за влијание.

Конкретно, променливиот домен на информацискиот простор и медиумскиот пејзаж е *четвртата* голема промена што влијае на денешната безбедносна средина. Дигитализацијата и социјалните медиуми како нови создавачи на мислење ја променија брзината со која патуваат информациите, начинот на кој се произведуваат информациите и начинот на кој луѓето се поврзуваат преку националните граници. Оваа промена ја поттикна потребата да се разберат различните политички и стратешки култури бидејќи информациите произведени во една земја може да се толкуваат на други, многу различни начини на друго место. Исто така, чуварите на информации се менуваат. Интернетот стана ново бојно поле каде сè уште се

формулираат правила. Лажните вести, конфузијата на содржината и „фактите“ засновани на одредени мислења ја агитираат јавноста. Довербата која е еден од основните столбови на функционалните општества се повеќе еродира.

Петтата промена е променливата природа на конфликтот и војната. Во денешните војни, војниците не треба да умираат и треба да се избегнуваат цивилни жртви. Оваа констатација доведе до дебата за нејасните линии меѓу војната и мирот. Ситуацијата со нејасните линии меѓу војната и мирот се апострофира и претставува предизвик за традиционалните воени сили, како и за традиционалното внатрешно спроведување на законот. Исто така, поттикнува хибридни закани, кои се обидуваат да останат под отвореният конфликт. Тие сè повеќе наликуваат на натпревари меѓу општествата, а не на армиите.

И на крај, *шестата* промена се однесува на промената на генерациите. Тоа значи дека ја оставивме зад себе Студената војна, па дури и ерата по Студената војна. Студената војна имаше две многу различни карактеристики, кои го оддржуваа многу јасно светскиот поредок: доминираа односите на суперсилите и нивната идеолошка борба меѓу комунизмот и капитализмот, додека стравот од нуклеарна војна бил водилка за многу одлуки поврзани со безбедносните политики. За време на ерата по Студената војна, глобализацијата, нагласувајќи ги идеите за интеграција и меѓузависност, станува модерен начин за опишување на светот. Денешната нова генерација е дигитална генерација информирана од два контрадикторни трендови – космополитизам и неонационализам. Историската меморија се менува и заедно со генерациите, што остава простор за политичко манипулирање со историските настани (Treverton, F., G., 2018).

Вака детерминираната природа на светските промени ги допира сите држави во светот. Но, каков е одговорот кон овие промени и нови хибридни закани. Покрај националната регулатива, земјите членки на ЕУ и на НАТО се отворено повикани

да членуваат во Хибридниот центар за извонредност (ХЦИ). ХЦИ е меѓународна, автономна организација базирана на мрежа која промовира пристап на целата влада и целото општество за справување со хибридните закани. Официјалната инаугурација на ХЦИ се одржа на 3 октомври 2017 година. Соработката ЕУ-НАТО е клучен предизвик за спротивставување на хибридните закани - и голема можност за активностите на Центарот. ХЦИ треба да служи како центар на експертиза што ќе ги поддржува индивидуалните и колективните напори на учесниците да ги подобрат нивните цивилно-воени способности, отпорност и подготвеност да се спротивстават на хибридните закани со посебен фокус на европската безбедност. Целта е Центарот да го понуди ова колективно искуство и експертиза за доброто на сите учесници, како и на ЕУ и НАТО. Центарот ќе следи сеопфатен, мултинационален, мултидисциплинарен и академски пристап. Целта на ХЦИ е да обезбеди унапредување на заедничкото разбирање на хибридните закани на стратешко ниво и промовирање на развојот на сеопфатен одговор од целата влада на национално ниво и координиран одговор на ниво на ЕУ и НАТО. Седиштето на ХЦИ се наоѓа во Хелсинки, Финска.

Со оглед на краткиот период од воспоставувањето на ХЦИ, сè уште има многу области во кои центарот треба да се фокусира. Вклучувајќи вежби и обуки, спротивставување на мешањето во изборите, одвраќање во опкружување со хибридна закана, заштита на критичната инфраструктура од хибридни закани и концептуално моделирање за хибридни закани. Центарот треба да стане и доверлив партнер за актерите во академската заедница.

НАТО паралелно со ЕУ и во многу случаи заедно со неа, исто така, прави многу во овој контекст. На самитот на НАТО во Варшава во јули 2016 година беше донесена одлука за седумте основни барања за отпорност на НАТО кои веќе ги опишавме претходно. На самитот на НАТО во Брисел во јули 2018 година беше договорено да се формираат т.н. контрахибридни тимови за поддршка. Во однос на одговорот на НАТО на

хибридни закани и дезинформации, тој исто така донесе две важни одлуки: да воспостави стратешки комуникациски способности во седиштето на НАТО и да иницира формирање на Центарот за извонредност на НАТО за стратешки комуникации (Рига). Вежбите за управување со кризи на НАТО почнаа да вклучуваат хибридни сценарија кои опфаќаат дезинформации, закани за критичната инфраструктура и ситуации во „сивата зона" – просторот и времето помеѓу војната и мирот. Исто така, како дел од одговорот на НАТО на хибридните закани, започнати се редовни дискусии на Северноатлантскиот совет (NAC) базирани на хибридни сценарија (Bajarūnas, E., 2020).

1.2.1. Концептите на хибридно војување и хибридна закана

Како се дефинира концептот на хибридно војување и хибридна закана? Одговорот на ова прашање е во суштината на изменетата природа на современото војување и потребата од јакнење на отпорноста и заштитата на критичната инфраструктура. Двата составни делови на хибридното војување се конвенционално и неконвенционално војување. И двата термина „конвенционално" и „неконвенционално" се доволно широки термини, овозможувајќи им на актерите да вградат голем број алатки и можности во нив без прибегнување кон додавање нешто повеќе. Во теоријата, најчесто се среќава дефиниција дека хибридното војување претставува комбинација од повеќекратни конвенционални и неконвенционални алатки за војување. Тие алатки најчесто се: дипломатијата, информациското војување и пропаганда, поддршка за локални немири, нерегуларни сили, специјални сили, редовни воени сили, економско војување и сајбер напади (Najžer, B., 2020).

Франк Хофман ги дефинира хибридните војни како низа различни начини на војување, вклучително и конвенционални способности, нерегуларните тактики и формации, терористичките акти вклучувајќи неселективно насилство и принуда и криминални активности (Hoffman, F. G., 2007: 14).

Оваа дефиниција претставува резултат на новите лекции научени од делувањето на „Хезболах“, како и од конфликтите во Чеченија, Авганистан и Ирак. Ако претходно критиката на дефинициите за хибридни војни главно се засноваа на потпирање на недржавните актери, Хофман ја пласира својата дефиниција велејќи дека хибридните војни можат да бидат спроведени од двете завојувани држави, но и од различни недржавни актери.

Една од најсеопфатните дефиниции за хибридна војна ја нуди Најжер. Имено, тој потенцира дека хибридното војување е посебна форма на конфликт на ниско ниво што опфаќа широк спектар на способности. Тоа е намерно прикриено спојување на конвенционално и неконвенционално војување кое се спроведува под единствена централна власт и раководство на државен или недржавен актер. Целта на хибридното војување е да се постигнат политички цели кои не би биле остварливи или би биле со превисоки трошоци, преку употреба на која било друга форма на војување поединечно. Миксот од конвенционалното и неконвенционалното му овозможува на актерот да ја искористи стратешката или доктринарната слабост на противникот, притоа одржувајќи го негирањето за вмешаност во конфликтот и секако, стратешкото изненадување (Najžer, B., 2020: 29).

Од друга страна, терминот хибридна закана се однесува на акција спроведена од државни или недржавни актери, чија цел е да ја поткопа или да ѝ наштети на целта преку влијание врз нејзиното донесување одлуки на локално, регионално, државно или институционално ниво. Таквите активности се координирани и синхронизирани и намерно се насочени кон ранливоста на демократските држави и институции. Активностите може да се одвиваат, на пример, во политички, економски, воени, цивилни или информативни домени. Тие се спроведуваат со користење на широк опсег на средства и се дизајнирани да останат под прагот на откривање и припишување. Хибридното дејство се карактеризира со двосмисленост бидејќи хибридните актери ги замаглуваат вообичаените

граници на меѓународната политика и дејствуваат во интерфејс меѓу надворешното и внатрешното, легалното и нелегално и мирот и војната. Нејаснотијата се создава со комбинирање на конвенционални и неконвенционални средства – дезинформации и мешање во политичка дебата или избори, критични нарушувања или напади на инфраструктурата, сајбер-операции, различни форми на криминални активности и, конечно, асиметрична употреба на воени средства и војување.

Користејќи ги горенаведените неконвенционални и конвенционални средства заедно, хибридните актери го прикриваат своето дејство во нејасно, комплицирајќи ја атрибуцијата и одговорот. Употребата на различни посредници или прокси актери го поддржува постигнувањето на овие цели. Хибридното дејство е исплатливо бидејќи ја претвора ранливоста на целта во директна сила и предност за хибридниот актер.

Тековната транзиција во меѓународните структури на моќ обезбедува плодна средина за хибридна акција. Засилениот конфликт на вредности меѓу Западот и авторитарните држави ги еродира меѓународните норми и институции и ги прави отворените западни општества цели на сеопфатна хибридна акција. Неодамнешниот развој на модерната технологија и сè покомплексното информациско опкружување обезбедуваат моќни инструменти за хибридните актери.

Според тоа, основните карактеристики на хибридните закани се:

- координирана и синхронизирана акција која намерно ја таргетира системската ранливост на демократските држави и институции преку широк опсег на средства;

- активности кои ги искористуваат праговите на откривање и припишување, како и различните интерфејси (војна-мир, внатрешна-надворешна безбедност, локално-државно и национално-меѓународно);

– активности насочени кон влијание на различни форми на одлучување на локално (регионално), државно или институционално ниво, дизајнирани да продолжат и/или да ги исполнат стратешките цели на актерот додека ја поткопуваат и/или повредуваат целта (Hybrid CoE, 2022), (Steingartner, W., Galinec, D. 2021).

1.3. Тероризмот како хибридна закана

Променетата природа на тероризмот како хибридна закана можеме да ја разбереме доколку ја прифатиме констатацијата дека крајот на 20 век и почетокот на 21 век претставува клучниот период во историјата на безбедноста кога се случува рапидна транзиција од аналогниот во дигитализираниот глобализиран свет. Во една таква средина, доаѓа то трансформација на теоризмот или како што Антинори наведува „медијаморфоза на тероризмот". Овој процес претставува трансформација во која медиумите не се само извори на информации кои генерираат терор, како што тоа го предвидуваат традиционалните пропагандни стратегии, туку медиумите сами по себе прераснуваат во терор како асиметрична закана во глобализираната современа реалност преку насилниот нексус: акција – презентација.

Тероризмот презема нови методи и применува нова околина на делување. Теористите стануваат е-теорристи и применуваат „сајбер - тероризам", нагласувајќи ја улогата на технологијата во смисла на напад, дигитален терор и (сајбер) социјален тероризам користејќи ги социјалните мрежи (Antinori, A. 2019: 24).

Тероризмот во моментов е една од најголемите закани, што мора да се истакне, од сите хибридни закани. Теористите оперираат истовремено во многу земји користејќи смртоносни методи против земјите членки на Европската Унија и НАТО. Покрај тоа, сите терористички напади ја попречуваат глобалната соработка за извршување на цивилни и воени мисии

со цел да се стабилизира ситуацијата во земјата домаќин. Отсуството на навремена акција доведува до дестабилизација на состојбите во многу држави.

Мора да се земе предвид дека терористичките организации, кои исто така се перцепирани како „хибридни актери", можат да постигнат вистински оперативни успеси, бидејќи контролираа големи територијални проширувања во Сирија и Ирак. Покрај тоа, активното присуство на терористи на социјалните мрежи за пропагандни цели, исто така, претставува важен елемент на хибридна активност (Olech, A. 2021).

Променетата природа на терористичко делување станува сè поактуелна во напорите за изградба на отпорни општества и потребата од изградба на ефикасни системи за заштита на критичната инфраструктура.

1.4. Хакерски напади и подривачки технологии

Живееме во свет во кој интернетот со својот развој придонесува онлајн-бизнисот да бележи огромен напредок. Забрзаниот развој на интернетот доведе до големи придобивки како што се електронската трговија, електронската пошта, лесен пристап до огромни податочни множества и сл. Тоа значи дека сè поголем број на компјутери се поврзуваат на интернет, бежични уреди и мрежи. Од тие причини, како резултат на иновативните придобивки на интернетот, администрацијата, приватната индустрија и редовниот компјутерски клиент имаат сè поголема загриженост и страв од евентуално криминално хакирање на нивните информации или приватни податоци.

Хакирањето, во основа, претставува неодобрена употреба на компјутерски системи. Хакерите се лица, програмери кои заобиколувајќи ги безбедносните системи, упаѓаат во туѓа компјутерска рамка или собираат информации без овластување (Kumar, S., Agarwal, D. 2018).

Критичната инфраструктура не е имуна на ваков вид напади. И покрај заштитните безбедносни системи, бројни се примерите за неовластено прекинување во функционирањето и оштетување на критичната инфраструктура. Како главни карактеристики на хакирањето можат да се издвојат: неовластен пристап до информацискиот систем, насилно пробивање или пристапување кон системот на заштита, висока професионалност и знаење за да се постигне упадот на системот, вообичаено, местото на нападот е оддалечено од местото на напаѓачот, делокругот на хакерскиот напад може да биде и извршување шпионажа, измама, проневера, кражба на услуги, саботажа, ширење на вируси и сл., хакерите вообичаено дејствуваат во група или самостојно. Како резултат на ваквите дејства, особено кај критичната инфраструкра можни се разни последици како што е нарушување на системот за заштита, блокирање или забавување на нормалното функционирање на системите, неовластени пристапи, оштетувања, модифицирање или уништување на податоци, кражби, нелегална дистрибуција на малициозни програми или ширење на вируси. Македонското општество не е имуно на овој вид напади. Според, Националниот центар за одговор на компјутерски инциденти, во 2020 година се регистрирани сериозни хакерски напади на вкупно 92 јавни веб-страници, споредено со 113 во 2019, 196 во 2018 и 349 во 2017 година. Од нив, 6 се официјални страници на организации од владин сектор под gov.mk доменот.

Во 2020 година биле нападнати веб-страниците на Државната изборна комисија со фамозниот пад на сајтот вечерта по парламентарните избори, Дирекцијата за заштита и спасување и во три наврати Општина Кичево. Во 2019 нападите над државните институции биле уште почести. Хакерски биле нападнати: Владата на 7 септември 2019, Секретаријатот за европски прашања во два наврати, скопското јавно претпријатие „Улици и патишта“, Општина Богданци и други (А., К. 2020).

Денес, еден од основните начини на кои владите ја обликуваат геополитиката е преку хакирање други земји. Моќта и

флексибилноста на хакерите се недоволно ценети. Постојат и владини хакери кои постојано наоѓаат начини да ги унапредат интересите на своите држави и да ги попречат интересите на нивните противници. Како боксер кој победува на поени наместо со нокаут удар, тие можат да бидат ефективни без да бидат видливи или да пролеваат крв (Buchanan, B., 2020).

Аналогно на претходните констатации, технолошкиот напредок кој го овозможува 5Г мрежата има навистина импресивни можности за корисна употреба. Терминот 5Г ја означува 5-та генерација на мобилни телекомуникациски врски, чија главна карактеристика е брзината на пренос на податоци и можноста за масивно поврзување на уреди. Секоја глобална техничко-технолошка иновација покрај придобивките во себе крие и можности за злоупотреба и користење како подривачка технологија.

Сферата на критичната инфраструктура, како и одбраната и безбедноста, не се имуни на потенцијалните закани од 5Г технологијата. Познати се полемиките и генералниот став на Западот за повлекување или забрана за работа на „Хуавеј“, технолошкиот гигант од Кина. Опасноста произлегува од потенцијалите на оваа технологија, каде што кинеската влада преку контролата врз безжичниот и телекомуникацискиот столб во светот ќе користи 5Г технологија како Тројански коњ за комерцијални и воени цели или за шпионажа и хибридно војување (Evans, V. C. 2020)

Доколку ја анализираме само 2020 година за 5G технологиите, ќе ја согледаме растечката загриженост на европските земји. Така на пример, во јуни 2020 година, данскиот министер за одбрана потенцира дека владата сака да ги исклучи добавувачите од земји кои не се сметаат за безбедносни сојузници, иако сè уште не е донесена официјална одлука. Во јули 2020 година, Владата на Велика Британија го исклучи „Хуавеј“ од нејзините 5G мрежи, строго наредувајќи целосно отстранување на неговата опрема до 2027 година. Покрај тоа, во истиот месец 2020 година, Франција им кажува на телекомуникациските

оператори дека нивните лиценци за опремата на „Хуавеј“ нема да бидат обновени откако ќе истечат, што значи де факто постепено укинување до 2028 година. Оттука, оваа практика продолжува во август 2020 година со новиот нацрт-закон за ефикасно исклучување на „Хуавеј“ од 5G мрежите на Романија. Исто така, Словенија потпиша заедничка изјава за соработка и безбедност на 5G полето заедно со САД, Полска, Романија, Естонија, Летонија и Чешка (Mileski, T., Albrecht, E. 2021).

Во делот на подривачките технологии, можеме да ги сврстиме и се позачестената употреба на дроновите. Интересно, употребата на овие иновативни технологии се поврзува со терминот „сива зона“ и стратешкиот пејсаж кој се повеќе ке прикажува предизвици во сивата зона кои не се ниту целосна војна, ниту целосен мир. РАНД Корпорацијата ја дефинира сивата зона како оперативен простор помеѓу мирот и војната, кој вклучува принудни дејствија за промена на статус кво под прагот што, во повеќето случаи, би поттикнал конвенционален воен одговор, често со замаглување на границата помеѓу воените и не - воени дејствија и припишување на настани. Во публикациите од Центарот за стратешки и меѓународни студии (CSIS), стратегијата на сивата зона е дефинирана како напор или серија на одвраќање и уверување надвор од стабилна состојба што се обидува да ги постигне своите безбедносни цели без прибегнување кон директна и значителна употреба на сила. Вклучувајќи се во стратегијата на сивата зона, актерот се обидува да избегне преминување на прагот што резултира со војна.

Изменетата природа на војувањето, стратегијата на хибридни војни, хибрини закани, прокси и сајбер војување и сл., овозможуваат и почеста употреба на дроновите. Воените дронови активно се користат при оперативна употреба во две мисии: извидување и целни убиства. Притоа, нивните уникатни функции без екипаж се корисни во таквите мисии. Покрај тоа, употребата на дроновите се смета за помалку скапа во однос на меѓународната репутација. Во однос на овие особености, дроновите совршено се вклопуваат како мерка за стратегија

на сивата зона и емпириски е докажано дека е тоа така (Hwang, W. J. 2021).

Ваквиот развој на настаните, уште повеќе ја зголемува ранливоста на критичната инфраструктура. Особено што целите на напади со дронови можат да вклучуваат постројки за складирање гориво или вода, гасоводи, постројки за дистрибуција на електрична енергија и локации за снабдување со храна кои имаат минимален персонал кој ги опслужува или воопшто го немаат (Pledger, T. 2021). Тоа значи дека и во тој домен отпорноста и заштитата на критичната инфраструктура мора постојано да се надградува и подобрува.

1.5. Климатски промени

Денес, светот живее во динамично време каде што интензитетот и катастрофичните последици од промените во сферата на животната средина ја наметнуваат потребата од сериозно опсервирање на природните настани. Тие сè почесто се манифестираат и сè посериозно ја загрозуваат безбедноста на државите, индивидуите, но влијаат и на заштитата на критичната инфраструктура.

Во една видоизменета меѓународна констелација на состојби, односи и процеси, климатските промени се појава која високо котира во политичките и академските дебати. Но, која е природата на климатските промени? Како тие влијаат и ја загрозуваат критичната инфраструктура и воопшто, како ги моделираат односите помеѓу државите, регионите и целокупната меѓународна заедница?

Природата на заканите од климатските промени тргнува од теоријата за ефектот на „стаклена градина“ и научниот консензус за нејзиното влијание врз климатските промени. Тоа значи дека бројни човечки активности, како што се горењето на фосилните горива, зголемувањето на атмосферската концентрација на гасовите кои ја предизвикуваат „стаклената

градина“, се главните промотори на глобалното затоплување и климатските промени (Милески, Т. 2011).

Бројни дискусии за националната безбедност, климатските промени и хибридното војување едвај се вкрстуваат и покрај тоа што се многу видливи и застапени во дискусиите за променливата природа на конфликтот и безбедноста. Кога се споменуваат климатските промени, тоа е типично во контекст на тоа како променливите услови на животната средина може да забрзаат одредени компоненти на хибридната војна, како што е тероризмот на пример.

За разлика од традиционалните концепции за стратешка безбедност која се однесува на воена акција, климатските промени ги истакнуваат начините на кои не само човековата безбедност е ставена на ризик, но и како актерите можат да ги искористат предностите или да ги принудат промените во животната средина со цел да ги поткопаат противниците. Уште од времето на Сун Цу е напишано дека создавањето ранливост кај противникот е премногу скапо, при што е направен исклучок кога станува збор за искористување на факторите на животната средина. Евидентно е дека во дваесет и првиот век, ние исто така гледаме можности за асиметрична акција против противниците преку отворање на ранливости на животната средина (Briggs, C. M. 2020).

Најголемиот број на стручна литература сè повеќе ја прифаќа стратегијата за адаптација на климатските промени. Во тој контекст најважниот момент во делот кој се однесува на заштитата на критичната инфраструктура е приодот кон изградба на отпорно општество. Чинителите (агентите) на таквата отпорност (на пр. високото раководство, избраните функционери) можат да предводат и да организираат акција за климата. Притоа, нивната способност да ги спроведуваат целите и политиките во практика во голема мера е одредена од робусноста на институциите (на пр. стратешки планови, политики) и системите (на пр. инфраструктура, екосистеми) (Birchall, S. J., Bonnett, N. 2021).

Последиците од климатските промени можат да влијаат на секој дел од критичната инфраструктура. Како пример ќе го наведеме енергетскиот систем, каде ефектите можат да бидат од производство до крајна употреба. Во овој сектор од критичната инфраструктура климатските промени резултираат со повеќе проблеми:

- помалку ефикасно производство, пренос и дистрибуција на електрична енергија поради повисоките температури;
- штета од шумски пожар;
- штети од поплави;
- штети од невреме;
- зголемен ризик од физичко оштетување и прекин на напојувањето со електрична енергија и гориво;
- нарушување на железничкиот и патниот транспорт на сурова нафта и други нафтени продукти;
- зголемување на побарувачката за климатизација и природен гас во лето.

Природните катастрофи што се случија во периодот од 1995 до 2015 година беа претежно настани поврзани со временските услови (околу 90%) низ целиот свет. Само во 2017 година, 93% од 710 релевантни катастрофи со загуби беа припишани на настани поврзани со временските услови. Во однос на настанатите загуби кои се случиле во 2017 година, истата ја позиционира како втора најскапа, по претрпени штети, година во историјата. Неодамнешните забележани промени во ваквите настани сè повеќе се припишуваат на антропогени емисии на стаклени гасови (GHG). Во однос на предвидувањата на климатските модели, констатациите и сугестиите се во насока дека ќе има значителни промени во климатските екстреми и во иднина. Потенцијалните влијанија на климатските екстреми врз критичната инфраструктура вклучуваат различни

ефекти. Тие можат да бидат директни и да се манифестираат како директни оштетувања на физичката инфраструктура и индиректни како попречување на синџирите на снабдување и производство на суровини (Kumar, N. et.al. 2021).

За жал, метеоролошките податоци покажуваат постојан пораст на температурата од 1950-тите на глобалната сцена. Ова има голем број на ударни ефекти во различни сектори од критичната инфраструктура. Заради ваквите процеси важно е да се земат предвид брзите климатски промени и веднаш да се преземат мерки за адаптација и отпорност (Mikellidou, C. V., et.al. 2018).

Одговорот на современите предизвици од климатски промени, во енергетската сфера треба да е во синергијата помеѓу подобрувањето на отпорноста на енергетската критична инфраструктура на екстремни климатски настани и транзицијата кон енергија со помала количина на јаглерод. Плаќањето и реставрирањето на климатски штети може да го загрози финансирањето на транзицијата кон обновливите извори на енергија и други мерки со ниска содржина на јаглерод. Финансирањето на транзицијата кон чиста енергија во услови на растечко нарушување на климата ќе бара креативни опции од креаторите на политиките и бизнисите. Ќе треба да се земат предвид иновативните јавно-приватни структури при изнаоѓање опции за климатска адаптација на енергетските системи (Ogden, M., J. et. al. 2019).

2 ГЛАВА

КРИТИЧНА ИНФРАСТРУКТУРА: ЕУ И НАТО ДИМЕНЗИЈА

2.1. Концепт на отпорност и неговата важност

Бројните научни анализи за катастрофите, како и креаторите на политики, во последните дваесет години го фокусираат своето внимание на отпорноста. Најчесто, академските дебати и истражувања се во насока на изнаоѓање одговори дали општествените или природните системи можат да издржат или брзо да се опоравaт од некаков стрес или нарушување или дали овие системи можат да избегнат сопствен колапс поради некоја внатрешна ранливост. Од друга страна, креаторите на политиките и функционерите се фокусираа на изнаоѓање алатки за процена и квантификација на отпорноста како поддршка на нивниот институционален мандат за подготвеноста при катастрофи. Притоа, се јавуваат многу критики, особено во контекст на ненавремена реакција на владите, широка корупција и неизвршување на своите улоги во услови на управување со кризите (Kendra, J. M. et.al. 2017).

Природните и човечките опасности може да резултираат со значителна штета и нарушување на заедниците,

вклучително и нивните згради, инфраструктурните системи, на економијата и достапноста на социјалните услуги. Концептот на отпорност на заедницата, кој вклучува планирање за отпор, апсорбирање и брзо закрепнување од нарушувачките настани, се стекна со актуелност во последната деценија низ целиот свет.

Концептите на отпорност воопшто, како и отпорност кон ризични настани нашле широка примена во голем број дисциплини, вклучително психологија и психијатрија, науки поврзани со јавното здравје и науки за животната средина, инженерство и пошироките економски, социјални и бихејвиорални науки. Овие концепти се применети на феномени од различни размери и сложеност, од компоненти на инженерски системи на јавна инфраструктура, или социјални групи до системи и мрежи на системи како што се заедници, социо-еколошки системи, регионални економии и мрежи на инфраструктурни системи.

Марија Колиу и нејзините соработници даваат пресек на автори и литература во која се посочуваат примери за отпорност на специфични инфраструктурни системи. Така на пример, првата дефиниција е од Холинг во 1973 година, кој е заслужен заради тоа што е еден од првите истражувачи кој ја дефинирал отпорноста како способност на еколошките системи да апсорбираат и одбиваат надворешни удари. Гордон, во 1978 година нуди сличен пристап при потенцирањето на отпорноста на физичките структури, без разлика дали се инженерски или природни, и нивната способност да се спротивстават, апсорбираат или отстрануваат енергетски оптоварувања додека ја одржуваат својата форма и структура. Тимерман во 1981 година, инспириран директно од Холинг, беше еден од првите автори кои размислуваа за отпорност кон катастрофи и опасности, повторно се фокусирал на способностите на системи за закрепнување од нарушувачки настан. Фокусот на отпорноста од удари и брзото закрепнување остануваат централен интерес за повеќето дефиниции за отпорност, вклучувајќи ги и двете на Милети во 1999 година и на Патон и Џонстон од

2001 година. Овие автори забележале дека при справувањето со општествените системи, способноста за ефективно искористување на физичките и економските ресурси со ограничена зависност од надворешни (екстра-локални) ресурси промовира брзо закрепнување.

Во првата деценија од дваесет и првиот век беше забележано додавање на критични димензии. Односно, додавање на човечките и социјалните фактори на концептот на отпорност, особено кога се апострофира отпорноста од ризични настани. На пример, Фолке и соработниците, во 2002 година сугерираат дека вклучувањето на човечките и социјалните фактори како дел од социо-еколошките системи бара признавање на учењето и адаптацијата како критични компоненти на отпорност. Од ваква перспектива, отпорноста не е едноставно способност за спротивставување или апсорбирање на системски шокови и брзо закрепнување од влијанијата, но и да научи да се прилагодува на идните шокови и ранливости. Бруно и соработниците, во 2003 година понудиле сеопфатен фокус на отпорноста на општествениот систем со силен акцент на изградената средина. Притоа, предложиле дека отпорните системи се отпорни на опасности, способни за брзо закрепнување кога ќе бидат погодени, како и да го намалат идното влијание преку учење и адаптација како дел од процесот на закрепнување.

Овој трипартитен поглед на отпорноста: намалување на влијанијата или последиците, намалување на времето за закрепнување и намалување на идните ранливости, преовладува во последната деценија. Тенденцијата во многу скорешни дефиниции е да се имаат предвид сите три димензии на отпорност кога се разгледуваат пошироките социјални системи, како што се заедниците. Така на пример во САД терминот отпорност беше дефиниран во Директивите за претседателска политика ППД – 8 од 2011 година како „способност за прилагодување на променливи услови и издржливост, како и брзо закрепнување од прекини поради итни случаи.“ ППД – 21 од 2013 година ја прошири дефиницијата на „способноста да се

подготви и да се прилагоди на променливите услови и издржливост и брзо закрепнување од нарушувања.“ Овие ППД воспоставија заеднички дефиниции за употреба од страна на федералните агенции и федерално спонзорирани истражувања за насоки, алатки и метрика за отпорност. Конечно, националните академии на САД во 2012 година, исто така, ја дефинираа отпорноста како „способност за подготвеност и планирање, апсорбирање, закрепнување и поуспешно приспособување на несакани настани (Koliou, M. et.al. 2018).

На меѓународно ниво постојат иницијативи кои ја вклучуваат меѓународната стратегија на Обединетите нации за намалување на ризици од катастрофи, како и програмата на Фондацијата „Рокфелер“ за 100 отпорни градови. Фондацијата „Рокфелер“ програмата за 100 отпорни градови ја лансираше во 2013 година за да изгради урбана отпорност низ целиот свет. Програмата за 100 отпорни градови има цел да ја спроведе урбаната отпорност според целите за одржлив развој на Агендата на ОН за одржлив развој 2030 година и Рамката Сендаи за намалување на ризикот од катастрофи во период од 2015 до 2030 година. Овие рамки ја поврзуваат отпорноста на катастрофи и намалувањето на ризикот од катастрофи со прашањата за ранливост, климатски промени, егзистенција, обнова и правичност (Hofmann, S. Z. 2021).

Брајан Волкер дава неколку клучни преопраки за отпорноста. Притоа, наведува дека отпорноста е главно учење како да се менувате за да не бидете променети. Објаснува дека обидот да се заштити системот со негово одржување во постојана состојба ја намалува неговата отпорност. Притоа, изложеноста на целиот опсег на социјални и еколошки варијации е неопходна за одржување и градење на отпорност. Понекогаш, намерната трансформација на системот е неопходна за тој да продолжи да го дава она што е фундаментално од вредност за општеството (Walker, B. 2020).

2.2. Разбирањето на отпорноста во рамките на ЕУ

Комуникацијата на Европската комисија од 2012 година за пристапот на ЕУ кон отпорноста понуди општа дефиниција за отпорноста како „способност на поединецот, домаќинството, заедницата, земјата или регионот да издржат, да се прилагодат и брзо да закрепнат од стресови и шокови". Концептот на отпорност има две димензии: инхерентна сила на еден субјект – поединец, домаќинство, заедница или поголема структура – за подобро да се спротивстави на стресот и шокот и капацитетот на овој субјект брзо да го надмине негативното влијанието. Затоа, зголемувањето на отпорноста (и намалувањето на ранливоста) може да се постигне или со зајакнување на силата на субјектот, или со намалување на интензитетот на ударот, или пак со двете. Притоа, потребна е повеќеслојна стратегија и широка системска перспектива насочена и кон намалување на повеќекратните ризици од кризите и во исто време подобрување на механизмите за брзо справување и адаптација на локално, национално и регионално ниво.

Зајакнувањето на отпорноста лежи во интерфејсот на хуманитарната и развојната помош. Зајакнувањето на отпорноста бара долгорочен пристап заснован на ублажување на основните причини кои придонесуваат за кризи и зајакнување на капацитетите за подобро управување со идната неизвесност и промена (European Commision, 2012: 5).

Ова разбирање на отпорноста има широката употреба на концептот во екологијата, инженерството и психологијата и е во согласност со дефинициите на владите на земјите членки на ЕУ, меѓународните организации и невладините организации. Концептот на отпорност е во спротивност со претходните парадигми во безбедноста и градењето на мирот со признавање на неизбежноста од шокови и стресови. Како практична последица, напорите веќе не се фокусирани исклучиво на спречување на шокови, туку на капацитетот на заедницата

да ги одржи своите основни функции во случај на шок и навремено да се рехабилитира од шоковите (Amadio Viceré, M.G., Frontini, A. 2020).

На 28 јуни 2016 година, високата претставничка за надворешна и безбедносна политика и потпретседател на Европската комисија, Федерика Могерини, официјално ја претстави „Глобалната стратегија на ЕУ за надворешна и безбедносна политика". Додека вниманието на шефовите на држави и влади беше фокусирано на исходот од британскиот Референдум и многумина сугерираа дека презентацијата на ЕУГС треба да се одложи или дури и целосно да се прекине, ставот на Могерини беше дека сега е моментот кога на ЕУ ѝ е потребна Глобална стратегија.

Отпорноста е дефинирана во Глобалната стратегија на ЕУ како „способност на државите и општествата да се реформираат, со што ќе издржат и закрепнуваат од внатрешни и надворешни кризи". Поконкретно, иницијатива е дадена кон градењето „државна и општествена отпорност на нашиот исток и југ". Состојба која е идентификувана како еден од петте клучни приоритети за надворешната акција на ЕУ (покрај изградбата на сопствената безбедност; следење интегриран пристап кон конфликтите и кризите; поддршка на кооперативните регионални поредоци и посветеност на реформираниот мултилатерален систем на глобално владеење заснован на правила). Меѓу другото, референците за издржливи и отпорни општества, држави и демократии се протегаат надвор од овој специфичен дел до други делови на документот кои ја вклучуваат и отпорноста на критичната инфраструктура, мрежите и услугите и издржливоста на демократиите на ЕУ.

Ова, секако, не е првпат отпорноста да се споменува во документ на ЕУ. Отпорноста првпат беше прифатена од развојната заедница во Брисел, следејќи ги сличните трендови во системот на ОН, Организацијата за економска соработка и развој и другите земји членки на ЕУ. Пристапот на ЕУ кон отпорноста е проследен со Акциониот план за отпорност во

земји подложни на кризи за 2013-2020 година. Овој и други документи дополнително ја препознаваат потребата да се даде приоритет на голем број елементи во циклусот на политиките на ЕУ: процена на ризик, намалување на ризикот, превенција, ублажување и подготвеност, како и брз одговор и закрепнување од кризи (Juncos, E., A. 2017).

2.3. Создавање и развој на нормативната рамка во Европската Унија за заштита на критичната инфраструктура

Како резултат на терористичките напади од 11 септември 2001 година во САД и отпочнатата глобална војна против теоризмот, ЕУ ги насочува сопствените напори и дебати за заштита на критичната инфраструктура кон одбрана од тероризмот. Во една таква констелација на настани, во јуни 2004 година, Европскиот совет побара од Европската комисија да подготви сеопфатна стратегија за областа на критичната инфраструктура во ЕУ и да воспостави нормативна рамка за нејзина заштита. Европската комисија во октомври 2004 година го усвојува првиот документ од оваа област насловен како „Комуникација за заштита на критичната инфраструктура во борбата против теорризмот". (COM/2004/702). Комуникацијата содржи предлози околу тоа што треба Европа да направи за да спречи терористички напади врз критични инфраструктури, за подобрување на нивото на подготвеност за вонредни ситуации, за подигање на нивото на отпорност кај таквите инфраструктури, како и за развивање на нивната способност за одговор на напади. Со овој документ започнуваат интензивни напори кај телата на Европската Унија, како и соработката со земјите членки и со поединечните експерти за развој на нормативната рамка и идентитетот на Унијата во областа на критичните инфраструктури.

Во 2005 година, Комисијата изработи Зелена книга за Европската програма за заштита на критична инфраструктура, во која се понудени можни политики за тоа како Комисијата може да воспостави програма за заштита на критичната инфраструктура и Информативна мрежа за предупредување за критична инфраструктура. Следната година, 2006, Европската комисија усвои Европска програма за заштита на критична инфраструктура, која ги зема предвид сите ризици кога станува збор за заштитата на критичната инфраструктура, но која најмногу се занимава со проблемот на тероризам. Во април 2007 година, Советот на Европската Унија ја разгледа Европската програма за критична инфраструктура и донесе заклучоци во кои се наведува дека крајната одговорност за управување со клучните решенија за заштита на инфраструктурата е кај земјите членки во рамките на нивните државни граници. Покрај ова, тој побара од Комисијата да развие европска постапка за идентификација и означување на европски критични инфраструктури и процена на потребата за подобрување на нивната заштита. Веднаш потоа, во 2008 година, Советот на Европската унија го усвои клучниот документ во областа на критичните инфраструктури во Европската Унија - Директивата на Советот 2008/114/ЕК од 8 декември 2008 година за идентификација и означување на европската критична инфраструктура и процена на потребата за подобрување на нивната заштита која повеќе не е насочена кон заканата од тероризам, туку има цел да воспостави сеопфатен процес на заштита на критичната инфраструктура како на ниво на земјите членки, така и на Унијата во целост.

Според Директивата 2008/114/ЕК, под критична инфраструктура се подразбираат средствата, системите или деловите од нив кои се наоѓаат во земјите членки и кои се од суштинско значење за одржувањето на виталните општествени функции, здравјето, сигурноста, безбедноста, економската или социјалната благосостојба на луѓето и чие нарушување или уништување би имало значително влијание во една земја членка како резултат на неисполнувањето на тие функции. Под европска критична инфраструктура, пак, се подразбира

критичната инфраструктура која се наоѓа во земјите членки и чие нарушување или уништување би имало значително влијание врз најмалку две земји членки. Значењето на влијанието се проценува врз основа на вкрстени критериуми. Ова вклучува ефекти кои произлегуваат од меѓусекторската зависност од други видови инфраструктура. Директивата 2008/114/ЕК се применува од 12 јануари 2009 година, додека земјите членки имаа рок да ја пренесат во нивните национални законодавства до 12 јануари 2011 година во секторите енергетика и транспорт, додекаа земјите кандидати за полноправно членство во Европската унија мора да ја спроведат истата пред нивното официјално пристапување кон Унијата. Заради сознанието дека интернетот и процесите во сајбер-просторот сè повеќе влијаат на поврзаноста на критичните инфраструктури, Европската Унија мораше да преземе чекори за регулирање на оваа област. Во 2013 година, Европската комисија, заедно со високиот претставник на Европската Унија за надворешни работи и безбедносна политика, промовираше Стратегија за сајбер-безбедност на Европската Унија. Акцентот беше поставен на отворен, сигурен и безбеден сајбер-простор, што претставуваше сеопфатна визија на ЕУ за тоа како најдобро да ги поддржи земјите-членки и другите засегнати страни во спречувањето и реагирањето на компјутерските нарушувања и напади (Mitrevska, M. Mileski, T. Mikac, R. 2019).

2.3.1. Директива 2008/114/ЕК

Во воведните одредби од Директивата 2008/114/ЕК, Советот на Европската унија презеде чекори за истакнување основни упатства за сите засегнати страни. Беше потенцирано дека првиот чекор во повеќефазниот пристап е насочен кон идентификација и означување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита. Притоа, фокусот првенствено паѓа врз секторот за енергија и транспорт, но треба да се земат предвид и другите значајни сектори, како што се секторите за информатичко-комуникациска технологија. Исто така, а следново е

и особено важно, земјите членки и сопствениците или операторите на горенаведените европски критични инфраструктури треба да ја поседуваат основната и конечна одговорност за заштита на критичната инфраструктура во Европа. Ова претставува продолжување на обврската за заштита издадена од Советот во април 2007 година, кога истиот ја разгледуваше Европската програма за заштита на критична инфраструктура, притоа донесувајќи заклучоци за заштитата на националните критични инфраструктури во кои беше нагласено дека конечната одговорност за заштитата лежи кај земјите членки. Бидејќи во крајна линија европските критични инфраструктури се првенствено национални, и кога тие се од заемно значење за две земји членки, тие се сметаат како европски.

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

Главниот дел на Директивата 2008/114/ЕК се занимава со постапката за идентификација и означување на европските критични инфраструктури. Постапката за идентификација беше уредена во Членот 3 од Директивата и прилогот кон него. Се состои од неколку чекори кои подразбираат терминолошко

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

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

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

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

Постапката за означување на европски критични инфраструктури е уредена во Членот 4 и истата може да се примени по претходно спроведување на постапката за идентификација на потенцијалните европски критични инфраструктури.

Кога една земја-членка идентификувала потенцијална критична инфраструктура на територијата на други земји-членки или открила дека има своја инфраструктура на нејзината територија што е значајна за соседните земји, таа истите е задолжена да ги информира за тој податок. Се разгледува само инфраструктурата која е од суштинско значење за одржување на виталните функции на општеството, здравјето, сигурноста, безбедноста и економската или социјалната благосостојба на луѓето, а чие нарушување или уништување би имало значително влијание врз една или две земји членки. Потоа, следи процес на билатерални или мултилатерални дискусии меѓу државите со цел да се разгледаат состојбите и потенцијалните негативни ефекти од застојот или дефектот во работењето на утврдената инфраструктура. На покана на земјите членки, Европската комисија може да учествува во овие дискусии. По извршената анализа, за да се идентификува потенцијалната критична инфраструктура како европска критична инфраструктура, потребна е согласност од земјата членка на чија територија е откриена и назначена како европска критична инфраструктура. Во случај на неможност да се постигне договор меѓу земјите членки, тие можат да се обратат до Комисијата, која може да се вклучи во дискусијата и да го олесни постигнувањето на договор меѓу државите.

По успешните преговори меѓу земјите членки, следниот чекор е да се информираат сопствениците или операторите на критичната инфраструктура дека нивната инфраструктура е идентификувана и означена како европска критична инфраструктура. Земјата членка на чија територија се наоѓа оваа европска критична инфраструктура е одговорна за информирање на сопственикот или операторот и исто така е должна на годишно ниво да ја известува Комисијата за бројот на означени европски критични инфраструктури по сектор и за бројот на земји членки кои зависат од секоја означена европска критична инфраструктура. Информациите за означените инфраструктури се класифицираат според соодветното ниво на тајност на податоците и нивниот идентитет им е познат само на земјите членки кои ги делат или на каков било начин

зависат од истите. Интерес на Комисијата е да добие колку што е можно посеопфатни информации од земјите членки за ризиците, заканите и слабостите во секторите каде се означени европски критични инфраструктури, како и информации за меѓусекторските зависности и преземените чекори за намалување на ризиците, заканите и слабостите, со цел да се разработат соодветни предлози за заштита на набљудуваните инфраструктури.

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

Следната важна одредба се однесува на назначувањето офицер за врски за безбедност. Државата треба да овозможи секој сопственик или оператор да назначи безбедносен координатор во рамките на европската критична инфраструктура или офицер за врски задолжен за безбедносни работи. Споменатиот претставува важна хоризонтална и вертикална врска меѓу елементите на системот на критични инфраструктури, како и лице за контакт со законодавецот и другите критични инфраструктури. Понатаму, државата треба да назначи национална контакт-точка која ќе биде одговорна за соработка со Комисијата, другите држави, како и со сопствениците или операторите на европските критични инфраструктури означени на нејзината територија (Mitrevska, M. Mileski, T. Mikac, R. 2019).

2.3.2. Директива 2016/1148 за мрежните и информатичките системи низ Унијата

Континуитетот на интерес за критичните инфраструктури во Европската Унија доведе до создавање на Директивата 2016/1148. Таа се однесува на мрежните и информатичките системи и услуги кои играат клучна улога во општеството. Нивната сигурност и безбедност се од суштинско значење за економските и општествените активности, а особено за функционирањето на внатрешниот пазар. Обемот, честотата и влијанието на безбедносните инциденти се зголемуваат и претставуваат голема закана за функционирањето на мрежните и информатичките системи. Овие системи исто така може да станат цел на намерни штетни активности насочени кон оштетување или прекинување на работата на системите. Ваквите инциденти можат да го попречат извршувањето на економски активности, да создадат значителни финансиски загуби, да ја поткопаат довербата на корисниците и да предизвикаат голема штета на економијата на Унијата. Затоа, за да ги поврзе клучните области, чинители и процеси беше донесена Директивата за МИС, а со цел да се зголеми нивото на заштита и воведување на минимум заеднички стандарди во оваа област.

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

Основна цел на Директивата за МИС е да обезбеди заедничко ниво на безбедност на мрежните и информатичките

системи во сите земји членки, чии неправилности предизвикани од безбедносни инциденти може да имаат силни последици врз општеството или економијата на земјата. Притоа, Директивата за МИС воведува регулаторни елементи кои овозможуваат трајно следење на состојбата со автоматизацијата и дигитализацијата во одбележаните сектори. Покрај тоа, таа воведува обврска за спроведување на технички и организациски мерки за управување со ризици и мерки за спречување и минимизирање на ефектите од инциденти во безбедноста на мрежните и информатичките системи, воведувајќи и обврска за известување за инциденти кои можат да имаат значителни ефекти врз континуитетот во давањето услуги (Mitrevska, M. Mileski, T. Mikac, R. 2019).

2.3.3. Ревизија на Директивата за заштита на критичната инфраструктура од 2008 година

На 16 декември 2020 година, потпирајќи се на наодите од евалуацијата, Комисијата претстави нов предлог за директива за отпорност на критичните субјекти (COM/2020/829), заедно со поддршка на проценатa на влијанието. Со оглед на важноста на сајбер-безбедноста за отпорноста на критичните субјекти, Комисијата паралелно поднесе и предлог за ревидирана директива за безбедност на мрежите и информатичките системи МИС („МИС 2“). За да се обезбеди целосна кохерентност, обврските за сајбер-отпорност според МИС 2 ќе важат и за критичните субјекти идентификувани според новиот предлог.

Самиот предлог за критичните субјекти одразува промена од сегашниот пристап кој се фокусира на заштитата на индивидуалните средства кон зајакнување на отпорноста на критичните субјекти кои управуваат со нив. Додека пристапот за сите опасности на постојната директива останува валиден, новиот предлог ги опфаќа денешните реални и сложени аспекти, притоа земајќи ги предвид: широкиот опсег на ризици, вклучувајќи природни опасности, хибридни акции спонзорирани од држави, тероризам, инсајдерски закани, пандемии и

(индустриски) несреќи; нови технологии, како што се 5G и дронови; и меѓусебно поврзан пристап, бидејќи опасностите може да генерираат каскадни ефекти врз обезбедувањето услуги во други сектори и преку границите.

Предлогот ќе бара од секоја земја членка да усвои национална стратегија за зајакнување на отпорноста на критичните субјекти и да презема редовни процени на ризикот. Постапката за идентификување на критичните инфраструктури би била различна од онаа наведена во Директивата 2008/114/ЕК. Друг нов елемент во предлогот би бил Комисијата да има специфичен надзор над критичните субјекти од особено европско значење, давајќи ѝ поцентрална улога отколку според сегашната процедура.

Друга впечатлива разлика во споредба со постојната директива од 2008 година е предложеното секторско проширување. Предлогот го проширува опсегот на директивата за да ги вклучи банкарството, инфраструктурата на финансискиот пазар, здравството, водата за пиење, отпадните води, дигиталната инфраструктура, јавната администрација и просторот, заедно со енергијата и транспортот (European Commision, 2020).

Врз основа на новите трендови, особено појавата на пандемијата со КОВИД-19 која доведе до ревалоризација на општествените потреби во услови на здравствена криза. Ранливоста на синџирот на снабдување со медицински кислород како критична услуга стана очигледна на почетокот на пандемијата. Овој ланец вклучува многу секвенци на настани и дејства потребни за производство, дистрибуција и транспорт на медицински кислород. Овој пример, како и другиот со лична заштитна опрема што беше од суштинско значење за медицинскиот персонал, покажа дека значењето на она што е суштинско може драстично да се промени за краток временски период. Оваа промена во дефинирањето на критичната инфраструктура е почетна точка за воведување и спроведување на пристапот на отпорност и еластичност при заштитата на критичната инфраструктура. На овој начин, не

само што конкретниот предмет или средство би бил заштитен, туку и финалниот производ и исходот од она што би требало да го испорача суштинската услуга. Друг важен аспект во однос на дефинирањето на критичната инфраструктура е содржината на терминот.

Опишувајќи ја критичната инфраструктура како систем, често сфатен како комплексна мрежа од тврди компоненти како што се информатичкиот хардвер, уреди или технологија, се чини дека недостасува или не е соодветно нагласена меката компонента, човечката компонента. За време на пандемијата се покажа како незаменлива улогата на основните работници кои директно комуницираат со системот и кои управуваат или олеснуваат средства, објекти, системи или мрежи, покрај одговорните за процесите на донесување одлуки и управување со кризи. Поради ограничувањата за патување, протокот на основниот персонал беше запрен. Недостигот од персонал е примарен проблем за операторите со критична инфраструктура за време на пандемијата. Ситуацијата е уште посериозна ако сфатиме дека во случај на критична инфраструктура, повеќето позиции не можат да се пополнат со случајни лица, бидејќи тие бараат посебни знаења, вештини, а понекогаш и безбедносен сертификат. Овие пречки произлезени од кризата создаваат долг процес, што го загрозува континуитетот на основните услуги.

Пандемијата со КОВИД-19 наведе многумина да сфатат дека природните опасности се сè уште присутни и може да биде уште потешко да се предвидат во иднина. Пандемијата понуди нов тип на закана, имено закана со постојан карактер. Овој вид закана може да биде „новото нормално“ на кое треба да се прилагодиме. Избувнувањето на КОВИД-19 затекна многу од операторите на критичните инфраструктурни во состојба на изненадување, а понекогаш и паника. Во многу случаи, недостатокот на планирање за континуитет на деловното работење кое ги опфаќа средствата за идентификување ризици, поставување на цели и воспоставени соодветни практики за

ублажување и управување со ризикот, дефинитивно го загрози континуитетот на услугата.

Тежината на ситуацијата предизвикана од пандемијата со КОВИД-19, и покрај нејзините негативни конотации, може да се искористи како можност да се испита реалната состојба на заштита на критичната инфраструктура. Пандемијата покажа дека има уште многу да се направи и во непредвидливи времиња треба да почнеме да дејствуваме што е можно поскоро. Пред сè, од клучно значење е да се разбере критичната инфраструктура во смисла на основни услуги/функции, а не само физички објекти или средства. Ова би овозможило критичната инфраструктура да се гледа како систем на системи, кој поради својата меѓусекторска природа и неговите зависности и меѓузависности не може да се ограничи само на еден сектор. Понатаму, човечкиот аспект во однос на критичната инфраструктура треба да стане поочигледен. Сегашниот пристап за заштита на критичната инфраструктура треба да се надгради. Во светлината на неодамнешните, неочекувани настани, сегашниот фокус на превентивните активности треба да се промени. Односно, треба да се замени со пристап заснован на отпорност, кој би ги идентификувал и намалил ранливостите и, според тоа, ќе ги минимизира ефектите од потенцијалните закани. Овој пристап, исто така, ќе овозможи да се нагласи важноста на способностите на субјектите кои спроведуваат акции за одговор и закрепнување. Ова исто така би помогнало за понепречено приспособување кон нова ситуација и средина по кризата. Покрај тоа, операторите со критична инфраструктура треба да се фокусираат на идентификација на ранливости во организацијата и меѓу системите и да применат соодветни контрамерки. Заштитата на критичната инфраструктура зависи од различни субјекти. Во неа се вклучени државата, операторите на критичната инфраструктура, како и општеството и медиумите. Затоа, воспоставувањето нова рамка на хоризонтална и вертикална соработка и комуникација меѓу засегнатите страни во голема мера ќе придонесе за процесот на градење побезбедна и поотпорна критична инфраструктура (Tomalska, A. 2022).

2.4. НАТО пристапот кон отпорноста

Концептот на отпорност во одбраната и безбедноста се развива преку вклучување на широк и повеќедимензионален сет на ранливости и поврзани стратегии за ублажување низ спектарот на воени и невоени механизми на одговор. Во овој поглед, Агендата за отпорност на НАТО има тенденција да расте и да презема нови задачи бидејќи разбирањето на факторите на ризик и можните контрастратегии се развиваат паралелно со текот на времето.

Поимот за отпорност на земјите членки на НАТО преку одржување и развивање на нивниот индивидуален и колективен одбранбен капацитет е втемелен во Основачкиот договор на Алијансата од 1949 година и, особено, во Членот 3 каде имплицитно се дефинира внатрешната димензија на отпорноста во однос на способностите, а капацитетот за колективна одбрана е операционализиран преку одбранбеното планирање и процесот на развој на способностите на НАТО. Лондонската декларација, произлезена од Состанокот на лидерите на НАТО на 3-4 декември 2019 година, го проширува концептуалниот опсег на отпорноста со вклучување, за прв пат, и на општествата на земјите членки на НАТО, заедно со отпорноста на критичната инфраструктура и енергетската безбедност како и безбедни и еластични системи за обезбедување на комуникациската безбедност на земјите на НАТО. Освен отпорноста на општествата, експлицитно артикулирана за прв пат, другите области веќе се дел од Агендата за отпорност на НАТО (London Declaration, 2019).

Силната страна од Агендата за отпорност на НАТО лежи во областа на цивилната подготвеност, која доаѓа како неопходност од брзото менување на безбедносното опкружување и зајакнатата одбранбена и одвраќачка положба на Алијансата со оглед на зголемените терористички и хибридни закани насочени кон цивилното население и критичната инфраструктура на евроатлантската територија. На Самитот во Варшава во 2016 година, сојузничките лидери одлучија да ја подобрат отпорноста на НАТО во целиот спектар на закани и се согласија за седум

основни барања за национална отпорност според кои земјите членки можат да го измерат нивото на подготвеност. Тоа се: гарантирање на континуитет во работата на владините и критичните владини служби; отпорност на енергетските снабдувачи; способност за ефективно справување со неконтролираното движење на луѓето; отпорни ресурси на храна и вода; способност да се справи со масовни жртви; отпорни цивилни комуникациски системи; и отпорни системи за цивилен транспорт.

Кризата со пандемијата КОВИД-19 неспорно ја тестираше подготвеноста за отпорност на Алијансата и нејзините земји членки, вклучително и во здравствениот сектор. Тој сектор не беше експлицитно идентификуван како посебна област на барања пред ова, на пример, во однос на медицинските резерви и подготвеност во ситуации на пандемии. Пандемијата ги тестираше механизмите на НАТО за консултации и координација за време на вонредна состојба и брзината на одговор за ублажување на последиците од здравствената криза и во земјите на НАТО и во партнерите. Тоа се одвиваше преку капацитетите за брз одговор доделени на Евро-атлантскиот координативен центар за одговор при катастрофи (EADRCC) како главен механизам на НАТО за цивилен одговор во итни случаи. Кризата со КОВИД-19, исто така, изложи и други аспекти на отпорност што треба да се земат предвид, како што е одговор на дезинформации во кризни ситуации. Паралелно, одговорот на пандемијата доведе до прашања поврзани со робусноста и доверливоста на синџири на снабдување во опкружување кое треба да обезбеди и гарантира брза реакција пришто се очекува надзорот и контролата да бидат ограничени и минимизирани и на тој начин да доведе до зголемување на ризикот од измама и лошо управување со ресурсите.

Од овие причини, размислувањето за отпорност не може да постои изолирано од капацитетот на меѓународните организации и националните влади да предвидат кој од широкиот спектар ризици и ранливости ќе претставува безбедносен предизвик во еден или друг момент и соодветно да подготви механизми за справување, управување со последици и стратегии за ублажување. Оттука, разбирањето на целината и опсегот на

потенцијалните безбедносни ризици преку нивната сложеност, без оглед на перцепциите за нивната веројатност за појава е услов *sine qua non* за дизајнирање на адекватни и нарачани решенија. На некои од тие решенија можеби ќе им требаат години за да се имплементираат и да се вградат во организациските системи, за да се обезбеди ефективен одговор кога е потребно.

Наца Миланова констатира дека отпорноста станува концепт за собирање за меѓународните организации кои треба да ги премостат различните политички заедници и да ги урнат секторските силоси. Бидејќи е неприкосновен и неоспорен, концептот на отпорност е привлечен за креаторите на политики и имплементаторите како референтна точка при дизајнирање политики и програмски интервенции во различни контексти низ повеќе дисциплини и сектори. Сепак, отпорноста е еден од оние поими што може да страдаат од дефинитивно разбирање на нејзините концептуални параметри и практични импликации. Во контекст на дискусиите за тоа како да се операционализира отпорноста, се гарантира анализа на ризиците и ранливостите со посилен акцент на причинските ефекти. Работата на НАТО на градење на ефективни и ефикасни одбранбени институции и на минимизирање на ризикот од корупција во одбранбениот и поврзаниот безбедносен сектор преку зајакнување на институционалната отпорност и организациски интегритет, транспарентност и одговорност може да ја прошири дискусијата за отпорноста (Milanova, N. 2020).

2.5. НАТО стратегиска рамка за заштита на критичната инфраструктура

Генерално, можеме да се согласиме дека НАТО ги регулира и строго ги заштитува своите критични инфраструктури уште од своето основање. Според Основачкиот документот на Алијансата, постојат неколку можни сценарија во кои НАТО треба да има улога во заштитата на критичната инфраструктура.

1. Поддршка на воените операции на Алијансата во рамки на одредбата од Членот 5.

2. Поддршка на операциите за одговор на криза надвор од одредбата во Членот 5.

3. Поддршка на националните авторитети во вонредни состојби од невоен карактер.

4. Поддршка на националните авторитети во заштитата на нивното население од последиците на оружјето за масовно уништување.

5. Ко-партнерство со партнерите во полето на цивилното планирање за итни ситуации (Babos, 2016).

Според Протоколот креиран во периодот на Студената војна, НАТО обезбедува сигурност на критичната инфраструктура на Алијансата и на нејзините земји членки. Во насока на обезбедување координиран пристап за цивилно планирање на итни ситуации, клучната улога му е доделена на Високиот комитет за цивилно планирање на итни ситуации, кој директно го известува Северноатлантскиот совет. Цивилното планирање на итни ситуации е важна активност во процесот на предвидување и е насочена кон координирање на националните ресурси. Во контекст на природните и од човек предизвикани катастрофи, договорите ја зацврстуваат улогата на НАТО во итни ситуации. Како примери можат да се напоменат „НАТО политиката за асистенција при несреќи во мирни услови“(“NATO Policy on Disaster Assistance in Peace Time”) од 9 мај 1995 година или изјавата „Подобрена практична соработка во полето за помош при катастрофи“ (“Enhanced Practical Cooperation in the field of Disaster Relief”) од 29 мај 1998 година. Покрај тоа, Стратегискиот концепт на НАТО од 1999 година ги признава големите катастрофи како извор на загриженост за безбедноста и стабилноста.

Терминот „заштита на критичната инфраструктура“– според Директивата на Клинтон од 1998 година, а по

терористичкиот акт од 11 септември 2001 година, веднаш бил ставен на дневниот ред на Северноатлантскиот совет. По нападите од 11 септември 2001 година, НАТО-самитот во Прага го иницираше „Акциониот план за вонредни состојби". Конкретно во Членот 4, точка б од Декларацијата за одржаниот самит стои: „...ние сме посветени, во соработка со нашите партнери, целосно да го имплементираме Акциониот план за планирање на вонредни состојби за подобрување на граѓанската подготвеност против можни напади врз цивилното население со хемиски, биолошки или радиолошки агенси. Ние ќе ја зголемиме нашата способност да обезбедиме поддршка, кога тоа ќе биде побарано, да им помогнеме на националните власти да се справат со последиците од терористичките напади, вклучувајќи ги и нападите со хемиско, биолошко, радиолошко и нуклеарно оружје на критичната инфраструктура, како што е предвидено во Акциониот план на цивилното планирање на вонредни ситуации" (Prague Summit Declaration, 2002). Покрај тоа, се планирале вежби за тестирање и евентуално подобрување на интероперабилноста. Во исто време, беше објавен и Партнерскиот акционен план против тероризмот. По 11 септември беше разгледана подготвеноста на земјите членки на НАТО во сферата на заштитата на критичната инфраструктура. Резултат на таквата активност претставува концепт-документот за заштита на критичната инфраструктура, подготвен од Високиот комитет за цивилно планирање на вонредни ситуации. Главните цели се сумирани во размена на информации помеѓу засегнатите страни, помош и развој на програми за обука и едукација кои придонесуваат кон идентификација на критичната инфраструктура, одредување на истражувања за поддршка на заштитата на критичната инфраструктура и помош во текот на вежбовните активности. Планирачките одбори и комитети на Високиот комитет за цивилно планирање на вонредни ситуации ги започнале неопходните студии. Националните експерти од владите и индустријата, како и воените претставници, координирале планирање на осум технички домени: цивилен воздушен сообраќај, цивилна заштита, безбедност на храна, индустриско производство и логистика,

внатрешен копнен транспорт, работи од областа на медицината, испорака, и на крај, цивилни електронски комуникации.

Во 2005 година Високиот комитет за цивилно планирање на вонредни ситуации го усвои и прилагоди Акциониот план во насока да ги покрие напорите за време и после терористички напади со хемиско, биолошко, радиолошко и нуклеарно оружје. Планот се фокусирал на заштита на критичната инфраструктура и поддршка на жртвите. Консеквентно на ова, зголемената активност на европските сојузници на полето на заштитата на критичната инфраструктура е резултат на терористичките напади во Мадрид од 2004 година, сајбер-нападите на Естонија од 2007 година, руско-грузискиот конфликт од 2008 година, пиратските напади кои во континуитет се случуваат од 2008 година во Аденскиот Залив и брегoвите на Сомалија, како и ескалацијата на руско-украинските односи. НАТО, денес, покрај концепциските и стратегиски документи за заштита на критичната инфраструктура, исто така креира и спроведува политика и практики на оперативно ниво (Babos, 2016: 12).

На стратегиско ниво, почетоците на интересот и активностите на НАТО во сферата на заштитата на критичната инфраструктура датираат уште од 1990 година и Самитот на НАТО одржан во Лондон. Како резултат на насоките дадени на Лондонскиот самит се креира нов стратегискиот концепт на НАТО во 1991 година. Во овој стратегиски документ, Алијансата започнува со промовирање на безбедноста на критичната инфраструктур поврзана со енергетските витални ресурси. Имено, според Стратегискиот концепт на НАТО од 1991 година, нарушувањето на протокот на виталните ресурси е дефиниран како потенцијална безбедносна закана за интересите на Алијансата (Параграф 12) (The Alliance's New Strategic Concept, 1991). Истата оваа констатација, Алијансата на Самитот во Вашингтон во 1999 година ја споменува и во тогаш одобрениот нов стратегискиот концепт (Параграф 24) (The Alliance's Strategic Concept, 1999). Според содржината на Стратегискиот концепт на НАТО усвоен на Самитот во Лисабон од 2010 година,

критичната инфраструктура за прв пат јасно и недвосмислено се споменува во делот за сајбер-заканите. Во Параграф 12 се потенцира дека сајбер-заканите стануваат сè почести, повеќе организирани и поскапи за штетата што ја предизвикуваа врз владината администрација, бизнис-заедницата, економијата и потенцијално врз транспортот и мрежите за снабдување, како и друга критична инфраструктура. Притоа, се потенцира дека сајбер-заканите достигнуваат праг кој претставува закана на националниот и евроатлантскиот просперитет, безбедност и стабилност. Странските воени и разузанвачки служби, организирани криминални групи, терористи и/или ектремисти, секој може да биде извор на сајбер-напади. Во Параграфот број 19 од Стратегискиот концепт се потенцира заложбата за развивање на капацитети кои ќе придонесат за енергетската безбедност, вклучувајќи ја и заштитата на критичната енергетска инфраструктура и транзитните области и правци, соработка со партнерите и консултации меѓу сојузниците врз основа на стратегиски процени и планирање на непредвидени ситуации (Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2010: 11-17).

Стратегиските определби за критичната инфраструктура на НАТО втемелени во неговите стратегиски концепти се одраз на интензивните дебати за енергетската безбедност како предмет околу кој интензивно се дебатира на меѓународно рамниште. Активноста на НАТО во оваа сфера практично датира и пред истата да е вклучена во стратегиските концепти. Имено, за време на Студената војна Алијансата одржувала и обезбедувала гасоводен систем за снабдување со природен гас на сопствените сили и критичната инфраструктура во Европа. Токму овој дискурс ќе ни послужи подетално да ја објасниме комплексната содржина за местото, улогата и вклученоста на НАТО во заштитата на критичната инфраструктура. НАТО ќе го усвои својот нов стратегиски концепт на самитот во Мадрид во 2022 година. Најавено е дека притоа ќе се дефинираат безбедносните предизвици со кои се соочува Алијансата и ќе се опишат политичките и воените задачи што НАТО ќе ги изврши за да ги реши.

2.6. НАТО и критичната инфраструктура: актуелни состојби

Денес НАТО функционира и егзистира во драстично видоизменета средина. Пандемијата со КОВИД-19 и воената криза во Украина наложија динамични промени со цел навремено и адекватно справување со современите безбедносни предизвици во хибридната средина. На Самитот на НАТО одржан во Брисел во 2021 година започната е подготовката за адаптација на НАТО за период до 2030 година.

Но, пред да се фокусираме на Самитот на НАТО во Брисел од 2021, треба да се забележи дека со избувнувањето на пандемијата КОВИД-19, НАТО за прв пат во својата историја мораше да се соочи со напад врз секоја од своите земји членки одеднаш. Имајќи ја предвид позадината на политичките тензии во Алијансата во изминатите неколку години, немаше многу причини да се биде оптимист за одговорот на НАТО, особено во моментот кога трансатлантските сојузници не успеаја да се координираат за ограничувањата на патувањата и започнаа натпреварување во контекст на набавките на медицинска опрема. И покрај тоа, НАТО можеше да го искористи своето искуство во управувањето со кризи и помош при катастрофи за да обезбеди два вида одговори.

Прво, НАТО се фокусираше на обезбедување на континуитет на своите операции додека го штитеше својот персонал, за да спречи здравствената криза да влијае на подготвеноста. Повеќето мисии на НАТО беа зачувани, но некои наидоа на привремена суспензија. Воените вежби беа редизајнирани, вклучително и вежбата на НАТО „DEFENDER-Europe 20“, насловена како: „Платформа за зајакнување на готовноста и интероперабилноста на сојузничките сили“, предводена од САД, со цел спречување на понатамошно ширење на вирусот преку движење на копнените трупи. Вежбата беше најголемо распоредување на сили од САД во Европа во последните 25 години. Конкретно 20 000 војници беа распоредени директно од САД

во Европа. Тоа ја покажува посветеноста на САД кон НАТО и нивната решеност да застанат на страната на своите европски сојузници и партнери. Дополнително, огранокот на јавната дипломатија на НАТО ги зголеми напорите за спротивставување на дезинформациите кои доаѓаа од Кина и Русија.

Второ, во услови на многу мала меѓународна соработка, НАТО формираше Работна група за КОВИД-19, чија цел беше да ја координира испораката на медицинска помош низ и надвор од територијата на Алијансата. Ваквите дејствија, иако беа извршени преку средствата на земјите членки на НАТО и со релативно ограничен опсег, беа важно сведоштво за реактивната способност на Алијансата и за солидарноста меѓу земјите членки. Сепак, разумно е да се помисли дека можеше да се направи повеќе ако Алијансата не мораше да се соочи и да ги надмине политичките тензии преку Атлантикот, а земјите членки соработуваа од самиот почеток под раководство на најсилната членка на НАТО.

Од ова искуство за НАТО произлегоа многу важни лекции, од подобрување на отпорноста кон надворешните закани до инвестирање во подготвеност за катастрофални сценарија како глобална пандемија. Фактот дека КОВИД-19 ќе продолжи да ја нарушува глобалната економија и синџирите на снабдување, со што ќе има негативно влијание врз трошоците за одбрана и одбранбената индустрија на земјите. Сепак, со оглед на издржливоста што досега ја покажа Алијансата, КОВИД-19 нема да биде одлучувачки фактор за иднината на НАТО. Наместо тоа, шансите за НАТО да работи ефикасно во однос на растечките глобални предизвици на крајот ќе зависат од обновувањето на трансатлантските односи (De Maio, G. 2020).

Во насока на обновување на сојузништвото во НАТО и неговата готовност за справување со широк спектар предизвици и Хамилтон потенцира дека НАТО мора да се сврти кон решавање на проблемите во новата ера на постојани закани и предизвици кои не се географски ограничени. Притоа, реафирмирањето на кохезијата на НАТО како сојуз на демократии ќе

биде најважно. Секоја од основните задачи на НАТО – одбрана и одвраќање, управување со кризи и кооперативна безбедност – мора да еволуира за да одговори на новите видови опасности. Според Хамилтон, Алијансата треба да додаде четврта основна задача за сеопфатна отпорност: способност да се предвиди, спречи и, доколку е потребно, да се заштити од нарушувања и да се движи напред кон критичните функции на сојузничките општества. Притоа, поспособна Европа е од суштинско значење за секоја од овие задачи (Hamilton, D.S. 2022).

Ваквата состојба, претставуваше увертира на Самитот во Брисел 2021 година НАТО да ја потенцира заложбата за зајакнување на отпорноста. Со тоа се потврдува дека националната и колективната отпорнот се суштинската основа за веродостојно одвраќање и одбрана и ефикасно исполнување на основните задачи на Алијансата, како и од витално значење за нејзините напори за заштита на вредностите на општествата, населението и заедничките вредности. Со тоа НАТО ја обновува и ја зајакнува посветеноста што ја презема во 2016 година од Самитот во Варшава со дополнително зајакнување на националната и колективна отпорност и цивилна подготвеност во сè посложената безбедносна средина.

За погледот кон НАТО во 2030, Бриселскиот самит претставува договор за зголемување на отпорноста на Алијансата. Притоа се потенцира дека отпорноста останува национална одговорност, при што ќе се усвои поинтегриран и подобро координиран пристап. Главната цел е да се намали ранливоста и да се обезбеди ефективно функционирање во услови на мир, криза и конфликт. Понатаму, се констатира дека НАТО се справува со заканите и предизвиците кон отпорноста од државните и од недржавните актери, кои имаат различни форми и вклучуваат употреба на различни тактики и алатки. Тие вклучуваат конвенционални, неконвенционални и хибридни закани и активности; терористички напади; зголемени и пософистицирани малициозни сајбер-активности; сè поприсутни непријателски информативни активности, вклучително и дезинформации, насочени кон дестабилизација на општествата

и поткопување, како и обиди за мешање, во демократски процеси и доброто владеење. Констатирано е дека посветеноста на НАТО од Самитот во Варшава влијаела на зголемување на отпорноста од овие закани и предизвици. И дека треба да се продолжи во таа насока (Strengthened Resilience Commitment, 2021).

3 ГЛАВА

КОМПАРАТИВЕН ПРИКАЗ НА ПРИСТАПОТ ВО КРЕИРАЊЕ НА СИСТЕМ ЗА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА: СЛУЧАЈ ХРВАТСКА, СРБИЈА И ЦРНА ГОРА

3.1. Различни пристапи кон единствена цел: систем за заштита на критична инфраструктура

Во последните десет до петнаесет години, зајакнувањето на отпорноста и заштитата на критичната инфраструктура од сите видови закани (природни, техничко-технолошки опасности и антропогените закани и ризици), влегува во сите сфери на бројни држави, акцентирајќи ја важноста на критичната инфраструктура како приоритетно безбедносно прашање. Научната анализа покажува дека критичната инфраструктура

најмногу се проучува од аспект на националната безбедност, но во последните години интересот за заштита на критичната инфраструктура се шири и од страна на Европската Унија и НАТО Алијансата. Но, исто така, анализата укажува дека интересот за заштита на критичната инфраструктура се шири и преку промовирање на иницијативата за прекугранична соработка, како можност за создавање на отпорна меѓународна мрежа, како на пример во ЕУ. Кога на ова ќе се надоврзе и фактот дека поширокатa општествена заедница се соочува со комплексно безбедносно опкружување, изложено на бројни закани, станува јасно зошто се иницираат потребни и значителни ангажмани на сите општествени актери, кои индиректно или директно, се инволвирани во процесот на заштитата на критичната инфраструктура. Оттаму, оправдано произлегува и потребата од заштитата на критичната инфраструктура, каде што е неопходно да се опфатат активности насочени кон подобрување на отпорноста на системот, на објектите и на мрежите, а пред сè, превенцијата треба да добие главна улога.

Во тој контекст, треба да се потенцира дека реалната ограниченост на ресурсите (финансиски, човечки или организациски) често пати, заштитата ја стават на маргините. Затоа е неопходно да се подигне свеста, а пред сè, да се истакне важноста на критичната инфраструктура и нејзината заштита на ниво на стратешки менаџмент во организациите, или пак во компаниите, или на ниво на државата како систем. Според оценката на експертите за критична инфраструктура, во современите услови заштитата значително ќе се зголеми и од свесноста на носителите на одлуките, кои пак, можат директно да влијаат на одлуките на другите учесници на системот. Заради објаснување на вкупниот контекст, потребно е да се укаже дека изградбата на адекватен систем е исклучително важна задача за секоја држава, независно од нејзиниот развој. Но, она што засега доминира, и тоа во поширoки рамки, е фактот дека секоја земја во светот зависи од критичната инфраструктура. Современиот свет стана многу зависен од одредени видови критична инфраструктура, како што е енергетиката (електрична енергија, нафта или гас), телекомуникациите,

транспортот, финансискиот сектор и секое нивно нарушување води до сериозни потешкотии, кои генерално влијаат и врз функционирањето на општеството (Lazari A., Mikac R., 2022:3-4).

Интересен е фактот дека пристапот на регулација на ова подрачје се разликува од држава во држава, во зависност од перцепцијата за заканите, старите искуства и знаењето, стабилноста на државните институции и сл. Притоа, не смее да се игнорира фактот дека, покрај сличности и разлики на развиеноста на државите, сите под влијание на новите безбедносни предизвици треба континуирано да го организираат, надградуваат и подобруваат системот за заштита на критичната инфраструктура.

Во оваа смисла, меѓу аналитичарите постои едногласност дека размената на добрите практики и искуства помеѓу државите од регионот, или пак, внатре во рамките на Европската Унија, или надвор од нејзините граници, е повеќе од потребно.

Имено, истражувањата покажуваат дека е потребно преку ширење на мрежата на учесници да јакне отпорноста и заштитата на националната и на европската критична инфраструктура. Притоа, како аргумент можат да се расчленат следниве неколку релации по ова прашање:

Прво, *потребата од постојано јакнење на отпорноста на критичната инфраструктура.*

Второ, *способноста и можноста на национално ниво да се воспостави систем за заштита на критичната инфраструктура.*

Трето, *европската критична инфраструктура е добра подлога за понатамошен развој на ова подрачје.*

Во таа насока, се наметнува потребата за една соодветна анализа на пристапот кон остварувањето на заштита на критичната инфраструктура. За таа цел, ќе се анализираат три држави, и тоа: Хрватска, Србија и Црна Гора. Всушност,

изборот на овие земји нема цел поединечната анализа да биде обемна ниту пак, неминовно репрезентативна, туку изборот е направен:

1. Од аспект на Европска Унија, каде што ЕУ има изградено насоки за нормативно регулирање на прашањата од сферата на идентификација, означување и заштита на европската критична инфраструктура, со посебен акцент на обврските произлезени од *Директивата на Советот на ЕУ 2008/114/ЕК за идентификација и означување на европската критична инфраструктура.* Исто така, со оваа Директива се утврдува дека земјите членки се одговорни за воспоставување рамка за заштита на европските критични инфраструктури. Но, исто така, овој пристап за многу земји претставуваше јасна покана за дефинирање на начините за заштита на нивната национална критична инфраструктура. За таа цел за анализа е избрана Република Хрватска, земја членка на ЕУ и како искуство од активностите во фаза до стапување во полноправно членство. Важно е да се посочи пристапот на Република Хрватска, како дел од процесот на постигнување на полноправно членство во Европската Унија, која во оваа фаза се обврза нормативно да ги подреди и уреди прашањата за идентификација, означување и заштита на европската критична инфраструктура, преку транспортирање на Директивата ЕУ 2008/114/ЕК во нејзино законодавство и нејзино применување до моментот на стапување во полноправно членство (Mikac, R. 2019:131). Процес кој како позитивен пример е од големо значење за Република Северна Македонија, Република Србија и Република Црна Гора.

2. Од аспект на земји со перспектива за членство во ЕУ, како на пример Република Северна Македонија, Република Србија и Република Црна Гора, кои до постигнување на полноправно членство во Европска

Унија треба нормативно да ги подредат и уредат прашањата за идентификација, означување и заштита на европската критична инфраструктура.

3. Од аспект на НАТО, каде што во повеќе земји е утврдена прецизна индикативна спецификација на критичната инфраструктура. А самото членство во НАТО, за Хрватска, Црна Гора и Северна Македонија значи дека сме рамноправен дел од колективната безбедност, која може да ни помогне и да ја подобриме отпорноста на критичната инфраструктура. Во контекст на ова, важно е да се напомене дека после Варшавскиот самит во 2016 година, прашањето за критичната инфраструктура и нејзината отпорност е повеќе акцентирано во сите НАТО документи. Конкретно, тоа значи дека се дефинирани клучни области според кои НАТО ќе ја цени отпорноста во секоја земја членка. Или пак, преку документите НАТО се поставува како актер кој е подготвен да придонесе кон континуитет во владеењето и испораката на основните услуги – „continuity of government“, и тоа во широка смисла, од енергија, транспорт, комуникации и др. Од овој аспект, од особено значење е да се посочи дека НАТО и сојузниците, вклучително и ние, мора да ја регулираме отпорноста на критичната инфраструктура.

4. Од аспект на безбедноста, Хрватска, Северна Македонија, Србија и Црна Гора имаат исто безбедносно опкружување, ранливоста на регионот и степенот на порозност/хибридни закани.

5. Од аспект на тековниот развој на оваа област во Република Хрватска, Република Србија и Република Црна Гора, важно е да се спомене дека сите три држави имаат донесено Закон за критична инфраструктура.

6. Од аспект на национален пристап кон утврдување на критериуми за процена на критичната инфраструктура.

Затоа, основна задача на оваа анализа е преку овие примери да го проучи тековниот развој на оваа област, посветено внимание на стратешки и нормативни документи, заокружена законска рамка со која го започнаа процесот на изградба на систем за заштита на критичната инфраструктура.

3.2. Пристапот на Република Хрватска во заштитата на критичната инфраструктура

Република Хрватска е европска држава, во геополитичка смисла средноевропска и средоземна држава, сместена во Западен Балкан. Хрватска од април 2009 година е земја членка на НАТО и од јули 2013 година таа е членка на ЕУ. Таа е држава што опфаќа површина од 87.661 км², а копно 56.594 км², со вкупен број на население во 2020 година од 4.047.680 жители, според Светска банка (The World Bank, 2020).

Хрватска во моментов не располага со систем за заштита на критичната инфраструктура кој би можел да се смета за целосно воспоставен како таков. Но, пред сè, мора да се нагласи дека контурите на системот пополека се поставуваат. Изгледа дека напорите во последните пет години се насочени за негово спроведување. Токму затоа, од голема важност се обврските што ги постави Хрватска за побрз развој на системот за заштита на критичната инфраструктура. Меѓутоа, Хрватска тоа не го препушти на спонтано и неорганизирано, некоординирано дејствување, туку осмислено и планирано ги насочуваше активностите кон остранување на слабостите и создавање на услови за побрз развој. Всушност, таа тенденција веќе се воочува преку поставена нормативна основа и усвоен Закон за критична инфраструктура, со што ја постави неопходната начелна нормативна рамка за започнување на плански развој на овааа област. Исто така, настојувањата се насочени кон определување на клучни актери, со цел да се изнајде основа врз која ќе се темелат и воспоставените процеси.

Имајќи ја предвид ваквата системска уреденост, може да се заклучи дека таа претставува основа за понатамошниот развој на оваа област и дека нејзиниот развој тргнува по нагорна линија. Всушност, тоа е еден од показателите дека планираните активности и нивната операционализација даваат придонес за побрз и поефикасен развој кон градење на систем за заштита на критичната инфраструктура. Сето тоа е потврдено низ неколкуте различити развојни фази, нивно надополнување и изнаоѓање нови решенија (Mikac, R. 2019:128).

Оттука, имајќи ја предвид насоченоста на Хрватска кон изградбата на системот за заштита на критична инфраструктура, од една страна, и голем број на активности, од друга страна, анализата укажува дека Хрватска поминува низ четири фази, и тоа:

Прва фаза, период до влегување во членство во НАТО и Европската Унија и воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура (од 2008 година до 2013 година).

Втора фаза, продолжување на процесот на воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура (од 2014 година до 2015 година).

Трета фаза, структурни предизвици за воспоставување на систем за заштита на критичната инфраструктура (од 2016 година до 2018 година) (Mikac, R. 2018:105).

Четврта фаза, подготовка на нов Закон за критична инфраструктура (од 2019 година до денес).

3.2.1. Прва фаза – од 2008 до 2013 година

Хрватска во периодот од 2008 година до 2013 година обрна внимание во однос на заштитата на критичната инфраструктура во своите стратешки документи и нормативни акти од полето на одбраната и безбедноста. Овие акти претставуваат

основа за идентификувањето и заштитата на критичната инфраструктура, предуслов за формирање комплетна рамка на закон и правила за да го започне процесот на развој на системот за заштита на критичната инфраструктура.

Набљудувано од тој контекст, можеме да констатираме дека вниманието е сосредоточено на неколку стратегиски документи и на одредени национални закони, и тоа:

- Национална стратегија за заштита од и борба против тероризмот, донесена во 2008 година;
- План за заштита и спасување;
- Закон за приватна заштита, донесен 2010 година;
- Процена на ризици за Република Хрватска од природни и техничко-технолошки катастрофи и големи несреќи (донесен во 2013 година);
- Национална стратегија и Акцискиот план за непролиферација на оружје за масовно уништување (донесен 2013 година).

Од анализа на донесените стратегиски и национални закони, можеме да извлечеме неколку констатации, и тоа:

Прво, концептот на критична инфраструктура се согледува од аспект на заштитата од терористичките закани.

Второ, Хрватска треба да изгради национални капацитети за заштита на критичната инфраструктура.

Трето, не е дадена дефиниција за критична инфраструктура, туку таа се споменува во контекст на вршење преглед на обврските што ги имаат учесниците вклучени во спроведувањето на мерките за заштита и спасување (План за заштита и спасување, 2010 година).

Четвртата констатација произлегува од анализа на Законот за приватна заштита од 2010 година, во кој се посочува

дефиницијата за критична инфраструктура. Притоа, мора да се има предвид дека со клучната законска нормативна рамка, државата предвидува дека треба да се заштитат критичните инфраструктурни објекти, но сопственикот или управителот е тој кој одлучува на каков начин истото ќе се спроведе (Mikac, R. 2019:129). Следејќи ја анализата, се констатира дека приватните агенции за обезбедување располагаат со значителни капацитети и за таа цел истите ќе се ангажираат.

Петтата констатација е дека во стратегиските документи (Проценатa на ризиците) Хрватска критичната инфраструктура ја става во поширокиот контекст на заштитата од природни и антропогени извори на закани. Меѓутоа, од аспект на истражувањето на позитивните практики за регулирање на критична инфраструктура, треба да се нагласи дека во рамките на овој документ се споменува „концептот на заштита на критичната инфраструктура“ и тоа како „заеднички назив за мрежите и системите кои се клучни за функционирањето и животот на заедницата, а чие оштетување или уништување може да предизвика привремени или долгорочни нарушувања и кризи, и коишто се од особен интерес и значење за Република Хрватска како целина, но делумно и за единиците на локалната и регионалната самоуправа“ (Влада на Република Хрватска, 2013/6:72). Притоа мора да се има предвид дека до 2013 година „критичната инфраструктура во Хрватска не е дефинирана, ниту пак, воопшто е проценета потребата од заштита и обезбедување, континуирано функционирање на истата, а особено при итни состојби“. Следејќи го овој недостаток, Република Хрватска изработува предлог-закон за критична инфраструктура, кој е втор позитивен момент што ги зема предвид деловите од законодавството на ЕУ содржани во Директивата 2008/114/ЕК на Советот, од 8 декември 2008 година, за идентификација и означување на европската критична инфраструктура и процена на потребата за подобрување на нивната заштита (Европска Унија 1.345/75, 23.12.2008) и го усогласува националното законодавство со таа регулатива на Европската Унија. (Влада на Република Хрватска, 20136:73). Проценатa на ризикот ја подвлекува потребата од подигнување на нивото на нивото на безбедноста на критичната инфраструктура што ќе ја

овозможи идната нормативна рамка и одредбите кои би требало со истата да се пропишат (Микац, Р. 019: 130).

Оттука, основна е констатацијата дека решението на овие причини ќе се овозможи со идната нормативна рамка и одредбите кои би требало со истата да се пропишат во Република Хрватска. За таа цел, Република Хрватска во наредниот период презеде значаен чекор. Конкретно, со цел да ја имплементира Директивата на Европската Унија, хрватската Влада во 25.12. 2010 година донесе Одлука за формирање на Меѓуресорска работна група за подготовка на активности потребни за дефинирање и утврдување на националната критична инфраструктура во Република Хрватска (Čemerin, D. 2013:442).

Шестата констатација произлегува од анализа на Националната стратегија и Акцискиот план за непролиферација на оружје за масовно уништување, донесени во 2013 година, според кои заштитата на критичната инфраструктура се споменува како конкретна цел. Притоа, треба да се нагласи дека конкретна цел е заштитата на критичната инфраструктура и населението од криза предизвикано од масовно уништување.

Истражувањата покажуваат дека во донесените стратегиски документи и национални закони во периодот од 2008 година до 2013 година, се препознава дека постои јасен интерес за нормативно обликување на концептите поврзани со критичната инфраструктура. Но, лимитирачка околност претставува тоа што до 2013 година сè уште „ниеден документ не обезбеди целосно решение за управување со ризиците по функционирањето на критичната инфраструктура, како и рамка за нејзина заштита, пред сè поради податокот дека ова не беше посочено како главна цел во наведените документи“ (Mikac, R. 2019: 130).

Оттука, од особено значење е да се посочи дека донесените стратегиски документи и националните закони во периодот до пристапување кон Европската Унија имаат големо значење за остварување на позитивните цели иницирани од

законодавците и експертите во оваа област, а ќе издвоиме дека „се препознаваат како усогласен став околу потребата да се воспостави конкретна област посветена на развојот на критичната инфраструктура".

Подеднакво е значајно да се издвои уште еден момент. Конкретно, како негативен заклучок во однос на начинот на кој се разгледувала и артикулирала заштитата на критичната инфраструктура во стратегиските документи и закони, клучно е дека таа не била воопшто оформена како целина.

Исто така, од анализата на овој период произлегува една „позитивна тенденција", која не само што доминира потребата од дефинирање на критичната инфраструктура, туку може слободно да се заклучи дека и се препознава јасната потреба од посебно нормативно регулирање на оваа област. За таа цел, формираната Меѓуресорска работна група за подготовка на активности потребни за дефинирање и утврдување на националната критична инфраструктура во Република Хрватска, ќе даде посебен придонес.

На ова ќе се додаде и дека решавањето на критичната инфраструктура во Република Хрватска започна под силно влијание на Директивата 2008/114/ЕК на Советот од 8 декември 2008 година за идентификација и означување на европската критична инфраструктура и процена на потребата за подобрување на нејзината заштита, во 2011 година со која се регулира прашањето за Европската критична инфраструктура, при што се наведената Директива 2008/114/ЕК утврдува дека земјите членки се одговорни за воспоставување на нормативна рамка за заштита на европските критични инфраструктури, што за многу земји исто така претставуваше јасна покана за дефинирање на начините за заштита на нивната национална критична инфраструктура (Mikac, R. 2019:131).

Треба да се истакне дека, како дел од процесот на постигнување на полноправно членство во Европската унија, Република Хрватска се обврза нормативно да го подреди и уреди прашањата за идентификација, означување и заштита

на европската критична инфраструктура преку транспонирање на Директивата 2008/114/ЕК, во нејзино законодавство и нејзино применување до моментот на стапување во полноправно членство. Значајно е да се нагласи дека овој чекор на Република Хрватска, во оваа фаза треба да го следи и Република Северна Македонија.

Сублимирајќи ја анализата што се занимава со регулирање на областа на „управување и процена на ризик", се утврдува заклучокот дека Република Хрватска ја подвлекува потребата од подигнување на нивото на безбедноста на критичната инфраструктура, и тоа од неколку причини:

- критичната инфраструктура како темел на националната и јавната безбедност, како и на одржливиот развој и напредокот од клучен интерес, не само за населението/поединците, туку и за целокупното стопанство, општествената активност и за државата во целина;

- изложеност на опасности од природно потекло, од технички и/или технолошки процеси, вклучувајќи ги и терористичките активности во реалниот и во сајбер- просторот;

- ставањето акцент на ранливоста на критичната инфраструктура и спреченост на Република Хрватска во полн капацитет да развие алтернативни системи. Ранливоста се зголемува и поради меѓусебната поврзаност и меѓузависноста на голем број на сектори од критична инфраструктура, како на национално ниво, така и со клучните инфраструктурни сектори на соседните и на другите земји;

- недостаток од интегриран, единствен и сеопфатен систем за управување со кризи (Mikac, Cesarec, Larkin. 2018:106).

Во таа насока, Република Хрватска во 2013 година го донесе Законот за критична инфраструктура, со кој се уредуваат

правата, овластувањата и обврските на Владата на Република Хрватска и централните органи на државната управа, како и овластувањата, правата и обврските на сопствениците или управителите на критичната инфраструктура во идентификувањето, означувањето и заштитата на националната критична инфраструктура и обезбедување на нивно непречено функционирање. Но, она што го прави законот поактуелен е констатацијата дека тој:

- ги утврдува и прави дистинкција помеѓу дефинициите за национална и европска критична инфраструктура;
- ги утврдува и секторите на критична инфраструктура;
- го утврдува процесот на управување со критичната инфраструктура;
- го утврдува начинот на изработка на анализите на ризик;
- ги утврдува плановите за безбедност на сопственикот или управителот на критичната инфраструктура;
- ја утврдува позицијата и улогата на офицерите за врска за безбедноста за критичната инфраструктура; и
- потврдува дека европската критична инфраструктура е заштитена со истите мерки кои важат и за националната критична инфраструктура (Прилог бр.1: види стр. 167, Закон за критична инфраструктура на Република Хрватска)

Во овој контекст треба да се потенцира фактот дека методологијата користена при изработка на Законот за критична инфраструктура во Република Хрватска, може да биде одлична појдовна рамка за Република Северна Македонија во фаза кога ја иницира изработката на Закон за критична инфраструктура.

Од анализа на Законот не е тешко да се констатира дека тој ги постави основите за започнување на повеќересорска соработка, и тоа во:

- идентификувањето на националната критична инфраструктура;
- означувањето на националната критична инфраструктура;
- заштитата на националната критична инфраструктура; и
- соработка со соседните земји и тела на Европската Унија во означувањето и заштитата на критичната европска инфраструктура на територијата на Република Хрватска и другите земји.

По усвојувањето на нормативната рамка, се создадоа клучни предуслови за отпочнување на процес на спроведување сеопфатни дејствија за заштита, зајакнување на отпорноста и намалување на негативните влијанија во случај на закани по критичната инфраструктура (Mikac, R. 2019:133). Во овој контекст е и аргументацијата на група автори (Nađ, I., Rukavina, F., Raić, M. 2015:78) кои сметаат дека по донесувањето на подзаконските акти, неопходно е да се идентификуваат одредени критични инфраструктури од национално значење кои се во надлежност на одредени сектори на органите на централната државна управа, со цел да се обезбеди интегритет на заштитата и да се намалат негативните ефекти во случај на закани за критичната инфраструктура.

Не е тешко да се констатира дека со донесениот Закон за критична инфраструктура, Република Хрватска ги создаде темелите и ги постави предусловите за воспоставување на систем за заштита на критичната инфраструктура, како на домашните, така и на европските, доколку некои се означени како такви на територијата на Република Хрватска (Mikac, R. 2019:133).

Во рамките на активностите што се преземаат од страна на Република Хрватска, произлезени од Законот за критична инфраструктура, ќе ги издвоиме усвоените две уредби (Одлука за означување на областите во кои органите на државната управа на централно ниво ги идентификуваат националните критични инфраструктури и списоците со редоследност на областите со критични инфраструктури и Правилникот за методологијата за изработка на деловна анализа на ризици за критичната инфраструктура), кои помогнале да се обликува нормативната рамка во областа на постигнување безбедност и зајакнување на отпорноста на критичната инфраструктура.

Следејќи ги политиките и активностите на Република Хрватска во однос на регулирање на заштитата на критичната инфраструктура, можеме да констатираме дека постојат неколку клучни прашања кои се од посебен интерес за Република Северна Македонија во овој период:

- Законот претставува системска уредба за критична инфраструктура и главна нормативна точка за следење и спроведување на сите активности поврзани со заштитата на критичната инфраструктура.

- Со Законот за критична инфраструктура се овозможува да се пропишува заштитата на истата само на национално ниво без да се наметнуваат обврски на единиците на локалната самоуправа.

- Задолжително да се назначи координативно тело (Министерство за одбрана или Министерство за внатрешни работи).

3.2.2. Втора фаза – од 2014 година до 2015 година

Анализата и пристапот, а и понудените решенија на Република Хрватска, продолжија со развојот на целиот процес на заштита на системот за критична инфраструктура и во наредната втора фаза, од од 2014 година до 2015 година. Во овој

процес, поголемо влијание имаат двете стратегии, заедно со придружни акциски планови:

- Национална стратегија за спречување и борба против тероризмот; и
- Национална стратегија за сајбер безбедност.

Во овие стратегии беа забележани позитивноста, решенијата, како на пример областа на критичната инфраструктура е силно препознаена и застапена, или пак, терористичката закана и потенцијалниот напад врз националната критична инфраструктура, чиј прекин во работењето или испораката на стоки и услуги може да има сериозни последици врз националната безбедност, здравјето и животот на луѓето, имотот и животната средина, безбедноста и економската стабилност и континуираното функционирање на државниот апарат (Mikac, R. 2019:140).

Всушност, од посебно значење се определените активности во Националната стратегија за спречување и борба против тероризмот, потребни за заштита на критичната инфраструктура од тероризам, кои прецизно се наведени преку неколку мерки, и тоа:

- развој и зајакнување на националните капацитети за заштита на луѓето и имотот;
- означување и навремено активирање на посебен режим за заштита на локации и објекти од особено значење за одбраната на земјата;
- заштита на дипломатските, конзуларните и другите претставништва на Република Хрватска во странство;
- информирање на хрватските граѓани и правни лица за нивото на терористичките закани во земјите во кои патуваат или работат;
- заштита на дипломатските, конзуларните и другите странски претставништва на територијата на Република Хрватска;

- прилагодување на постојните концепти во областа на националната безбедност и правната рамка за воспоставување на системи за управување со вонредни состојби и кризни ситуации, а со тоа и во случај на терористички активности;

- зајакнување на системот за заштита и надзор на државната граница;

- зајакнување на контролата на вооружувањето и разоружувањето, како и складирањето на оружје, експлозиви и други средства што може да се искористат за извршување на терористички напади;

- зајакнување на надзорот врз превозот/сообраќајот и употребата на стоки со двојна намена;

- воспоставување на систем за заштита на критичната инфраструктура, со почитување и примена на постојните секторски мерки, планови и надлежности за заштита и воспоставување на систем за продолжување на критичните операции на деловната инфраструктура;

- зајакнување на системот за цивилна заштита;

- зајакнување на надзорот во однос на можните сајбер-напади (Национална стратегија за спречување и борба против тероризмот, точка 2.3).

Оттука, врз основа на анализата на Националната стратегија за сајбер-безбедност и Акцискиот план за имплементација на Националната стратегија за сајбер-безбедност, можеме да го заклучиме следното:

- Двата документи обрнуваат внимание на критичната инфраструктура во многу посилна мерка отколку други национални стратегии, процени и планови од нејзиното усвојување (Mikac, R. 2019:140).

- Анализата покажа дека Стратегијата посветува многу простор на критичната комуникациска информатичка инфраструктура, односно инфраструктура која е доведена во врска со управувањето со сајбер-кризите.

- Анализата покажа дека Стратегијата ја нагласува важноста на Законот за критична инфраструктура. Имено, Стратегијата истакнува пет цели кои треба да се реализираат за да се заштити критичната комуникациска и информатичка инфраструктура и делотворно да се управува со сајбер-кризите, и тоа:

    - Прва, утврдување на критериуми за препознавање на критичната комуникациска и информатичка инфраструктура .

    - Втора, утврдување на задолжителни безбедносни мерки што ги применуваат сопствениците или управителите на означената критична комуникациска и информатичка инфраструктура.

    - Трета цел, зајакнување на превенцијата и заштитата преку управување со ризици.

    - Четврта, зајакнување на јавно-приватните партнерства и техничката координација во обработката на инциденти поврзани со компјутерската безбедност.

    - Петта, воспоставување на капацитети за ефективна реакција кон заканата што може да предизвика сајбер-криза (Национална стратегија за сајбер безбедност, точка 5.2.).

Со определените цели стана очигледно дека тие се важен аргумент во поддршката на потребата да се идентификува комуникациска и информатичка инфраструктура и сите потребни постапки што беа пропишани со него, а кои не беа имплементирани.

3.2.3. Трета фаза – структурни предизвици за воспоставување на систем за заштита на критичната инфраструктура (од 2016 година до 2018 година)

Максимата на создавањето на соодветен систем за заштита на критичната инфраструктура, значеше континуирана работа и инвестирање во развојот на областа, проследено со континуирано спроведување на прописите, мерките и постапките во заштитата на критичната инфраструктура, која успешно продолжи и во третата фаза.

Анализата на овој период укажа на преземени нови активности и изработени два важни документи во областа на националната безбедност кои ја стават критичната инфраструктура во списокот на приоритети а тоа се:

- *Стратегијата за национална безбедност на Република Хрватска;*
- *Законот за систем на внатрешна безбедност.*

Објаснувањето на аналитичарот Микац укажува дека Стратегијата за национална безбедност на Република Хрватска, меѓу другото, носи девет стратегиски цели за Република Хрватска кои подразбираат конкретно спроведување на националната безбедносна политика. Микац, на пример, вели дека „големо внимание се посветува на критичната инфраструктура со првичната определба дека за безбедно општество, потребно е да се заштити животот, да се спасат луѓето и да се заштити критичнатsa инфраструктура“ (Mikac R. 2018: 126).

Во овој контекст значајно е да се забележи дека е „наведена потребата да се утврди кои делови од критичната инфраструктура мора да останат во мнозинска сопственост на државата, со што ќе се спречи вложените максимални напори за спречување и заштита на некоја критична инфраструктура потоа да

бидат легитимно купени на берзата со преземање на мнозинскиот удел во компанијата од страна на некој кој е потенцијално несоодветен да управува со истата“ (Mikac, R. 2019:144). Ова решение спаѓа во редот на т.н.мерка на афирмативна акција кои се во функција на обезбедување на критичната инфраструктура, а како решение треба да го примени и Република Северна Македонија, и тоа во фаза на подготовка и измени на стратегии.

Исто така, во овој период во Република Хрватска од исклучително значење е и *Стратегијата за националната безбедност,* како основен стратешки документ, *Законот за систем на внатрешна безбедност* и *Законот за сајбер-безбедност,* во кои се истакнати политиките и инструментите за остварување на националните визии и интереси, а посебно место се посветува и на концептот на критичната инфраструктура.

Имено, со овие документи и активности Република Хрватска уште еднаш ја потврдува определбата да ја идентификува и посочи критичната инфраструктура. Исто така треба да се прецизира дека овие акти ја истакнаа потребата од измена и дополнување на Законот за критична инфраструктура.

3.2.4. Четврта фаза – подготовка на нов Закон за критична инфраструктура (од 2019 година до денес)

Имајќи го во вид фактот дека областа на критичната инфраструктура претставува мошне динамична сцена, во која своја улога играат најразлични актери, политики, потреби и начини на согледување на нештата, а истата претставува и дел од националната безбедност и токму затоа таа е во фокусот на вниманието при многу настани и случувања во Република Хрватска. Затоа, треба да се земе предвид дека во изминатите години Република Хрватска на овој план презеде многу позитивни чекори. На пример, презеде едно прагматично решение, конкретно, со донесувањето на Законот за критична

инфраструктура и придружните документи, Хрватска ги вклучи сите главни сектори. Во дадените околности корисно е во четвртата фаза, која сè уште е отворена, и ќе биде корисно постојните активности да се прилагодат кон сегашниот контекст и при идентификацијата и означувањето на првите критични национални инфраструктури, акцентот да се стави врз два клучни сектори: транспортот и енергетскиот сектор, со цел да се остане во тек со сето она што е од најголем интерес за Европската комисија. Во овој период, Хрватска треба да работи и на други сектори за да ја добие целокупната слика за состојбите и да го изгради системот за заштита на критичната инфраструктура. Нивото на заштита ќе зависи од приоретизација на секој сектор, според секторски и меѓусекторски критериуми, т.е. преку проценување „што е повеќе, а што е помалку важно за Хрватска". И оттука е разбирливо што шест години од донесувањето на Законот за критична инфраструктура, Република Хрватска не успеа во процесот на воспоставување на систем за заштита на критичната инфраструктура. Аналитичарите ги утврдија позитивните, но и негативните чекори и решенија и Република Хрватска во изминатата година интензивно работи на изработка на нов Закон за критична инфраструктура, кој треба да ги реши отворените прашања, проблеми и предизвици.

3.3. Пристапот на Република Србија во заштитата на критичната инфраструктура

Република Србија е европска континентална држава, во геополитичка смисла сместена во Југоисточна Европа, поточно, сместена во Западен Балкан. Таа е држава што опфаќа површина од 77.474 км^2, со вкупен број на население во 2020 од 6.899.126 жители, според Светска банка (The World Bank, 2020).

Ефикасен систем за заштита на критичната инфраструктура создава предуслови за нормално и непречено

функционирање на државата и општеството. Затоа, клучен фактор за намалување на ризиците и зголемувањето на заштитата на критичната инфраструктура е во воспоставување на сеопфатен пристап, конструктивна соработка која ќе е заснована на заедничко регулаторно опкружување, стандарди, заемна доверба, обука, истражување и развој и размена на информации (Pavić M., Jokanović I., 2021:18-19). Република Србија во моментов не располага со систем за заштита на критичната инфраструктура кој би можел да се смета за целосно воспоставен како таков. Но, и за Република Србија, мора да се нагласи дека во последните пет години контурите на системот пополека се согледуваат во насока на негово поставување и спроведување и за тоа сведочат промените во стратегиските, нормативната и институционална рамка за заштита на критичната инфраструктура. Во овој контекст, Кековиќ е експлицитен: Република Србија идентификувањето на критичната инфраструктура не го започна од нула, бидејќи некои постоејни правни акти дадоа солидна почетна основа (Keković, Z. 2022:73). Неговиот став кореспондира со оној на Милосављевиќ и Вучиниќ, кога велат дека „уште во екс СФРЈ во средината на педесеттите години, националната критична инфраструктура била штитена преку внатрешната безбедност, со помош на полициски и разузнавачки служби“ (Milosavljević B., Vučinić D. 2021:45). Во овој контекст, Милосављевиќ и Вучиниќ се експлицитни: „критичната инфраструктура и целиот друг државен или јавен имот биле заштитени со сеопфатна мрежа, позната како систем на општествена замозаштита“ (Milosavljević B., Vučinić D. 2021:45). Нивните ставови кореспондираат со оние на Павиќ и Јокановиќ (Pavić M., Jokanović I. 2021:19), кога велат дека „последните години Република Србија вложува значајни напори во создавање на интегриран систем за заштита и спасување, кој адекватно ќе одговори во услови на загрозување, пред сѐ на човечкиот живот, но и на критичните национални ресурси“.

Оттука, имајќи ја предвид насоченоста на Република Србија кон изградбата на системот за заштита на критична

инфраструктура, од една страна, и голем број на активности, од друга страна, анализата укажува дека Србија поминува низ три фази, и тоа:

Прва фаза, или најдолгата фаза.

Втора фаза, продолжување на процесот на носење на законска рамка за критичната инфраструктура (од 2009 година до 2018 година), вклучително и активности во делот на евроинтеграција на Србија во Европската Унија.

Трета фаза, која претставува период на структурни предизвици за воспоставување на систем за заштита на критичната инфраструктура (од 2018 година до денес).

3.3.1. Прва фаза

Во развојот на системот за заштита на критичната ионфраструктура значајна е Првата фаза, која е најдолга од временска дистанца. Имено, во овој период се донесени повеќе законски и стратешки документи од полето на одбраната и безбедноста, и без амбиција да ги анализираме сите, акцент ќе ставиме само на неколку. Според анализата, постои став дека уште во екс СФРЈ во средината на педесеттите години, националната критична инфраструктура била штитена преку внатрешната безбедност, со помош на полициски и разузнавачки служби. Овој тренд продолжил и во втората половина на седумдесеттите години од XX век, познат како систем на општествена самозаштита. Според анализата на Милосављевиќ и Вучиниќ, после тоа, следува период од 1973 до 1990 година, во кој е имплементиран концептот на оптествената замозаштита. Според нив, донесени се два закони, и тоа: Закон за основите на општествена самозаштита и Закон на систем за општествена самозаштита, со кои нормативно се регулира организацијата, правата и должностите на Службата за заштита во претпријатијата. За нашата анализа значајни се двата закони. Конкретно, Законот за основите на општествена самозаштита претставува правна

и политичка рамка за организирање и спроведување на општествената самозаштита на имотот на претпријатијата, на активностите на локалната заедница и на секој граѓанин како субјект на јавната безбедност. Оптествената замозаштита се одвивала преку три нивоа:

- внатрешна стручна контрола;
- самоуправна работничка контрола и
- физичко-техничко и противпожарно обезбедување.

Додека со Законот на системот за општествена самозаштита се регулира делокругот на работењето на службата за обезбедување во организациите и нивното место во системот за безбедност (Milosavljević B., Vučinić D. 2021:46).

Следен документ кој заслужува внимание е Уредбата за објекти и региони од посебно значење за одбрана на Република Србија. Во согласност со Уредбата, утврдено е дека за објекти од посебно значење за одбрана на Република Србија се сметаат оние за кои со процена се утврдило дека со нивното оштетување, односно откривање на видот, намената или локацијата, кога за нив е одредена тајност, може да настанат тешки последици за одбраната и безбедноста на државата. Со други зборови, во оваа група спаѓале објекти и региони во доменот на сообраќајот, телекомуникации и врски, енергетика, водостопанство и индустријата (Milosavljević B., Vučinić D. 2021:47). Авторите во центарот на својата анализа констатираат дека во овој документ не се наведува тероризмот како безбедносен ризик, предизвик или закана, но се спомнуваат големи технички системи, објекти и реони како клучни објекти „кои можат да бидат загрозени, кои имаат посебно значење од аспект на одбрана на земјата и со нивното загрозување ќе биде загрозен континуитетот во функционирање на државата и општеството (Milosavljević B., Vučinić D. 2021:47).

3.3.2. Втора фаза – од 2009 година до 2018 година

Втората фаза е периодот од 2009 година до 2018 година. Фаза кога Србија донесе повеќе стратешки документи и нормативни акти од полето на одбраната и безбедноста, во кои посебен акцент беше ставен во однос на заштитата на критичната инфраструктур. Овие акти претставуваат основа за идентификувањето и заштитата на критичната инфраструктура, предуслов за формирање комплетна рамка на закон и правила за да го започне процесот на развој на системот за заштита на критичната инфраструктура.

Набљудувано од тој контекст, можеме да констатираме дека вниманието е сосредоточено на неколку закони, подзаконски акти и стратегиски документи релевантни за заштита на критичната инфраструктура, и тоа:

- *Закон за планирање и градење, Национално собрание на Република Србија, 2009 година;*
- *Закон за тајност на податоците, Национално собрание на Република Србија, 2009 година;*
- *Закон за вонредна состојба, Службен гласник на Република Србија, бр.111/2009.*
- *Уредба за содржина и начин при изработка на план за заштита и спасување во вонредни ситуации.*
- *Национална Стратегија за заштита и спасување во вонредни ситуации, Национално собрание на Република Србија, 2011 година;*
- *План за заштита и спасување во вонредни состојби, Влада на Република Србија, 2011 година;*
- *Насока за методологијата за процена на ризикот, Влада на Република Србија, 2011 година;*

- *Закон за приватна безбедност, Национално собрание на Република Србија, 2013 година;*
- *Закон за информатичка безбедност, Национално собрание на Република Србија, 2016 година;*
- *Закон за заштита на животната средина, Национално собрание на Република Србија, 2018 година;*
- *Закон за води, Национално собрание на Република Србија, 2018 година;*
- *Закон за намалување на ризиците од катастрофите и управување со вонредни состојби, Национално собрание на Република Србија, 2018 година;*
- *Закон за критична инфраструктура, Национално собрание на Република Србија, Службен гласник бр.87/ 2018 година.*

Постојат истражувања според кои се тврди дека Република Србија направила значајни напори во создавањето на интегриран систем за заштита и спасување, кој на адекватен начин може да одговори и во услови на загрозување на критични национални ресурси. Потврда за ова е Законот за вонредна состојба кој е усвоен во 2009 година и со кој државата го определила Министерството за внатрешни работи да биде надлежно за изработка на процена за загрозеност од елементарни непогоди и други несреќи (Škero M., Alejević V. 2015:201). Исто така, во согласност со Законот, чл.46, се *„пропишува дека со проценатa за загрозеност се идентификуваат потенцијалните извори на загрозување, како и можните последици, потреби и можности при спроведување на мерки и задачи за заштита и спасување од елементарни непогоди и други несреќи"*.

Во Планот за заштита и спасување во вонредни состојби е истакната проценатa на критичната инфраструктура од аспект на природните катастрофи и други големи несреќи. Меѓутоа, ниту овој ниту другите наведени документи не ја дадоа дефиницијата за поимот на критичната инфраструктура.

Во Насоката за методологијата за процена на ризикот и во плановите за заштита и спасување во вонредни состојби, утврдени се критериуми за процена на критичната инфраструктура, а за секторите земени е предвид нивната ранливост од природни катастрофи и други несреќи. Меѓутоа, ќе се согласиме дека од националното законодавство, методологијата го содржи најсеопфатниот пристап кон заштитата на критичната инфраструктура, таа беше фокусирана на идентификување на изворите на закани и особено на последиците што нарушувањето или прекинот на работата на објектите може да го има врз економијата и екологијата. Во рамките на оваа анализа може да се посочи дека оваа методологија не вклучуваше пристап од сите опасности, ниту пак, мерки за подобрување на отпорноста што би можеле да ги намалат негативните ефекти од природните и другите катастрофи врз инфраструктурата, вклучително и каскадните ефекти предизвикани од меѓузависности. Конкретно, Законот за одбрана (Народно собрание на Република Србија, 2018 година), со подзаконските акти се однесуваат главно на одбранбената индустрија на Србија, но и на други индустриски и инфраструктурни објекти, со кои за време на војна, вонредна состојба или мобилизација на Армијата на Србија, првенствено ќе се обезбедуваат објектите пропишани од Министерството за одбрана.

Друг релевантен закон за идентификација на критичната инфраструктура е Законот за планирање и градење и неговите придружни планови, како на пр. Просторен план на Република Србија, проследен со регионални и локални планови и др. Посебно се важни просторните планови на областите за специјална намена, кои речиси целосно се совпаѓаат со критичната инфраструктура.

Една од најважните законски новини предвидена со Законот за информатичка безбедност е формирањето на Национален центар за превенција од безбедносни ризици во ИКТ системи, тело задолжено за брз одговор на инциденти, како и собирање и размена на информации за безбедносните

ризици на информациските и комуникациските системи (чл.5, став 1).

Како што може да се заклучи, до донесувањето на Законот за критична инфраструктура ова прашање не беше системски регулирано. Во овој случај, примарно екстерната ориентација на Србија кон прилагодувањето на заштитата на критичната инфраструктура, ја заменува една широка агенда на процеси и законско решение. Тоа, всушност, е и дел меѓу обврските на Република Србија во процесот на пристапување кон Европската Унија. Република Србија во 2018 година го донесе Законот за критична инфраструктура и овој закон ги регулира националните и европските критични инфраструктури, идентификација и назначување на критичната инфраструктура на Република Србија, заштита на критичната инфраструктура, јурисдикцијата и одговорноста на органите и организациите од областа на критичната инфраструктура и информации, известување, поддршка за донесување одлуки, заштита на податоци, управување и надзор на критичната инфраструктура. Според овој закон, национална критична инфраструктура се дефинира како системи, мрежи и објекти или нивни делови, чиешто нарушување во работата или прекин во испораката на стоката може да предизвика сериозни последици за националната безбедност, здравјето и животите на луѓето, имотот, животната средина, безбедноста на граѓаните, економската стабилност или загрозување на функционирањето на Република Србија (чл.4 од Законот за критична инфраструктура, 2018).

Од анализа на Законот за критична инфраструктура, ќе го издвоиме и чл.6, во кој се наведени сектори, во кои се врши идентификацијата и се определува критичната инфраструктура. Конкретно, следните сектори се идентификувани како критична инфраструктура, и тоа:

- енергија,
- транспорт,
- снабдување со вода и храна,

- јавно здравје,
- финансии,
- телекомуникации и ИТ,
- заштита на животната средина и
- функционирање на државните органи.

Во согласност со истиот член 6, покрај горенаведените сектори, критична инфраструктура може да се определи и во други сектори на предлог на министерства надлежни за одредена област.

Според чл.7, став 6 нуди специфично решение. Имено, Законот предвидува дека заштитата, складирањето, користењето, контролата и надзорот на критичната инфраструктура во надлежност на Министерството за одбрана и Вооружените сили на Србија се врши во согласност со Законот за одбрана и Законот за вооружени сили на Србија. Додека пак, со чл.9 се задолжуваат операторите за критична инфраструктура да определат офицери за врска, односно лица кои ќе служат за контакт помеѓу операторот и министерствата, како важни институти за заштита на критичната инфраструктура.

Исто така, во Законот се нагласува дека критичната инфраструктура мора да има приоритет при изработката на планските документи од областа на просторното и урбанистичкото планирање, документите од областа на националната безбедност и од областа на намалување на ризикот и управување со итни случаи.

Развојот на системот за заштита на критичната инфраструктура во Србија има приоритетно значење, но, според оценката на аналитичарите, значајно внимание се посветува и на потребата да се донесат и сет подзаконски акти со цел поблиску да ги уреди поединечните области во заштитата на критичната инфраструктура. Тоа е еден од показателите дека Србија во рамките на остварување на таа потреба и обврска,

донесе и Упатство за методологијата за процена на ризик од природни и други непогоди, Процена на ризик од природни и други непогоди и Планови за спасување и заштита во итни случаи (Влада на Република Србија, 2019). Овие активности се потврда дека Србија има сеопфатен пристап кон креирање на систем за критична инфраструктура. Како потврда за тоа е уште еден подреден документ донесен со Законот за намалување на ризикот од катастрофи и управување со вонредни состојби. Во таа насока, Србија веќе ги дефинираше правилата за процена на ризикот што пак, ги вклучува објектите и другата инфраструктура од особено значење за критичната инфраструктура.

Оттука, интеракцијата на овие активности за заштита на критичната инфраструктура ја креира успешноста на имплементацијата, подготовката и усвојувањето на соодветна законска регулатива, која е само прв чекор од неколкуте неопходни, со кој може да се обезбеди ефективен и високо квалитетен систем за заштита на критичната инфраструктура.

Имено, аналитичарите сметаат дека најцелосно согледување на Законот за критична инфраструктура, нормативната рамка во согласност со стратегиите и законодавството, одбраната, информациите и другите безбедносни прописи обезбедуваат рамка за многу оперативни активности за исполнување на имплементација на законската регулатива донесена за заштита на критичната инфраструктура.

Исто така, треба да се земе предвид Акцискиот план за Поглавјето 24 за пристапување на Србија во Европска Унија, според која Министерството за внатрешни работи на Србија е одговорен орган за Законот за критична инфраструктура. Конкретно, во рамките на Министерство за внатрешни работи, Секторот за управување со вонредни состојби игра важна улога како централно одговорен орган и за подготовка и координација на законодавната рамка за заштита на критичната инфраструктура и за нејзино спроведување. Делот за европска критична инфраструктура е прецизиран и во Законот за критична инфраструктура од чл.12 до чл.19. Конкретно, во

Законот се дефинира и статусот на европската критична инфраструктура, на подрачје на Република Србија, кое го одредува Владата на предлог на Министерството за внатрешни работи и врз основа на барањата и согласност на заинтересираните држави членки на ЕУ. Исто така, Владата има обврска да ги информира државите членки на ЕУ за одредена европска критична инфраструктура на просторот на Република Србија (Milosavljević, B., Vučinić, D. 2021:53). Според Кековиќ, најтешката задача ќе биде поврзана со усогласување на сите други национални стратешки документи и нивните измени на релевантна основа за спроведување на областа за заштита на критичната инфраструктура (Keković, Z. 2022: 108).

Од анализа на донесениот Закон за критична инфрастуктура, можеме да извлечеме неколку констатации, и тоа:

Прво, во следниот период ќе биде неопходно да се даде приоритет на идентификување на сектори од критичната инфраструктура и да се регулираат аспектите на заштитата на критичната инфраструктура, кои се покажаа како особено проблематични во европската и глобалната практика.

Второ, регулирано јавно-приватно парнерство.

Трето, регулирање на размената на класифицираните информации.

Четврто, потребно е да се дефинираат критериуми за идентификација на потенцијални закани/ризици и меѓузависности приспособени на различни сектори на критична инфраструктура во согласност со меѓународните, европските и националните правила и стандарди. Во рамките на овој процес, различити министерства и сектори имаат различни критериуми и класификации на објекти кои се во нивна надлежност. Треба да се истакне мислењето на Кековиќ, според кој Законот за одбрана дава дефиниција на објекти кои се од особено значење за националната одбрана, додека пак, во Планот за одбрана се споменуваат стотина техничко-технолошки системи, со соодветните одбранбени планови. Оттука, тој смета дека е можно

во идните планови за заштита на критичната инфраструктура да биде вклучен и планот за одбрана (Keković, Z. 2022:73-77).

Петто, дефиницијата на релевантните критериуми за определување на критичната инфраструктура во Република Србија е директно поврзана со степенот до кој системите, процесите и активностите ќе станат критична инфраструктура. Но, денес, три и пол години од донесувањето на Законот за критична инфраструктура, аналитичарот Кековиќ констатира дека прекумерното и нереално дефинирање на критериумите за определување на критичната инфраструктура може да резултира со создавање на теоретски дефиниран систем кој во практиката не ќе може да се воспостави. Ова го потенцира и фактот што борбата за зголемување на влијанието меѓу институциите на државната администрација претставува многу важен ризик, кој нема негативно влијание само во областа на критериумите, туку и во областа на овластувањето во делот на контрола и последователно управување со системот за критична инфраструктура и, следствено, поголемо влијание и финансиски ресурси (Keković, Z. 2022:74).

Шесто, неопходно е да се земат предвид односите меѓу бизнисите, особено оние кои се во конкуренција на истиот потсектор на управувањето со критичната инфраструктура.

Седмо, неопходно е да се земат предвид односите меѓу државното и локалното ниво на управување што може да резултира со полошо функционирање на заштитата на критичната инфраструктура. Во овој поглед, *„отпорноста на критичната инфраструктура претставува интеракција на национална отпорност (бидејќи тоа се објекти од национално значење), социјална отпорност (тие обезбедуваат придобивки и благосостојба на заедниците кои ги користат нивните производи и услуги) и организациска отпорност (бидејќи тие се социо-технички системи)“ (*Keković Z., Ninković V. 2020:162). Од досегашната анализа стана очигледно дека е неопходно во Србија, преку разни фази, да дојде до развој на системот за заштита на критична инфраструктура, каде што локалната заедница и

нејзините интереси ќе бидат земени предвид. Всушност, сите овие активности се исклучително важни бидејќи се поврзани и се остваруваат во координација и јасна поделба на надлежностите и одговорностите на сите субјекти.

3.3.3. Трета фаза – од 2018 година до денес

Во Република Србија од донесувањето на Законот за критична инфраструктура во ноември 2018 година, условно можеме да кажеме дека започнува третата фаза од развојот на системот за критична инфраструктура. Процесот на идентификување, приоритет, заштита, отпорност и законско регулирање на областа критична инфраструктура е на самиот почеток. Од овој аспект, од особено значење е да се посочи значењето на подзаконските акти кои се однесуваат на овој закон, а кои се во постапка на донесување. Всушност, сите активности поврзани со усвојување на закони и подзаконски акти поврзани со критичната инфраструктура ќе помогнат во идентификација на сектори и капацитети за критична инфраструктура. Исто така, во рамките на следните активности, во оваа фаза треба да се направи приоритизација, бидејќи не сите сектори и капацитети за критична инфраструктура се подеднакво критични од аспект на нарушувања на нивното работење или пак, прекин на набавки на стоки и услуги. Она што треба да се нагласи е дека во процесот на воспоставување на нормативната рамка законодавецот најчесто го презема Acquis Communautaire in the EU context, кој е во контекст на ЕУ и отвора јавна дискусија со сите засегнати страни (Kekovi ć, Z. 2022:75-77).

Од изнесеното може да се заклучи дека идентификувањето и приоритизацијата на секторите и објектите на критична инфраструктура, како и усвојувањето на методологијата за процена на ризикот на критичната инфраструктура, улогата на јавно-приватното партнерство во областа на критичната инфраструктура, како и размената на класифицираните податоци се главни, но според Зоран Кековиќ (Kekovi ć, Z. 2022: 75-77), не и единствените предизвици со кои законодавците,

сопствениците и операторите на критичната инфраструктура и други засегнати страни во Србија ќе се соочат во наредниот период. Законот ги постави основите за започнување на повеќересорска соработка во идентификувањето, означувањето и заштитата на националната критична инфраструктура, но останаа неколку предизвици, кои можат да се надминат со донесување на подзаконски акти. Важноста на овој закон се состои од податокот дека истиот претставува системска уредба за критичната инфраструктура и главна нормативна точка, според која ќе може да се следи и спроведуваат сите активности во оваа област. За сето тоа да може да се реализира, потребна е едукација и подигање на свеста на сопствениците и операторите на критичната инфраструктура, усвојување и имплементација на национални и меѓународни стандарди и подобрена соработка со академските институции. Меѓу аналитичарите постои став дека *„ова прашање е исклучително важно, бидејќи процесот на определување на приоритети предизвика многу несогласувања меѓи сопствениците и операторите на критичната инфраструктура од една страна, и пратениците од друга страна“* (Kekovi ć, Z. 2022:75-77).

Според анализите на Кековиќ, воспоставување на механизмот за јавно-приватно партнерство во арена на заштита и отпорност на критичната инфраструктура е од особена важност, бидејќи во текот на процесот на либерализација повеќе објекти ќе преминат во приватна сопственост и приватниот безбедносен сектор ќе игра сè поважна улога.

Што се однесува до прашањето за спроведување на класифицирани податоци во системот за заштита на критичната инфраструктура, заради неговата сложеност ќе треба внимателно да се разгледа ова прашање од сите засегнати страни.

Од мноштвото активности, предизвици и обврски кои произлегуваат со донесувањето на Законот за критична инфраструктура, истражувачите ја утврдуваат и потребата да се воспостави ефикасен безбедносен систем за чувствителни и класифицирани размени на податоци на „хоризонтално“ ниво,

односно размена на податоци меѓу секторите и критични инфраструктурни системи, во споредба со „вертикалното“ ниво кое сè уште е распространето, но не и доволно брзо и ефикасно (Keković, Z. 2022:75-77).

И сосема на крај, ќе го парафразирам Џорџ Орвел, кога вели „сите се еднакви, но некои се поеднакви од другите“. Можеби затоа, сосема е логичен ставот „дека малите држави поинаку ја перцепираат состојбата на (не)безбедност од позицијата која ја имаат големите и богатите држави“. Дали малите држави, како Хрватска, Србија и Црна Гора од позиција која ја имаат и перцепцијата на (не)безбедност, можат преку носењето на Закон за критична инфраструктура, истата да ја уредат и меѓусебно да ги усогласат одредбите во законите? Дека треба и дека можат, констатираат Павиќ и Јокановиќ (Pavić M., Jokanović I. 2021: 23). Имено, тие сметаат дека министерствата на секоја од трите држави треба да бидат контакт-точки, кои, во име на нивните влади, ќе соработуваат со надлежните органи на другата држава и на ниво на Европската Унија, со цел размена на информации за критичната инфраструктура и спроведување на утврдените активности за нивна заштита и обезбедување на непрекинато функционирање. Затоа што само така може „да се одреди критичната инфраструктура и притоа да се користат критериумите усогласени со критериумите на Европската Унија, но секако, тие мораат да бидат недвосмислено формулирани и на ниво на државите во регионот. Во овој процес, критериумите треба да опфатат:

- *човечки загуби* (се проценува бројот на загинати или повредени поради прекин во функционирањето на поедини критични инфраструктури);

- *економски загуби* (се проценува според важноста на економските загуби или намалениот квалитетот на производи или услуги, вклучувајќи го и можното влијание на животната средина);

- *влијание врз јавноста* (се проценува дека преку нарушување на секојдневниот живот, вклучувајќи ги загубите

на основните услуги, ќе се влијае врз довербата на јавноста) (Pavić M., Jokanović I., 2021: 23).

3.4. Пристапот на Црна Гора во заштитата на критичната инфраструктура

Црна Гора е земја членка на НАТО. Таа е држава што опфаќе површина од 13.812 км^2, со вкупен број на население во 2020 година од 621.306 жители, според Светска банка (The World Bank, 2020). Црна Гора е средоземна и југоисточноевропска парламентарна република. Црна Гора е земја членка на НАТО и земја кандидат за членство во Европска Унија од јуни 2012 година кога Европскиот совет ја одобри одлуката за отворање на пристапните преговори. Веќе скоро десет години земјата минува низ преговарачки процеси.

Црна Гора во моментов не располага со систем за заштита на критичната инфраструктура кој би можел да се смета за целосно воспоставен како таков. Но, мора да се нагласи дека и Црна Гора, како и Хрватска и Србија, пополека ги воспоставува контурите на системот и тој од ден на ден сè повеќе добива значење и ги проширува појдовните детерминанти што ја определуваат неговата функционална инкорпорираност како важно безбедносно прашање. Со оглед на тоа и со оглед на целта на заштитата на критичната инфраструктура, организацијата на системот за заштита во Црна Гора се засновува врз систем на државни институции и би можел да биде соодветна рамка за систем за заштита на критична инфраструктура. Сето тоа покажува дека широкиот спектар на планирање на активности бара внимателна координација на придонесите на повеќе министерства и национални агенции кои денес се инволвирани и насочени кон заштитата на критичната инфраструктура. Всушност, сите овие активности на Црна Гора се иницирани од настаните кои ги карактеризираат современите меѓународни односи и кои влијаеја и доведоа до зголемување на бројот

на безбедносни предизвици и закани со висок степен на неизвесност, непредвидливост и дисконтинуитет. Во овој контекст, Марјановиќ е експлицитен: *„повеќето држави денес зависат од критичната инфраструктура, која е столб на националната економија, безбедност и напредок, и се обидуваат да обезбедат ефективен и ефикасен одговор на современите закани како што се тероризмот, организираниот криминал, природните катастрофи или сајбер криминалот, особено во контекст на итните случаи. Секоја држава, регион или поединечен сектор од критична инфраструктура се одговорна за идентификување на заканите од кои се обидуваат да се заштитат"* (Marjanović, M. 2015:97). Неговиот став кореспондира со она за кое се залага денес Црна Гора.

Всушност, таа тенденција веќе се воочува преку поставената стратешка и нормативна рамка за заштита на критичната инфраструктура и тоа преку збир на документи кои обезбедуваат конкретни норми, директиви, јурисдикции и одговорности. Така поставените темели овозможуваат увид во задачите за имплементација на националниот систем за управување со критична инфраструкттура, заснован на Законот за определување и заштита на критичната инфраструктура донесен во декември 2019 (Injac, O. 2022:83). Со овој закон, Црна Гора ја определи одговорноста на засегнатите страни на критичната инфраструктура и се постави неопходната начелна нормативна рамка за започнување на плански развој на оваа област.

Всушност, сите овие активности се насочени кон изградбата на системот за заштита на критична инфраструктура, а анализата укажува дека Црна Гора низ процес на организирање на систем за заштита на критичната инфраструктура поминува низ три фази, и тоа:

Прва фаза, период до влегување во членство во НАТО и пристапните преговори со Европската Унија и воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура:

Втора фаза, продолжување на процесот на воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура и носење на Закон за одредување и заштита на критичната инфраструктура (2019 година);

Трета фаза, структурни предизвици за воспоставување на систем за заштита на критичната инфраструктура (од 2019 година до денес).

3.4.1. Прва фаза

Црна Гора во последните години обрна внимание во однос на заштитата на критичната инфраструктура, во своите стратешки документи и нормативни акти од полето на одбраната и безбедноста. Од овој аспект, од особено значење е да се посочи значењето на неколку закони, бидејќи истите претставуваат основа за идентификувањето и заштитата на критичната инфраструктура, односно, предуслов за формирање комплетна рамка на закон и правила, со кои се определуваат одговорности на засегнатите страни. Овие активности, се еден од показателите дека Црна Гора, посветено и организирано го започне процесот на развој на системот за заштита на критичната инфраструктура.

Набљудувано од тој контекст, можеме да констатираме дека вниманието е сосредоточено на неколку стратегиски документи и на одредени национални закони, и тоа:

- *Закон за државен имот 2009 и 2011 година;*
- *Методологија за избор на критична информатичка инфраструктура (2014 година);*
- *Закон за одбрана;*
- *Закон за информациска безбедност;*
- *Закон за заштита и спасување;*

- *Закон за заштита на лица и имот*;
- *Национална стратегија за сајбер безбедност (2018-2022);*
- *Стратегија за национална безбедност на Црна Гора од 2018 година.*

Имајќи го предвид фактот дека создавањето на соодветен, ефикасен и ефективен систем на заштита на критичната инфрастуктура, бара континуирана работа и инвестирање во развојот на областа, парафразирањето на Роберт Микац се чини сосема на место: „неопходно е да се утврдат претпоставките за изготвување силна нормативна рамка, проследено со координирано спроведување на активности". Со други зборови, не само што и натаму е валидно да се тврди дека овие активности се со цел да обезбедат усогласено спроведување на прописите, туку дури и со мерките и постапките во заштитата на критичните инфраструктури се помага и олеснува тој процес". Во тој контекст, може да се каже дека во правниот систем на Црна Гора од 2016 година се посветило внимание и Министерството за информатичко општество и телекомуникации, како надлежен орган, изработило Закон за измени и дополнување на Законот за информциска безбедност, според кој е дефинирана критична информатичка инфраструктура. Исто така, на предлог на истото министерство, Владата на Црна Гора усвоила Методологија за избор на критична информатичка инфраструктура. Врз основа на Методологијата, Министерството за јавна управа, кое наследило одредени надлежности на Министерството за информатичко општество и телекомуникации, во соработка со други надлежни институции ја дефинирале листата на критична информатичка инфраструктура во Црна Гора, и во тек е изработка на Уредба за мерки на заштита. Почетната листа на критична информатичка инфраструктура е усвоена и следен чекор е нејзината имплементација во соработка со сопствениците на критичната инфраструктура (Mujević, M., Korač, S. 2020:712).

Законот за државен имот е донесен во 2009 година, и со него се дефинираат природните ресурси, државниот и јавниот имот, личниот имот и инфраструктурата кои се од интерес за државата (Injac, O. 2022:84). Имено, и со овој закон индиректно се дефинира критичната инфраструктура.

Севкупните досегашни предизвици се актуелизираа повторно во 2017 година со изготвување на втората *Националната стратегија за сајбер-безбедност* (2018-2022). Важно е да се посочи дека и во рамките на првата стратегија, беше обрнато големо внимание на критичните инфраструктури (точка 3, стр.12); конкретно, во неа се содржани седум клучни стратешки цели, од кои ќе ја издвоиме заштитата на критичната информатичка инфраструктура. Во втората стратегија се нагласува важноста на критичната инфраструктура, како и важноста на критични комуникациски и информатички инфраструктури со цел „зголемување на отпорноста/намалување на ранливоста на комуникациските и информатичките системи, намалување на последиците од негативните случувања (природни и техничко-технолошките несреќи и можните напади (намерни или ненамерно, овозможување на брзо и ефикасно закрепнување и продолжување на работата (стр.12).

Мујевиќ и Корач (2020:714) сметаат дека *Законот за одбрана*, кој покрај заштитата на критичната инфраструктура ја издвојува и потребата од јакнење на функциите во управувањето во услови на вонредни и кризни состојби, а кои претставуваат ризик за националната безбедност, како и овозможување соодветен придонес за заштита и зајакнување на националната безбедност на сите нивоа на државата и општеството. Водени од овие аргументи, тие препорачуваат дека сите овие елементи треба да се имаат предвид при изработка на Законот за критична инфраструктура. И според нив, очигледно е дека е потребен „робусен и сеопфатен пристап кон областа критична инфраструктура и Законот за заштита на критичната инфраструктура треба да ја одрази свеста за постоење на нови ризици и потреба од соработка на сите сегменти на општеството“.

Според *Стратегија за национална безбедност,* Црна Гора се определила кон три стратешки национални интереси, кои се реализираат преку четиринаесет стратешки интереси и цели. Во неа се наведува дека една од тие стратешки цели е достигнување на највисокиот степен на безбедност и заштита на населението, како и на критичната инфраструктура. Мујевиќ и Корач утврдуваат дека „делот поврзан со критична инфраструктура е исклучително квалитетно поставен и овозможува цела низа на политички насоки, за кои е потребно да се доработат и вклучат во Законот за критична инфраструктура. Еднакво важно е и што со Стратегијата е одредено воспоставувањето на системот на државна безбедност, кој треба да обезбеди усогласеност на подготовките и спроведувањето на прописите со кои ќе се одредуваат безбедносните мерки и постапки важни за националната безбедност, со акцент на критичната инфраструктура (Mujević, M., Korač, S. 2020:714).

Законот за заштита на лица и имот, усвоен во 2018 година, претставува правна рамка со која се регулира задолжителната техничка и физичка заштита на објекти и имот во кој се врши дејност од јавен интерес, дејности кои претставуваат зголемена опасност за животот и здравјето на луѓето, како и објекти со чие оштетување или уништување би можеле да настапат потешки последици по животот и здравјето на поголем број на луѓе (чл.13). Во истиот член се наведени задолжително заштитените објекти, по следниот редослед:

- објекти за снабдување и складирање на нафта, нафтени деривати и гас;
- објекти за снабдување и производство на вода;
- објекти за производство, преработка, дистрибуција и складирање на храна;
- објекти за производство, пренос и дистрибуција на електрична енергија;

- објекти во кои се произведуваат, користат или скаладираат радиоактивни и други опасни и штетни материи;

- објекти на сообраќајната инфраструктура (автобуски и железнички станици, аеродроми и сл.);

- објекти на финансиски институции и др.

Според досега изнесеното, може да се заклучи дека повеќето од наведените објекти се дел од критичната инфраструктура, која е наведена и регулирана во Законот за одредување и заштита на критична инфраструктура, донесен во 2019 година.

Законот за заштита и спасување опфаќа „збир на мерки и активности кои се преземаат со цел откривање и спречување на опасности од природни непогоди, пожари, техничко-технолошките несреќи, хемиска, биолошка, нуклеарна и радиолошка контаминација, последици од воено рушење и тероризам, епидемии и други несреќи, како и спасување на граѓаните и материјалните добра загрозени од нивното дејство". Исто така, овој закон ги истакнува и дефинира приоритетите за заштита на луѓето, материјалните добра, културното наследство и животната средина. Ова законско решение е важно бидејќи ќе придонесе за постигање на безбедносни услови што ќе овозможат континуиран развој на државата и општеството. Со овој закон индиректно се управува заштитата на критичната инфраструктура, преку регулирање на националните и локалните институции, процена на ризиците и подготовка на плановите за заштита и спасување (Injac, O. 2022:84). Нешто што е особено важно за дискурсот во рамките на создавање на ефикасен систем за заштита на критична инфраструктура, со што ќе се создадат предуслови за нормално и непречено функционирање на општеството и државата воопшто. За таа цел, секоја држава треба континуирано да вложува значајни напори и координирани активности, со цел изработка на адекватни механизми на заштита.

Во овој дел треба да се истакне мислењето на Мујевиќ и Корач, кои сметаат дека „отежнувачка околност во целокупниот процес при креирање на адекватниот механизам за заштита е широкиот спектар на сектори кои ги опфаќа критичната инфраструктура, како што се: енергетиката, собраќајот, снабдувањето со вода, здравство, финансии, електронски комуникации и информатички и комуникациски технологии, заштита на животната средина и др. Делумниот или пак, целосниот прекин во работењето на овие инфраструктури, може да го наруши нормалното функционирање на едниот систем и да се загрози безбедноста на државата". Авторите истакнуваат дека „кога е во прашање заштитата на критична инфраструктура, заедничка цел кон која треба да тежнеат сите уредени држави, па и Црна Гора, е изградба на адекватни механизми кои ќе спречат создавање на услови кои можат да доведат до откажување на одредена инфраструктура, или пак, несреќи, или напади на кој било од елементите на системот" (Mujević, M., Korač, S. 2020:715). Се што е посочено е навистина значајно и неопходно во процесот што следи за Црна Гора. Останува прашањето колку од тоа Црна Гора ќе може да го направи во наредната фаза, да ги искористи најдобрите практики, искуства и да ги имплементира, во фаза на изработка на Закон за заштита на критичната инфраструктура.

3.4.2. Втора фаза

Донесените нормативни и стратегиски акти ја акцентираа важноста на заштитата на критичната инфраструктура. Но тоа не беше доволно бидејќи системот за заштита на истата сè уште не беше поставен. Во такви околности се создаде можност Црна Гора да ја иницира и реализира потребата од носење на Закон за критична инфраструктура. Во декември 2019 година црногорскиот Парламент го усвои Законот за одредување и заштита на критичната инфраструктура. Целта на овој закон е да се идентификува, определи и заштити критичната инфраструктура, како и да се дефинираат надлежностите, одговорноста и другите прашања од значење за националната

заштита на критичната инфраструктура. Во Законот, исто така, е регулирана и европската критична инфраструктура (од чл.24 до чл.30), а законските одредби ќе се применуваат по влез на Црна Гора во Европска Унија (чл.38). Нормативното обликување на заштитата на критичната инфраструктура се дефинира како „збир на активности и мерки кои имаат за цел да спречат оштетување или уништување на критичната инфраструктура во случај на закани, да обезбеди функционирање на критичната инфраструктура во случај на оштетување и да спречи штетни последици во понатамошната работа, односно оштетување и уништување на критичната инфраструктура (чл.3)

Гледано од аголот на националната критична инфраструктура, може да заклучиме дека истата опфаќа повеќе сектори, кои меѓусебно се зависни. Конкретно, Законот ги определил следните главни сектори, и тоа:

- енергија;
- транспорт;
- водоснабдување;
- здравство;
- финансии;
- електронски комуникации;
- информатичка и комуникациска технологија;
- заштита на животната средина;
- функционирање на државните институции;
- и други области од јавен интерес (чл.9).

Критериумите за одредување на критичната инфраструктура може да бидат секторски или меѓусекторски (чл.6). Впрочем, таквото определување води кон утврдување на

критериумите за критична инфраструктура и тоа во рамките на секторите, а одговорноста е на министерствата кои се надлежни за одредените сектори (чл.7). Во овој дел, важно е да се наведе дека „одлуката за критериумите за утврдување на секторите на критичната инфраструктура ја носи Владата, на предлог на Министерството за внатрешни работи, кое пак, ќе ги координира активностите на одговорните министерства за утврдување на критичната инфраструктура“ (чл.7). Вака регулирани секторските критериуми за одредување на критичната инфраструктура, според Ињац (2022:83), може да создадат пречки поради можните несинхронизирани пристапи и должината на процесот. Но, добра страна е што сите оператори на критична инфраструктура се обврзани да назначат координатор за критична инфраструктура, кој е стручно оспособен за заштита на критичната инфраструктура, со положен стручен испит за заштита на критичната инфраструктура и др. (чл.18).

3.4.3. Трета фаза

Со процесот на иплементација на Законот за одредување и заштита на критичната инфраструктура, започна третата фаза од развојот на системот за заштита на критична инфраструктура во Црна Гора.

Конкретно, имплементацијата на процесот за заштита на критичната инфраструктура во Црна Гора се одвиваше низ три фази, и тоа:

- *идентификација на потенцијалната критична инфраструктура;*
- *одредување на критичната инфраструктура (на сектори и меѓусектори); и*
- *заштита на критичната инфраструктура.*

Анализата покажа дека непосредно по донесувањето на Законот за одредување и заштита на критичната

инфраструктура започна првата фаза од идентификација на потенцијалната критична инфраструктура. Гледајќи од позитивна перспектива, во оваа фаза Црна Гора многу бргу ја покрена иницијативата за изработка на регулатива потребна да се усогласи со законодавството на Европската Унија. Тоа беше основа за процесите кои се одвиваа во наредниот период. Конкретно, продолжувањето на тој процес беше поттикнато преку иницијативата на Министерството за внатрешни работи за формирање на формална меѓуресорска Работна група, која беше задолжена за изработка на Уредба за меѓуресорски критериуми за одредување на критичната инфраструктура. Овој процес е многу важен бидејќи со оваа уредба треба да се пропишат секторските критериуми за одредување на критичната инфраструктура и тоа во енергија, транспорт, снабдувањето со вода, здравство, финансии, електронски комуникации и информатичка и комуникациска технологија, заштита на животната средина и функционирање на државните институции.

Исто така, важно е да се спомене дека Работната група била составена од членови претставници на Министерството за внатрешни работи, на Министерството за сообраќај, на Министерството за економија, на Министерството за одржлив развој и туризам, на Централната банка на Црна Гора, на Министерството за јавна управа, на Министерството за здравство и на академската заедница.

Анализата укажува дека постои јасен интерес за имплементирање на Законот. Во тој поглед, посебно место и значење имаат активностите на Работната група. Имено, таа доставила предлог до Владата да утврди дека за критична инфраструктура се смета онаа инфрастуктура која во случај на застој во работењето:

- влијае на сериозно нарушување на работата или во работата може да предизвика прекин во снабдувањето со електрична енергија во траење од најмалку три дена на подрачје со повеќе од 30.000 жители;

- ќе доведе до нарушување на работата или прекин на работата во снабдувањето со нафтени деривати во траење од најмалку седум дена на подрачје со повеќе од 30.000 жители;

- оштетување на инфраструктурата која предизвикува недостаток на вода за пиење, за најмалку седум дена на територија на која живеат и работат повеќе од 15.000 жители и др. (Mujević M., Korač S. 2020:715).

Кога се разгледуваат одредбите на Уредбата, се покажува како позитивно искуство од пристапот, решението, или пак, може да се забележи дека сеофатно се одредени секторските критериуми во области, и тоа: енергетика, транспорт, снабдување со вода, здравство, финансии, информатичка и комуникациска технологија, заштита на животната средина. Ова е пример кој може да ѝ помогне на Северна Македонија во фазата на изработка на закон за критична инфраструктура и подзаконски акти, со кои нормативно и стратешки ќе се постави, регулира и развие системот за заштита на критичната инфраструктура.

Додека пак, за заштитата на критичната инфраструктура како трета фаза од имплементацијата на процесот на заштита на критичната инфраструктура треба да се наведе дека до денес не постои единствен, однапред утврден институционален модел, кој ќе укаже дека државата треба да ја штити својата критична инфраструктура. Аналитичарите Мујевиќ и Корач, сметаат дека од Владата на Црна Гора се очекува да избере рамка која најдобро одговара на нејзините карактеристики во поглед на заканите, големината и структурата на нејзината економија, како и нивната култура на јавната политика и воспоставени институционални практики. Од аспект на управување со критичната инфраструктура, посебно треба да се земе предвид основната уставна структура на државата (Mujević M., Korač S. 2020:715).

И сосема на крај, од анализата на донесениот Закон за одредување и заштита на критична инфрастуктура, можеме да извлечеме неколку констатации, и тоа:

Прво, во Црна Гора до денес не е создаден систем за заштита на критична инфраструктура. Оттука, без исклучоци, систем за заштита на критичната инфрастуктура и неговата ефикасност може да создаде предуслови за нормално и непречено функционирање на целокупниот општествен систем. Според тоа, фактите говорат дека во Црна Гора до денес се прават големи напори за да се утврдат и имплементираат соодветни механизми за заштита на критичната инфраструктура. Тука сосема се во право Мујевиќ и Корач кои тврдат дека отежнувачките фактори во овој поглед се првенствено поврзани со широкиот опсег на витални сектори опфатени со критичната инфраструктура (Mujević M., Korač S. 2020:718).

Второ, во следниот период ќе биде неопходно да се даде приоритет на идентификување на сектори од критичната инфраструктура и да се регулираат аспектите на заштитата на критичната инфраструктура, кои се покажаа како особено проблематични во европската и глобалната практика.

Трето*, ј*авното-приватно партнерство во областа на заштитата на критичната инфраструктура се воспостави во многу сектори во Црна Гора, а најфундаментално е во форма на техничка и физичка заштита на критичната инфраструктура. Во Црна Гора компаниите од енергетскиот и транспортниот сектор сè уште се во државна сопственост и во овие два сектори се присутни одредени форми на јавно-приватно партнерство во областа на заштитата на критичната инфраструктура (Injac, O. 2022:88)

Четврто, потребно е во услови на кризни состојби политиката на заштита на критичната инфраструктура да претставува еден сложен збир на различити стратегии, методологии и планови, со што приоритет ќе се даде на превенцијата на заканите и ризиците и на тој начин директно ќе се влијае врз спречување на поголеми последици за критичната инфраструктура

во државата. Комплексноста на оваа проблематика бара мултидисциплинарен пристап и примена на наменски изработени алатки за заштита на критичната инфраструктура.

Петто, потребно е државата во рамките на прифатениот концепт на безбедност задолжително да алоцира ресурси за заштита на критичната инфраструктура, затоа што само така може да смета дека системот за безбедност, како сложен систем е прилагоден да ѝ служи на заедницата. И, ако тргнеме од ставот на Мујевиќ и Корач дека критичната инфраструктура е сплет од физички и логички мрежи, дека и двете димензии во голема мера се во експанзија, тогаш оправдана е препораката дека „оние кои се ангажираат во процесот на заштита на критичната инфраструктура, треба континуирано да се стекнуваат со знаења и вештини, и со тоа би успеале да го следат напредокот на технологијата која сè повеќе и сè побргу се имплементира во системот на критичната инфраструктура". Тогаш Црна Гора е на добар пат да изгради систем за заштита на критичната инфраструктура, кој со време ќе стане ефикасен и ефективен.

4 ГЛАВА

НАЦИОНАЛЕН ПРИСТАП КОН ОТПОРНА И БЕЗБЕДНА КРИТИЧНА ИНФРАСТРУКТУРА

4.1. Пристапот на Република Северна Македонија во заштитата на критичната инфраструктура

Република Северна Македонија е земја членка на НАТО. Таа е држава што опфаќе површина од 25.713 км^2, со вкупен број на население од 1.836.713 жители (Државен завод за статистика, 2022). Северна Македонија се наоѓа во Југоисточна Европа, во центарот на Балканскиот Полуостров. Република Северна Македонија е со статус земја кандидат за членство во Европска Унија од 17 декември 2005 година, кога Европскиот совет ја одобри одлуката за отворање на пристапните преговори. Веќе скоро седумнаесет години земјата минува низ преговарачки процеси.

Северна Македонија во моментов не располага со систем за заштита на критичната инфраструктура и усвоен Закон за критична инфраструктура. Оваа област се регулира парцијално во неколку законски и стратегиски акти. И денес, во услови

кога државите се соочуваат со голем број на закани и ризици, коишто ја надминуваат првобитната рамка на подготвеност и одговор кон истите, законското регулирање на заштитата на критичната инфраструктура, пред сè, е потреба и предизвик. Кога на ова ќе се надоврзе и изменетата слика која може да се опише како ново безбедносно опкружување во кое заканите и ризиците сè повеќе произлегуваат и од невоената сфера на безбедноста, а таквото безбедносно опкружување станува многу подинамично и неизвесно, исполнето со предизвици и опасности, тогаш е јасно зошто и од каде се наметнува потребата државите да понудат сеопфатен одговор. Драстичните промени во безбедносното опкружување, предизвикани од енормната дистрибуција на закани и ризици предизвикаа промени во разбирањето и перцепирањето на заштитата и градење на отпорно општество. Значајно е да се нагласат неколку прашања кои во одредена мерка влијаат врз управувањето со ризикот и во правецот на дебатите кои придонесоа да се искристализира она што денес се нарекува проширен и продлабочен пристап на идентификување на т.н. организации од висока доверливост (High Reliability Organizations), кои, всушност, претставуваат посебни системи кои се дел од општествениот систем, а кои имаат континуирана оперативност без грешки, дури и во време на околности кои се повеќеслојно турбулентни и опасни (Roberts, K.H. 1990), а кои може да се идентификуваат како систем за контрола на воздушниот сообраќај (Weick, K.E. 1990), здравствени институции (Chassin and Loeb, 2013), односно како дел од критичната инфраструктура. Затоа е неопходно подготвеноста на Република Северна Македонија да биде разбрана во целата своја комплексност, од превенција до заштита, од мултисекторски пристап во намалувањето на ризиците и заканите по критичната инфраструктура, па сè до индивидуална надлежност и одговорност на институциите, да ги обезбеди неопходните нормативни, институционални и оперативни услови за воспоставување на заштитата на критичната инфраструктура. Безбедноста е конструкција и последица на фактори кои дејствуваат на различити нивоа и влијаат врз не/сигурноста и во контекст на класификација на заканите и

ризиците конкретно за критичната инфраструктура особено значаен е придонесот на Богнар (2009), кој за разлика од минатото, наведува повеќе сектори како економија, и тоа со посебен акцент на банкарството и финансиите, транспортот (со посебен акцент на аеродромите и железниците), дистрибуцијата, енергетиката, здравството, комуникациите, комуналните услуги, снабдувањето со храна, како и клучните владини услуги. Анализата покажува дека некои од критичните елементи во наведените сектори не се конкретно „инфраструктура", туку се мрежа или пак, снабдувачки синџири, директно поврзани со суштински производи и услуги. Токму затоа, се зголемуваат факторите кои им се закануваат на различни елементи од инфраструктурата. Затоа што критичната инфраструктура ги претставува мрежите, објектите и системите дистрибуирани во просторот, чиј континуитет во работата е под влијание на бројни природни, техничко-технолошки и антропогени фактори. Од друга страна, посебно внимание треба да се посвети на зависноста и меѓузависноста на оперативноста на критичката инфаструктура која произлегува од ефектите на самата нејзина природа, структурата и деловните процеси кои влијаат на критичната инфраструктура. Затоа е важно да се потенцира дека разни области во светот имаат свои специфични природни закани и ризици кои се повторуваат, се во интеракција со други и претставуваат потенцијална и – или директна закана за критичната инфраструктура. Потребно е поединечни национални анализи да тргнат од пристапот на Европската Унија, како таа го креираат процесот на заштитата на критичната инфраструктура, за да се добие ситуациска слика на заканите и ризиците кои, покрај другите вредности, ги загрозуваат критичните инфраструктури.

Оттука, имајќи го предвид пристапот на Северна Македонија кон изградбата на системот за заштита на критична инфраструктура, од една страна, и активностите, од друга страна, анализата укажува дека поминува низ две фази, и тоа:

Прва фаза, период до влегување во членство во НАТО;

Втора фаза, активности насочени кон воспоставување регулаторна и стратегиска рамка за заштита на критичната инфраструктура за подготовка на Закон за критична инфраструктура (од 2019 година до денес).

4.1.1. Прва фаза

Во Северна Македонија постои основна позиција според која целокупната заштита на државата од аспект на зачувување на функционирањето на критичната инфраструктура мора да се заснова на „пакетот за заштита" на инфраструктурата. Во изминатиот перид Северна Македонија презеде и реализираше голем дел стратешки и нормативни активности кои ја акцентираат важноста на критичната инфраструктура и потребата од нејзина адекватна заштита, како важно безбедносно прашање.

Во редот на најважните активности се: дефинирање на објекти како критична инфраструктура, дефинирање на мерки за нивна заштита и безбедност и дефинирање на задолженија и одговорности. Особено е значајно да се забележи дека детерминирањето на критичната инфраструктура во Северна Македонија не е во согласност со насоките за нормативно регулирање на прашањата од сферата на идентификација, означување и заштита на европската критична инфраструктура, со посебен акцент на обврските произлезени од директивата на Советот на ЕУ 2008/114/ЕК за идентификација и означување на европската критична инфраструктура како и проценета од потребата за подобрување на нејзината заштита – Директива на Советот на ЕУ 2008/114/ЕК.

Во обид да се преземат и имплементираат нормативни активности, кои пред сè, треба да ја акцентираат важноста на критичната инфраструктура и потребата од нејзина адекватна заштита, најважно од сè, е обврските кои Северна Македонија треба да ги преземе да не бидат само ad hok механизми, туку тие треба да претставуваат сеопфатен одраз на европскиот

пристап кон заштитата на критичната инфраструктура. Според тоа, Северна Македонија мора да има способности да понуди експлицитна алтернатива на „заканите за критичната инфраструктура".

Набљудувано од тој контекст, можеме да констатираме дека вниманието е сосредоточено на неколку стратегиски документи и на одредени национални закони, и тоа:

- Национална стратегија за сајбер безбедност на Република Македонија (2018-2022);
- *Закон за одбрана;*
- *Закон за внатрешни работи;*
- *Закон за управување со кризи;*
- *Закон за заштита и спасување;*
- *Националната стратегија за заштита и спасување;*
- *Планот за заштита и спасување;*
- *Закон за приватно обезбедување;*
- *Стратегија за одбрана на Република Северна Македонија.*

Националната концепција за безбедност и одбрана е основен документ кој ги истакнува политиките и инструментите за остварување на националните визии, ставови и интереси на државата, нејзиното безбедносно опкружување, политиката на националната безбедност, како и целите, насоките, областите и инструментите за нејзино остварување. Исто така, Националната концепција за безбедност и одбрана ги утврдува погледите и ставовите во однос на одбраната, менаџментот со кризи, со посебен акцент на оптимизацијата на безбедносните ресурси, организацијата и насоките за зголемување на можностите и подготвеноста на Република Македонија за одговор на предизвиците, ризиците и опасностите за безбедноста на земјата (точка 3 од Воведот). Во периодот што претстои, овој

документ треба да биде основен при дефинирање и градење на систем за заштита на критичната инфраструктура.

Иницијативата за развојот на целиот процес на заштита на системот за критична инфраструктура и утврдување на потребата од неговото воспоставување е поттикната преку изготвување и носење на *Национална стратегија за сајбер безбедност*. Во овој документ областа на критичната инфраструктура е силно препознаена и застапена и е перцепирана од аспект на заштита од сајбер-инциденти и злоупотреби, што ги прави овие закани едни од посериозни врз критичната инфраструктура. Стратегијата посветува многу простор на критичната комуникациска и информатичка инфраструктура доведена во врска со управувањето со сајбер-кризите. Исто така, Стратегијата ја потенцира потребата од зајакнување на националните капацитети за превенција и заштита од сајбер-безбедност, како и спроведување активности за подигање на националната свест за сајбер-безбедност. Ова стратегија ја врамува критичната инфраструктура во еден поширок опсег, каде што напоменува дека прекин во нудењето на одредени услуги кои се зависни од информациско-комуникациски технологии може да биде од критично значење за функционирањето на државата. Стратегијата ги дефинира сајбер-физичките закани врз критичната инфраструктура, и тоа: зголемен број сајбер-напади, вклучувајќи и индустриска сајбер-шпионажа, сајбер-вандализам и идентификација на ранливости кај енергетскиот сектор, транспортните системи и други делови од критичната информатичка инфраструктура.

Законот за внатрешни работи ја регулира обврската на полицијата да ги заштити важните објекти коишто се специфични, односно се дел од критичната инфраструктура. Во својата нормативна рамка, во чл.23 во рамките на надлежностите на Управата за безбедност и контраразузнавање стои дека меѓу другите надлежности е и „надлежноста за работи кои се однесуваат на спротиставување и заштита од тероризам“. Во рамките на овој закон во директна форма не се споменува

концептот на заштита на критичната инфраструктура, туку тој дел индиректно се препознава во чл.23.

Законот за одбрана, со кој Северна Македонија веќе долго време воспостави процес на идентификација и заштита на објекти кои се од круцијална важност за одбраната на државата. Сериозна анализа заслужуваат одредени делови и ставови изнесени во предлог-Законот за одбрана кои ги дефинираат правилата и критериумите за означување и заштита на објекти од особена важност за одбраната на државата во контекст на актот за одбрана, со јасно дефинирана методологија за процена и анализа на ризици и план за заштита на воени, како и други определени објекти (чл.42 и 43). Анализита укажува дека за најголем број на објекти може да се претпостави дека ќе се преклопуваат со потенцијалните објекти на критичната инфраструктура и тоа пред сè поради исклучителна сличност, а во во помал број и еквивалентност. Со други зборови, тоа ќе покрене повеќе прашања со различити димензии. Прво, во новиот акт за критична инфраструктура објектите треба да се вклучуваат и разграничат. Второ, од два паралелни процеси произлегува за објекти дека се еднакво важни, за да бидат класифицирани како објекти од специјална важност за Министерството за одбрана на државата, односно објекти на критичната инфраструктура, со два различити потребни системи за координација.

Законот за приватно обезбедување, кој не ја дефинира критичната инфраструктура, туку во својата нормативна рамка предвидува Владата да определува кои правни лица се должни да имаат приватно обезбедување и тоа во услови кога вршењето на нивната дејност е поврзано со ракување со радиоктивни материи, други по луѓето и околината опасни материи, предмети и објекти од особено културно и историско значење и во други случаи кога е тоа во интерес на безбедноста, односно одбраната на Република Македонија (чл.44). Од овој закон произлезе и потребата за носење на Одлука за определување на правните лица кои се должни да имаат приватно обезбедување. Оваа одлука овозможува приватните агенции за

обезбедување со своите капацитети за заштита на средствата, и тоа со човечки ресурси и со технички решенија, да придонесат да се обезбеди високо ниво на системска безбедност на критичната инфраструктура, а пред сè да дадат придонес во однос на мерките за превенција. Токму затоа, во Одлуката таксативно е наведено обезбедувањето на правни лица чија дејност е поврзана со ракување со радиоактивни материи или пак, други по луѓе и околината опасни материи; за производство и промет на големо со лекови и медицински помагала; за производство и промет на запаливи течности и гасови; за вршење на превоз на опасни материи и за ракување со предмети и објекти од особено културно и историско значење.

Следен закон кој заслужува внимание е *Законот за управување со кризи*. Овој закон разви политики кои ги вклучија главните актери, и тоа: Владата, органите на државната управа и државната власт, Армијата и силите за заштита и спасување. Иако во овој закон областа критична инфраструктура не е застапена, таа силно се препознава и се подразбира дека „материјалните добра" ја претставуваат инфраструктурата, а со оглед на фактот, ги посочува и степените на надлежност и тоа на министрите за внатрешни работи, за здравство, за одбрана, за транспорт и врски и за надворешни работи, тогаш е јасно дека лидерската функција ја има Владата во заштитата и на критичната инфраструктура. Законот посветува многу простор на одговорноста на секоја од институциите вклучени во органите и телата во системот за управување со кризи, и тоа во делот на мерки и активности за собирање на информации и идентификување на безбедносните ризици и опасности, вклучувајќи ги и оние кои ја загрозуваат безбедноста на критичната инфраструктура. Во делот на законската легислатива и овластувањата, важно е да се нагласи дека институциите опфатени во системот за управување со кризи, врз основа на нивни процени, прецизно ги утврдуваат целите, задачите и спроведувањето на потребните дејства за превенција, рано предупредување и справување со кризи. Исто така, треба да се забележи дека актерите во системот за управување со кризи се должни меѓу себе да комуницираат, координираат и соработуваат со

Центарот за управување со кризи при извршувањето на должностите утврдени со Законот (чл.37). Важно е да се укаже дека Центарот за управување со кризи во целост ја има исполнето ова законска одредба, воспоставувајќи ВЕБ базиран интегриран ГИС, каде постои инвенторизација на елементите на критичната инфраструктура која е во согласност со Уредбата за методологијата за изработка на проценатa на загрозеноста на безбедноста на Република Македонија од сите ризици и опасности (донесена 2005 год.) и Методологија за процена на штети од елементарни непогоди и други непогоди (донесена во 2001 година). Важноста на овој закон се состои од податокот дека истиот претставува основа за планско, навремено, целосообразно и координирано донесување на одлуки, насоки и препораки за преземање на мерки за превенција, како и за најоптимално справување со кризна состојба, врз база на која се изработува процена на загрозеност на безбедноста на Република Северна Македонија од сите ризици и опасности (донесена од Владата на Република Северна Македонија на 05.11.2019 година). Во рамките на документот Процена на загрозеност на безбедноста на Република Северна Македонија од сите ризици и опасности, во делот „Елементи на ризикот" е ставена критичната инфраструктура во поширок контекст: хидрографска мрежа, водостопанска инфраструктура, комуникациска мрежа, сообраќај и врски, патна мрежа – по видови на патишта и останата инфраструктура, по видови. Во рамките на овој документ наведен е дел за процена на ранливост и изложеност на посебните елементи кон кои е насочен ризикот, преку идентификација на типологијата на објектите и нивниот број на инфраструктурата и на критичните објекти кои се чувствителни на конкретна опасност, со мапирање, доколку е можно (точка 2.2.), прецизно е наведена процена на влијанието (ранливост и изложеност) од конкретната опасност брз објекти и инфраструктура (точка 2.4.).

Следен важен документ, на кој ќе се осврнеме, е поврзан со значењето на заштитата и спасувањето на критичната инфраструктура, а тое е *Законот за заштита и спасување,* што го организираат и спроведуваат не само државните и органите на

управата, туку и сите јавни установи, трговски друштва, меѓу кои и енергетските оператори. Според овој закон, заштитата и спасувањето се остваруваат преку поголем број на мерки и активности, меѓу кои: набљудување, откривање, следење и проучување на можните опасности од природни непогоди и други несреќи, преземање превентивни мерки, известување и предупредување, одредување и спроведување на заштитните мерки, надзор на спроведувањето на заштитата и спасувањето, идентификација и процена на опасностите и др. Овој закон претставува системска уредба со која се наведени мерки и активности кои се преземаат и за процена и спречување на други несреќи, а кои Законот ги дефинира како настани кои се резултат на одредени превиди и грешки во извршувањето на секојдневните стопански и други активности, како и невнимание при ракување со опасни материи и средства при производство, складирање и транспорт на истите (пожари, големи несреќи во патниот, железничкиот и воздушниот сообраќај, индустриски несреќи предизвикани од експлозии и други техничко-технолошки причини, излевање на нафта и други закани од поголем размер.) Иако заштитата на критичната инфраструктура експлицитно не е наведена во Законот, сепак, таа се препознава во предвидените мерки и активности, како пример можеме да го наведеме законското решение „намерни превиди или грешки, како саботажи или диверзија“ при ракување со наведените опасни материи, во кои поголем дел спаѓаат во примарни или финалните продукти на еден вид критична инфраструктура, односно енергетскиот сектор во Северна Македонија. Една нормативна точка за следење и спроведување на активности за заштита на критичната инфраструктура се препознава и во вкупно осумте начела на кои се засновува заштитата и спасувањето, и тоа од аспект на енергетската инфраструктура, и тоа: секој има право на заштита и спасување од природни непогоди и други несреќи, Република Северна Македонија, општините, јавните претпријатија, установи и служби и трговските друштва се должни, навремено да ги организираат и преземат превентивните и оперативните мерки за заштита и спасување од природни непогоди и други несреќи; секое

физичко и правно лице во согласност со Законот, одговара за неспроведување на предвидените мерки за заштита и спасување итн. За заштита на критичната инфраструктура важно е начелото кое ги обврзува институциите на системот за безбедност и компаниите од јавниот и приватниот сектор, каде што припаѓаат енергетските оператори, да организираат и преземаат, пред сè оперативни, а на кои стратегиите за заштита на критичната инфраструктура им даваат клучна улога во процесот на постигнување на целите на соодветните национални стратегии.

Во *Националната стратегија за заштита и спасување*, заштитата на критични инфраструктури се согледува од аспект на планирањето на заштитата и спасувањето. *Планот за заштита и спасување* не дава дефиниција за критичната инфраструктура, иако концептот се препознава при објаснувањето на обврските на учесниците во системот на заштита и спасување. Планот за заштита и спасување се изработува врз основа на Проценатa на загрозеност од природни и други несреќи, додека за потребите на приватниот сектор, вклучувајќи ги и енергетскиот оператор, авиотранспортот (кои се во приватна сопственост) и др., за кои, врз основа на расположливите информации, проценатa ја донесува орган кој управува со истите. Исто така, менаџментот донесува и План за заштита и спасување според кој ги презема мерките и активностите за обезбедување на инфраструктурата од природни катастрофи и други закани.

Од анализите на актуелните согледани практики, се утврди дека јавното-приватно партнерство во последните години во Република Северна Македонија стана клучна иницијатива и доби изразена улога. Тоа, секако, се должи на фактот дека секој субјект придонесува за специфичните ресурси на системот, учествува во планирањето, донесувањето одлуки и се стреми на полето на јакнење на отпорноста и заштитата на критичната инфраструктура. Важноста на јавното- приватно партнерство се состои од фактот дека приватниот сектор е најчесто сопственик, како и менаџер на повеќе национални

критични инфраструктури: комуникацискиот, информациско-технолошкиот сектор и др. (како на пример Македонски Телеком, Аеродроми ТАВ), па затоа е разбирливо дека приватниот сектор е најдобро запознаен со барањата за критичната инфраструктура – слабости и предности, и мора да биде дел од јакнењето на отпорноста и заштитата на критичната инфраструктура. Токму затоа ја имаат одговорноста да ја заштитат 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. Оттука, сосема разбирливо е дека приватниот сектор за критичната инфраструктура ја има одговорноста да ја заштити инфраструктурата што е важна за функционирањето на целокупното општество и ова не е возможно да биде направено ефикасно, ефективно и без поголема цена ако нема соработка со јавните институции. Оваа соработка создава и бројни проблеми, и тоа во делот на размена на сензитивни информации и податоци, а кои се клучни за заемна доверба, како и размена на знаења и искуство. Овие проблеми ја наметнуваат потребата да се работи на понатамошно зајакнување и поголема јавно-приватна соработка. Можеби преку анализа на „Македонски Телеком“, технолошкиот лидер во земјата кој е дел од групацијата „Дојче Телеком“, ќе се дојде до податок дека тој ги спроведува сите процедури, стандарди и знаења прифатени на севкупно ниво на „Дојче Телеком АГ Корпорација“. Исто така, анализата покажува дека сите мерки се на повисоко ниво споредбено со нашата држава, којашто нема воспоставено единствен систем (закон и стратегија) за заштита на критичната инфраструктура. Заканите стануваат посложени и го загрозуваат функционирањето на инфраструктурите, што е голем предизвик за државата, нејзините тела и оператори. Токму затоа, отвореното партнерство со приватниот сектор, јавниот сектор може да промени многу,

односно подобро да го постави и менаџира системот со поголем квалитет.

Македонскиот нормативен модел од приватно-јавно партнерство е уреден со Законот за концесии и јавно-приватно партнерство (2012). Овој закон пропишува можност за договорно регулирана соработка која за приватното обезбедување би се однесувала на јавна набавка на услуга. Концептот на јавно-приватно партнерство во секторот за приватно обезбедување во Македонија во извесна форма се применува со донесувањето на Законот за обезбедување на лица и имот. Ова законско решение е лимитирано за инвестирање во конструкцијата и одржувањето на објектите и не е во целост приспособено за целосните потреби на критичната инфраструктура. Еден од начините кои ќе помогнат да се надмине овој проблем е да се воспостави јавно-приватно партнерство, конкретно кооперација во различити области во критичната инфраструктура, со јасно дефинирани заемни права и обврски, лесно имплементирани за двете страни (Mitrevska, 2022).

Стратегија за одбрана на Република Северна Македонија е стратешки документ кој ги *„идентификува клучните карактеристики на современото безбедносно опкружување, ја наѓласува нашата одбранбена политика, издава насоки за адаптација на субјектите од системот за одбрана, неопходните ресурси и одбранбените способности потребни за нејзино остварување“* (точка три од Воведот). Нешто што е особено важно за дискурсот во рамките на ова истражување е податокот дека концептот на критична инфраструктура е застапен во оваа Стратегија, конкретно во точка 21 од делот *Закани, ризици и предизвици по одбраната* се наведува дека „во однос на идентификување безбедносни предизвици, закани и ризици системот за одбрана на Република Северна Македонија ќе гради капацитети и способности за одговор на истите во услови на воени и кризни ситуации, сајбер и хибридни закани, тероризам, активности на странски и недржавни актери, *закани врз критичната инфраструктура* и нелегална трговија со конвенционално оружје, оружје за масовно уништување и нуклеарна

технологија. Респектирајќи ги овие сознанија, можеме да заклучиме дека оваа Стратегија, акцентирајќи ја важноста на критичната инфраструктура, треба да биде еден од стратегиските акти кои ќе се користат при изработка на Законот за критична инфраструктура.

Во однос на справувањето со хибридни закани, беше усвоена Стратегија за градење отпорност и справување со хибридни закани, донесена во 2021 година, според која *„хибридните закани се однесуваат на комбинација од злонамерни и субверзивни активности, конвенционални и неконвенционални методи (дипломатски, воени, екномски, технолошки), кои се употребени на координиран начин од државни или недржавни субјекти за постигнување на специфицирани цели"*. Исто така, со Стратегијата се регулира ранливоста која се таргетира во неколку оперативни области, и тоа*: политички сектор, економија, одбранбено-безбедносен сектор, граѓански сектор и инфраструктура (точка 3.2., стр.9)*.

Сублимирајќи ја анализата на клучен дел на законите и стратегиските акти од областа на безбедноста и одбраната, можеме да заклучиме дека во Република Северна Македонија:

- Ниту еден од документите не обезбедува целосно решение за управување со ризици за функционирањето на критичната инфраструктура, како и рамка за нејзина заштита.

- Од анализата на еден дел од нормативните решенија, може да се заклучи дека во нив се посветува внимание за заштита на оваа област. Но, исто така анализата покажува дека е направен голем исчекор и дека ја акцентираат важноста на заштитата на критичната инфраструктура и дека се одлична почетна основа за изработка на Закон за критична инфраструктура.

- До ден-денес не е изработен Закон за критична инфраструктура. Токму затоа, засегнатата професионална и научна јавност во Република Северна

Македонија го зголеми интересот за предметната област.

- Во фаза на означување на критичната инфраструктура, која следува по идентификацијата, треба да се посвети големо внимание на критериумот критичност и на националното значење на конкретна инфраструктура.

- Владата треба да донесе Одлука за доделување статус на критична инфраструктура.

- По означувањето на критичната инфраструктура, потребно е да се спроведе приоритизација, бидејќи целокупната критична инфраструктура не бара еднакво ниво на заштита, ниту пак, сите критични инфраструктури поседуваат иста важност.

- Во оваа фаза потребно е да се воведат и соодветни меѓународни признати стандарди кои се во функција на процена на ризиците и одржување континуитет во делувањето на критичната инфраструктура.

- Во поглед на соработката меѓу заинтересираните страни, клучен елемент е постоењето на јавно-приватно партнерство и воспоставување квалитетна соработка. За таа цел, потребно е да се воспостави прифатлив заеднички модел на соработка во оваа област со јасно утврдени заемни права и обврски.

- Додека Хрватска, Србија и Црна Гора напредуваат во развојот на националните политики за заштита на критичната инфраструктура, Северна Македонија сè уште го бара своето место и улога во оваа област. Токму затоа, во оваа фаза потребно е да се следат европските позитивни практики, како што е примерот на Хрватска.

- Токму затоа, сметаме дека и оваа монографија ќе даде инпут и ќе иницира политичка поддршка за носење на Законот за критичната инфраструктура.

4.1.2. Втора фаза

Во Република Северна Македонија до денес не е донесен Закон за критична инфраструктура и оваа област е регулирана во рамките на други закони и подзаконски акти. Анализирани се еден дел од нормативни решенија, каде што во нив се посветува внимание за заштита на оваа област. Анализата покажува дека е направен голем исчекор, но, исто така, пропуштени се можности да се донесе посебен закон за критична инфраструктура. Исто така, анализата за состојбата во Северна Македонија укажува на потребата од систематизиран пристап кон постојната инфраструктура и потребата инфраструктурата да се дефинира како критична, заради можноста да биде потенцијална цел. Затоа, за почеток:

- Потребно е да се утврди листа на критичната инфраструктура и стандардите за заштита на критичната инфраструктура и на последиците врз истата, а пред сè, подобрување на отпорноста, односно безбедна инфраструктура од можни човечки, физички и сајбер-закани.

- Значајно е да се забележи дека детерминирањето на критичната инфраструктура во Северна Македонија не е во согласност со насоките за нормативно регулирање на прашањата од сферата на идентификација, означување и заштита на европската критична инфраструктура, со посебен акцент на обврските произлезени од Директивата на Советот на ЕУ 2008/114/ЕК за идентификација и означување на европската критична инфраструктура, како и проценатa од потребата за подобрување на нејзината заштита – Директива на Советот на ЕУ 2008/114/ЕК;

- Доменот на заштитата на критичната инфраструктура во Република Северна Македонија потребно е истовремено да се развива во два паралелни процеси. Постојат две главни насоки, првата е обележана со

националниот развој на овој домен, односно час поскоро иницијативата да се преточи во Закон за критична инфраструктура, а другата насока се базира на имплементацијата на политиките и процесите кои ЕУ ги има иницирано и истите ги координира во доменот на заштита на критичната инфраструктура.

- Заштитата на критичната инфраструктура е одговорност и обврска на целото општество, затоа е потребен консензус на национално ниво во однос на националната програма за заштита на критичната инфраструктура, која е тешко да се постигне без неопходна политичка поддршка која треба да обезбеди нормативно регулирање и услови за развој и напредок на процесот.

- Владата на Северна Македонија треба да им даде овластување на одредени министерства да бидат координатори на целиот систем.

- Владата треба да обезбеди стратегиска рамка која е од суштинско значење за успешно функционирање на системот, соработката, комуникацијата и координацијата на сите актери.

- Државните институции треба да одлучат дали со Законот за критична инфраструктура ќе се регулира само прашањето на европска критична инфраструктура (како што го бара Директивата од 2008 година) или пак, истовремено ќе се регулира националната и европската инфраструктура.

- Потребно е да се определи бројот на сектори кои можат да се идентификуваат и одредат како национални критични инфраструктури, со цел да се обезбедат холистички пристап за заштита и намалување на негативните влијанија во случај на закана за критичната инфраструктура.

- Според Директивата од 2008 година, секоја држава мора да ја идентификува и одреди и европската критична инфраструктура, и тоа во два сектори: транспорт и енергетика. Во оваа фаза треба да се има предвид дека на ниво на Европската Унија е изработена нова CIP директива, која наскоро ќе ја замени Директивата од 2008 година и според новиот предлог ќе има 10 сектори. Оттука, предлог е Северна Македонија при изработка на Законот да ги одреди сите 10 сектори во кои ќе може да ја идентификува и одреди како критична инфраструктурата (да се поклопуваат секторите од CIP Директивата и Законот).

- Јакнење на отпорноста и заштитата на критичната инфраструктура треба да се отвори кон сите актери во македонското општество, и тоа покрај државните институции (со посебен акцент на безбедносните институции) да бидат вклучени и регулаторни агенции, оператори на критичната инфраструктура, агенции и тела, како на пример Комората за приватно обезбедување и академската заедница. Тоа значи, дека во Законот треба да се нагласи местото и улогата на јавното-приватно партнерство.

- Во Законот за критична инфраструктура треба да се назначи безбедносен координатор кој ќе претставува клучна фигура која во сите тела и органи ќе биде задолжена за работите околу критичната инфраструктура.

- Потребно е да се организира и дефинира местото и улогата на посебен Центар за заштита на критичната инфраструктура, во кој ќе се собираат податоците и ќе се координираат активностите.

- Со носење на Законот за критична инфраструктура, потребно е да се започне со изградбата на системот за заштита на критичната инфраструктура и на самиот

почеток да се направи Акциски план кој ќе ја определи динамиката на активностите.

4.2. Концептот на еластичност и оптимизирање на моделот за градење систем за заштита на критичната инфраструктура

Прашањата поврзани со заштитата на критичната инфраструктура сè повеќе ги преокупираат академиските и политичките дебати. Значењето на критичната инфраструктура за современите општества и нивната отпорност претставува главни и неодминливи атрибути во настојувањата да се овозможи непречено функционирање на виталните делови од критичната инфраструктура. Предизвиците кои доаѓаат од страна на природните и од човек предизвикани непогоди и несреќи се мултиплицираат во последните децении. Современата научна анализа потврдува дека нема интегрирана рамка што води сметка за природата и редоследот на појавување на повеќе опасности и нивното влијание, како и пристапот кон заштитата на критичната инфраструктура. Оттука, кај државите со воспоставен систем за заштита на критичната инфраструктура, актуелно се наметнуваат прашањата за нејзината еластичноста, воедно и отпорноста на нивните општеството. Во тој поглед тоа претставува тренд и празнина која недвосмилесно постепено треба да се потполни.

Комплементарноста на двата концепта за заштита и еластичност на критичната инфраструктура не значи дека тие се идентични. Имено, подобрувањето на еластичноста на критичната инфраструктура претставува актуелен приоритет за државите ширум светот. Растечките закани, како и неконвенционалните напади врз критичната инфраструктура ги поместуваат границите на традиционалната процена на ризикот и напорите за ублажување на ризиците. Евидентно

е дека одредени закани не можат да се предвидат, додека намалувањето на сите можни ризици на минимално можно ниво не е секогаш рентабилно. Ова го фокусира вниманието кон приоритетизирање на еластичноста со цел да го обезбеди континуитетот на услугата како резултат на девастирачките и деструктивни настани, особено во случаи кога тие стануваат крајно непредвидливи.

Македонското општество не е изземено од глобалните политички, безбедносни и економски токови. Во поглед на заштитата на критичната инфраструктура, македонското општество е на стартна позиција. Тоа налага, пред да се утврди стратегиската и национална рамка за обезбедување ефикасни чекори кон градење на ефикасен систем за заштита и еластичност на критична инфраструктура, да се одбере пристапот кон оптималниот модел и да се отпочне неговото реализирање. Оптималниот модел базиран на најдобрите практики од „доброволниот" и „мандатниот" пристап во заштитата на критичната инфраструктура, треба да се гради врз основа на добрите практики и искуствата на другите држави. Имајќи предвид дека се доцни со почетокот на изградбата на системот за заштита на критичната инфраструктура, компаративниот и аналитички пристап се поставува како врвен приоритет со цел да се отпочне одлучно креирањето на предусловите за исполнување на концептот за заштита, но и еластичност на критичната инфраструктура, а со самото тоа и поголема отпорност на македонското општество.

На самиот почеток од процесот на креирање општествена отпорност, заштита и еластичност на критичната инфраструктура мора да знаеме кон што треба да се стремиме. ЕУ моделот (Директивата 2008/114/ЕК) е повеќе ориентиран кон заштитата, иако од 2012 година општествената отпорност (отпорноста на заедниците) и еластичноста на критичната инфраструктура сè повеќе се споменува. Притоа, треба да се напомене дека постојат и други модели, како на пример нордискиот модел каде отпорноста на виталните општествени функции е главниот приоритет. Во организациските и технолошките домени, овој нордиски

пристап е повидлив во доменот на општествената отпорност, каде клучните играчи се националната и локалните власти. Кога станува збор за операторите на критичната инфраструктура, концептот на отпорност е сè уште прилично апстрактен и нема конкретна операционализација. Останува отворената дилема дека интеракцијата помеѓу властите и операторите на критичните инфраструктури, без разлика дали се дискутира во однос на регулативата, државната поддршка, јавно-приватно партнерство или корпоративната општествена одговорност, останува слабата алка во постигнувањето отпорност на критичната инфраструктура во практиката. Големо прашање е дали воопшто може да се постигне. Прегледот на концептуалните пристапи на нордиските земји кон кризите поврзани со критичната инфраструктура, сепак остават впечаток дека овие земји се прилично „прогресивни" и отсекогаш имале поширока и похолистичка филозофија од онаа што првично ја понуди Европската комисија, заснована на приоритет на заштитата на критичната инфраструктура од тероризам (Pursiainen, C. 2018).

Секако, кога веќе сме во можност да ги согледаме двата модела, крајната цел за заштита на критичната инфрструктура треба да кореспондира со растечките концепти на општествена отпорност (потенцирано од ЕУ и НАТО) и еластичност на критичните инфраструктурни системи, мрежи, објекти и делови на објекти.

4.3. Опис на концептот за еластичност на критичната инфраструктура

Во оваа прилика ќе се осврнеме на прегледот и анализата на соодветната литература која понуди докази дека концептот на „еластичноста" нема единствена дефиниција, особено кога се смета за атрибут на специфичен систем. Претходни студии на оваа тема нудат бројни и разновидни дефиниции за овој концепт, дури и во иста област на студии можат да се пронајдат разлики помеѓу дефинициите за еластичност, како

во случајот на инфраструктурните системи. Повеќето студии кои се занимаваат со еластичноста на инфраструктурните системи се осврнуваат на прашањето за надворешни опасности за системот, кои, доколку се појават и предизвикаат нарушување, може да имаат негативни влијанија и од структурна и од оперативна природа, или и од двете, со потенцијални последици врз општеството, економијата и/или животната средина.

Конкретно, кога зборуваме за заштита на критичната инфраструктура, треба да е јасно дека истата не е возможно да се постигне во оптимално ниво најмалку од две причини. Првата е од финансиска природа, додека втората се однесува на заканите и ранливоста кои постојано се развиваат и трансформираат. Оттука, одредени процеси, системи или индивидуи можат да предизвикаат инциденти и акциденти или ненамерни како и намерни опструкции и напади. Ваквите сознанија алудираат на моментот дека сите субјекти вклучени во обезбедувањето на заштита на критичната инфраструктура мора да бидат свесни дека ефективната заштита треба да се надополни со развој на еластичноста на критичната инфраструктура.

Иако заштитата и еластичноста на критичната инфраструктура се комплементарни концепти, мораме да ги објасниме и прифатиме разликите меѓу нив. Накратко, заштитата се однесува на способноста да се спречат или намалат ефектите од непријатни и ненадејни настани, додека еластичноста е олицетворена во способноста да се намали големината, влијанието и времетраењето на прекинот во функционирањето и се однесува на брз пристап кон сите компоненти и процеси, од физички компоненти до капацитетот за управување, како и квалитетот на човечките ресурси. Притоа, еластичноста тежнее кон развој и одржување на системот и неговата способност да се спречи, апсорбира, адаптира и да закрепне по секаков можен напад.

Иако своето потекло го има во сферата на психологијата, концептот на еластичност, поради неговата разновидност, исто така се применува и во полето на безбедноста. Во

безбедносната сфера, под еластичност се подразбираат различни фактори кои придонесуваат кон јакнење на безбедноста преку индиректни мерки и дејствија. Во доменот на заштитата на критичната инфраструктура, еластичноста треба да се апсолвира како начин за зголемување на безбедноста преку идентификување и имплементирање на мерки што можат да се преземат и на критично инфраструктурно ниво, но особено на ниво на организации и процеси кои обезбедуваат влезни податоци или користат излези (излезни солуции) од таа инфраструктура.

Наједноставно, еластичноста може да се дефинира како способност на инфраструктурата да се подготви за справување со променливи услови и прилагодување на нив, како и брзо да се спротивстави и да закрепне од нарушувањето, вклучително и намерни напади, несреќи или природни катастрофи. Еластичен критично-инфраструктурен систем претставува систем способен на антиципација и апсорбирање на потенцијалните нарушувања, развивање адаптивни средства и давање одговори насочени или кон создавање на способност да издржи нарушување или да закрепне што е можно поскоро по одреден инцидент (Cîrdei, I. A. 2018).

Следејќи го истиот тренд, Канцеларијата на ООН за намалување на ризикот од катастрофи ги дефинира еластичните системи како силни (издржливи на надворешни нарушувања) и флексибилни системи (можност за враќање назад). Поконкретно, еластичноста е поистоветена со капацитетот на системот, заедницата или општеството потенцијално изложени на опасности да се прилагодат, со отпор или промена, со цел да се постигне и одржи прифатливо ниво на функционирање и структура. Ова е одредено од степенот до кој социјалниот систем е способен да се организира за да ги зголеми своите капацитети за учење од минатите катастрофи за подобра заштита во иднина и да ги подобри мерките за намалување на ризикот. Оваа дефиниција додава нов аспект што треба да се разгледа, а тоа е организацијата што се очекува од општеството или од заедницата во врска со процесот на донесување одлуки и

превентивните активности за време и по нарушувачкиот настан, што е клучно за справување со вонредна состојба, во кој контекст директно се вклучени луѓе.

За да се реализираат претходно наведените аспекти, потребно е да се развие спефична култура која ќе ја промовира еластичноста и ќе ги одржува во контакт сите субјекти кои имаат улога во процесот на заштитата на критичната инфраструктура на која може да влијаат последиците од непредвидливите настани или кои можат директно или индиректно да придонесат кон обновувањето и воспоставувањето нормално функционирање и редуцирање на последиците. Целиот систем мора да функционира на ефикасен начин, а еластичноста треба да се воспостави многу пред да дојде до одредена криза, бидејќи истата се развива прилично бавно и тешко, со човечки и материјални напори. Неуспех во овие обиди значи дека секоја наредна криза мора да биде поука за намалување на негативните ефекти од потенцијалните природни или антропогени катастрофи. Предностите на концептот за еластичност мора да се согледаат како дополнителна заштита која ја зајакнува не само безбедноста на инфраструктурниот елемент, но исто така и на целото општество.

Анализирајќи бројна литература (Mottahedi, A., et.al. 2021) и поставувајќи ја во корелација со променетото стратегиско опркружување, хибридните закани и новите субверзивни технологии, можеме да понудиме уникатен модел за изградба на сеопфатен систем за заштита на критичната инфраструктура во Северна Македонија. Тоа значи постојана надградба на општествената отпорност, воспоставување на систем за заштита на КИ и надградба на постојните модели со она што ние го нарековме концепт на еластичност на критичниот инфраструктурен систем. Притоа, мислиме на намалување на времето за закрепнување на КИ системите или враќање во пред-нарушената состојба. Оттука, општествената отпорност и заштитата треба да бидат во функција на еластичноста на КИ системот.

Во контекстот на концепцискиот приод кон изградбата на македонскиот систем за заштита на критичната инфраструктура, треба да се потенцира важноста на еластичноста која претставува само една компонента од крајно сложениот механизам за заштита. Еластичноста треба да е комплементарна на општествената отпорност и на подигнатиот ефективен систем на заштита на критичната инфраструктура. Ова треба да нè наведе на размислата за постоење концепт за „одбрана во длабочина", што подразбира повеќе одбранбени слоеви во кои секој елемент придонесува за обезбедување на целината преку изведување на основните функции и земајќи ги предвид каскадните ефекти од различните несакани настани.

4.4. Можен модел и институционален пристап кон изградбата на систем за заштита на критичната инфраструктура.

Треба да се потенцира дека не постои однапред потврден институционален модел којшто укажува како државата треба да ја штити сопствената критична инфраструктура. Тоа значи дека најнапред е потребна сеопфатна анализа на ранливоста и карактеристиките на заканите, големината и структурата на економијата, спецификите на јавните политики и воспоставената институционална практика. Со други зборови, Владата на државата мора да ги има предвид гореспомнатите елементи при изборот на оптималната рамка за заштита на критичната инфраструктура.

Генерално, во современата практика пристапот кон заштитата на критичната инфраструктура вообичаено е базиран на два основни модели. Едниот пристап е модел кој се базира на принципите на саморегулација, потстрек и доброволно почитување. Овој модел е т.н. „доброволен пристап", кој произлегол врз основа на политиките кои се сосредоточени на

необрзувачки насоки. Според карактеристиките на овој модел, сите заинтересирани страни од јавниот и приватниот сектор се поттикнуваат да придонесат во процесот на дефинирање и примена на политиките за заштита на критичната инфраструктура преку препораки, договарање и креирање на заедничка перцепција заради остварување на заеднички цели. Во овој случај, обврзувачката сила на законодавните и регулаторните норми се користи само како дополнителна алатка, освен, според анализата на одредени сектори на критичната инфраструктура во различни земји, на пример нуклеарниот сектор, каде имаат примарна улога.

Вториот модел се темели на премисите дека соработката во областа на заштитата на критичната инфраструктура најдобро се остварува преку воспоставување на обврзувачки правни аспекти, но и санкции за операторите со критичната инфраструктура. Овој модел е наречен „мандатен пристап“ и бара од операторите да се придржуваат до бараните стандарди во рамки на предвидените рокови. Анализирајќи ги пристапите на поголем број држави, генерално може да се констатира дека тие не ги следат оригиналните пристапи туку имплементираат елементи од едниот и од другиот модел. Оттука, во поглед на пристапот или моделот на заштита на критичната инфраструктура можат да се определат или дефинираат како доминантно „доброволни“ или доминантно „мандатни“. Најдобри примери за „доброволен“ пристап има кај САД, Велика Британија, Швајцарија и Канада, додека примери за „мандатни“ пристапи се Франција, Шпанија, Белгија и Естонија. (Mujević M., Korač S. 2020).

Сепак, треба да се спомене дека најголемиот предизвик за државите претставува изборот на најдобриот модел кој мора да кореспондира со националните потреби. Ова треба особено да се има предвид при воспоставувањето на моделот за да се одбегне воспоставувањето на структура и да се преземат процеси кои во практиката се покажува дека не се соодветни и не се адекватни. Ваквите недоследности најчесто се одбегнуваат со воспоставување на механизми со кои се обезбедува

конзистентна политика и стратегија во сферата на заштитата на критичната инфраструктура кои повремено подлежат на ревизиони процеси. На пример, САД кои започнаа со чист концепт на доброволно учество на операторите во заштитата, со текот на времето идентификуваа потреба за јакнење на нормативната рамка за заштита. Ваквите процеси и примери од различно дизајнирани модели на заштита на критичната инфраструктура мора да се земат предвид при изборот на македонскиот модел за изградба на системот за заштита и еластичност на критичната инфраструктура.

4.5. Оптимизирање на моделот за изградба на систем за заштита и еластичност на критичната инфраструктура.

Во претходно направената анализа на стратегиските и нормативните решенија поврзани со критичната инфраструктура, а со желба да се олеснат и правилно реализираат одредени чекори, авторите силно ќе апострофираат и повторат одредени претходно изнесени констатации. Можниот модел за изградба на системот за заштита на критичната инфраструктура треба да се потпира на три генерално издиференцирани рамки (стратегиска, нормативна и организациска).

А) Стратегиска рамка

Анализирајќи ги пристапите и моделите за заштита на критичната инфраструктура, како и сознанието дека критичната инфраструктура претставува платформа за одржување на развојот на секое општество и држава, Владата на државата треба да биде вклучена во системот на заштита на критичната инфраструктура како предлагач на закони и подзаконски акти и има задача да им даде овластување на одредени министерства

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

После Владата, следниот најважен актер е координаторот (одредено министерство) на целиот систем за заштита на критичната инфраструктура. Постојат различни примери и практики за тоа кое тело е соодветно за оваа улога. Во повеќе европски земји функцијата е доделена на Министерството за внатрешни работи. Оттука, постојат различни решенија и практики, но секоја земја треба сама да го препознае најсоодветниот модел. Од сеопфатната анализа може се предложи Министерството за одбрана или Министерството за внатрешни работи да биде координатор на целиот систем за заштита на критичната инфраструктура. Доколку МО/МВР е координатор на системот, тоа ќе ја има улогата да комуницира директно со сите актери на системот, со меѓународни актери и да доставува извештаи до Владата. Организацискиот пристап кон имплементацијата на заштитата на критичната инфраструктура во Европската Унија и земјите кои се стремат кон полноправно членство (како Република Северна Македонија) е даден во Директивата 2008/114/ЕК за идентификација и утврдување на европските критични инфраструктури и процена на потребата за подобрување на нивната заштита – главен документ на Европската Унија за критичната инфраструктура. За да можеме одлучно да зачекориме кон имплементација на горенаведеното, од корист за креаторите на политиките се неколку почетни препораки.

Во изградбата на системот за заштита на критичната инфраструктура потребно е да се тргне од стратегиската рамка. Неопходно е јакнењето на заштитата на

критичната инфраструктура да се вгради во една од стратегиите на Република Северна Македонија. Притоа има неколку можности:

Прво. Предлог за изработка на Стратегија за заштита на критичната инфраструктура како посебен стратегиски документ. Оваа стратегија треба да претставува синтеза на определувачки и обврзни ставови кои се тесно поврзани со заштитата на критичната инфраструктура. Определбите треба да бидат во функција на ефикасно решавање на актуелни и идни безбедносни предизвици и закани на државно, на регионално и на пошироко ниво, самостојно и во соработка со сојузниците и партнерите во рамките на колективните системи за безбедност – НАТО. Како и да е, стратегиското решение треба да претставува рамка која ја детерминира развојната компонента и улогата на сите субјекти во зајаканувањето на заштитата на критичната инфраструктура, но и нејзината еластичност. Посебното стратегиско решение би било подолготрајна и посеопфатна опција од ажурирањето на одредени стратегиски документи кои би го скратиле времето за отпочнување на конкретни активности.

Анализирајќи повеќе национални стратегии за заштита на критичната инфраструктура (Франција, Германија, Велика Британија и САД), и покрај одредени разлики, во сите доминираат некои базични приоритетни области кои придонесуваат во детеминирањето на ефективна холистичка стратегија за заштита на критичната инфраструктура. Обие области генерално вклучуваат:

Визија/цели – развојот на која било стратегија за заштита на критичната инфраструктура вклучува формулирање на стратегиските цели (визии) кои можат да се поделат во поединечни цели кои понатаму се мерлива категорија.

Администрирање на безбедноста на критичната инфраструктура – Администрација/структура на управување се однесува на именувањето надлежни и овластени тела за заштита на критичната инфраструктура, дефинирање на улогата и

одговорноста на секое тело, како и рамката за соработка помеѓу јавните и приватните институции.

Јавно-приватни партнерства – Секоја национална програма за заштита вклучува соработка на засегнатите страни, особено преку јавно-приватно партнерство, вклучувајќи ги јавните тела и сопствениците/операторите на критичната инфраструктура.

Размена на информации – Размената на информации алудира на постоењето свест за заканите и ранливоста за да се обезбеди рано предупредување на засегнатите страни и генерално, за споделување информации и соодветно знаење за самите ризици и закани.

Законодавно-регулаторна рамка – Носењето закони претставува значајна алатка за да се обезбеди, меѓу другото, дека јавните и приватните тела реагираат на нивните улоги и одговорности, како и почитување на специфичните безбедносни стандарди.

Идентификација и процена на националната критична инфраструктура – Идентификацијата и проценатa на националните критични средства (сектори, потсектори, услуги и специфични потсистеми) претставува предуслов за имплементација на националните политики за заштита на критичната инфраструктура. Значаен критериум за класификација на критичната инфраструктура е, меѓу другите, степенот и важноста на меѓусебните врски и меѓузависностите меѓу критичната инфраструктура.

Процена на ризик – Клучен елемент на стратегијата за заштита на критична инфраструктура е методолошката евалуација на заканите и процена на безбедносните ризици што произлегуваат од националните критични инфраструктури.

Ризици и управување со кризи – Мерките за одговор на итни ситуации треба да обезбедат продолжување на

работата или брза санација на критичниот субјект (Petrakos, N., Kotzanikolaou, P. 2019).

Второ. Доколку се утврди потребата од ревизија на постојната или изготвување на нова стратегија за национална безбедност, потребно е да се посвети простор за критичната инфраструктура во стратегијата. Неспорно е дека во Стратегијата за национална безбедност треба да се наведе дел за критичната инфраструктура. Фактичката состојба укажува дека во Стратегијата за одбрана од 2020 година е спомната критичната инфраструктура.

Имено, Стратегијата за одбрана произлегува од Уставот на Република Северна Македонија, трајните определби од Националната концепција за безбедност и одбрана, Законот за одбрана и стратегиската определба на Владата на Република Северна Македонија за интеграција во евроатлантските структури. Критичната инфраструктура е спомната во делот на најголемите опасности по националната безбедност.

Конкретно, во точка 18, „Сајбер нападите и загрозувањето на информатичката безбедност се актуелен и растечки предизвик по глобалната безбедност. Најсериозни потенцијални последици од сајбер-нападите е загрозувањето на функционирањето на критичната инфраструктура, вклучително и онаа на безбедносниот систем и системот за одбрана на Република Северна Македонија".

Во точка 21, „Во однос на идентификуваните безбедносни предизвици, закани и ризици системот за одбрана на Република Северна Македонија ќе гради капацитети и способности за одговор на истите: во услови на воени и кризни ситуации, сајбер и хибридни закани, тероризам, активности на странски и недржавни актери, закани по критичната инфраструктура и нелегална трговија со конвенционално оружје, оружје за масовно уништување и нуклеарна технологија".

Во точка 52, „Во услови кога надлежните државни институции (вклучително и локалната самоуправа) не можат да се

справат со кризи, односно закани по внатрешната безбедност, закани по критичната инфраструктура, елементарни непогоди, технолошки катастрофи, епидемии и климатски промени, како и при загрозување на границите на Република Северна Македонија, Армијата ќе дава поддршка на цивилната компонента на системот за одбрана, како и на полицијата во согласност со утврдените процедури".

Во точка 77, „Со прецизно идентификување и приоритетизирање на критичната инфраструктура ќе се обезбеди поефикасна заштита на истите во согласност со националните интереси и воспоставените меѓународни стандарди" (Стратегија за одбрана на РСМ, 2020).

Исто така, во Стратегискиот одбранбен преглед (СОП) од 2018 година, критичната инфраструктура е спомната во делот на Заканите и предизвиците, поконкретно во делот за компјутерскиот криминал и загрозувањето на информатичката безбедност со што може да биде загрозено функционирањето на елементите на критичната инфраструктура. Во СОП е наведено дека Одбраната ќе учествува во изработка на листа на национална критична инфраструктура. (СОП, 2018).

Трето. Доколку постои или е во фаза на изготвување Стратегија за сајбер-безбедност, критичната инфраструктура може да се спомне во неа. Ваква стратегија е изготвена во 2018 година и во неа има делови кои се насочени кон заштитата на критичната информатичка инфраструктура како дел од севкупната критична инфраструктура. Исто така, донесен е и Акциски план за заштита на критичната информатичка инфраструктура (Национална стратегија за сајбер безбедност на Република Македонија, 2018-2022). Како стратегиска цел во рамките на Националната стратегија на Република Македонија за борба против тероризмот 2018-2022, препозната и спомната е заштитата на критичната инфраструктура (Национална стратегија за борба против тероризам БПТ, 2018).

Б) Нормативна рамка

Нормативно, може да се предложи изработка на Закон за заштита на критична инфраструктура. Додека истиот не ги помине сите предвидени фази за негово донесување, тематиката за критичната инфраструктура може привремено да се уреди во рамките на некој друг закон или подзаконски акт (претпоставка е дека процедурите за тоа се пократки и побрзо може привремено да се уреди проблематиката).

При изработката на нормативната регулатива за критичната инфраструктура препораката е да се регулираат првенствено подрачјата на енергетиката и транспортот – овие два сегмента ги бара Европската Унија од своите земји членки и оние кои имаат намера да пристапат. Доколку се вклучат и останатите сектори од критичната инфраструктура може да се повтори искуството на Хрватска веднаш на почеток да го успори и усложни процесот. Затоа препорака е да се тргне со секторите енергетика и транспорт. Во претстојните нормативни решенија (закон и подзаконски акти), секако дека треба да се предвидат можностите за регулирање на европската критична инфраструктура.

Особено значајно е во Законот или во подзаконските акти да биде спомнат безбедносниот координатор кој претставува клучна фигура која во сите тела и органи ќе биде задолжена за работите околку критичната инфраструктура. Во Хрватска постои безбедносенн координатор на ниво на министерство и на ниво на објект кој е означен како критична инфраструктура. Министерот одредува кој ќе биде безбедносен координатор за критична инфраструктура во неговото министерство, додека генералниот директор на објектот кој е одреден како критична инфраструктура одредува кај него кој ќе биде безбедносен координатор. Искуствата покажуваат дека постојат и студиски програми кои едуцираат кадар за безбедносни координатори. Таков е примерот на Романија која им овозможува на физичките лица да се школуваат за безбедносни координатори и потоа да бараат вработување по тој основ во министерствата

или објектите од критичната инфраструктура. Доколку се следи овој пример, покрај креирањето и акредитирањето на вакви студиски програми, потребно е како ново работно место – безбедносен координатор за критична инфраструктура, да се вброи во класификацијата на работни места во државата.

Понатаму, во Законот или во подзаконските акти треба да се нагласи местото и улогата на јавното-приватно партнерство. Ова е од исклучително значење, затоа што дел од критичната инфраструктура е управувана од приватни компании. Законот за приватно обезбедување од 2020 не содржи ниту една определба која се однесува на критичната инфраструктура.

Значаен сегмент во Законот или во подзаконските акти треба да претставува акцентирањето на школувањето, едукацијата и тренингот.

В) Организациска рамка

Организациските аспекти на имплементацијата на мерките и активностите за заштита на критичната инфраструктура треба да му припаднат на новоформираниот Центар за заштита на критичната инфраструктура. Од тие причини, можеби Министерството за одбрана или Министерството за внатрешни работи се добар избор како државно координативно тело за овој процес. Ова од причини што во Центарот би требало да се собираат податоци и да се координираат активности. Исто така, во Законот или во подзаконските акти важно е да се наведе дека работите околу заштитата на критичната инфраструктура ќе се одвиваат преку Центарот за заштита на критична инфраструктура.

Исклучително значајно, за да не се блокира процесот уште од самиот почеток, ознаките на тајност на почеток треба да бидат најниските можни. Во креирањето на стратегиските решенија и законското решение треба да се формира меѓуресорска група која ќе вклучи поширок круг на стручни лица, од универзитетите, министерствата, коморите, приватниот сектор.

После донесување на Законот, понатаму потребно е со подзаконски акти да се регулираат и уредат поединечните процеси.

По донесување на Стратегијата и Законот, потребно е да се започне со изградбата на системот за заштита на критична инфраструктура. Значајно е да се спомене дека системот се гради со едукација, работилници и запознавање на сите фактори во тој процес. Оптимално, би ја издвоиле потребата за креирање петгодишен акциски план за дејствување.

4.6. Заклучок

Претходните констатации упатуваат на заклучок дека македонското општество задоцнето влегува во процесот на креирање ефикасен систем за заштита на критичната инфраструктура. Интензитетот на несаканите појави, природни или антропогени, искуствено покажува дека и поразвиени општества се соочуваат со проблеми при воспоставувањето на ефикасни системи за заштита на критичната инфраструктура. Личните и искуствата на другите држави укажуваат дека аналитички и компаративно можеме да извлечеме силни позитивни страни и да ги превенираме правовремено недостатоците во изградбата на системот за заштита.

Сложеноста на широкиот спектар сектори во рамки на критичната инфраструктура, од самиот почеток, упатува на сознанието дека процесот на изградба на системот е долгогодишен и макотрпен. Ако на тоа се надоврзе сложеноста на политиките за заштита на критичната инфраструктура и најновите трендови за примена на концептот за еластичност на истата, ќе констатираме дека нововоспоставената динамика на ризици и закани бара нови одговори од безбедносните системи. Тоа значи воспоставување на нови институции во рамките на безбедносниот систем, кои како интегрален нивен дел со интердисциплинарен пристап ќе ги анализираат најновите трендови во поглед на ризиците и заканите по различни критериуми. Традиционалните елементи на безбедносните

системи не би имале голема ефикасност во поглед со справувањето на современите ризици и закани, особено сајбер-заканите и сл. Оттука, мора да се дозволи простор за научните институции, приватниот сектор и на ред други субјекти кои, посредно или непосредно, придонесуваат во работата на критичната инфраструктура.

Македонскиот систем за заштита на критичната инфраструктура мора да се базира на мандатниот модел во развојот и воедно да ги интегрира концептите за отпорност на општеството, заштита и еластичност на критичната инфраструктура. Можеби преамбициозно во прв момент, но подобро од сам почеток да се имаат предвид најновите трендови во развојот на системите за заштита на критичната инфраструктура. Само на овој начин современото отпорно општество е подложно на развој преку ефикасното функционирање на критичната инфраструктура. Тоа подразбира мрежи за непречено обезбедување јавни услуги, подобрување на квалитетот на животот, одржување на приватниот профит и економски раст.

ПРИЛОЗИ

Прилог бр. 1: ХРВАТСКА
Закон за критични инфраструктури
Народне новине бр. 56/2013,

I. ОСНОВНИ ОДРЕДБИ

член 1

(1) Со овој закон се регулираат националните и европските критични инфраструктури, секторите на националните критични инфраструктури, управувањето со критичната инфраструктура, подготовката на анализа на ризик, планот за безбедност на сопствениците/управителите, безбедносниот координатор за критична инфраструктура, ракувањето со чувствителни и класифицирани податоци и надзор над спроведувањето на овој закон.

(2) Овој закон го транспонира во законодавството на Република Хрватска acquis communautaire содржано во Директивата на Советот 2008/114/ЕК од 8 декември 2008 година за идентификација и назначување на европската критична инфраструктура и процена на потребата за подобрување на нивната заштита (SL L 345/75, 23 декември 2008 година).

член 2

Одредени термини во смисла на овој закон го имаат следново значење:

1. Анализата на ризик значи разгледување на можни сценарија за закана со цел да се проценат ранливостите и потенцијалното влијание на критичните прекини или уништување на инфраструктурата.

2. Европска критична инфраструктура значи критична инфраструктура од интерес за најмалку две земји-членки или една земја-членка, лоцирана на територијата на друга земја-членка.

3. Меѓусекторски одредници значат збир на општи одредници според кои се проценува ризикот за поединечни критични инфраструктурни системи и мрежи во сите сектори.

4. Чувствителни податоци се податоци за критична инфраструктура кои се означени како класифицирани податоци во согласност со посебен пропис.

5. Контактната точка е централно тело на државната управа што комуницира во име на државата со надлежните органи на Европската Унија и другите земји со цел размена на информации за критичните инфраструктури и спроведување на утврдените активности во нивна заштита и обезбедување континуитет.

6. Секторски одредници значат збир на специфични одредници кои се користат за процена на ризикот за секторски критични системи и мрежи.

7. Координатор за безбедност на критичната инфраструктура е лице кое работи на прашања поврзани со заштита на критичната инфраструктура помеѓу сопствениците/управителите и органите на централната државна управа одговорни за одреден сектор на критична инфраструктура.

8. Безбедносен план на сопственикот/управителот значи план кој обезбедува доверливост, интегритет и достапност на организациски, кадровски, материјални, информациско-комуникациски и други решенија, како и континуирани и чекор-по-чекор безбедносни мерки потребни за континуирано работење на критична инфраструктура.

9. Управување со критична инфраструктура е обезбедување услови за работа и континуирано работење на критичната инфраструктура.

10. Сопственици/управители се правни лица одговорни за управување со критична инфраструктура.

11. Заштита на критичната инфраструктура значи активности насочени кон обезбедување на функционалност, континуитет и испорака на услуги/стоки од критична инфраструктура и спречување на загрозување на критичната инфраструктура.

II. НАЦИОНАЛНИ КРИТИЧНИ ИНФРАСТРУКТУРИ

член 3

Националните критични инфраструктури се системи, мрежи и објекти од национално значење чиј прекин или прекин на снабдувањето со стоки или услуги може да има сериозни последици за националната безбедност, здравјето и животот на луѓето, имотот и животната средина, безбедноста и економската стабилност и континуираното функционирање на владата.

член 4

(1) Секторите на националните критични инфраструктури можат особено да бидат:

- енергија (производство, вклучувајќи резервоари и брани, пренос, складирање, транспорт на енергенси и енергија, системи за дистрибуција),
- комуникациска и информатичка технологија (електронски комуникации, пренос на податоци, информациски системи, обезбедување аудио и аудиовизуелни медиумски услуги),

- транспорт (патен, железнички, воздушен, поморски и внатрешен воден транспорт),
- здравство (здравствена заштита, производство, трговија и контрола на лекови),
- управување со водите (регулаторни и заштитни водни конструкции и комунални водни структури),
- храна (производство и снабдување со храна и систем за безбедност на храна, залихи),
- финансии (банкарство, берзи, инвестиции, осигурување и платежни системи),
- производство, складирање и транспорт на опасни материи (хемиски, биолошки, радиолошки и нуклеарни материјали),
- јавни услуги (обезбедување јавен ред и мир, заштита и спасување, итна медицинска помош),
- национални споменици и вредности.

(2) Покрај секторите наведени во став 1 на овој закон, Владата на Република Хрватска со одлука може да определи критични инфраструктури од други сектори.

член 5

(1) Владата на Република Хрватска со посебна одлука ги определува секторите од кои органите на централната државна управа ги идентификуваат поединечните национални критични инфраструктури, со цел да се обезбеди сеопфатна заштита и да се намалат негативните ефекти во случај на закана од критична инфраструктура, на предлог на централниот орган на државната управа во чиј делокруг на работа се заштитата и спасување и го утврдува редоследот на критичните инфраструктурни сектори поради нивното значење за општото функционирање на државата (рангирање на критичните инфраструктурни сектори поради нивната критичност) и заштита на критичните инфраструктури на државно ниво.

(2) Владата на Република Хрватска на предлог на надлежните органи на централната државна управа со посебна одлука ги потврдува идентификуваните критични инфраструктури.

член 6

(1) Централниот орган на државната управа во чиј делокруг се активностите за заштита и спасување, во соработка со надлежните органи на централната државна управа од чиј делокруг е поединечната критична инфраструктура, редовно врши следење, процена на заканите и предлага оперативни и други мерки за процена на критичноста и потребите од предлог мерки за управување и заштита на критичните инфраструктури.

(2) Централниот орган на државната управа надлежен за заштита и спасување доставува годишен извештај до Владата на Република Хрватска и до комисијата на хрватскиот парламент надлежен за национална безбедност за бројот на националните критични инфраструктури по сектори и нивната критичност и спроведување на мерките за заштита на критичната инфраструктура.

член 7

(1) Органите на централната државна управа во соработка со надлежните регулаторни агенции се одговорни во рамките на својот делокруг за идентификација (означување) на поединечни системи или нивни делови како национални критични инфраструктури, обезбедувајќи управување со критичните инфраструктури и нивна заштита.

(2) Раководителот на органот на централната државна управа од ставот (1) на овој член ќе донесе одлука за утврдување на националната критична инфраструктура врз основа на одлуката на Владата на Република Хрватска за потврдување на идентификуваната критична инфраструктура од член 5 став 2 од овој закон и ја доставува на спроведување на сопственикот/управителот на инфраструктурата и централниот орган на државната управа кој е надлежен за заштита и спасување.

(3) Сопствениците/управителите на идентификуваните (назначени) критични инфраструктури се директно одговорни за управувањето и заштитата на критичните инфраструктури во сите услови.

член 8

Критериумите за определување на поединечни мрежи, системи и објекти за национална критична инфраструктура претставуваат класифицирани информации и се означени со соодветно ниво на тајност во согласност со посебните прописи за тајност на податоците.

III. АНАЛИЗА НА РИЗИК ЗА ИДЕНТИФИКАЦИЈА НА КРИТИЧНИ ИНФРАСТРУКТУРИ

член 9

(1) Анализата на ризик ги утврдува вкупните ефекти од прекините на критичната инфраструктура и се врши во согласност со меѓусекторските и секторските критериуми.

(2) При анализата на ризикот на сите критични инфраструктури се применуваат меѓусекторски критериуми по следниот редослед и вклучуваат:

1. човечки загуби (проценет можен број на жртви или повреди поради нарушување на одредена критична инфраструктура);

2. економски загуби (проценети во поглед на важноста на економската загуба и/или влошување на квалитетот на производите или услугите, вклучително и можните ефекти врз животната средина);

3. влијание врз јавноста (што се оценува во однос на влијанието врз довербата на јавноста, физичкото страдање и

нарушувањето на секојдневниот живот, вклучително и губењето на основните и јавните услуги).

(3) Секторските критериуми ги утврдуваат надлежните органи на централната државна управа во соработка со регулаторните агенции и стручните здруженија за секој поединечен сектор.

член 10

(1) Органите на централната државна управа во соработка со надлежните регулаторни агенции изготвуваат анализи на ризик и секторски планови за обезбедување на работа на критичните инфраструктури со обезбедување на снабдување со стоки/услуги за секторски критични инфраструктури од нивниот делокруг.

(2) Органите на централната државна управа соработуваат со надлежните регулаторни агенции при изготвувањето на анализи на ризик и планови за обезбедување на работа на критичните инфраструктури, имајќи ги предвид постојните секторски процени за ранливост и планови за продолжување на работата за одделни сектори изготвени врз основа на други секторски прописи кои ги опфаќаат со овој закон утврдените ризици, доколку можат целосно да ги заменат анализите на ризик и плановите за осигурување на работата на критична инфраструктура.

(3) При проценатa на ризикот и потребното ниво на заштита, мора да се земе предвид влијанието на одреден сектор или мрежа на критична инфраструктура врз други критични инфраструктури и да се обезбеди размена на податоци неопходни за подготовка на анализи на ризик.

член 11

(1) Сопствениците/управителите на поединечна критична инфраструктура се должни да изготват анализа на ризик, како основа за изготвување на Планот за безбедност врз основа на критериумите од член 9 на овој закон.

(2) При изготвувањето на анализа на ризик, сопствениците/управителите соработуваат со органите на централната државна управа во чиј делокруг се наоѓа критичната инфраструктура, надлежните регулаторни агенции и централниот орган на државната управа во чиј делокруг се активностите за заштита и спасување.

(3) Раководителот на органот на централната државна управа во чиј делокруг се активностите за заштита и спасување, во соработка со органите на централната државна управа надлежни за стопанство, транспорт, здравство, финансии, земјоделство, внатрешни работи и одбрана, донесува Правилник за методологијата за анализа на деловниот ризик на критичните инфраструктури.

IV. БЕЗБЕДЕНОСЕН ПЛАН НА СОПСТВЕНИЦИТЕ/УПРАВИТЕЛИТЕ

член 12

(1) Сопствениците/управителите на критичната инфраструктура се должни да изготват безбедносен план на сопственикот/управителот кој вклучува мерки за заштита и обезбедување продолжување на делувањето на критичните инфраструктурни операции и испораката на услуги/стоки. Рокот за изработка на безбедносните планови на сопственикот/управителот е 6 месеци од приемот на актот на надлежното централно тело кое ги определува како национална критична инфраструктура.

(2) Планот за безбедност на сопственикот/управителот може да се замени со постоечки еквивалентни документи изготвени врз основа на други секторски прописи. Централниот орган на државната управа во чиј делокруг се наоѓа критичната инфраструктура од ставот 1 на овој член ја утврдува еквивалентноста

на документите изготвени врз основа на други секторски прописи.

член 13

(1) Сопствениците/управителите на критичната инфраструктура се должни да донесат План за безбедност по претходна согласност на органот на централната државна управа во чиј делокруг се наоѓа критичната инфраструктура. Во процесот на издавање одобренија, надлежните органи на централната државна управа се должни, во соработка со надлежните регулаторни агенции, да утврдат дали Планот за безбедност е изготвен во согласност со меѓусекторските и секторските критериуми.

(2) Безбедносниот план на сопственикот/управителот на критични инфраструктури е дел од деловниот план на правното лице и не е јавно достапен.

(3) Безбедносниот план на сопственици/управителите на критична инфраструктура треба да содржи најмалку:

1. идентификација на важни делови или објекти на мрежата,

2. спроведување на анализа на ризик врз основа на сценарија со висока закана, ранливости на секој објект, систем, мрежа и функционалност и можни последици во редовното работење и во случај на прекин на критичната инфраструктура, вклучувајќи го и ризикот од напуштање на локацијата на критичната инфраструктура.

3. идентификација, селекција и одредување на сите неопходни мерки и процедури за намалување на ранливоста и обезбедување на работа на сите идентификувани критични делови или објекти на мрежата или системот, разликувајќи ги следните мерки:

- постојани безбедносни мерки и процедури (технички, организациски, комуникациски мерки и мерки и процедури за рано предупредување и подигање на свеста) со кои се утврдуваат неизбежните безбедносни трошоци и се применуваат континуирано,

- степенувани безбедносни мерки кои се активираат во зависност од зајакнувањето на заканите.

(4) Безбедносните планови се преиспитуваат во рок од една година од поставувањето на критичната инфраструктура, а редовно еднаш годишно.

V. БЕЗБЕДНОСЕН КООРДИНАТОР ЗА КРИТИЧНА ИНФРАСТРУКТУРА

член 14

(1) Органите на централната државна управа определуваат координатор за безбедност на критичната инфраструктура и негов заменик за секој сектор од критична инфраструктура од нејзиниот делокруг.

(2) Сопствениците/управителите на критичната инфраструктура назначуваат координатор за безбедност на критичната инфраструктура кој е одговорен за комуникација во врска со безбедносните прашања помеѓу сопствениците/управителите на безбедноста и надлежниот орган на централната власт одговорен за критичната инфраструктура, со цел да се обезбеди заштита и континуитет на критичната инфраструктура.

VI. ЕВРОПСКИ КРИТИЧНИ ИНФРАСТРУКТУРИ

член 15

(1) Европските критични инфраструктури се инфраструктури од интерес за најмалку две земји членки или една земја членка, лоцирани на територијата на друга земја-членка.

(2) Европските критични инфраструктури може да се назначат во сектори определени од Европската комисија.

(3) Доколку се исполнети условите од став 1 на овој член, Европската критична инфраструктура на територијата на Република Хрватска ја утврдува Владата на Република Хрватска на барање и во договор со заинтересираните земји членки на Европската Унија ги информира заинтересираните земји членки за утврдување на европска критична инфраструктура на територијата на Република Хрватска.

(4) Податоците поврзани со назначувањето на поединечна критична инфраструктура за европска критична инфраструктура претставува класифицирана информација и се означени со соодветно ниво на тајност. Критериумите за утврдување на степенот на тајност на таквите информации се пропишуваат со одлука на Владата на Република Хрватска.

(5) Органите на централната државна управа за одлуката на Владата на Република Хрватска од ставот (3) на овој член ги известуваат сопствениците/управителите на критичната инфраструктура од нивниот делокруг и надлежните регулаторни агенции.

(6) Доколку критичната инфраструктура од значење за Република Хрватска се наоѓа на територијата на друга земја членка на Европската Унија, Владата на Република Хрватска ќе му предложи на надлежниот орган на таа земја означување на европска критична инфраструктура.

(7) Доколку земјата членка на чија територија се наоѓа критичната инфраструктура не го прифати предлогот на Република Хрватска, Владата на Република Хрватска ќе ја информира Европската комисија за тоа и ќе побара нејзино вклучување.

(8) При определувањето на европската критична инфраструктура во Република Хрватска, ќе се применуваат одредбите од овој закон кои се однесуваат на определувањето на националната критична инфраструктура и секторските и

меѓусекторските критериуми наведени во овој акт, со што се обезбедува учество на овластени претставници на заинтересирани земји членки.

член 16

Европските критични инфраструктури на територијата на Република Хрватска се заштитени на ист начин како и националните критични инфраструктури, освен ако прашањето не е поинаку регулирано со регулативите на Европската Унија.

член 17

(1) Владата на Република Хрватска донесува годишен извештај за бројот на европските критични инфраструктури по сектори и бројот на заинтересирани земји кои зависат од секоја конкретна критична инфраструктура, на предлог на органот на централната државна управа надлежен за заштита и спасување во кои се идентификувани европските критични инфраструктури.

(2) Извештајот од ставот (1) на овој член се доставува до Европската комисија и до заинтересираните земји кои зависат од одредени критични инфраструктури.

(3) На секои две години, Владата на Република Хрватска до Европската комисија доставува резиме на општи податоци за видовите опасности, закани и слабости идентификувани во секој сектор во кој е идентификувана европска критична инфраструктура во Република Хрватска.

(4) Извештајот од став 1 и резимето од став 3 на овој член се класифицирани информации и се означуваат со соодветно ниво на тајност.

член 18

(1) Контакт-точка за потребите од размена на информации и координација на активностите поврзани со европската критична инфраструктура со другите земји-членки и органите на

Европската унија е централниот орган на државната управа надлежен за заштита и спасување.

(2) Размената на информации за европските критични инфраструктури преку контакт точките на земјите-членки не ги исклучува правата и обврските на другите органи на централната државна управа за размена на информации, знаења и искуства со слични тела на други држави.

VII. ПОСТАПУВАЊЕ СО ЧУВСТВИТЕЛНИ ПОДАТОЦИ

член 19

Постапувањето со чувствителните податоци за националната и европската критична инфраструктура се одвива во согласност со посебните прописи од областа на безбедноста на информациите и меѓународните договори. Покрај податоците класифицирани во согласност со овој закон и означени со соодветно ниво на тајност, во областа на заштитата на критичната инфраструктура ќе бидат класифицирани и други податоци поврзани со поединечна критична инфраструктура, доколку класификацијата на таквите податоци е неопходна за заштита на вредностите заштитени со прописот за тајност на податоците.

VIII. НАДЗОР

член 20

(1) Инспекциски надзор над спроведувањето на овој закон од страна на сопствениците/управителите на критичните инфраструктури вршат органите на централната државна управа во

чиј делокруг се наоѓаат одредени критични инфраструктури и надлежните регулаторни агенции.

(2) Во инспекцискиот надзор инспекторот врши надзор над лицата кои се должни да ги спроведуваат мерките и активностите од овој закон, исполнувањето на условите и начинот на работа на лицата под надзор, врши непосреден увид во општите и поединечните акти и презема мерки определени со овој закон.

(3) Доколку во инспекцискиот надзор инспекторот констатира повреда на одредбите од овој закон, особено на одредбите од членовите 11 до 14 на овој закон, има право и обврска да нареди мерки за отстранување на констатираните неправилности во разумен рок.

(4) Доколку инспекцискиот надзор утврди дека е повреден овој закон, инспекторот има право и обврска без одлагање:

- да поведе прекршочна постапка,

- да презема други мерки и врши други дејствија што е овластен да ги преземе и врши врз основа на овој закон и посебните прописи.

(5) Доколку при увидот инспекторот утврди дека не е овластен непосредно да постапува, веднаш ќе го извести надлежниот централен орган на државната управа или регулаторната агенција и ќе побара поведување постапка и преземање мерки согласно посебните прописи.

член 21

За да се обезбеди унифициран пристап кон анализата на ризик од критична инфраструктура, надзор над примената на меѓусекторските критериуми од член 9 став 2 на овој закон од страна на сите учесници во спроведувањето на Законот ќе врши централна држава орган на управата надлежен за заштита и спасување, а примената на секторските критериуми во анализата на ризик од член 9 став 3 на овој закон ја вршат

органите на централната државна управа и регулаторните агенции во секторот од нивниот делокруг.

IX. ПРЕКРШОЧНИ ОДРЕДБИ

член 22

(1) Глоба од 500.000,00 до 1.000.000,00 куни ќе му се изрече за прекршок на сопственикот/управителот на критична инфраструктура ако:

- не изготвува анализа на ризик, како основа за изготвување на безбедносен план врз основа на критериумите од член 9 на овој закон (член 11 став 1);

- не изготви и донесе безбедносен план на сопственикот/управителот кој опфаќа мерки за заштита и обезбедување на продолжување на делувањето на критичната инфраструктура и испорака на услуги/стоки (член 12 став 1 и член 13 став 1);

- не определи координатор за безбедност за критична инфраструктура (член 14 став 2).

(2) За прекршокот од ставот (1) на овој член ќе се казни и одговорното лице на сопственикот/управителот на критична инфраструктура.

X. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

член 23

Органите на централната државна управа се должни на Владата на Република Хрватска да ѝ предложат критична инфраструктура од секторот од нивниот делокруг и степенот на

нивната критичност во рок од шест месеци од денот на влегувањето во сила на овој закон.

член 24

Правилникот од член 11 став 3 на овој закон, раководителот на централниот орган на државната управа во чиј делокруг се работи за заштита и спасување ќе ја донесе во рок од шест месеци од денот на влегувањето во сила на овој закон.

член 25

Раководителите на органите на централната државна управа се должни да донесат секторски критериуми од овој закон во рок од шест месеци од денот на влегувањето во сила на овој закон.

член 26

Овој закон влегува во сила осмиот ден од денот на објавувањето во Службен весник, освен членовите 15-18 од овој закон, кои влегуваат во сила со денот на пристапувањето на Република Хрватска во полноправно членство во Европската Унија.

Класа: 022-03 / 13-01 / 68

Загреб, 26 април 2013 година

Прилог бр.2: СРБИЈА
Закон за критичната инфраструктура
„Службен весник на РС“, бр.87 од 13.11.2018 год.

I. ОСНОВНИ ОДРЕДБИ
Предмет на Законот

член 1

Со овој закон се уредува националната и европската критична инфраструктура, идентификацијата и утврдувањето на критичната инфраструктура на Република Србија (во натамошниот текст: критична инфраструктура), заштитата на критичната инфраструктура, надлежноста и одговорноста на органите и организациите од областа на критичната инфраструктура (во натамошниот текст: надлежни тела и организации) и информации, известување, поддршка на одлуки, заштита на податоци, управување и надзор на критичната инфраструктура.

Значењето на изразите

член 2

Одредени термини употребени во овој закон го имаат следново значење:

1) критични инфраструктурни сектори се подрачја утврдени со овој закон, во кои се врши постапката на идентификација и утврдување на критична инфраструктура;

2) идентификација на критична инфраструктура е постапка на определување системи, мрежи, објекти или нивни делови во одреден сектор кои согласно утврдените критериуми се идентификуваат како критична инфраструктура;

3) определување на критична инфраструктура е постапка на определување на системи, мрежи, објекти или нивни делови како критична инфраструктура во согласност со овој закон;

4) заштита на критичната инфраструктура е збир на активности и мерки насочени кон обезбедување на функционирање на критичната инфраструктура во случај на нарушување или уништување или заштита во случај на закани и спречување на последиците од нарушување или уништување;

5) оператори на критична инфраструктура се државни органи, органи на автономната покраина, органи на единиците на локалната самоуправа, јавни претпријатија, трговски друштва или други правни лица кои управуваат со системи, мрежи, објекти или нивни делови што се означени како критична инфраструктура;

6) Безбедносен план на операторот за управување со ризик е план изготвен од операторот со критична инфраструктура, кој ги дефинира безбедносните цели и мерки на операторот врз основа на анализата на ризикот содржана во планот;

7) офицер за врска е лице вработено кај оператор со критична инфраструктура, кое е контакт помеѓу операторот на критична инфраструктура и министерството надлежно за внатрешни работи (во натамошниот текст: Министерството);

8) европска критична инфраструктура значи критична инфраструктура лоцирана на територијата на земја членка на Европската Унија, чиешто нарушување или уништување би имало значително влијание врз најмалку две земји членки.

Принципи на работа

член 3

Надлежните органи и организации, граѓаните и другите субјекти се должни при преземањето мерки и активности утврдени со овој и со други закони, програми, планови и други документи од областа на критичната инфраструктура да ги следат следните начела:

1) начело на интегриран пристап – во заштитата на критичната инфраструктура пред, за време и по нарушување или

нарушување на критичната инфраструктура, учествуваат сите надлежни органи и организации, граѓани и други субјекти, земајќи ги предвид различните видови опасности кои произлегуваат од анализата на ризик, земајќи ја предвид меѓузависноста на критичниот инфраструктурен сектор и нивната интеракција;

2) начело на одговорност – операторите со критична инфраструктура се директно одговорни за функционирањето на критичната инфраструктура, а за подобрување на заштитата на критичната инфраструктура, покрај операторите, сите надлежни органи и организации, граѓаните и другите субјекти;

3) начело на заштита од разни видови закани – операторите, надлежните органи и организации, граѓаните и другите субјекти во обезбедувањето на континуирано работење на критичната инфраструктура се должни да ги земат предвид различните видови ризици;

4) начело на континуирано планирање на заштитата на критичната инфраструктура – заштитата на критичната инфраструктура се заснова на постојан процес на анализа на ризик за функционирање на критичната инфраструктура и процена на соодветноста на мерките за заштита;

5) начело на размена на податоци и информации и заштита на податоците – операторите, надлежните органи и организации, граѓаните и другите субјекти се должни навремено и континуирано да разменуваат потребни податоци и информации истовремено штитејќи ги податоците во врска со критичната инфраструктура, во согласност со прописите со кои се уредува заштитата на класифицирани податоци.

Критична инфраструктура

член 4

Критична инфраструктура се системи, мрежи, објекти или нивни делови, чијшто прекин или прекинот на испораката на стоки

или услуги може да има сериозни последици врз националната безбедност, здравјето и животот на луѓето, имотот, животната средина, безбедноста на граѓаните, економската стабилност или да го загрози функционирањето на Република Србија.

Министерството регулира, планира, координира, контролира активности, комуницира и обезбедува информации поврзани со критичната инфраструктура.

II. ИДЕНТИФИКАЦИЈА И ОПРЕДЕЛУВАЊЕ НА КРИТИЧНА ИНФРАСТРУКТУРА

Идентификација на критична инфраструктура

член 5

Идентификацијата на критичната инфраструктура се врши по сектори во согласност со утврдените критериуми.

Министерствата надлежни за одредени области се задолжени за спроведување на процесот на идентификување на критичната инфраструктура во одреден сектор.

Критериумите за идентификација на критичната инфраструктура и начинот на известување ги пропишува Владата.

Сектори на критична инфраструктурна

член 6

Секторите во кои се идентификува и одредува критичната инфраструктура се:

1) енергија;

2) сообраќај;

3) снабдување со вода и храна;

4) здравствена заштита;

5) финансии;

6) телекомуникациски и информациски технологии;

7) заштита на животната средина;

8) функционирање на државните органи.

Покрај секторот од ставот 1 на овој член, критична инфраструктура може да се определува и во други сектори, на предлог на министерството надлежно за одредена област, согласно со овој закон.

Владата со акт од член 5 став 3 на овој закон го пропишува определувањето на секторите од ставот 2 на овој член и критериумите за идентификација на критичната инфраструктура во тие сектори.

Одредување на критична инфраструктура

член 7

Критичната инфраструктура ја утврдува Владата на предлог на Министерството.

Министерствата надлежни за критичните инфраструктурни сектори се должни до Министерството да достават предлози за критична инфраструктура во нивниот сектор во рок од шест месеци од донесувањето на актот од членот 5 став 3 на овој закон, а по завршувањето на постапката за идентификација во согласност со утврдените критериуми.

Министерствата надлежни за критичните инфраструктурни сектори се должни редовно и најмалку квартално да го известуваат Министерството за новите промени во нивниот сектор.

Министерствата надлежни за критичните инфраструктурни сектори се должни секоја година до Министерството да доставуваат предлози за измени на критичната инфраструктура во нивниот сектор, најдоцна до 31 октомври, по завршување на постапката за идентификација.

Министерството може да ги посочи потенцијалните критични инфраструктури на министерствата надлежни за секторите на критичната инфраструктура.

Заштитата, складирањето, користењето, контролата и надзорот на критичната инфраструктура во надлежност на Министерството за одбрана и Армијата на Србија се врши во согласност со Законот за одбрана и Законот за Армијата на Србија.

Законот за означување на критичната инфраструктура се ажурира секоја година, најдоцна до 31 декември.

III. ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

План за безбедност на операторот за управување со ризик

член 8

Безбедносниот план на операторот за управување со ризик е документ со кој се определуваат мерки за намалување на ризикот, се дефинираат одговорностите и се утврдуваат должностите и се воспоставува рамка за дејствување за елиминирање или намалување на последиците од безбедносните закани дефинирани во анализата на ризик, што е составен дел на планот.

Операторите со критична инфраструктура се должни да подготват План за безбедност за операторите за управување со

ризици и да добијат согласност од Министерството веднаш, а најдоцна шест месеци по утврдувањето на системите, мрежите, објектите или нивните делови за критична инфраструктура.

Методологијата, начинот на подготовка и содржината на Планот за безбедност на операторот за управување со ризици ги пропишува министерот надлежен за внатрешни работи (во натамошниот текст: министерот).

Офицер за врска

член 9

Операторите на критична инфраструктура мора да имаат офицер за врска, односно лице кое служи како контакт помеѓу операторот и Министерството, кое обезбедува постојана контрола на ризиците и заканите, информира за промени во критичната инфраструктура, го информира Министерството за процена на ризик, закана и ранливост, го координира планот за безбедност на операторот за управување со ризик, врши тестирање преку вежби и други активности предвидени со планот и ги извршува сите други задачи поврзани со критичната инфраструктура.

Офицерот за врска го именува Министерството на предлог на операторот со критична инфраструктура од редот на вработените.

Операторот на критична инфраструктура до Министерството поднесува предлог за именување на офицери за врска најдоцна три месеци по назначувањето на системи, мрежи, објекти или нивни делови за критична инфраструктура.

Предложеното лице мора да има лиценца за офицер за врска.

Дозволата од ставот 4 на овој член Министерството ја издава на лице кое има:

1) високо образование (магистерски академски студии, специјалистички академски или специјалистички стручни студии, односно додипломски студии во траење од најмалку четири години според прописот со кој се уредува високото образование до 10 септември 2005 година);

2) положил посебен стручен испит за офицер за врски.

Полагањето на посебен стручен испит од точка 2) на овој член го организира и спроведува Министерството.

Начинот и програмата за полагање на посебниот стручен испит ги пропишува министерот.

Операторите со критична инфраструктура обезбедуваат континуитет на функцијата на офицерот за врска во случај на негово отсуство со известување на Министерството за привремено извршување на овие задачи од друго лице, со сите потребни информации.

Критична инфраструктура во планските документи

член 10

При изготвување на плански документи од областа на просторното и урбанистичкото планирање, документите од областа на националната безбедност и намалувањето на ризикот и управувањето со вонредни состојби, критичната инфраструктура мора да се третира на посебен начин, особено во делот на превентивните активности и активности поврзани со одговорите при вонредни ситуации каде треба да има приоритет.

Републички штаб за вонредни состојби

член 11

Во случај на појава на загрозување, попречување на работа или уништување на критична инфраструктура, управувањето

и координацијата на спроведувањето на мерките и задачите во наведените околности ги презема Републичкиот штаб за вонредни состојби, согласно со закон.

Министерството обезбедува стручна поддршка на персоналот од ставот 1 на овој член и ги доставува сите потребни податоци и информации заради непречено вршење на работите во извршувањето на поставените задачи.

IV. ЕВРОПСКА КРИТИЧНА ИНФРАСТРУКТУРА

Поим

член 12

Европската критична инфраструктура е критична инфраструктура од интерес за најмалку две земји членки на Европската Унија.

Утврдување на европската критична инфраструктура

член 13

Европската критична инфраструктура може да се дефинира во сектори дефинирани од Европската комисија.

Европската критична инфраструктура на територијата на Република Србија, на предлог на Министерството, ја утврдува Владата на барање и во договор со заинтересираните земји членки на Европската Унија и ги известува заинтересираните земји членки за утврдување на европска критична инфраструктура за територијата на Република Србија.

Доколку критичната инфраструктура од значење за Република Србија се наоѓа на територија на друга земја членка

на Европската Унија, Владата ќе му предложи на надлежниот орган на таа држава утврдување на европската критична инфраструктура.

Заштита на европската критична инфраструктура

член 14

Европската критична инфраструктура на територијата на Република Србија е заштитена на ист начин како и критичната инфраструктура на Република Србија, освен кога таа е поинаку регулирана со прописите на Европската унија.

Известување за европска критична инфраструктура

член 15

Владата усвојува годишен извештај за бројот на европската критична инфраструктура по сектори и за бројот на заинтересирани земји кои се засегнати од секоја конкретна критична инфраструктура, на предлог на Министерството.

Извештајот од став 1 на овој член се доставува до Европската комисија и до заинтересираните земји засегнати од секоја конкретна критична инфраструктура.

Размена на информации за европската критична инфраструктура

член 16

Контакт-точка за потребите за размена на информации и координација на активностите поврзани со Европската критична инфраструктура со другите земји-членки и тела на Европската Унија е Министерството.

V. ПОСТАПУВАЊЕ СО КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Одредување и размена

член 17

Одредени податоци за критична инфраструктура може да се класифицираат како класифицирани информации во согласност со прописите што ја регулираат доверливоста на податоците.

Класифицираните информации поврзани со европската критична инфраструктура се разменуваат со странски земји и тела на Европската Унија во согласност со законот со кој се регулира доверливоста на податоците и потпишаните меѓународни договори за размена на доверливи информации.

VI. НАДЗОР

Надлежност

член 18

Надзор над примената на овој закон и прописите донесени врз основа на него врши Министерството.

Министерството врши инспекциски надзор преку инспектори.

Овластувања на инспекторите

член 19

При вршењето на инспекциски надзор, инспекторот има право:

1) ја утврдува состојбата на исполнување на обврските предвидени со овој закон, предупредува на констатираните неправилности и определува мерки и рокови за нивно отстранување;

2) врши увид во документите поврзани со критичната инфраструктура;

3) го проверува спроведувањето на издадените наредби и заклучоци и наредбите за мерки за извршување;

4) наложува подготовка, донесување и ажурирање на документите предвидени со овој закон;

5) наложува прекинување на мерките и дејствијата кои не се во согласност со Планот за безбедност на операторот за управување со ризик;

6) наложува отстранување на констатираните недостатоци во спроведувањето на пропишаните мерки утврдени со Планот за безбедност на операторот за управување со ризик;

7) поднесува предлог за поведување постапка за утврдување прекршочна одговорност против правни и одговорни лица;

8) наредува да се преземат итни мерки;

9) презема други мерки за кои е овластен со закон.

Против решението на инспекторот може да се изјави жалба во рок од осум дена од денот на доставувањето на решението.

Жалба против решението на инспекторот донесено врз основа на став 1 т 5) и 8) на овој член не го одлага извршувањето на решението.

VII. КАЗНЕНИ ОДРЕДБИ

член 20

Глоба во износ од 100.000 до 1.000.000 динари ќе се изрече на јавно претпријатие, друштво или друго правно лице кое стопанисува со системи, мрежи, објекти или нивни делови што се означени како критична инфраструктура ако:

1) не добие согласност од Министерството за планот за безбедност на операторот за управување со ризици (член 8 став 2);

2) не достави до Министерството предлог за именување офицер за врска (член 9 став 3);

3) не постапи по наредба на инспекторот (член 19 став 1).

член 21

Глоба од 50.000 до 100.000 динари ќе му се изрече за прекршокот и на одговорното лице во надлежниот државен орган, органот на територијалната автономија или органот на единицата на локалната самоуправа, ако:

1) не достави до Министерството предлози за критична инфраструктура во својот сектор (член 7 став 2);

2) не го известува Министерството за нови промени во својот сектор (член 7 став 3);

3) не достави до Министерството предлози за измена на критичната инфраструктура во својот сектор (член 7 став 4);

4) не постапи по наредба на инспекторот (член 19 став 1).

VIII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Рок за донесување на подзаконски акти

член 22

Подзаконските акти за спроведување на овој закон ќе се донесат во рок од шест месеци од денот на влегувањето во сила на овој закон.

Рок за усогласување на општиот акт

член 23

Измените и дополнувањата на актот за внатрешна организација и систематизација на работните места во Министерството за внатрешни работи ќе направи министерот во рок од 30 дена од денот на влегувањето во сила на овој закон.

Примена на одредбите за европската критична инфраструктура

член 24

Одредбите на овој закон кои се однесуваат на европската критична инфраструктура ќе почнат да се применуваат со денот на пристапувањето на Република Србија во Европската Унија.

Влегувањето во сила

член 25

Овој закон влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Србија“.

Прилог бр. 3: ЦРНА ГОРА

Закон за утврдување и заштита на критична инфраструктура

Законот е објавен во „Службен весник на Црна Гора“, бр. 72/2019 од 26.12.2019 г. година, а стапи во сила на 3.1.2020 година.

I. ОСНОВНИ ОДРЕДБИ

Предмет

член 1

Критичната инфраструктура се утврдува и заштитува на начин и под услови пропишани со овој закон, меѓународните договори и стандардите на Европската Унија.

Критична инфраструктура

член 2

Критичната инфраструктура вклучува системи, мрежи, објекти или нивни делови лоцирани на територијата на Црна Гора, чиј прекин, односно прекин на испораките на стоки или услуги преку овие системи, мрежи, објекти или нивни делови може да има сериозни последици за националната безбедност, здравјето и животите на луѓето, имотот, животната средина, безбедноста на граѓаните, економската стабилност, односно вршење работи од јавен интерес.

Заштита на критична инфраструктура

член 3

Заштита на критичната инфраструктура е збир на активности и мерки насочени кон спречување на појава на прекини, оштетување или уништување на критична инфраструктура во случај на закана, обезбедување на функционирање и отпорност на критичната инфраструктура во случај на прекини или оштетувања и спречување на последиците на прекини, односно оштетување или уништување на критична инфраструктура.

Употреба на родово сензитивен јазик

член 4

Поимите употребени во овој закон за физички лица од машки род ги означуваат истите поими во женски род.

Значењето на термините

член 5

Термините употребени во овој закон го имаат следново значење:

1) оператори на критична инфраструктура се државни органи, органи на државната управа, органи на локалната самоуправа, органи и служби на локалната самоуправа формирани во согласност со законот со кој се уредува локалната самоуправа, компании и други правни лица кои користат или управуваат со системи, мрежи, објекти, односно нивни делови кои се означени како критична инфраструктура;

2) анализата на ризик подразбира разгледување на можни опасности и конвенционални или хибридни закани со цел да се проценат можните последици од прекини во работењето или евентуално нарушување на критичната инфраструктура, нејзино оштетување или уништување;

3) критична информациска инфраструктура опфаќа информациски системи управувани од оператори со критична инфраструктура, чие прекинување или уништување би ги загрозило животот, здравјето, безбедноста на граѓаните и функционирањето на државата и од чие функционирање зависи вршењето на работите од јавен интерес;

4) чувствителни информации за заштита на критичната инфраструктура се информации за критична инфраструктура кои, доколку бидат откриени, би можеле да се користат за планирање и преземање активности што ќе предизвикаат нарушување или прекин во работата на критичната инфраструктура или нејзино оштетување или уништување;

5) Европска критична инфраструктура значи критична инфраструктура лоцирана на територијата на земја-членка на Европската унија, чие нарушување, прекин, оштетување или уништување би имало значителни последици за најмалку две земји-членки.

II. ОПРЕДЕЛУВАЊЕ НА КРИТИЧНА ИНФРАСТРУКТУРА

Критериуми за определување на критична инфраструктура

член 6

Критичната инфраструктура се утврдува врз основа на критериуми поврзани со процена на можни последици од пореметувања или евентуално нарушување на критичната инфраструктура во областа на енергетиката, транспортот, водоснабдувањето, здравството, финансиите, електронските комуникации и информациско-комуникациските технологии, заштитата на животната средина, функционирање на државните органи, како и во други области од јавен интерес (во натамошниот текст: критериуми за утврдување на критична инфраструктура).

Критериумите за определување на критичната инфраструктура можат да бидат секторски и меѓусекторски.

Секторски критериуми за утврдување на критична инфраструктура

член 7

Секторските критериуми за утврдување на критичната инфраструктура се утврдуваат врз основа на анализите на ризик за секој сектор од критичната инфраструктура направени од министерствата надлежни за одредени сектори, имајќи ги предвид карактеристиките на овие сектори.

При одредувањето на проценатa на ризикот и потребното ниво на заштита на критичната инфраструктура, мора да се земе предвид влијанието на еден критичен инфраструктурен сектор врз критичната инфраструктура на другите сектори, со цел да се обезбеди размена на податоци потребни за анализа на ризик.

Секторските критериуми за определување на критичната инфраструктура ги пропишува Владата на Црна Гора (во натамошниот текст: Владата).

Актот од ставот 2 на овој член се означува со соодветен степен на тајност, согласно со законот со кој се уредува тајноста на податоците.

Меѓусекторски критериуми за одредување на критична инфраструктура

член 8

Меѓусекторските критериуми за утврдување на критичната инфраструктура се одредуваат врз основа на анализа на ризик што се однесува на сите сектори на критичната инфраструктура.

Меѓусекторските критериуми од ставот 1 на овој член се:

- можен број на загинати или повредени поради сериозни дефекти или нарушување на критичната инфраструктура;

- економски последици, можни економски загуби и/или влошување на квалитетот на производите или услугите, како и можни последици по животната средина поради сериозни дефекти или нарушување на критичната инфраструктура;

- влијание врз националната безбедност;

- влијание врз јавноста, односно можни последици од прекини во работата или прекин на функционирањето на критичната инфраструктура врз довербата на јавноста и редовните животни активности.

Систем, мрежа, објект или дел од нив може да се определи како критична инфраструктура доколку исполнува барем еден од критериумите од ставот 2 на овој член.

Сектори на критична инфраструктура

член 9

Критичните инфраструктурни сектори се области во кои се идентификува и утврдува критичната инфраструктура и тоа енергија, транспорт, водоснабдување, здравство, финансии, електронски комуникации, информатички и комуникациски технологии, заштита на животната средина, функционирање на државните органи, како и други области од јавен интерес.

Обврска на операторот на критичната инфраструктура

член 10

Министерствата надлежни за секторите за кои се утврдени секторските критериуми за утврдување на критичната инфраструктура на операторите со критична инфраструктура им

даваат информации за секторските критериуми пропишани со актот од членот 7 став 3 на овој закон за тие сектори.

Операторите со критична инфраструктура, врз основа на меѓусекторски и секторски критериуми за утврдување на критичната инфраструктура, проценуваат кои системи, мрежи, објекти или нивни делови што ги користат или управуваат претставуваат критична инфраструктура во одреден сектор на критичната инфраструктура и го известуваат министерството одговорно за тој сектор.

Известувањето од став 2 на овој член содржи детален опис и техничка спецификација на системи, мрежи, објекти или нивни делови кои претставуваат критична инфраструктура и други податоци за кои се оценува дека се релевантни за утврдување на критичната инфраструктура, како и причини зошто операторот на критична инфраструктура смета дека овие системи, мрежи, објекти или нивни делови претставуваат критична инфраструктура.

Одредување на критична инфраструктура

член 11

Министерствата надлежни за одделни сектори утврдуваат дали системите, мрежите, објектите, односно нивните делови од членот 10 став 2 на овој закон ги исполнуваат критериумите од чл. 7 и 8 од овој закон и даваат предлози за утврдување на критична инфраструктура за тие сектори кои ги доставуваат до органот на државната управа надлежен за внатрешни работи (во натамошниот текст: Министерството).

Консолидираните предлози од ставот 1 на овој член Министерството ги доставува до Владата.

Врз основа на консолидираните предлози од ставот 2 на овој член, Владата ја утврдува критичната инфраструктура.

Известувањето од членот 10 став 3 на овој закон, предложено од ст. 1 и 2 и актот од ставот 3 на овој член се означува со соодветен степен на тајност, согласно со законот со кој се уредува тајноста на податоците.

Промени во критичната инфраструктура

член 12

Операторот со критична инфраструктура е должен најмалку еднаш годишно да доставува известување до министерството надлежно за одреден сектор за состојбата, односно промените во системите, мрежите, објектите или нивните делови што се користат или управуваат, а кои се означени како критична инфраструктура.

Врз основа на известувањето од ставот 1 на овој член, министерството надлежно за одреден сектор утврдува дали е потребно да се направат измени или дополнувања во однос на утврдувањето на критичната инфраструктура во тој сектор.

Доколку утврди дека е потребно да се направат измени, односно дополнувања од ставот 2 на овој член, министерството надлежно за одреден сектор ќе даде предлог за измени, односно дополнувања за утврдување на критичната инфраструктура, кој го доставува до Министерството.

Предлогот од ставот 3 на овој член Министерството го доставува до Владата заради изменување или дополнување на актот од членот 11 став 3 на овој закон.

Известувањето од ставот 1 на овој член и предлогот од ставот 3 на овој член се означува со соодветно ниво на тајност, согласно со законот со кој се уредува тајноста на податоците.

III. ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Начин на заштита на критичната инфраструктура

член 13

Заштитата на критичната инфраструктура се врши со примена на физичка и техничка заштита, на начин и под услови пропишани за заштита на објекти и простори во кои се вршат активности од јавен интерес, активности кои претставуваат зголемена опасност по животот и здравјето на луѓето, како и оштетените или уништените објекти кои може да имаат сериозни последици по животот и здравјето на поголем број луѓе, во согласност со законот со кој се уредува заштитата на лицата и имотот што не го обезбедува државата, освен ако со овој закон поинаку не е определено.

По исклучок од став 1 на овој член, начинот на заштита на критичната информатичка инфраструктура, како и начинот на заштита на критичната инфраструктура што ја користи или управува органот на државната управа надлежен за одбраната, органот на управата надлежен за полициските работи, Армијата на Црна Гора и Агенцијата за национална безбедност се врши согласно посебен закон.

Безбедносен план

член 14

Операторите со критична инфраструктура, освен операторите кои користат или управуваат со информациски системи и други оператори од членот 13 став 2 на овој закон, се должни да изработат безбедносен план за заштита на критичната инфраструктура што ја користат или управуваат (во натамошниот текст: безбедносен план). Безбедносниот план ќе добие согласност од Министерството во рок од една година

од донесувањето на актот од членот 11 став 3 на овој закон со кој системите, мрежите, објектите или делови од објектите што ги користат или управуваат се означени како критична инфраструктура.

Безбедносниот план особено содржи:

1) опис на системи, мрежи, објекти или нивни делови што претставуваат критична инфраструктура;

2) анализа на ризик; и

3) активности и мерки насочени кон спречување на појава на прекини, оштетување или уништување на критичната инфраструктура во случај на закана, да се обезбеди функционирање на критичната инфраструктура во случај на прекини или оштетувања и да се спречат последиците од прекини, или оштетување или уништување на критичната инфраструктура , и тоа:

- постојани безбедносни мерки (технички, организациски, комуникациски и мерки за рано предупредување и подигање на свеста) кои континуирано се преземаат; и

- преземени безбедносни мерки во зависност од нивото на ризици и закани за функционирањето на критичната инфраструктура.

Деталната содржина на безбедносниот план ја пропишува Министерството.

Безбедносниот план и актот од ставот 3 на овој член се означуваат со соодветно ниво на тајност, согласно со законот со кој се уредува тајноста на податоците.

План за заштита како безбедносен план

член 15

Доколку операторот со критична инфраструктура има план за заштита и зајакнување на отпорноста на системите, мрежите,

објектите или нивните делови што се користат или управуваат, а кои се означени како критична инфраструктура, изготвен во согласност со законот кој ја регулира заштитата на лицата и имотот што не е предвиден од страна на државата, односно законот со кој се уредува безбедносната заштита на бродовите и пристаништата или друг посебен закон, тој план ќе се смета за безбедносен план доколку комисијата од членот 16 на овој закон утврди дека ги исполнува условите за заштита на критична инфраструктура во согласно со овој закон.

Согласност за безбедносниот план

член 16

За да се даде согласност на безбедносните планови и да се утврди дали плановите за заштита од членот 15 на овој закон ги исполнуваат условите за заштита на критичната инфраструктура, Министерството формира комисија.

Доколку планот за безбедност не ги исполнува условите согласно со членот 14 на овој закон, комисијата од ставот 1 на овој член ќе му даде упатства или препораки на операторот со критична инфраструктура како да го измени планот.

Комисијата од ставот 1 на овој член, пред да го одобри планот за заштита од членот 15 на овој закон, во соработка со претставници на министерството надлежно за одреден сектор, ќе утврди дали планот ги исполнува условите за заштита на критична инфраструктура.

Доколку комисијата од ставот 1 на овој член утврди дека планот за заштита од членот 15 на овој закон не ги исполнува условите за заштита на критичната инфраструктура, ќе постапи на начинот од ставот 2 на овој член.

Операторите со критична инфраструктура се должни да постапуваат според упатствата, односно препораките од ст. 2 и 4 на овој член во рок од 90 дена.

Операторите се должни да го ревидираат безбедносниот план, односно планот за заштита од член 15 на овој закон.

Креирање безбедносен план

член 17

Безбедносниот план го подготвува лице вработено кај оператор со критична инфраструктура кое има:

- VIII степен на образовна квалификација и најмалку пет години работно искуство во заштита на критична инфраструктура во секторот за критична инфраструктура за кој е изготвен безбедносниот план или заштита во смисла на законот со кој се уредува заштитата на лица и имот што не е обезбедена од државата; и

- уверение за положен стручен испит за заштита на критична инфраструктура.

Доколку операторот со критична инфраструктура нема вработен кој ги исполнува условите од став 1 на овој член, може да ја довери изработката на безбедносен план на компанија, друго правно лице или претприемач што врши заштитни работи во согласност со законот со кој се уредува заштитата на лица и имот што не ги обезбедува државата и има вработено лице кое ги исполнува условите од ставот 1 на овој член.

Координатор

член 18

Операторите со критична инфраструктура, освен операторите кои користат или управуваат со информациски системи и други оператори од член 13 став 2 на овој закон, се должни во рок од шест месеци од редот на своите вработени да назначат лице за заштита на критичната инфраструктура (во натамошниот текст: координатор) од денот на донесувањето на актот од членот 11 став 3 на овој закон, со кој системите, мрежите,

објектите или нивните делови што ги користат или управуваат се означуваат како критична инфраструктура.

Координатор може да биде лице кое:

1) има постојан или одобрен престој во Црна Гора;

2) има VIII степен на образование;

3) има општа здравствена способност;

4) не е осуден за кривично дело за кое се гони по службена должност, односно против него не е поведена кривична постапка за такво кривично дело;

5) е стручно оспособен за заштита на критична инфраструктура; и

6) има положено стручен испит за заштита на критична инфраструктура.

Здравствената способност од ставот 2 точка 3 на овој член се докажува со потврда издадена од надлежната здравствена установа, согласно со закон.

Уверението од ставот 3 на овој член содржи оцена за здравствената способност на лицето за заштита на критичната инфраструктура и не смее да содржи информации за неговата здравствена состојба.

Операторите со критична инфраструктура се должни најдоцна во рок од 15 дена од денот на именувањето на координаторот, податоци за координаторот да доставуваат до Министерството, како и за секоја промена на овие податоци да го известат Министерството во рок од пет дена од денот на промената.

Работи на координаторот

член 19

Координатор:

1) ги следи прописите и меѓународните договори од областа на заштитата на критичната инфраструктура;

2) го следи спроведувањето и ревизијата на безбедносниот план, односно планот за заштита од членот 15 на овој закон;

3) посредува во комуникацијата меѓу операторот со критична инфраструктура и министерството одговорно за одреден сектор во однос на заштитата на критичната инфраструктура;

4) подготвува и спроведува обуки за вработените во операторите на критична инфраструктура за заштита на критичната инфраструктура и води евиденција за нивните обуки;

5) ги советува вработените во операторите на критична инфраструктура за заштита на критичната инфраструктура; и

6) врши други работи согласно со овој закон.

Обука и полагање на тековниот испит за заштита на критична инфраструктура

член 20

Обуката од член 18 став 2 точка 5 на овој закон ја врши организатор на образование за возрасни кој има лиценца издадена согласно со прописите со кои се уредува образованието на возрасните.

Обуката од член 18 став 2 точка 5 на овој закон се спроведува според образовната програма, согласно со прописите со кои се уредува образованието на возрасните.

Стручниот испит од членот 18 став 2 точка 6 на овој закон се полага пред комисијата за полагање на стручниот испит за заштита на критичната инфраструктура, формирана од министерот за внатрешни работи.

Министерството издава уверение за положен стручен испит за заштита на критична инфраструктура.

Членовите на комисијата за заштита на критичната инфраструктура имаат право на надоместок за својата работа, кој со решение го утврдува министерот за внатрешни работи, а кој се исплаќа од буџетот на Црна Гора.

Трошоците за полагање на стручниот испит за заштита на критична инфраструктура паѓаат на товар на операторот со критична инфраструктура, односно претпријатието, другото правно лице или претприемачот од членот 17 став 2 на овој закон.

Министерството ги пропишува програмата и начинот на полагање на стручниот испит за заштита на критична инфраструктура, составот на комисијата за полагање на стручниот испит за заштита на критична инфраструктура и висината на надоместокот за работата на таа комисија како и образецот за уверение од став 4 на овој член.

Координативно тело за заштита на критичната инфраструктура

член 21

Во случај на нарушување, односно оштетување или уништување на критичната инфраструктура, управувањето и координацијата на спроведувањето на мерките и активностите во согласност со овој закон ги презема координативен тим формиран во согласност со законот со кој се уредува заштитата и спасувањето.

Во работата на координативниот тим од ставот 1 на овој член, на покана може да учествуваат старешини и претставници на други органи на државната управа надлежни за одредени сектори од критичната инфраструктура, како и стручни лица од областа на заштитата на критичната инфраструктура.

Ракување со класифицирани информации и чувствителни информации

член 22

Операторите со критична инфраструктура, координаторите и другите субјекти, при извршувањето на нивните должности и при учеството во размената на податоци поврзани со

критичната инфраструктура, се должни да постапуваат со класифицирани информации поврзани со критичната инфраструктура во согласност со законот со кој се уредува тајноста на податоците.

Операторите со критична инфраструктура, координаторите и другите субјекти од ставот 1 на овој член се должни да користат чувствителни информации исклучиво заради заштита на критичната инфраструктура пропишана со овој закон.

Третман на лични податоци

член 23

Операторите на критична инфраструктура, координаторите и другите субјекти, при постапувањето со лични податоци поврзани со критична инфраструктура, се должни да постапуваат во согласност со законот со кој се уредува заштитата на личните податоци.

IV. ЕВРОПСКА КРИТИЧНА ИНФРАСТРУКТУРА

Утврдување на европската критична инфраструктура

член 24

Европската критична инфраструктура може да биде назначена во сектори идентификувани од Управата за заштита на критичната инфраструктура на Европската комисија.

Европската критична инфраструктура на територијата на Црна Гора ја утврдува Владата, на предлог на Министерството, а на барање и согласност на заинтересираните земји членки на Европската Унија.

Министерството ги информира заинтересираните земји членки на Европската Унија за утврдување на европската критична инфраструктура на територијата на Црна Гора.

Доколку нарушувањето, неисправноста, оштетувањето или уништувањето на критичната инфраструктура лоцирана на територијата на друга земја членка на ЕУ би имало значителни последици за Црна Гора, Министерството предлага утврдување на европската критична инфраструктура до телото на Европската комисија одговорно за заштита на критичната инфраструктура.

Заштита на европската критична инфраструктура

член 25

Европската критична инфраструктура на територијата на Црна Гора ќе биде заштитена во согласност со овој закон, освен ако поинаку не е пропишано со прописите на Европската Унија.

Известување за европска критична инфраструктура

член 26

Владата, на предлог на Министерството, го усвојува годишниот извештај за европската критична инфраструктура по сектори и бројот на заинтересирани земји погодени од одредена критична инфраструктура.

Извештајот од ставот 1 на овој член Министерството го доставува до органот на Европската комисија надлежен за заштита на критичната инфраструктура.

На секои две години, Владата на Црна Гора доставува до телото на Европската комисија одговорно за заштита на критичната инфраструктура преглед на податоци за видовите опасности, закани и слабости идентификувани во секој сектор во кој е утврдена европската критична инфраструктура во Црна Гора.

Извештајот од ставот 1 на овој член и податоците од ставот 3 на овој член се означуваат со соодветен степен на тајност, согласно со законот со кој се уредува тајноста на податоците.

Размена на информации за европската критична инфраструктура

член 27

Министерството е контакт-точка за размена на информации и координација на активностите поврзани со европската критична инфраструктура со другите земји членки и тела на Европската Унија.

Ракување со класифицирани информации и чувствителни информации

член 28

Операторите на европската критична инфраструктура, координаторите и другите субјекти од ставот 1 на овој член користат чувствителни информации поврзани со европската критична инфраструктура исклучиво заради заштита на европската критична инфраструктура.

Одредбите од ст. 1 и 2 на овој член се однесуваат и на непишани податоци разменети на состаноци во врска со заштитата на европската критична инфраструктура.

Третман на лични податоци

член 29

Операторите на Европската критична инфраструктура, координаторите и другите субјекти, кога се занимаваат со лични податоци поврзани со Европската критична инфраструктура, се должни да постапуваат во согласност со законот со кој се

уредува заштитата на личните податоци и меѓународните договори за размена на лични податоци.

V. ЕВИДЕНЦИИ

Евиденција која ја води Министерството

член 30

Министерството води евиденција за:

1) положен стручен испит за заштита на критична инфраструктура кој ги содржи следните податоци:

- реден број,

- име, презиме, единствен матичен број, пол, датум, место и земја на раѓање и живеалиште на лицето кое го положило стручниот испит,

- датум на полагање на стручниот испит,

- успех во полагањето на стручниот испит и

- број на уверение за положен стручен испит и датум на издавање;

2) одобренија за безбедносни планови, кои ги содржат следните информации:

- реден број,

- име, седиште и адреса на операторот на критична инфраструктура кој го изработил безбедносниот план,

- број и датум на одобрување на безбедносниот план,

- број на одобрен безбедносен план;

3) координатори, кои ги содржат следните информации:

- реден број,

- име и презиме на координаторот,

- име, седиште и адреса на операторот со критична инфраструктура назначен од координаторот,

- датум на именување на координаторот.

Евиденција која ја води операторот со критична инфраструктура

член 31

Операторот на критична инфраструктура води евиденција за:

1) критична инфраструктура, која ги содржи следните информации:

- реден број,

- број и имиња на системи, мрежи, објекти или нивни делови што претставуваат критична инфраструктура,

- места каде што се наоѓа критичната инфраструктура,

- информација дека операторот со критична инфраструктура не е должен да изготви безбедносен план во согласност со член 14 од овој закон;

2) безбедносни планови, односно планови за заштита од членот 15 на овој закон, кои ги содржат следните информации:

- реден број,

- датумот на испраќање на безбедносниот план до Министерството за одобрување и датумот на добивање одобрение;

- број на безбедносниот план, односно планот за заштита од членот 15 на овој закон;

- датумот на ревизијата на безбедносниот план, односно планот за заштита од членот 15 на овој закон;

3) координаторот, кој ги содржи следните информации:

- реден број,

- име, презиме, единствен матичен број, датум, место, земја на раѓање и престој на координаторот и

- датум на именување на координаторот.

Начин на водење евиденција

член 32

Евиденцијата од чл. 30 и 31 од овој закон се чуваат во писмена и електронска форма.

Тајните податоци внесени во евиденцијата од чл. 30 и 31 од овој закон се обработуваат и штитат во согласност со законот со кој се уредува тајноста на податоците, а личните податоци внесени во оваа евиденција се обработуваат во согласност со законот со кој се уредува заштитата на личните податоци.

VI. НАДЗОР

член 33

Надзор над спроведувањето на овој закон и прописите донесени врз основа на овој закон врши Министерството.

Инспекциски надзор, во согласност со овој закон и законот со кој се уредува инспекцискиот надзор, врши инспекторот за заштита на критична инфраструктура.

VII. КАЗНЕНИ ОДРЕДБИ

член 34

Глоба во износ од 2.000 до 15.000 евра ќе му се изрече на правно лице доколку:

1) најмалку еднаш годишно не доставува до министерството надлежно за одреден сектор на критична инфраструктура информации за статусот или промените во системите, мрежите, објектите или делови од нив што се користат или управуваат, а кои се означени како критична инфраструктура (член 12 став 1);

2) не изготви безбедносен план и не добие согласност од Министерството за тој безбедносен план во рок од една година од донесувањето на актот од членот 11 став 3 на овој закон (член 14 став 1);

3) не постапи во согласност со упатствата или препораките од член 16 ст. 2 и 4 од овој закон во рок од 90 дена (член 16 став 5);

4) еднаш во пет години, односно во случај на промена на околностите во функционирањето на системите, мрежите, објектите или нивните делови што ги користи или управува, а кои се означени како критична инфраструктура, не го ревидира безбедносниот план или план за заштита од член 15 на овој закон (член 16 став 6);

5) не определи координатор од редот на вработените во рок од шест месеци од денот на донесувањето на актот од членот 11 став 3 на овој закон, кои системи, мрежи, објекти или нивни делови ги користат или управуваат се означени како критична инфраструктура (член 18 став 1);

6) вработи лице кое не ги исполнува условите за координатор согласно со овој закон (член 18 став 2);

7) не достави податоци за координаторот до Министерството најдоцна во рок од 15 дена од денот на назначувањето на

координаторот и не го извести за каква било промена на тие податоци во рок од 5 дена од денот на промената (член 18 став 5);

8) не користи чувствителни информации исклучиво заради заштита на критичната инфраструктура пропишана со овој закон (член 22 став 2).

За прекршокот од ставот 1 на овој член ќе се казни и одговорното лице во правното лице во износ од 200 до 1000 евра.

член 35

Глоба од 200 до 1.000 евра ќе му се изрече за прекршок на одговорното лице во надлежниот државен орган, органот на државната управа, органот на локалната самоуправа, органот на локалната самоуправа, ако:

1) најмалку еднаш годишно не доставува до министерството надлежно за одреден сектор на критична инфраструктура информации за статусот или промените во системите, мрежите, објектите или делови од нив што се користат или управуваат, а кои се означени како критична инфраструктура (член 12 став 1);

2) не изготви безбедносен план и не добие согласност од Министерството за тој безбедносен план во рок од една година од денот на донесувањето на актот од членот 11 став 3 на овој закон (член 14 став 1);

3) не постапи во согласност со упатствата или препораките од член 16 ст. 2 и 4 од овој закон во рок од 90 дена (член 16 став 5);

4) еднаш во пет години, односно во случај на промена на околностите во функционирањето на системите, мрежите, објектите или нивните делови што ги користи или управува, а кои се означени како критична инфраструктура, не го ревидира безбедносниот план или планот за заштита од член 15 на овој закон (член 16 став 6);

5) не определи координатор од редот на вработените во рок од шест месеци од денот на донесувањето на актот од членот 11 став 3 на овој закон, кои системи, мрежи, објекти или нивни делови ги користат или управуваат се означени како критична инфраструктура (член 18 став 1);

6) вработи лице кое не ги исполнува условите за координатор во согласност со овој закон (член 18 став 2);

7) не достави податоци за координаторот до Министерството најдоцна во рок од 15 дена од денот на назначувањето на координаторот и не го извести за каква било промена на тие податоци во рок од 5 дена од денот на промената (член 18 став 5);

8) не користи чувствителни информации исклучиво заради заштита на критичната инфраструктура пропишана со овој закон (член 22 став 2).

VIII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Рок за донесување на подзаконски акти

член 36

Прописите за спроведување на овој закон ќе се донесат во рок од една година од денот на влегувањето во сила на овој закон.

член 37

Операторите со критична инфраструктура се должни известувањата од членот 10 став 2 на овој закон да ги достават до министерствата надлежни за одделни сектори во рок од шест месеци од донесувањето на актот од членот 7 став 3 на овој закон.

Примена на одредбите за европската критична инфраструктура

член 38

Одредбите од Глава IV на овој закон ќе се применува од датумот на пристапување на Црна Гора во Европската Унија.

Влегување во сила

член 39

Овој закон влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Црна Гора“.

ЛИТЕРАТУРА

1. Amadio Viceré, M.G., Frontini, A. (2020). Paths to Resilience: Examining EU and NATO Responses to the Tunisian and Egyptian Political Transitions. In: Cusumano, E., Hofmaier, S. (eds) Projecting Resilience Across the Mediterranean. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-23641-0_13;
2. Antinori, A. (2019). Terrorism and DeepFake: From hybrid warfare to post-truth warfare in a hybrid world. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics. Academic Conferences and publishing limited;
3. Babos T. (2016). The First Critical Infrastructure Protection Research Project in Hungary. In: L. Nádai and J. Padányi (eds.), Critical Infrastructure Protection Research, Topics in Intelligent Engineering and Informatics 12, Springer International Publishing Switzerland;
4. Bajarūnas, E., (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. European View 2020, Vol. 19(1) 62–70;
5. Birchall, S. J., & Bonnett, N. (2021). Climate change adaptation policy and practice: The role of agents, institutions and systems. Cities, 108, 103001;
6. Bognă B. (2009). The process of critical infrastructure protection, AARMS, Budapest, Hungary.
7. Briggs, C. M. (2020). Climate Change and Hybrid Warfare Strategies. Journal of Strategic Security, 13(4), 45–57. https://www.jstor.org/stable/26965517;

8. Brzezinski, Z. (2012). Strategic Vision: America and the Crisis of Global Power. New York: Basic Books;
9. Buchanan, B. (2020). The hacker and the state: cyber attacks and the new normal of geopolitics. Cambridge, Massachusetts: Harvard University Press;
10. Čemerin, D., (2011). Upravljanje kritičnim infrastrukturama, Zbornik radova IV međunarodne konferencije „Crisis Management Days", Veleučilište Velika Gorica, p.442., Croatia;
11. Chasin M. R., Loeb J. M., (2013). High-reliability health care:getting there from here, PubMed.gov;
12. Cîrdei, I. A. (2018). Improving the level of critical infrastructure protection by developing resilience. Land forces academy review, 23(4), 237-243;
13. COM/2004/702 final. (2004) Critical Infrastructure Protection in the fight against terrorism. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN;
14. COM/2020/829 final. (2020). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A829%3AFIN;
15. De Haas M., (2010) Russia's Foreign Security Policy in the 21st Century Putin, Medvedev and beyond. Routledge, London;
16. De Maio, G. (2020). NATO's Response to COVID-19: Lessons for Resilience and Readiness. Foreign Policy;
17. European Commision (2020). Proposal for a Directive on the resilience of critical entities. https://www.europeansources.info/record/proposal-for-a-directive-on-the-resilience-of-critical-entities/ (Accessed on 21.05.2022);
18. European Commision Comunication. (2012). THE EU APPROACH TO RESILIENCE: LEARNING FROM FOOD SECURITY CRISES. Brussels, 3.10.2012. COM (2012) 586

final. https://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf;

19. European Parlament (2021). European critical infrastructure: Revision of Directive 2008/114/ЕК. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)662604;

20. Evans, V.C., (2020). Future Warfare: Weaponizing Critical Infrastructure. Parameters 50, no. 2. doi:10.55540/0031-1723.1017;

21. Garg, Sh., Sushil., (2021). Determinants of deglobalization: A hierarchical model to explore their interrelations as a conduit to policy. Journal of Policy Modeling. Volume 43, Issue 2, March–April 2021, Pages 433-447. https://doi.org/10.1016/j.jpolmod.2021.01.001;

22. Hamilton, D. S. (2022). One Plus Four: What NATO's New Strategic Concept Should Say and How to Achieve It. Orbis, 66(1), 26-34;

23. Hoffman, F. G., (2007). Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, December 2007;

24. Hofmann, S. Z. (2021). 100 Resilient Cities program and the role of the Sendai framework and disaster risk reduction for resilient cities. Progress in Disaster Science, 11, 100189;

25. Hwang, W. J. (2021). How are drones being flown over the gray zone?. Defense & Security Analysis, 37(3), 328-34;

26. Hybrid CoE., (2022). Hybrid threats as a concept. Достапно на: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (пристапено на 06.05.2022);

27. Iglesias L. M., (2014). In: Geopolitical overview of conflicts 2014. Spanish Institute of Strategic Studies. Spanish Ministry of Defence;

28. Injac, O. (2022). The External Dimension of the European Union´s Critical Infrastructure- Protection Programme,

Edited by: Alekssandro Lazari&Robert Mikac, London: CRC Press Taylor&Francis Group Boca Ration;

29. Juncos E., A. (2017). Resilience as the new EU foreign policy paradigm: a pragmatist turn? European Security, 26:1, 1-18, DOI: 10.1080/09662839.2016.1247809;

30. Kaplan, R.D. (2010). Monsoon: The Indian Ocean and the Future of American Power. New York: Random House;

31. Keković Z., Ninković V., (2020). Towards a conceptualisation of resilience in security studies, Српска политичка мисао бр.1/2020;

32. Keković, Z. (2022). The External Dimension of the European Union´s Critical Infrastructure- Protection Programme, Edited by: Alekssandro Lazari&Robert Mikac, London: CRC Press Taylor&Francis Group Boca Ration;

33. Kendra, J. M., Clay, L. A., & Gill, K. B. (2017). Resilience and Disasters. Handbooks of Sociology and Social Research, 87–107. doi:10.1007/978-3-319-63254-4_5;

34. Koliou, M., van de Lindt, J. W., McAllister, T. P., Ellingwood, B. R., Dillard, M., & Cutler, H. (2018). State of the research in community resilience: progress and challenges. Sustainable and Resilient Infrastructure, 1–21. doi:10.1080/23789689.2017.1418547;

35. Kornprobst, M., Paul T. V., (2021). Globalization, deglobalization and the liberal international order. In: International Affairs, Volume 97, Issue 5, September 2021, Pages 1305–1316. https://doi.org/10.1093/ia/iiab120;

36. Kumar, N., Poonia, V., Gupta, B. B., & Goyal, M. K. (2021). A novel framework for risk assessment and resilience of critical infrastructure towards climate change. Technological Forecasting and Social Change, 165, 120532;

37. Kumar, S., Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. International

Journal of Advance Research in Computer Science and Management, 4(4), 2253-2257;

38. London Declaration - NATO (2019). https://www.nato.int/cps/en/natohq/official_texts_171584.htm;
39. Marjanović M. (2015). Critical Infrastructure Protection-role&rensponsibilities, Crisis Management Days, Croatia;
40. Mikac R., Cesarec I., Lars, R. (2018). Kritična infrastruktura-platforma uspješnog razvoja sigurnosti nacije, Zagreb: Naklada Jesenski i Turk;
41. Mikellidou, C. V., Shakou, L. M., Boustras, G., & Dimopoulos, C. (2018). Energy critical infrastructures at risk from climate change: A state of the art review. Safety Science, 110, 110-120;
42. Milanova, N. (2020). Institutional Resilience and Building Integrity in the Defense and Security Sector. Connections (18121098), 19(3);
43. Mileski, T., & Albrecht, E. (2021). European Union and China Relation: Strategic Partnership Through the Lens of Geopolitics and Geoeconomics. Contemporary Macedonian Defence. Vol. 21, No. 40, June 2021;
44. Mileski, T., (2015). Identifying the new Eurasian orientation in modern Russian geopolitical thought. EASTERN JOURNAL OF EUROPEAN STUDIES Volume 6, Issue 2, December 2015;
45. Mileski, T., Klimoska, K., (2021). "France's Geopolitical Vision for Europe and the Western Balkan: The Case of North Macedonia". The Review of International Affairs. Vol. LXXII, No.1181, January – April 2021 DOI: 10.18485/iipe_ria.2021.72.1181.2;
46. Milosavljević B., Vučinić D. (2021). The attitude towards the Critical infrastructure in the Republic Serbian, Vojno delo br.4/2021;
47. Mitrevska M. (2022). The External Dimension of the European Union´s Critical Infrastructure- Protection Programme,

Edited by: Alessandro Lazari & Robert Mikac, London: CRC Press Taylor&Francis Group Boca Ration;

48. Mitrevska, M., Mileski, T., Mikac, R. (2019). Critical infrastructure: concept and security challenges. Skopje: Friedrich Ebert Foundation;
49. Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: a systematic literature review. Energies, 14(6), 1571;
50. Mujević M., Korač S. (2020). Development of the concept of critical infrastructure protection in Montenegri-roads, experiences, role and responsibility, International Journal Knowledge, Vol.41.4;
51. Nađ I., Rukavina F., Raić M. (2015). Critical Infrastructure determinational and intersectorial criteria, Crisis Management Days, Croatia;
52. Najžer, B., (2020). The Hybrid Age: International Security in the Era of Hybrid Warfare. London: I.B. Tauris;
53. Nye, J.S. (2011). Future of Power. New York: Public Affairs.
54. Ogden, J. M., Greenberg, M. R., Jaffe, A. M., Busby, J., Blackburn, J., Copeland, C., Law, S., & Griffin, P. A. (2019). CLIMATE CHANGE IMPACTS ON CRITICAL U.S. ENERGY INFRASTRUCTURE. In Impact of Climate Risk on the Energy System: Examining the Financial, Security, and Technology Dimensions (pp. 32–43). Council on Foreign Relations. http://www.jstor.org/stable/resrep21839.6;
55. Olech, A. (2021). Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism. Institute of New Europe;
56. Pavić M., Jokanović I. (2021). Legislation on critical infrastructure in the Republic of Serbia, the region and the European Union, Journal of Faculty of Civil engineering 39;
57. Petrakos, N., Kotzanikolaou, P. (2019). Methodologies and Strategies for Critical Infrastructure Protection. In Critical

Infrastructure Security and Resilience (pp. 17-33). Springer, Cham;

58. Pledger, T. (2021). The Role of Drones in Future Terrorist Attacks. Associsation of the United States Army;
59. Prague Summit Declaration (2002). https://www.nato.int/cps/en/natohq/official_texts_19552.htm;
60. Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? International journal of disaster risk reduction, 27, 632-641;
61. Rhodes, M. Lozancic, D. (2010). A balanced view of the Balkans. Journal of European Security and Defense Issues Domestic Security Volume 1, Number 2 June 2010, p.p. 27-32;
62. Riegl, M., (2013). Introduction: Geopolitical and Geostrategic Threats of the Contemporary World. In: Strategic and Geopolitical Issues in the Contemporary World. Newcastle: Cambridge Scholars Publishing;
63. Riegl, M., Landovský, J., (eds.) (2013). Strategic and Geopolitical Issues in the Contemporary World. Newcastle: Cambridge Scholars Publishing;
64. Roberts, K.H. (1990). Some characteristics of higheliability organizations, Organization Science, I, 160-177;
65. Škero M., Alejević V. (2015). Zaštita kritične infrastructure I osnovni elementi uskladivanja sa Direktivom Saveta Evrope 2008/114/EK, Vojno delo br.3;
66. Steingartner, W., Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18(3), 25-45;
67. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. p.p 11-17. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (пристапено на 16.05.2022);

68. Strengthened Resilience Commitment. (2021) available on https://www.nato.int/cps/en/natohq/official_texts_185340.htm;

69. Tanter R, Psarouthakis J. (1999). Balancing in the Balkans. New York: St. Martin's Press;

70. The Alliance's New Strategic Concept (1991). https://www.nato.int/cps/en/natohq/official_texts_23847.htm;

71. The Alliance's Strategic Concept (1999). https://www.nato.int/cps/en/natolive/official_texts_27433.htm;

72. The World Bank (2020). Population, total – Croatia. https://data.worldbank.org/country/croatia?view=chart;

73. The World Bank (2020). Population, total – Serbia. https://data.worldbank.org/indicator/SP.POP.TOTL?locations=RS;

74. The World Bank (2020). Population, total – Montenegro. https://data.worldbank.org/country/montenegro?view=chart;

75. Tomalska, A. (2022). Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic. Security and Defence Quarterly. https://doi.org/10.35467/sdq/146603;

76. Treverton, F. G., Thvedt, A., Chen, R., A., Lee, K., and McCue, M. (2018). Addressing Hybrid Threats. Swedish Defence University;

77. Tsygankov. P. A, (2003). "Mastering Space in Eurasia: Russia"s Geopolitical Thinking After the Soviet Break-Up," Communist and Post-Communist Studies 36, no. 1. p.109;

78. Veiga, F. (2003). Balkanska zamka (1804–2001), Naučna knjiga, Beograd;

79. Walker, B. (2020). Resilience: what it is and is not. Ecology and Society, 25(2);

80. Weick, K.E. (1990). The vulnerable system: An analysis of the Tenerife airdcaster, Journal of Management, 16/3;

81. А., К. (2020, 10. септември) Државата под хакерски напади: Владата, ДИК, општини и служби трпеле сајбер-удари. *Фактор*. https://faktor.mk/drzavata-pod-hakerski-napadi-vladata-dik-opshtini-i-sluzbi-trpele-sajber-udari;

82. Државен завод за статистика на РСМ. Попис 2021. https://popis2021.stat.gov.mk/#;

84. Дугин, А. (2004). Основи геополитике 1. Зрењанин: Екопрес.;

85. Килибарда, З. (2008). Основе геополитике. Београд: Универзитет у Београду – Факултет безбедности;

86. Милески, Т., (2011). Еколошка безбедност: одржлив развој – одржлива безбедност. Скопје: Филозофски факултет.

Закони и стратегии

ЦРНА ГОРА

1. Zakon o državnoj imovini, Službeni list Crne Gore, br.21/2009 i 40/2011;
2. Zakon o zaštite I spašavanju, Službeni list Crne Gore, br.13/2007, 5/2008 I 32/2011;
3. Metodologija izbora kritične informatičke infrastructure, Ministarstvo za informaciono društvo i telekomunikacije, 2014;
4. Strategija za sajber bezbednost Crna Gora (2018-2022), Vlada Crne Gore, Ministarstvo javne uprave, Podgorica, 2017 godina;
5. Strategija za nacionalne bezbjednosti Crna Gore, Službeni list Crne Gore, br.85/2018;
6. Zakon o zaštiti lica I imovine, Službeni list Crne Gore, br.43/2018;
7. Zakon o odbrani Crne Gore, Službeni list Crne Gore, br.046/2019;
8. Zakon o određivanju I zaštiti kritične infrastructure, Službeni list Crne Gore,br.72/2019 https://me.propis.net/zakon-o-određivanju-i-zaštiti-kritične-infrastrukture/;
9. Zakon o informacionoj bezbjednosti, Službeni list Crne Gore, br.67/2021.

ХРВАТСКА

1. Nacionalna Strategija za prevenciju i suzbijanje terorizma, Vlada Republike Hrvatske, 2008;
2. Croatian Parlament (2010), Private Protection Act, Official Gazette, number 68/2003, 31/2010, 139/2010;
3. Plan zaštite i spašavanja na području Republike Hrvatske, Vlada Republike Hrvatske, 2010;

4. Procjena rizika od katastrofa za Republike Hrvatske od prirodnih I tehničko-tehnoloških katastrofa I velikih nesreća, Republika Hrvatska, Državna uprava za zaštitu I spašavanje, 2013;
5. Zakon o kritičnim infrastrukturama, Republika Hrvatska, Narodne novine br.56/2013;
6. Nacionalna Strategija kibernetičke sigurnosti, Republika Hrvatska, 2015;
7. Nacionalna Strategija i Akcijski plan za suzbivanje širenja oružja za masovno uništenje, Vlada Republike Hrvatske, 2013;
8. Zakon o sustavu domovinske sigurnosti, Republike Hrvatske, Službeni list br.108/2017;
9. Stretegija za nacionalne sigurnosti, Republike Hrvatske, Službeni list br.73/2017;
10. Zakon o kibernetičkoj sigurnosti, Republike Hrvatske, Službeni list br.64/2018.

СЕВЕРНА МАКЕДОНИЈА

1. Национална концепција за безбедност и одбрана, Службен весник на Република Македонија, бр.42/2001, 5/2003;
2. Закон за заштита и спасување, Службен весник на Република Македонија, бр.34/2004;
3. Закон за управување со кризи, Служен весник на Република Македонија, Скопје, бр.29/2005;
4. Закон за одбрана, Служен весник на Република Македонија, бр.185/2011;
5. Закон за приватно обезбедување, Службен весник на Република Македонија, бр.166/2012;
6. Закон за внатрешни работи, Служен весник на Република Македонија, бр.42/2014;

7. Национална стратегија за сајбер безбедност на Република Македонија (2018-2022), МИОА, 16.07.2018;
8. Национална стратегија за борба против тероризам БПТ, (2018). https://www.vlada.mk/node/14499;
9. Стратегија за одбрана на Република Северна Македонија, Службен Весник на Република Северна Македонија, бр.75/2020;
10. Стратегија за градење отпорност и справување со хибридни закани, Влада на Република Северна Македонија, април/ 2021. Стратегиски одбранбен преглед (2018). https://www.mod.gov.mk/inc/uploads/2021/06/%D0%A1%D0%9E%D0%9F-%D0%BC%D0%BA%D0%B4-%D0%B2%D0%B5%D1%80%D0%B7%D0%B8%D1%98%D0%B0-05-07-2018.pdf.

СРБИЈА

1. Zakon o zaštiti životne sredine,, Sl. Glasnik Republike Srbije, бр.135/2004;
2. Zakon o planiranju i izgradnji, Službeni list Republike Srbije, br.72/2009 I 81/2009;
3. Zakon o tajnosti podataka, Sl. Glasnik Republike Srbije, бр.104/2009;
4. Zakon o vodama, Sl. Glasnik Republike Srbije, бр.30/2010;
5. Uredba o sadržaju i načinu izrade planova zaštite i spasavanja u vanrednim situacijama, Sl. Glasnik Republike Srbije, бр.8/2011;
6. Zakon o vanrednim situacijama, Službeni list Republike Srbije, br.111/2009, 92/2011 i 93/2012;
7. Национална стратегија заштите и спашавања у ванредним ситуацијама, Службени гласник Републике Србије бр.86/2011;
8. Zakon o privatnom obezbeqenju, Sl. Glasnik Republike Srbije, бр.104/2013, 42/2015 i 87/2018;

9. Zakon o smanjenju rizika od katastrofa I upravljanju vanrednim situaciljama, Službeni glasnik Republike Srbije br.87/2018;
10. Zakon za kritičnu infrastrukturu, Sl.Glasnik Republika Srbija, br.87/2018 godina;
11. Zakon o informacionoj bezbednosti, Službeni list Republike Srbije, br.6/2016, 94/2017 i 77/2019;
12. Uputstvo o metodologiji izgrade i sadržu procene rizika od katastrofa i plana zaštite i spasavanja, Službeni list Republike Srbije, br.80/2019.

ИНДЕКС

А

Б

В

Г

Д

Е

Ж

З

И

Ј

К

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Ч

Ш

ЗА АВТОРИТЕ

Д-р Марина Митревска е редовен професор на Филозофскиот факултет – Универзитет „Св. Кирил и Методиј“ во Скопје. На додипломски студии ги предава предметите Кризен менаџмент, Хумана безбедност, Превентивна дипломатија и мировни операции и Хуманитарни интервенции. Раководител е на трет циклус докторски студии на студиската програма Безбедност, одбрана и мир при Филозофскиот факултет во Скопје. Во периодот 2017–2021 година таа била член на Одборот за акредитација и евалуација на високото образование. Член е на Одборот за доделување на наградата „Гоце Делчев“. Во периодот 2020–2022 година таа била избрана за прв претседател на Одборот за евалуација на високото образование, орган на Агенцијата за квалитет на образование. Член е на Одборот за евалуација на високото образование. Главен и одговорен уредник е на меѓународното научно списание „Современа македонска одбрана“. Член е на меѓународен уредувачки одбор на списанијата: „Teorija in praksa“ кое го издава Факултетот за општествени науки во Љубљана, „European Journal of Human Security“, кое го издава Факултетот за безбедност во Белград и „Безбедност“ кое го издава Министерството за внатрешни работи. Предава на

втор циклус студии на Факултетот за криминалистика, криминологија и безбедност во Сараево. Д-р Митревска е автор на универзитетски учебници и монографии и до денес има издадено четиринаесет книги, од кои три коавторство за критична инфраструктура: Handbook on Critical Infrastructure protection (2017), Critical Infrastructure-concept and security challenges (2019), The External Dimension of the European Union's Critical Infrastructure (2022). Автор е на повеќе од сто научни труда, раководител и член на повеќе научноистражувачки проекти. Мајка е на Марија и сопруга на Митко.

E-mail: marinamitrevska@yahoo.com

Д-р Тони Милески е редовен професор и истражувач во областа на политичката географија и геополитика, еколошката безбедност, енергетската безбедност, заштитата на критичната инфраструктура и миграциите и конфликтите. Вработен е на Универзитетот „Св. Кирил и Методиј“, Филозофски факултет – Институт за безбедност, одбрана и мир. Професорот Милески учествувал во повеќе научни и истражувачки проекти. Во октомври 2012 година, бил дел од меѓународната програма за лидерство, организирана од Амбасадата на САД, Програма што се одржала во Вашингтон, Њујорк и Бостон, САД. Во два наврати бил координатор на проекти преку ДААД фондацијата и Брандербуршкиот технички универзитет од Котбус, Германија. Првиот пат, во рамки на „ДААД универзитетскиот дијалог со Македонија“ темата на проектот била „Climate Change and Security: a Global Issue in a Local Context“, додека за вториот проект темата се однесувала на „Transposition of the Acquis Communautaire in Macedonia – with a special focus on climate change policy, air pollution, security matters and risk management“. Проф. Милески учествувал како уредник во преводот на книгата „Дипломатија“ од Хенри Кисинџер во рамки на проектот „Врвови на светската

филозофија, историја и психологија со психоанализа“ финансиран од Министерство за култура на Р. Македонија.

Во периодот од 2012 до 2014 година бил главен и одговорен уредник на меѓународното научно списание „Безбедносни дијалози“. Во неговиот мандат списанието добива меѓународна репутација и индексации во повеќе престижни бази на списанија како што се EBSCO, DOAJ, European Reference Index for the Humanities (ERIH) и многу други. Исто така, проф. Милески е член на уредувачкиот одбор на италијанскиот серијал на книги „Глоболитикал“, како и на списанието „Современа македонска одбрана“, кое го издава Министерството за одбрана. Од 2022 година проф. Милески е член на Уредувачкиот одбор на меѓународното списание „Меѓународни проблеми“ кое го издава Институтот за меѓународна политика и економија од Белград, Република Србија. Во рамките на тој Институт, проф. Милески е заменик-претседател на меѓународниот советодавен одбор. Татко е на Јована и Матеа и сопруг на Јелена.

Тој е автор на седум книги, неколку поглавја во книги и повеќе од деведесет научни трудови.

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

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

351.78(497.7)

МИТРЕВСКА, Марина
Кон отпорност и заштита на критичната инфраструктура : студија на случај на Република Северна Македонија / Марина Митревска, Тони Милески.
- Скопје : Фондација “Фридрих Еберт” - канцеларија Скопје, 2022. - 250 стр. ; 25 см

За авторите: стр. 245-249. - Библиографија: стр. 225-237. - Регистар. - Содржи и: Прилози 1-3

ISBN 978-608-270-006-9

1. Милески, Тони [автор]
а) Критична инфраструктура -- Заштита -- Македонија

COBISS.MK-ID 58005765

Professor Emeritus Нано Ружин

Заштитата на критичните инфраструктури претставува стратешки влог на XXI век, тоа е и основниот аналитичко-синтетички и научен рефрен на двајцата автори, проф. д-р Марина Митревска и проф. д-р Тони Милески, во трудот „Кон отпорност и заштита на критичната инфраструктура: студија на случај на Република Северна Македонија“. Додадената вредност на трудот е што авторите на релевантен начин ги инкорпорираат отпорноста и заштитата на КИ како трансцедентални фази во материјата на безбедноста на КИ. Во општиот контекст, може да се заклучи дека се работи за квалитетен научноистражувачки труд, кој расветлува една помалку позната и занемарена проблематика која денес е во центарот на сите безбедносни предизивици. Затоа мора да им се одаде голем омаж и комплименти на професорите Митревска и Милески за овој извонредно значаен, корисен и научен труд.

Проф. д-р Никола Дујовски

Со задоволство може да се констатира дека предложената книга претставува значаен придонес во концептуалното дефинирање на потребата и можностите за изградба на корисен систем за заштита на критичната инфраструктура, кој ќе се темели на меѓународните и регионалните искуства и стандарди, но и кој ќе ги отслика реалните потреби и можности на Република Северна Македонија. Авторите успеваат на само ним својствен начин да ги доловат најзначајните сегменти кои можат да бидат од пресудно значење за развојот на професионален интегриран пристап во кој повеќе различни државни институции ќе работат заеднички, а во исполнување на потребите од дополнителна гаранција на заштитата и безбедноста на граѓаните. Со силно уверување дека ваквите текстови се основната претпоставка за квалитетен пристап во кој универзитетските професори со силно практично и теоретско искуство, даваат несебичен придонес за развој на државата, за развој на политиките во безбедноста, за развој на квалитетни решенија. Таквите решенија се несомнена поддршка на напорите на властите за исполнување на стандардите и критериумите за членство во ЕУ, како и за градење на системот во кој сме препознаени како достоинствен и доверлив партнер во НАТО.