РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
УНИВЕРЗИТЕТ „СВ.КИРИЛ И МЕТОДИЈ“ – СКОПЈЕ
ФИЛОЗОФСКИ ФАКУЛТЕТ - СКОПЈЕ
ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР
СТУДИСКА ПРОГРАМА БЕЗБЕДНОСТ



Заштита на критичната инфраструктура од асиметрични закани

Ментор: Изработила:

Проф. д-р Оливер Бакрески Марија Стефанова

Скопје, 2024 година

Апстракт

 Безбедноста како поим може да се дефинира на повеќе начини зависно од кое гледиште е набљудувана, но сигурно е дека истата е систем во кој се заштитува територијалниот интегритет на една држава и нејзиниот суверенитет. Кога една безбедна средина доаѓа во допир со закана или постои ризик од закани (надворешни / внатрешни) тогаш не можеме да зборуваме за безбеден систем.

 Овој магистерски труд ќе се фокусира врз анализирање на безбедноста како нужност на една држава, и како асиметричните закани влијаат врз критичната инфраструктура која е основна физичка и организациска структура на едно општество, а е истовремено важна за непречено функционирање на истото.

 Главни прашања на кои треба да даде одговор овој магистерски труд се следните:

Прво: Што е безбедноста и како се обезбедува истата?

Второ: Што се асиметричните закани и како тие влијаат врз безбедноста и критичната инфраструктура?

Трето: Како да се заштити критичната инфраструктура од асиметричните закани?

Клучни зборови: безбедност, асиметрични закани, критична инфраструктура

Abstract

Security as a term can be defined in several ways depending on which point of view it is observed, but it is certain that it is a system that protects the territorial integrity of a state and its sovereignty. When a secure environment comes into contact with a threat or there is a risk of threats (external/internal) then we cannot talk about a secure system.

This master's thesis will focus on analyzing security as a necessity of a state and how asymmetric threats affect the critical infrastructure that is the basic physical and organizational structure of a society, and is at the same time important for its smooth functioning.

The main questions that this master's thesis should answer are the following:

First: What is security and how is it provided?

Second: What are asymmetric threats and how do they affect security and critical infrastructure?

Third: How to protect critical infrastructure from asymmetric threats?

Keywords: security, asymmetric threats, critical infrastructure

Содржина:

[1.Вовед 6](#_Toc178166179)

[1.1 Предмет на истражување 6](#_Toc178166180)

[1.2 Досегашни истражувања 9](#_Toc178166181)

[1.3. Предмет на истражување 10](#_Toc178166182)

[1.4. Цели на истражувањето 14](#_Toc178166183)

[1.5. Хипотетичка рамка 15](#_Toc178166184)

[1.6. Методи на истржувањето 16](#_Toc178166185)

[2. Критична инфраструктура 18](#_Toc178166186)

[2.1. Дефинирање и значење на критичната инфраструктура 18](#_Toc178166187)

[2.2 Листа на сектори на критичната инфраструктура 21](#_Toc178166188)

[Енергетски сектор 21](#_Toc178166189)

[Информатички и комуникациски технологии 22](#_Toc178166190)

[Сообраќај и транспорт 24](#_Toc178166191)

[Водата како критичен ресурс 25](#_Toc178166192)

[Храната како критичен ресурс 27](#_Toc178166193)

[Финансиски и банкарски сектор 28](#_Toc178166194)

[Здравствен систем 30](#_Toc178166195)

[3. Закани и заштита на критичната инфраструктура 31](#_Toc178166196)

[3.1 Дефинирање на заканите и ризиците за критичната инфраструктура 31](#_Toc178166197)

[3.2Природните непогоди како закана за критичната инфраструктура 32](#_Toc178166198)

[3.3Хибридни закани по системите за критична инфраструктура 34](#_Toc178166199)

[3.4 Сајбер нападикако закана по критичната инфраструктура 35](#_Toc178166200)

[3.5 Електро енергетската инфраструктура, транспорт на нафта и природен гас како потенцијални ранливи сегменти 37](#_Toc178166201)

[4.Дефинирање и видови на асиметрични закани 39](#_Toc178166202)

[4.1 Тероризам – терминолошко определување на поимот тероризам 40](#_Toc178166203)

[4.2 Видови на тероризам 44](#_Toc178166204)

[4.3Фактори кои влијаат на појавата на тероризмот 47](#_Toc178166205)

* [4.4 Теорија на игра и проценка на ризик од тероризам во критичната инфраструктура 49](#_Toc178166206)
* [4.5 Импликциите на тероризмот врз критичната инфраструктура 52](#_Toc178166207)

[5. Огранизиран криминал 55](#_Toc178166208)

[5.1.Дефинирање на поимот организиран криминал и облици на организиран криминал 55](#_Toc178166209)

[5.2. Фактори кои ги олеснуваат активностите на организираниот криминал 60](#_Toc178166210)

[6. Заштита на критичната инфраструктура од асиметрични закани 64](#_Toc178166211)

* [6.1 Импликациитена организираниот криминал врз критичната инфраструктура 68](#_Toc178166212)

[7. Заштита и пристапот на Република Северна Македонија во однос на критичната инфраструктура 76](#_Toc178166213)

[7.1. Креирање на ефикасна стратегија на енергетско – критичната инфраструктура на Република С. Македонија 82](#_Toc178166214)

[7.2. Законодавно и нормативно регулирање на безбедноста во Република Северна Македонија и пристапот кон асиметричните закани 84](#_Toc178166215)

[ЗАКЛУЧОК: 87](#_Toc178166216)

[Библиографија: 91](#_Toc178166217)

* [Интернет страници 97](#_Toc178166218)

### 1. Вовед

### 1.1. Предмет на истражување

Критичната инфраструктура како витална, комплексна и меѓусебно структурно поврзана целина е од исклучителна важност и значење за непреченото функционирање на државата. Таа е јасна дијалектика и синергија што ги поврзува индустрискиот сектор, комуникациските системи, енергетскиот сектор и другите сектори, системи и мрежи што се од големо значење за државата, бидејќи со неа се обезбедува потребната стабилност. Оттука нарушувањето или прекинот на работата на одредени сектори / системи може да доведе до сериозни последици што може да имаат и ослабувачки ефект врз безбедноста на државата, на националната економија, на економскиот развој и просперитет, на стабилниот енергетски сектор, односно нарушувањето или прекинот на работата на само еден од наведените сектори може да доведе до сериозни последици врз другите критични сектори.[[1]](#footnote-1)

Заштитата на критичната инфраструктура е есенцијален, односно суштински дел на националната безбедност на секоја држава, па оттука нејзината заштита е врвна цел и приоритет на секоја земја, особено ако се знае фактот дека општествените девијации (на пример: кражби, измами, индустриски шпиунажи, саботажи, диверзии, злонамерни оштетувања, и сл.), природните катастрофи, техничко-технолошките несреќи, човечките пропусти итн., сите може да предизвикаат големи човечки загуби и материјални штети. Ако на овие елементи се надоврзат и одредени специфични облици на загрозување, во чии рамки спаѓа и употребата на современите оружја и напредните технологии, вклучувајќи го и нуклеарниот материјал, хемиските и биолошките оружја, и слично, сето тоа е јасен сигнал дека имаме сериозен безбедносен ризик кој надополнет со веројатноста таквото оружје да биде употребено во акти на незаконско постапување и врз критичната инфраструктура, ја наметнува потребата од создавање соодветни механизми за заштита на критичната инфраструктура.[[2]](#footnote-2)

Според квалитетот и дијапазонот на тематско-проблемската елаборација на истражувачкиот проблем, заштитата на критичната инфраструктура од асиметрични закани во рамките на магистерскиот труд ќе се разгледува низ неколку сегменти. Прво, сегментот на прашања ќе се разгледува низ призмата на општите теоретски претпоставки поврзани со концептот на критичната инфраструктура. Второ, магистерскиот труд треба да одговори на прашањата „Со кои закани се соочува критичната инфраструктура?“ и „Дали потенцијалните закани по критичната инфраструктура можат да доведат до сериозни нарушувања?”. Третиот пристап се базира врз механизмите за заштита на критичната инфраструктура. На заштита на критичната инфраструктура се гледа како на преземање на потребните мерки за заштита со кои треба да се осигура подготвеноста на сите субјекти кои се вклучени во заштитата да манифестираат висока подготвеност и да ги стават на располагање сите ресурси кои им стојат на располагање за да се постигнат потребните приоритетни цели.

Во тој контекст, централните прашања за кои треба да се даде потребниот одговор се однесуваат на:

1. Зошто е значајна критичната инфраструктура за државата? и Дали државите градат соодветни стратегии за заштита на критичната инфраструктура? Анализите покажуваат дека критичната инфраструктура ги опфаќа секторите кои се витални за остварување на базичните операции во државата како што е уогата на енергетскиот сектор, транспортниот сектор, здраствениот сектор, итн.
2. Како ќе се манифестира одреден проблем во некој од секторите во ситуации кога ќе се случи дефект или крах на критичната инфраструктура? Кога настанува колапс на секторот се поставува прашањето како тој влијае врз останатите сектори.
3. Што презема државата за да ја заштити критичната инфраструктура, особено при изложеност на асиметрични закани? Важно е и прашањето за давање на заеднички синхронизиран одговор на сите субјекти кои што се вклучени во заштитата што во основа се врзува и за брзото опоравување и обновување.
4. Дали владината поддршка е клучна или подготвеноста на населението за соочување со потенцијалните закани е особено важно прашање, особено кога асиметричните закани се доживуваат како „употреба на иновативни стратегии, тактики и технологии од страна на послаба држава или недржавен противник, наменети за да се избегне моќта на посилните и да се искористи потенцијалната ранливост на поголем и технолошки посупериорен противник.[[3]](#footnote-3) Ова вклучува: селективна упортеба на оружје или воени средства од државна или недржавна група, што ќе се спротивстави, ќе се одврати или можеби ќе се порази, бројно и технолошко супериорна сила, како и користење на дипломатски и други невоени средства и тактики, со цел моќните воени сили да се обесхрабрат или да се ограничат во водење на воени операции.

### 1.2. Досегашни истражувања

Критичната инфраструктура била предмет на повеќе истражувања**.** Денес, во повеќе земји помалку или повеќе се дискутира за критичната инфраструктура, за нејзиниот развој и за нејзиното значење за општеството и државата. Оваа дискусија е поочигледна кога повеќе од јасно е дека најголем дел од инфраструктурните објекти се во раце на приватниот бизнис сектор. Во вакви околности се наметнува прашањето што е пресудно кај сопствениците: трката по профит или како да се оствари поголема заштита на критичната инфраструктура.

Се смета дека ова прашање можеби е секогаш на маргините. Оттука, таму каде безбедноста се зема предвид, тоа се прави или врз основа на постфестум дејствување или, пак, врз основа на изолиран напор, а не на мрежен и координиран пристап.[[4]](#footnote-4)

Анализата на странската литература укажува на тоа дека бројни автори посветиле многу внимание на овој сегмент прашања. И во случајот со Република Македонија може да се каже дека направен е еден сериозен исчекор на ова прашање. Во неколку студии и монографии со поддршка на Комората за приватно обезбедување и на други фондации, даден е определен придонес во расветлување на прашањата поврзани со критичната инфраструктура. Оттука се смета дека се дадени базичните теоретски претпоставки, но сепак од анализата на целокупната литаратура може да се согледа дека недостасуваат емпириски истражувања што секако дека сами по себе ќе ги согледаат и анализираат повеќето аспекти особено на вработените во овој сектор.

Резултатите од истражувањето треба да ја потврдат оправданоста и фактот дека асиметричните закани оставаат силни влијанија врз инфраструктурата и нејзините сектори во државата и ја нарушуваат безбедносната состојба на општеството во целина. Истовремено самиот резултат и заклучок од целата анализа треба да резултира со имплементирање на излезни решенија во услови на нарушување на безбедноста и заштита на критичната инфраструктура како резултат на асиметричните закани.

### **1.3. Предмет на истражување**

Критичната инфраструктура претставува значаен сегмент во заштитата на основните столбови на човековото дејствување и живот. Критичната инфраструктура претставува средство или систем, кој суштински придонесува за одржување на виталните општествени функции. Оштетувањето на критичната инфраструктура, уништувањето или прекинот на функционирањето на овие системи, предизвикано од природни катастрофи, малициозно однесување, криминални активности и тероризам, може да предизвика значајни последици по безбедноста на луѓето, општествата и меѓународниот поредок.[[5]](#footnote-5) Оттука, предмет на истражување на магистерскиот труд со наслов „Заштита на критичната инфраструктура од асиметрични закани“, е да се согледа нивото на подготвеност на државните и недржавните актери во заштита на критичнните инфраструктурни објекти од разни криминални активности и закани од тероризам. Ако на овие елементи се надоврзат и одредени специфични облици на загрозување, како што се употребата на современите оружја и напредните технологии, итн., сето тоа говори дека е сè поприсутна веројатноста за употреба на одредени форми во акти на незаконско постапување и врз критичната инфраструктура. Од друга страна ова е јасен сигнал дека државата мора да гради соодветни механизми и капацитети за заштита на критичната инфраструктура.

Во рамките на магистерскиот труд поимовно и категоријалното определување се однесува на следните клучни поими: безбедност, инфраструктура, критична инфраструктура, асиметрични закани, тероризам, организиран криминал, заштита на критична инфраструктура.

* **Безбедност** – безбедноста е состојба во која е осигуран урамнотежениот физички, духовен, душевен и материјален опстанок на поединецот и на општествената заедница во однос на другите поединци, општествени заедници и природата, или безбедноста во суштина претставува иманентен структурален дел на општеството што во себе вклучува определена состојба, односно определени особини на состојбата, а исто така и дејност, односно систем.[[6]](#footnote-6) Исто така, безбедност се дефинира и како „правно уредување и обезбедување на општествените односи и унапредување на состојбата во државата, што овозможува ефективна заштитеност на државата и на граѓаните кои во неа живеат од сите (надворешни и внатрешни) противправни акти (активности) со кои се загрозува уставниот поредок, суверенитетот, независноста и територијалниот интегритет на државата, работата на државните органи, извршување на стопанските и општествените дејности и остварување на слободата, правата и должностите на човекот и граѓанинот.“[[7]](#footnote-7)
* **Инфраструктурата** претставува основна физичка и организациска структура што му е потребна на едно општество, животна средина, организација или институција непречено да функционира во сопствените рамки.“ Исто така, инфраструктурата е множество на меѓусебно структурно поврзани елементи што обезбедуваат поддршка за целокупното функционирање на една средина.[[8]](#footnote-8)
* **Критична инфраструктура** е суштински важна за непречено функционирање на општеството. Во овој контекст, Европската Унија критичната инфраструктура ја дефинира преку директивата 2008/114/ЕС каде истата е дефинирана како: „средство, систем или дел од него лоциран во земјите членки што е од суштинско значење за одрување на виталните општествени функции, здравјето, безбедноста, економската или социјалната благосостојба на луѓето чие нарушување или уништување би имало значително влијание во земјата членка како резултат на неуспехот да се оддржат тие функции“. Директивата посебно ја препознава европската критична инфраструктура, како критична инфраструктура чие нарушување или уништување би имало трансгранични ефекти во земјите членки, и која треба како таква да биде издвоена преку заедничка процедура. Во Талинскиот прирачник, под критична инфраструктура се подразбираат физички или виритуелни средства и средства што се во јурисдикција на државата и се толку витални што нивно оневозможување или уништување може да ги ослабне националната безбедност, економијата, јавното здравство и безбедноста или животната средина.[[9]](#footnote-9)
* **Асирметрични закани** – нов термин кој се користи за опишување на оружје и тактики кои се користени од страна на релативно слабите непријатели заради заобиколување на технолошката доминација на западните нации,[[10]](#footnote-10) или терминот се користи за опишување на нападите на кои државата како институција нема адекватна одбрана и чии тактики се специфични по форма и се со изразени цели.[[11]](#footnote-11)
* **Тероризам –** тероризмот е безбедносна закана. Токму затоа сите современи држави во рамките на безбедносните стратегии, заштитата од тероризам им е главен приоритет. Секоја држава води безбедносна политика и изготвува безбедносна стратегија која содржи конкретни мерки и активности за спротивставување на овој феномен.[[12]](#footnote-12) Европската Унија се обиде да даде дефиниција на тероризмот, и таа засега е прифатена од земјите членки во кои е нагласено дека терористичкото дело преставува намерен акт во кое по својата природа и содржина сериозно загрозува одредена земја или пак дури и меѓународната организација преку заплашување на популацијата, нелегално присилување на влада или пак организација, напад врз личен живот и интегритет, дестабилизирање на сите политички, уставни или социјални структури, киднапирање на заложници, уништување на јавни добра, институции и инфраструктура со цел да се загрози човечкиот живот или нанесе економска штета, потоа, киднапирање на луѓе во јавен транспорт (авиони, возови и слично), производство на оружје за масовно уништување и негова употреба, прекин на водоснабдување, енергија и слично, како и учеството во тие терористички групи, нивно финансирање и слично.[[13]](#footnote-13)
* **Организиран криминал –** е постојан криминален потфат кој што рационално врши профит од незаконски дејства и го оддржува своето незаконско постоење со употреба на сила, закани, монополска контрола или корумпирање на јавни службеници.[[14]](#footnote-14)
* Заштитата на критичната инфраструктура, подразбира сите добра, имот и физички и логички системи, неопходни за минимум изведба на економијата и на владата.[[15]](#footnote-15)

### 1.4. Цели на истражувањето

Истражувањето има за цел да даде објаснување на тоа како асиметричните закани влијаат врз критичната инфраструктура, и како истата да се заштити од нив.

Истражувањето има општа и посебни цели.

Општата цел на ова истражување е насочена кон добивање на теоретски и емпириски сознанија за критичната инфраструктура која е перманентно изложена на закани што е особено важна и комплексна тама за дискусија, а истовремено да се анализираат асиметричните закани и како тие влијаат врз виталната инфраструктура ако се земе предвид фактот за нивниот интензитет и разорноста.

Посебните цели се насочени кон:

1. Да се согледа местото и улогата на критичната инфраструктура во државата;
2. Да се објаснат активностите што ги преземаат субјектите кои што се задолжени во заштита на критичната инфраструктура;
3. Да се анализира на кои асиметрични закани може да биде изложена критичната инфраструктура,
4. Да се согледа кои механизми ѝ стојат на располагање на државата во заштита на критичната инфраструктура,
5. Да се види што е тоа што ги мотивира стопанствениците на инфраструктурни објекти повеќе пари или поголема безбедност,
6. Да се согледа дали субјектите на објектите од критичната инфраструктура работат според строгите законски регулативи и прописи во заштита на инфраструктурните објекти,
7. Да ce согледаат позитивните и негативните страни од ангажирањето на приватните

агенции за обезбедување во заштита на критичната инфраструктура;

1. Да се утврди кои закани ќе предизвикаат повеќе штета, и каква стратегија води државата да ја обезбеди потребната заштита.

### 1.5. Хипотетичка рамка

Врз основа на вака поставените цели на истражувањето, би ги поставиле следните општа и посебни хипотези:

Степенот на заштита на критичната инфраструктура од асиметрични закани зависи од подготвеноста и пристапот на државата кон остварување на потребното ниво на заштита на критичните инфраструктурни објекти. Покрај општата хипотеза ќе бидат определени и следните поединечни хипотези:

1. Инфраструктурата е клучната алка која придонесува кон нормално функционирање на едно општество, а „здравата“ инфраструктура придонесува за развој, опстанок и непречено функционирање на една држава.
2. Одговорот на потребните закани по критичната инфраструктура зависи од ефикасното функционирање на безбедносниот систем, а за да се оствари овој предизвик потребно е да се унапредуваат и континуирано да се надоградуваат механизмите кои треба да го дадат потребното зачувување на критичната инфраструктура.
3. Заштитата на критичната инфраструктура приднесува да се обезбеди потребната виталност на државата и остварување на потребната стабилност.
4. Постоењето на потребната законска регулатива, како и соодветни стратегии за заштита на критичната инфраструктура ќе влијаат врз обликување на потребната рамка за превенција и заштита.
5. Асиметричните закани директно влијаат врз инфраструктурата на една држава. Нивното рано откривање и превенција е клучно за обезбедување на безбедноста во државата, зачувување на критичната инфраструктура и граѓаните како составен дел на истата.

### 1.6. Методи на истржувањето

Со ова истражување ќе се пристапи согледување на определени состојби и тенденции во однос на заштита на критичната инфраструктура од асиметрични закани.

Од методолошка гледна точка, имајќи ги предвид целите, ова истражување има:

1. **Експликативен карактер *-*** теориско истражување кое се однесува на заштита на критичната инфраструктура од асиметрични закани што се насочени кон обезбедување специфични и широки интереси, наменети за унапредување на националните цели.
2. Д**ескриптивен карактер *-*** целта е да се даде поширок опис и дискрипција на критичната инфраструктура.
3. **Структурален карактер *-*** има за цел да го одреди составот на појавата и улогата на асиметричните закани врз националната безбедност.

Имајќи ја предвид комплексноста и повеќедимензионалноста на ова истражување, изборот на методите за анализа на добиените податоци ќе се врши според карактерот и целите на овој труд. За таа цел ќе биде применет **интегралниот** (квантитативно-квалитативниот и аналитичко-синтетичкиот) пристап, со утврден аналитички концепт за потврдување на веродостојноста на мисловната активност, кои ќе ја имаат носечката улога во анализата и презентирањето на проблемот. Исто така ќе бидат применети и историскиот метод, дескриптивниот метод, компаративниот метод, итн. Користејќи го историскиот метод, ќе се направи историска ретроспектива на појавата и развојот на критичната инфраструктура во македонската држава, а преку компаративниот метод се извршува делумна квалитативна и квантитативна селекција и анализа на прибраните податоци. Врз основа на добиениот теоретски материјал, може да се утврди степенот на варијабилноста на промените и состојбите што се истажуваат и да се утврди нивната детерминираност.

Во ова истажување ќе бидат користени секундарни извори на податоци, нормативни и правни акти, политички документи, договори, протоколи, заклучоци, итн. Значи а**нализа на содржината** ќе се применува за анализа на различни извори на литература (домашни и странски), анализа на законски документи и акти. Анализата, обработката на информациите и донесувањето на заклучоците од истражувањето ќе помогнат за подобро разбирање на оваа област, додека м**етодот на индукција и дедукција** ќе се применува за донесување на заклучоци за тоа кој вид на законска регулатива е најефикасен и најупотребуван за разбирање на оваа област.

По потреба ќе се спроведе и емпириско истражување со избрана целна група за добивање на релевантни податоци.

Во фазата на прибирање на податоци за анализа ќе се искористат истражувања кои се направени во изминатиот период за кои постои соодветна документација.

При фазата за анализа на податоците се обработуваат веќе добиените информации, нивна селекција, разгледување, анализирање, оценка и усвојувње дали податоците содржајно се однесуват на проблемот на истражувањето, и дали правилно ја изразуваат насоката на проблемот – појавата.

### 2. Критична инфраструктура

### 2.1. Дефинирање и значење на критичната инфраструктура

Критичната инфраструктура како поим историски гледано се појавува уште во списите на Римската Империја, Древна Кина, колонијална Шпанија преку Јужна Америка. Што значи самиот концепт на критична инфраструктура датира уште од времето на зачетокот на цивилизацијата која со растот и развојот на општеството како и техничко технолошкиот развој се надградува и се дефинираа пооделно во различни земји.

Она што е карактеристично и својствено за критичната инфраструктура главно означува и ја опфаќа целокупната инфраструктура на една држава. За да се дојде до конечната дефиниција за тоа што означува терминот критична инфраструктура, прво треба да се дефинира поимот инфраструктура. Според законот за просторно и урбанистичко планирање на С. Македонија, инфраструктурата се дефинира на следниот начин: „Инфраструктура се постојаните и планираните подземни и надземни инсталации и градби од областа на сообраќајот, електричните инсталации, гасоводи, водовод и канализација, топлификација, телекомуникации и други инсталации.“[[16]](#footnote-16) Со други зборови инфраструктурата е организациска целина составена од пооделни сектори кои меѓусебно се поврзани, а истовремено му се потребни на едно општество заради негово непречено функционирање. Меѓутоа гледано од поширок аспект како дел од инфраструктурата на една држава исто така се и банкарскиот и финансискиот сектор, јавното здравје, прехранбениот сектор, и сл.

Поимот критична инфраструктура е клучен за правилно разбирање на заштитата на критичната инфраструктура. Придавката критичен доаѓа од старогрчкиот јазик, а во современиот македонски јазик е преземена од англискиот јазик. Од повеќето значења на придавката критичен, за поимот критична инфраструктура од значење се две. Првото значење на критичен означува нешто што е суштинско, неопходно, животно важно (витално), а второто значење се однесува на нешто решавачко, судбинско, пресвртно или преломно.[[17]](#footnote-17)

Современите држави денес официјално го имаат дефинирано поимот критична инфраструктура. Така, Министерството за внатрешни работи на САД утврдило дека „националната критична инфраструктура обезбедува есенцијални услуги што претставуваат поткрепа за американското општество и служат како `рбет или столб на националната економија, безбедност и здравје. Американските граѓани ја препознаваат критичната инфраструктура како: електричната енергија што ја користат во домовите, водата што ја пијат, транспортот со кој се движат, продавниците во кои купуваат и комуникациските системи со кои контактираат со пријателите и со семејството.[[18]](#footnote-18)

Во Италија, критичната инфраструктура ги вбројува сите објекти, системи, мрежи и функции – физички или виртуелни, што се витални за опстанокот на државата, чија инкапацитација или уништување би имало ослабувачко влијание врз безбедноста, националната економска безбедност, јавното здравје и сигурност, или која било комбинација од овие појави.[[19]](#footnote-19)

Во основа, терминот критична инфраструктура е во широка употреба во владини, раководни и академски терминологии и литература, но во голема мера е дефиниран со илустрација и категоризација наместо според збир на карактеристики, што може да се изолира со цел анализа и предвидување.[[20]](#footnote-20)

Значи критичната инфраструктура како поим означува елемент, систем или дел од систем, лоциран во одредена држава, чии основни функции и значење се поддршка на виталните општествени функции, здравјето, безбедноста, економската и социјалната благосостојба, а чие нарушување или деструкција би имало огромни последици во самата држава, заради неможноста да се одржат тие функции. Со оглед на фактот дека инфраструктурните мрежи се меѓусебно зависни, заемно влијаат една врз друга и имаат комплексни врски, нарушувањето на нивното функционирање може да доведе до огромни материјални и човечки загуби во општествата, дури и да доведе до крах на системите.[[21]](#footnote-21)

### 2.2. Список на сектори на критичната инфраструктура

Отсекогаш општествата зависеле од широк спектар на услуги кои со текот на времето и напредокот на техничко технолошкиот развој нивната важност се зголемувала и станале критични. Тоа би значело дека станува збор за физички средства, организации или мрежи чие што нарушување ќе предизвика трајна штета на економскиот живот на една држава.

Секоја држава различно ги дефинира секторите на критичната инфраструктура, но европската комисија има идентификувано сектори кои се од витален интерес и тоа: енергија, информациски и комуникациски технологии, вода, храна, финансии, јавна и законска заштита, јавна администрација, транспорт, хемиска и нуклеарна индустрија, простор и истражување. [[22]](#footnote-22)

Во продолжение ќе се осврнеме на подробно анализирање на овие сектори кои се апострофирани како важни, а воедно и критични во сите индикативни списоци на критичната инфраструктура.

### Енергетски сектор

Енергетскиот сектор сам посебе е клучен сектор на критичната инфраструктура кој е база и врз кој се потпираат останатите сектори на критичната инфраструктура. Истовремено е и зависен од другите сектори на критичната инфраструктура како што се информатичките технологии, водата, храната, комуникациите и слично, паралелно на ова енергетскиот сектор е и под постојан притисок и ризик од закани и ризици од недостиг на работна сила која е неквалификувана.

Секторот за енергетика се состои од разновидни и географски дисперзирани критични средства и системи кои честопати се меѓусебно зависни. Поделен е на три меѓусебно поврзани сегменти и тоа: електрична енергија, нафта и природен гас. Енергетската критична инфраструктура може да биде во сопственост на државни, федерални, локални и приватни субјекти, како и на некои други корисници, како што се, на пример, големите индустриски и финансиски институции.[[23]](#footnote-23)

Државните, локалните и територијалните агенции се клучни чинители во обезбедувањето сигурна енергетска инфраструктура на национално ниво. Тие се одговорни за планирање и одговор при итни случаи, развивање на политики и практики за енергетска безбедност и доверливост, како и олеснување на активностите за заштита на енергетскиот сектор. Во услови на криза граѓаните им се обраќаат на овие организации кои ја имаат најзначајната улога во подготовката и одговорот за снабдување со електрична енергија, како и ублажувањето на влијанието врз овој сектор од вонредни ситуации. [[24]](#footnote-24)

Енергетскиот сектор се соочува со широк спектар на ризици кои се развиваат, и може да се развијат потешкотии при проценката поради високото ниво на несигурност, зачестеноста или фреквенцијата на ризикот. Некои од овие ризици вклучуваат сајбер и физички безбедносни закани, временски непогоди, стара инфрастуктура како и климатски промени. Критична е способноста на енергетската инфраструктура да се прилагоди на овие закани, особено по опоравување од катастрофи, бидејќи многу од секторите на критичната инфраструктура како што се болниците, водите и отпадните води, системите, транспортот и телекомуникациите зависат директно од снабдувањето со електрична енергија. Поради тоа актерите кои се дел од енергетскиот сектор преземаат иницијативи за справување со ваков вид на ризици. [[25]](#footnote-25)

### Информатички и комуникациски технологии

Влијанието и употребата на информатичката технологија во голема мера го олеснува начинот на функционирање на луѓето на глобално ниво. Напредокот на овој вид на технологии денес во 21 век на сите ни отвори нови хоризонти на живеење и дејствување во секојдневието. Со достапноста на електронските уреди и интернетот со еден клик се задоволуваат многу потреби на глобалното население, луѓето имаат полесен пристап до поголем проток на информации, а со тоа се намалува употребата и функцијата на медиумите како единствен канал за примање на информации. Меѓутоа лесно достапните информации не ретко се злоупотребуваат и сè почесто интернет просторот се користи како канал преку кој може, а и не мора да се пласираат лажни информации, што значи достапните информации на интернет просторот не може да се контролираат во голема мера.

Информатичко–комуникациските технологии (ИКТ) вклучуваат напредни телекомуникациски системи, интернет мрежи, мултимедијални услуги, медиуми и нови технологии за економија, компјутерски структури и системи, знаења, технологии за управување со системи и роботика. ИКТ всушност е термин за чадор кој ги опфаќа сите комуникациски уреди или апликации што вклучуваат: радио и телевизија, мобилен телефон, компјутер, мрежен софтвер и хардвер, сателитски системи, итн., како и разни услуги и сродни апликации, како што се видео конференција и учење од далечина. [[26]](#footnote-26)

Информатичките технологии покрај тоа што се канал за трансфер и употреба на информации, тие се и нужност во секојдневното функционирање. Несомнено е дека информатичките информации се навлезени длабоко во сите сфери на општеството, тие се двигател на еден нов свет.

Овде се поставува прашањето како и колкава е важноста и вклученоста на информациските технологии во безбедноста? Веќе утврдивме и потврдивме дека информациските технологии се од главно значење за непречено функционирање на општеството, меѓутоа многу важен дел е и безбедноста на секторите кои што се служат со овие алатки како што е јавното здравство, економијата, образованието, и сл, а најважно е заштита на граѓаните кои користат информациски технологии, а воедно се и зависници од истите. Во овој контекст важно е да се напомене дека заштитата на информациските технологии треба да биде во насока на обезбедување на интернет просторот, протокот на информации, заштита на интернетот, мрежите и мрежните системи, телекомуникациските мрежи и уреди, односно заштита на сите фактори кои се корисници на технолошките пронајдоци и сите канали преку кои секојдневно циркулираат најразлични информации.

Брзината на развојот на овој сектор и секојдневната употреба го прави ранлив и примамлив за напади, затоа за негова заштита е потребна поголема меѓуинституционална соработка и изнаоѓање на креативни начини за негова заштита.

Вреди да се спомене и дека глобалното вмрежување во системот на комуникациска и на информатичка технологија стана основа на организираниот криминал, додека пак, тероризмот доби уште една алатка во свои раце. Од аспект на употреба на интернетот во функција на организираниот криминал и тероризмот би се издвоиле планирањето на противправните дејствија, крадење на податоци или хакирање, предизвикување насилства, регрутација и радикализација на корисниците на овие мрежи, и сл. Во овој контекст нападот на информатичките системи, може да се дефинира како директна акција против мрежата или информатичкиот систем, со цел неовластено да се пресретне или прекине некоја операција, да се преземе контрола или да се уништи, промени или корумпира податокот (со меморирање или обработка) .[[27]](#footnote-27)

Следствено на сето ова е дека улогата на државата во заштитата на информациските и комуникациските техноголии е клучна, но исто така и операторите кои се посредници во продавањето на интернет услуги треба да се насочат кон заштита на интернет просторот од грабежи, можноста за лесно пробивање на системи преку инсталирање на малциозни софтвери кои дејствуваат директно врз податоците што циркулираат во интернет просторот, да се спречуваат можните хакерски напади на софтверските програми, сè со цел да се заштитат сите сектори кои користат информатички и комуникациски технологии, но со акцент и на граѓаните и нивните податоци што се достапни на интернет просторот.

### Сообраќај и транспорт

Сообраќајната инфраструктура го претставува јадрото на стопанската инфраструктура, односно таа е основа за движење на луѓето, на предметите, стоките и информациите без коишто не би можело да се замисли развојот на човештвото. [[28]](#footnote-28)

Сообраќајната инфраструктура ја сочинуваат како патиштата за сите видови сообраќај, така и објектите кои се изградени на одредено место и служат за регулирање на безбедноста во сообраќајот и производство на сообраќајни услуги. Од моментот на проектирањето, изградбата, експлоатирањето и инвестициското и тековното одржување на сообраќајната инфраструктура, таа во поголема или помала мера влијае врз оптимизацијата на сообраќајниот систем, а интензитетот на нејзиното влијание во одредени сообраќајни гранки значително е променлив.[[29]](#footnote-29)

Улогата на сообраќајот во стопанскиот развој на една земја е многу значајна. Сообраќајот и стопанскиот развој се во меѓузависна положба која директно е поврзана со економијата на една земја. Парафразирано, развиена сообраќајна мрежа води кон прогрес на стопанството, а со тоа појака и посилна економија. Добрата инфраструктурна мрежа ја олеснува размената на стоки и услуги, сè со цел задоволување на основните потреби за живот на човекот.

### Водата како критичен ресурс

Она што е ретко е скапо, а водата како најважна на светот, напротив нема цена[[30]](#footnote-30)

Според календарот на Обединетите Нации 22 март е Светски ден на водата. Водата е основата за постоењето на живот на планетата Земја, а чистата вода за пиење и за одржување на хигиена е неопходна за оддржување на животот и здравјето на целиот жив свет. Водата е во основата на одржливиот развој и е клучот за социо-економскиот развој, здравите екосистеми и за самиот опстанок на човекот. Тоа е од витално значење за намалување на глобалното оптоварување со болести и подобрување на здравјето, благосостојбата и продуктивноста на населението. [[31]](#footnote-31)

Секторот за вода и отпадни води е сложен сектор, кој е составен од вода за пиење, како и инфраструктура за одпадни води со различни големини и типови на сопственост. Владеачките органи ко се однесуваат на секторот за води и отпадни води, обезбедуваат јавно здравје, животна средина како и заштита и безбедносни мерки. Овој сектор има свои уникатни ризици, вклучувајќи закани, ранливости и последици кои ги поттикнуваат активностите за безбедност и отпорност на секторот. Партнерите на секторот за вода и отпадни води заедно со ЕПА (Environmental Protection Agency) државните агенции и други федерални агенции, учествуваат во мисијата за заштита на јавното здравје, животната средина и безбедноста, како и активности за отпорност. [[32]](#footnote-32)

Безбедната вода за пиење е клучна за животот на поединецот и општеството. Инцидент со контаминација на водата за пиење ќе има далекусежни здравствени, економски, еколошки како и психолошки влијанија врз целата нација. Други критични услужни дејности исто така би биле нарушени со прекин на услугите за снабдување со вода, како заштитата од пожари, здравствена заштита, процес на греење и ладење, што пак резултира со значителни последици за националните или регионалните економии. Државните и федералните влади долго време беа активни во насока на справување со овој вид на ризици и закани преку регулативи, техничка помош, истражување и програми за достапност. Како резултат на тоа, развиен е обемен систем на прописи што ги регулираат максималните нивоа на загадувачи, стандардите за изградба и работа (главно имплементирани од државните регулаторни агенции) мониторинг, планирање одговор при итни случаи, обука, истражување, образование за подобро обезбедување на нацијата со вода за пиење.[[33]](#footnote-33)

Синтагмата дека без вода нема живот е потврдена со фактот дека на целиот жив и нежив свет му е потребна вода. Таа е дар на природата и сите ние имаме право на тој подарок. Водата е општо добро што нема и не знае за граници и не смее да биде во приватна сопственост или да се тргува со неа. Но, денес, всушност, сме сведоци на тоа. Природата не ни наплаќа за водата што ни ја дава, така што продавањето на водата за профит го уништува природното право на дарот на природата и ги лишува сиромашните од нивното основно човеково право.[[34]](#footnote-34)

Земајќи ја важноста на фодата во секојдневното функционирање може да се каже дека водата е еден од важните фактори на критичната инфраструктура која е цел на напади, па така главна задача на државите е да обезбедат чиста и исправна вода за населението.

### Храната како критичен ресурс

Храната е супстанца која се внесува во организмот за да ги задоволи гладта и хранливите потреби на луѓето, исто така храната е супстанца која со апсорбција во организмот придонесува за зачувување на хомеостазата, и како таква значително влијае врз физичката, менталната и духовната состојба на луѓето. [[35]](#footnote-35)

Она што е многу важно во контекст на храната е каква храна всушност луѓето внесуваат во својот организам, дали храната која секојдневно ја консумираме е безбедна за консумација? Зошто храната треба да биде безбедна за употреба?

Според Максвел и Франкенбергер постојат околу триесет дефиниции за тоа што претставува безбедна храна. Во 1979 тодина, Извештајот на светската програма за храна ја концептуализира безбедноста на храната, изедначувајќи ја со состојбата за снабдување и балансирана понуда и побарувачка на храна на меѓународниот пазар. Извештајот исто така нагласува дека зголемувањето на продукцијата на храна, во земјите во развој треба да биде основната база врз која се гради безбедноста на храната. [[36]](#footnote-36)

Според универзалната декларација за искоренување на глад и неисхранетост (1974) сите мажи, жени и деца имаат неотуѓиво право да бидат ослободени од глад и неисхранетост. [[37]](#footnote-37)

Во 1996 година Светскиот самит за храна, во својот план за акција ја прифаќа следната дефиниција: „Безбедноста на храната, на индивидуално, семејно, национално, регионално и глобално ниво се постигнува кога сите луѓе, во секое време имаат физички и економски пристап до доволна, безбедна и хранлива храна за задоволување на потребите за исхрана кои ќе им обезбедат активен и здрав живот“[[38]](#footnote-38)

На глобално ниво безбедноста на храната претставува голем проблем, посебно луѓето во земјите во развој немаат првенствено доволно храна, додека пак во останатиот дел од светот посебно во земјите во транзиција луѓето страдаат од небезбедна храна. Сиромаштијата како неизоставен дел од секојдневието, исто така е главна причина поради која постои небезбедна храна. Од друга страна пак конфликтите, тероризмот и еколошките катастрофи за кои секојдневно се известува по медиумите, во голем процент придонесуваат за небезбедна храна.

### Финансиски и банкарски сектор

Финансискиот сектор е разновиден. Секоја финансиска институција има единствени потреби, ресурси и планови за безбедност и издржливост во зависност од функциите што ги извршува, и нејзиниот пристап кон управувањето со ризикот. Ефективното намалување на физичкиот и сајбер-безбедносниот ризик на секторот, бара заедничко разбирање на критичните услуги што ги обезбедува секторот, специфичните безбедносни и отпорни ризици со кои се соочува, и механизмите за соработка што се користат меѓу засегнатите страни во секторот за безбедност и отпорност.[[39]](#footnote-39)

Финансискиот сектор вклучува илјадници депозитни институции, даватели на инвестициски производи, осигурителни компании, други кредитни и финансиски организации и даватели на критичните финансиски услуги кои ги поддржуваат овие функции. Финансиските институции варираат во голема мера по големина и присуство, почнувајќи од некои од најголемите светски глобални компании со илјадници вработени и многу милијарди долари во средства, до заедницата на банки и кредитни унии со мал број вработени кои им служат на поединечните заедници. [[40]](#footnote-40)

Депозитните институции од сите видови се примарни даватели на услуги за плаќања на големо и мало, како што се жични трансфери, тековни сметки, кредитни и дебитни картички. Депозитните институции и нивните даватели на технолошки услуги го олеснуваат спроведувањето на трансакциите низ платежната инфраструктура, вклучувајќи електронски системи за пренос на големи вредности, автоматизирани клириншки куќи (ACH) и автоматизирани машини за плаќања (ATM). Овие интитуции се примарна точка на контакт со секторот за многу индивидуални клиенти. Дополнително, депозитните институции им обезбедуваат на клиентите различни форми на продолжување на кредитите, како што се хипотеки и заеми со капитал за домови, заеми со обезбедени и необезбедени кредитни линии, вклучително и кредитни картички. Потрошувачите имаат повеќе начини за пристап до овие услуги. На пример, клиентите можат лично да уплатат депозити во филијала на депозитната институција, преку интернет, на банкомат, преку пошта, преку директен депозит користејќи АСН, преку далечинско собирање депозити или на мобилни уреди. [[41]](#footnote-41) Финансиските институции се соочуваат со развој на динамичен збир на ризици, вклучувајќи оперативен, ликвидносен, кредитен, правен и репутациски ризик. ЅЅР конкретно се фокусира врз подгрупа на фактори на оперативен ризик против кои не може да се држи капитал, а кои вклучуваат управување со можноста за физички инцидент или инцидент од сајбер безбедноста што ги загрозува критичните системи. Овие организации го формираат столбот на финансискиот систем на нацијата, и се витална компонента на глобалната економија. Овие организации се поврзани заедно преку мрежа на електронски системи со безброј влезни точки. Инцидентот без разлика дали е вештачки или природен кој ќе влијае врз овие системи може да има штетни влијанија врз економијата. [[42]](#footnote-42)

Повеќето од клучните услуги на секторот се обезбедуваат или се спроведуваат на платформи за информатичка или комуникациска технологија, при што ја прави сајбер безбедноста особено важна за банкарскиот сектор. Злонамерните сајбер актери го таргетираат секторот за финансиски услуги и истите значително се разликуваат во однос на мотивацијата и способноста чиј потенцијал е нарушување на критичните системи, па дури и ненамерно. Покрај тоа, секторот се соочува со постојани ризици поврзани со природни катастрофи, како и со поренцијал за физички напади. Ураганите, торнадата, поплавите и терористичките напади имаат потенцијал да предизвикат физички пореметувања што имаат значително влијание врз операциите на Секторот за финансиски услуги. [[43]](#footnote-43)

### Здравствен систем

Здравствената заштита опфаќа систем на општествени и индивидуални мерки, активности и постапки за зачувување и унапредување на здравјето, спречување и рано откривање и сузбивање на болести, повреди и други нарушувања на здравјето предизвикани од влијанието на работната и животната средина, навремено и ефикасно лекување, здравствена нега и рехабилитација.[[44]](#footnote-44)

Значи здравствениот сектор е многу важна карика и исклучително важна компонента, и треба да биде предмет на заштита од државата за да се намали ранливоста на овој сектор од потенцијални влијанија и ризици. Оттука денес болници, клиники и други вакви установи, се слободно достапни капацитети поради природата на работењето, и од тој аспект идентификацијата на потенцијалните закани и пристап до одредени ресурси го прави овој сектор многу комплексен кога станува збор за обезбедувањето. Како сериозен проблем во анализата на опасностите и загрозувањата што го следат овој сектор, претставува и потребата од преземање мерки во однос на спречување на ширење епидемии, изолираност, па сè до дистрибуција на залихи, лекови, енергенси, и слично. Од безбедносна перспектива предизвиците со кои се соочува овој сектор се бројни. Така, здравствените установи имаат контрола за ограничен пристап на посетители на кои често им се издава дозвола за влез. Сепак тие, но и просториите за итна помош, често се предмет на насилство и закани од страна на агресивни пациенти, членови на семејства или насилни групи.[[45]](#footnote-45)

Здравствениот систем е еден од најкомплексните системи на секоја држава. Државите имаат обврска да се грижат за здравјето на сопственото население, со обезбедување на квалитетни здравствени услуги, изградена здравствена инфраструктура со достапност на услугите кои на секој човек му се со закон загарантирани. Проблемот на здравствениот систем од секогаш бил јавното здравство, неговата невозможност да одговори и да се носи со скапите и инвазивни методи на лечење и дијагностика на комплексни дијагнози кои се резултат на демографската состојба, епидемиолошкиот притисок и брзиот развој на медицината.

### 3. Закани и заштита на критичната инфраструктура

### 3.1. Дефинирање на заканите и ризиците за критичната инфраструктура

Идентификацијата и процената на ризиците по критичната инфраструктура е најважниот чекор во креирањето на успешна стратегија за подобрување на безбедноста и нивна заштита. Идентификацијата на ризик е процес на наоѓање, пропишување и карактеризирање на ризичните елементи во согласност со целите на управување или процена на ризикот. Неопходно е да се идентификуваат изворите на ризик, настаните или збир на околности, како и нивните потенцијални последици.[[46]](#footnote-46)

Во литературата не постои единствена дефиниција за тоа што претставува ризикот, па така според неколкумина автори, ризикот претставува ситуација во која постои можност од отстапување во однос на посакуваниот резултат[[47]](#footnote-47), други пак сметаат дека ризикот е мерка на веројатност и дека последиците штетни за животот, здравјето, сопственоста, и/или животната средина, може да се појават како резултат на некои одредени опасности.[[48]](#footnote-48)

Во рамките на литературата која се однесува на проблемот на конципирањето и истражувањето на современите безбедносни закани, тешко може да се раздвои значањето на термините закана (thread) и ризик (risk). И двата термини, денес доминираат во безбедносните агенди и политичките и експертските дебати. Приближувањето на двата концепти, може да се извлече од неколку генерални пристапи кои го третираат проблемот на постоење на опасност за опстанокот или за нормалното функционирање на одреден субјект. [[49]](#footnote-49)

Природата на заканите, односно нивните комплексни карактеристики, исто така, стануваат предмет на приоритетен интерес, за разлика од статистичката агенда во која заканите се дефинираат како последица на не/функционирањето на меѓународниот систем. И војната е синоним на заканата, односно на организирано насилство. Заканите сè повеќе се анализираат и се поврзуваат со различни форми на индиректно насилство, кое потоа може да ескалира и во различни форми на директно насилство.[[50]](#footnote-50)

Терминот закана (thread) се однесува на несакан, намерен или ненамерен настан, кој може да предизвика повреда врз одреден субјект. Заканата, најчесто, ја користи ранливоста на оној кон кого е насочена. Таа може да се дефинира како секоја перцепција на несигурност (секоја форма на опасност) и како ризик (можност од потенцијална повреда).[[51]](#footnote-51)

Според Ленард Сјоберг, заканата се однесува на опасност за која постои висока веројатност дека ќе се случи и ќе предизвика последици.[[52]](#footnote-52) Сјоберг ги изедначува термините закана и ризик, и ги сведува на ниво на синоними, забележувајќи дека овие два термина се различно поставени и употребени во природните и општествените науки. Затоа ризиците и заканите треба да бидат анализирани во насока на различните перцепции кај луѓето.

Системот на критичната инфраструктура е под постојана закана по неговата безбедност. Во продолжение на ова поглавје, подетално ќе ги елаборираме заканите и ризиците со кои се соочува критичната инфраструктура.

### 3.2. Природните непогоди како закана за критичната инфраструктура

Природните (елементарните) непогоди и катастрофи можат да се случат во секое време и во секоја држава, и можат да бидат со сериозни последици. Еклатантни примери за тоа се земјотресите кои имаат голема разорна моќ, големите поплави што можат да предизвикаат уништување на имот и на плодни земјишта и да нанесат човечки жртви, како и големи пожари предизвикани од запаливи агенси, и слично. Природните непогоди и масовните несреќи може да се класифицираат во различни групи според различни критериуми. Секоја од овие групи има свои карактеристики, и има свои специфичности. Овие специфики ја условуваат организацијата и начинот на работа во отстранување на последиците од одредени елементарни непогоди и масовни несреќи. Природните непогоди и елементарните несреќи од катастрофите се разликуваат по: интензитет, по причина на појавување, и по зафатеност на територијата.[[53]](#footnote-53)

**Природните непогоди** се предизвикани од природни појави како: земјотрес, поплава, ветрови, итн., и имаат голем потенцијал на разурнувачка моќ и на нивното формирање и појава не може да влијае човекот, односно не зависат од човечката волја, т.е степенот до кој човекот учествува во нивното создаање. Значи, на нивнта појава и развој човекот не може да влијае, но постојат неелементарни непогоди за кои е одговорен човекот и неговата работа, како што се пожари, експлозии, техничко-технолошките катастрофи, и сл.[[54]](#footnote-54)

**Загрозеност од земјотреси –** Џон Мишел, англиски физичар кој прв дал добар опис за потресите според кој „Земјотресите се бранови во движење поставени со движечки карпести маси“. Земјотрес или потрес е природна појава, којашто е резултат на поместувањето на тектонските плочи, движењето на земјината кора, при што се ослободува голема енергија што води до потресување на земјата. Јачината на потресот зависи од повеќе фактори, како што се количеството на ослободена енергија, длабочината на хипоцентарот, оддалеченоста од епицентарот и составот на земјината кора. Земјотресот се манифестира со потрес или дислокација на земјиното тло. Низ целата планета има околу 13.000 земјотреси годишно. За среќа не се сите подеднакво со иста сила. Повеќето земјотреси може да се почуствуваат само со многу чуствителни сеизмолошки апарати. Големите земјотреси се јавуваат отприлика околу 16 пати годишно, а многу посилните уште помалку. Земјотресите не настануваат само поради поместувањето на карпестата маса. Така може и удар на метеорит да предизвика земјотрес, исто и вулканската ерупција, па дури и експлозија на атомска бомба. Вулканите често ќе ги најдеме на линиите на поместување, на места каде Земјината кора е многу тенка, така што притисокот таму придонесува за распрснување, при што вулканот потиснат со притисок надвор исфрла: гасови, пепел или течна магма.[[55]](#footnote-55)

**Загрозеност од поплави,** терминот поплава значи природен или вештачки начин на поплавување на теренот со излевање на вода на несакано место. Со оглед на географските, геолошките и хидрграфските карактеристики на земјата, има многу можности за поплави. Причини за поплавите се: обилни врнежи од дожд и покачување на нивото на водата, непристапност на водните патишта, уништување на брани или оштетување на резервоари, прелевање на реки и езера, теренско лизгање, топење на снегот и земјотреси. [[56]](#footnote-56)

**Загрозеност од пожари –** Пожарот претставува неконтролиран процес на согорувања, чија појава (пламен, топлина и продуктите на согорувањето) често го загрозуваат животот на луѓето, и може да предизвика огромни материјални штети. Најчести пожари се: на зелени и шумски површини; на станбени, јавни, комерцијални и други објекти; на објекти, инсталации и складишта на опасни материјали; на инфраструктурни објекти, инсталации и уреди. Шумски пожар се јавува во неколку форми, и тоа: слаб / мал или приземен пожар, кој зафаќа запалив материјал на земја и ниска вегетација, додека голем пожар се развива од слаб пожар кој постепено преминува кон поголем интензитет, а со него често се загрозени сите видови шуми. Подземниот пожар е многу ретка појава и се шири многу бавно. Како резултат на можни пожари од големи или од мали размери, може да се појават одредени последици: по населението што живее и работи во околината, по чуварите и спасителите, по работените и по објекти и инфраструктура.[[57]](#footnote-57)

### 3.3. Хибридни закани по системите за критична инфраструктура

Современата безбедносна слика се карактеризира со комплексни закани кои суштински се изменети од пред две децении. Закани од напад со конвенционално оружје се малку веројатни, но паралелно е зголемена опасноста од напади со неконвенционални средства. Од таа причина потребно е да се прошири разбирањето и визијата за одбрана на општеството преку препознавање на современиот спектар на закани. Секое современо општество треба да изгради ефикасен концепт за справување со низа предизвици како што се тероризмот, насилниот екстремизам и радикализам, пролиферацијата на оружје, прекинот во снабдувањето со енергија, како и одбрана од сајбер и хибридни закани. Оттука, секоја земја треба да биде способна за приспособување кон непредвидливата, комплексната и променлива безбедносна реалност. [[58]](#footnote-58)

Заканите доаѓаат од државни и недржавни актери, кои сè повеќе користат механизми на мека моќ (политички, економски, информациски), за да ги ослабнат институциите, економиите и општествата, и да ја загрозат нивната безбедност. Земајќи го предвид фактот дека современите закани имаат комплексна содржина, се наметнува и потребата од одговор на целокупното општество. Тоа подразбира, градење на национални капацитети за унапредување на отпорноста кон овие закани преку поширок, поинтегриран и подобро координиран пристап на национално ниво. [[59]](#footnote-59)

Поимот „хибридна закана“ се однесува на комбинација од злонамерни и субверзивни активности, конвенционални и неконвенционални методи (дипломатски, воени, економски, технолошки), кои се употребени на координиран начин од државни или недржавни субјекти за постигнување на специфицирани цели. Овие дејства се координирани, синхронизирани и се насочени кон ранливостите, односно слабите страни на избраната цел. Тие можат да бидат насочени кон кој било домен од општеството – политички, економски, воен, цивилен или информациски / информативен. Притоа се користи широк спектар на средства, дизајнирани да останат недетектирани. Хибридните закани претставуваат комбинација од воени и невоени средства, вклучувајќи дезинформации, сајбер-напади, економски притисок, употреба и распределување на нерегуларни вооружени групи, како и употреба на регуларни воени сили. Интензитетот и брзината на хибридните закани постојано се менува, како и нивниот размер и брзина.[[60]](#footnote-60)

### 3.4. Сајбер напади како закана по критичната инфраструктура

Живееме во дигитален свет каде што личните податоци се најважни. Важно е да се разбере дека личните податоци се поранливи од било кога. Често слушаме за упади во податоци и сајбер закани кои влијаат врз милони корисници. Повеќето компании и институции се борат да ги заштитат своите податоци од хакерите и сајбер криминалците. Сајбер безбедноста не се однесува само на организациите, туку и на личните компјутери, мобилни телефони и таблет уреди. Сајбер закана или закана по сајбер безбедност е малициозна активност осмислена за крадење или оштетување на податоци, или нарушување на системот на еден поединец или на цела организација.[[61]](#footnote-61)

Комплексноста и сложеноста на проблематиката која ја третира безбедноста на критичната инфраструктура, директно се врзува со стратегиите на националната безбедност на голем број држави каде што се добива поширока витална димензија, вклучувајќи економски, стопански, политички и еколошки прашања. Националната безбедност повеќе не подразбира исклучиво воени стратегии, туку сè почесто се настојува да се елиминираат невоените загрозувања со воочување на реалната опасност и ефикасна елиминација на истата. Често тоа претставува создавање стратегии на национална безбедност, низ еден деликатен и сеопфатен процес, вклучувајќи ја безбедноста на критичната инфраструктура како составен дел на безбедносниот концепт на секоја држава.[[62]](#footnote-62)

Сајбер заканите за критичната инфраструктура се разновидни и можат да потекнуваат од различни извори, вклучувајќи државни актери, криминални организации, терористи и други злонамерни субјекти. Овие закани се движат од софистицирани сајбер напади дизајнирани да ги дестабилизираат основните услуги, до обиди за кражба на чувствителни информации. Импликациите од таквите напади се длабоки, што потенцијално ќе доведе до значителни нарушувања во јавните услуги, економска нестабилност и загрозена национална безбедност.[[63]](#footnote-63)

Голем дел од оваа инфраструктура е контролирана од индустриски контролни системи – ИКС кои исто така се познати како „Надзорна контрола и стекнување со податоци“ (Supervisory Control and Data Acquisition – SCADA), програми кои се ранливи на хакирање или DDoS – напади.[[64]](#footnote-64)

Доколку заканата не може да предизвика хакирање во системот, тогаш секогаш е можно да се пробие заштитата поради човечки фактор, односно корисничка грешка. Кога нападот е успешен, опциите за извршување на посакуваниот удар се многубројни. Она што е важно за напоменување е дека повеќето инфраструктурни системи имаат слични проблеми: исти оперативни системи, недостаток на средина во која би можело да се тестира моменталната сајбер безбедносна состојба, локален менаџмент и нема присуство на надзор. Програмите се направени за специфични системи кои оригинално се поставени во затворени мрежи, па се направени со земање предвид на можноста за високи побарувања, но без заштита на доверливоста или интегрирани заштити. [[65]](#footnote-65) Психологијата на сопствениците на овие системи поаѓа од фактот што истите сметаат дека системите се направени специјално за нив со што нивната самодоверба се зголемува, мислејќи дека ќе останат имуни на хакерските напади, но реалноста е поинаква, затоа што неретко се случува сите компјутерски програми да се програмирани со ист програмски јазик, и сите корисници на програмите за работа да користат исти софтвери, без дополнителна заштита што придонесува до тоа да не се имуни на сајбер напади и нивната успешност.

### 3.5. Електро енергетската инфраструктура, транспорт на нафта и природен гас како потенцијални ранливи сегменти

По нападите на 11 септември 2001 година во САД, тероризмот, како потенцијална закана за безбедноста на нуклеарната енергетска инфраструктура во рамките на ЕУ, предизвика огромно внимание и неодложна потреба од итни мерки за нејзина заштита. Нуклеарниот тероризам има потенцијал да предизвика огромни човечки загуби, последици врз животната средина и дестабилизација на економската и безбедносната состојба.[[66]](#footnote-66)

Енергијата и геополитиката отсекогаш биле тесно поврзани. Треба да сe процени дали, кога и како енергијата може да се користи како инструмент за национална безбедност. Предизвиците на енергетската безбедност влијаат врз цела Европа: вклучително и преку диверзификација на енергетските патишта и извори, модернизација на постојната енергетска инфраструктура, безбедност на снабдувањето со енергија по конкурентни цени, и одбранбен елемент на критична енергетска инфраструктура. Енергетската безбедност е клучен елемент за Европа. Земјите-членки поддржуваат енергетски инфраструктурни проекти сè со цел да се зголеми енергетската безбедност, и да одговорат на растечката побарувачка за енергија во ЕУ. Заштитата на енергетската инфраструктура не е нова за Европа. Од 8 декември 2008 година, Советот ја издаде директивата 2008/114/EC19 за идентификација и назначување на европските критични инфраструктури, и проценка на потребата од подобрување на нивната заштита. Европската перспектива е сеопфатен пристап, иако спротивставувањето на заканите од тероризмот се сметаат за приоритет. Важна карактеристика на енергетскиот сектор е меѓузависноста на енергетската инфраструктура, како и зависноста на другите сектори од енергијата. Ова значи дека енергетскиот сектор како таков е уникатно критичен за земјите-членки, и следствено на тоа е исклучително атрактивна цел за непријателски напади (вклучувајќи терористички напади и сајбер војна). Ова не е нова закана. Од друга страна, транзитните земји би можеле да бидат добро заштитени од заканите од земјите што ги снабдуваат со енергија. На овој начин, постои стабилност и заштита на критичната енергетска инфраструктура. Енергетската безбедност на земјите-членки, исто така, може да биде нарушена со напади врз критичната енергетска инфраструктура, одвнатре и однадвор, транзитни прекини во клучните „точки на задушување“, сајбер закани, како и хемиски, биолошки, радиолошки, нуклеарни закани, намерни и случајни. Ваквите транснационални ризици за енергетската инфраструктура не бараат само координација на национално ниво и споделување разузнавачки информации меѓу владините агенции, индустриските играчи и локалните заедници, туку и усогласување на процедурите, преку националните граници.[[67]](#footnote-67)

Диверзификацијата на снабдувањето со енергија бара софистицирана и сложена инфраструктура, со акцент на прекугранични инфраструктурни проекти, кои ги исполнуваат меѓународните стандарди за енергетска безбедност. Овие стандарди може да вклучуват: спецификации за дизајн за толеранција на природни катастрофи, технички и оперативни спецификации кои ја ублажуваат заканата од катастрофални несреќи и безбедносни мерки за справување со заканите од терористички напади или сајбер војна. Како последица на тоа, важно е односите на една држава со нејзините соседи да ја зајакнат стабилноста на поширокиот регион, со што станува мост на нации со заеднички интереси - барем во енергетскиот сектор. Тоа може да ја направи енергетската инфраструктура на дадената држава почувствителна (во смисла дека е витална), но со оглед на непречените билатерални односи и учеството на таа држава во мултилатералните механизми, може да ја увери енергетската заедница за безбедноста на енергетскиот бизнис преку и во рамките на границата на таа држава. Факт е дека јавноста не ги поврзува лесно енергетската ефикасност и заштитата на животната средина со воените приоритети. Меѓутоа, со оглед на тоа што вооружените сили на земјите-членки се меѓу најголемите потрошувачи на енергија во Европа, енергијата може да стане значајна ранливост во воените операции (мир и војна), освен ако не се управува ефективно. Зголемувањето на воената опрема често доведува до зголемување на употребата на енергија, а со тоа и енергетска зависност, што пак ја зголемува сложеноста и трошоците за оперативно користење на опремата. Затоа, енергетската ефикасност може да биде критично важна за подобрување на воените капацитети и за одржување на автономија на единицата и оперативна отпорност на бојното поле. Факт е дека земјите-членки сами по себе не можат да обезбедат автономија само врз основа на националните капацитети, туку треба да ги земат предвид интеракциите во рамките на својата мрежа на стратешки партнери. Во суштина, треба да се сфати дека стратешката автономија не подразбира пристап до бесконечни домашни ресурси, туку разновидност на опции и избори во склопот на европскиот енергетски екосистем, вклучувајќи ја и европската одбранбена димензија. Диверзификацијата на снабдувањето со енергија, зголемувањето на придонесот од алтернативните извори на енергија т.е. обновливи извори на енергија и трошењето помалку гориво со спроведување мерки за енергетска ефикасност, ќе ја намали изложеноста на секторот на енергетска зависност и ќе го намали ризикот од идна енергетска нестабилност.[[68]](#footnote-68)

За европската заедница, енергетската безбедност и безбедноста на критичната енергетска инфраструктура претставуваат и предизвици и можности кои произлегуваат од потребата за подготовка, заштита и одговор на заканите. Во решавањето на сегашните и идните безбедносни и одбранбени потреби на Европа, ЕУ треба да ја зајакне својата стратешка автономија за да може да дејствува сама, како и со партнери секогаш кога е потребно. Променливиот безбедносен пејзаж во комбинација со новиот политички моментум бара од ЕУ да ги искористи постоечките капацитети во рамките на ЕУ, но и да инвестира во области кои бараат зајакнување. Енергетската безбедност и безбедноста на критичната енергетска инфраструктура лежат во срцето на амбициите на Унијата да ги заштити Унијата и нејзините граѓани, демонстрирајќи ја врската во овој поглед, помеѓу внатрешната и надворешната безбедност; каде што надворешната политика и активностите на ЕУ имаат директно влијание врз нејзината внатрешна безбедност и отпорноста на нејзината инфраструктура. Енергетскиот сектор се потпира врз голем број различни категории на инфраструктура, од кои сите сочинуваат различни компоненти на енергетскиот синџир. Постојат силни причини зошто енергетската инфраструктура стана толку важна. Во последните години инфраструктурата на транспорт, складирање, рециклирање и управување со извори на енергија станаа цел на криминални дејствија извршени од терористички групи, што може негативно да влијае врз воените операции. Неодамнешните истражувања покажуваат дека нафтената инфраструктура генерално се смета за најверојатна терористичка цел, поради големата зависност на европските држави и поради концентрацијата на ресурси во релативно мал број на земјите од третиот свет. Од друга страна, секторите за гас и електрична енергија, кои се потпираат врз регионалните инфраструктурни мрежи, се помалку атрактивни цели, бидејќи нападот би резултирал со локализирано и ограничено влијание. Европа е главен нето увозник на енергија, а во главниот потсектор на нафта и гас, таа доаѓа кон крајот на енергетскиот синџир. Тоа значи дека Европа е зависна од долга енергетска инфраструктура од која најголемиот дел се наоѓа во странство. Инфраструктурата лоцирана во трети земји може да биде попривлечна за терористите и може да има големи каскадни ефекти. Целосна заштита на критичната енергетска инфраструктура од сите видови на закани е практично невозможна. Главната цел на критичната енергетска инфраструктура е намалување на ризикот на прифатливо ниво и зголемување на отпорноста со урамнорежување помеѓу ефикасноста и еластичноста. Финална цел на критичната енергетска инфраструктура е обезбедување на континуирана услуга. [[69]](#footnote-69)

Нафтата и природниот гас се најкористените енергии во светот, придонесувајќи за 57,5% глобална потрошувачка на примарна енергија. Цевководите се критична инфраструктура за транспорт на нафта и природен гас, поврзувајќи ги производните области со рафинериите, хемиските фабрики, домашните потрошувачи и деловните потреби. Во Соединетите Држави има повеќе од 190.000 милји цевководи за течна нафта и над 2,4 милиони милји цевководи за природен гас (вклучувајќи ги и дистрибутивните линии што опслужуваат домови, канцеларии и деловни активности). Ова ја сочинува најголемата цевководна мрежа во светот. Сепак, нафтата и природниот гас се запаливи и експлозивни материи, кои обично се испорачуваат во услови на висока температура и висок притисок преку цевководните мрежи. Како резултат на тоа, најверојатно ќе се случат големи несреќи како што се пожар, експлозија и испуштање токсични нафтоводи на нафтоводите и гасоводите, што ќе резултира со жртви, економски загуби и еколошки проблеми, со што се намалува одржливоста на транспортот со гасоводи. Освен тоа, нафтоводите и гасоводите може да бидат оштетени од природни опасности, како што се земјотреси, поплави и молњи, што резултира со потенцијални негативни секундарни последици врз населението, животната средина или самата индустриска активност. За разлика од ненамерните настани, намерните напади врз системите за снабдување со енергија може да резултираат со потешки последици. Во Нигерија, во текот на 1993 и 2008 година се случија вкупно 15.718 намерни напади на нафтоводи. Поради суштинската улога во одржливоста на синџирот на снабдување со енергија, современото општество и економија, цевководите може да бидат нападнати од противници (терористички напади, крадци и криминалци), што резултира со економски загуби, жртви, загадување на животната средина, јавна паника, итн. За да се заштитат нафтоводите и гасоводите, направени се многу обиди за техничка безбедност, како што се проценка на ризик од несреќи, проценка на ризик од корозија, сеизмичка ранливост и проценка на безбедносниот ризик. Отпорноста на системите за нафтоводи и гас може да се дефинира како способност да се апсорбираат загубите и да се одржува или подобри снабдувањето со енергија и покрај оштетувањата на нафтоводот. Со оглед на случајните опасности, природните опасности и намерните закани за нафтоводите и гасоводите, зајакнувањето на отпорноста на системите за нафтоводи и гасоводи е важен метод за да се обезбеди одржливост на синџирот на снабдување со енергија. Откако оштетувањето на нафтоводот и гасоводот е неизбежно, еластичниот систем на гасоводот може ефикасно да ги ублажи последиците од штетата и брзо да закрепне од прекинот на снабдувањето. Сепак, ограничени истражувања се направени за отпорноста на системите за нафтоводи и гасоводи. Како резултат на тоа, треба да се посвети поголемо внимание на подобрување на еластичноста на системот за нафтоводи и гас, како што е формулирање на еластична стратегија за одговор при итни случаи и развој на робустен систем за гасоводи.[[70]](#footnote-70)

Преку напаѓање на електро-енергетската инфраструктура, транспортот на нафта и природен гас, теорирстичките организации можат да предизвикат сериозни последици по економијата на земјата преку уривање на власта и преземање на истата. На овој начин организираните криминални групи се борат против странските инвестиции кои имаат интерес во тој сектор во државата каде тие дејствуваат, и на крај нападите секогаш имаат една и единствена цел: остварување на финансиски профит. Градењето на ефикасна стратегија за заштита на критичната инфраструктура ќе донесе бенефит во заштитата на енергетската инфраструктура на државите.

### 4. Дефинирање и видови на асиметрични закани

Аисметричните закани се нов термин кој се користи за опишување на оружје и тактики кои се користени од страна на релативно слабите непријатели заради заобиколување на технолошката доминација на западните нации,[[71]](#footnote-71) или терминот се користи за опишување на нападите на кои државата како институција нема адекватна одбрана, и чии тактики се специфични по форма и се со изразени цели.[[72]](#footnote-72)

Во изминатите години термините „асиметрија“ и „асиметричен“ станаа тренд во американските стратегиски и политички науки. Користењето на овие два термина ги отвори проблемите на современата војна, и со тоа станаа централни концепти на американскиот дискурс за војната. Војни, непријатели, битки, стратегии, пристапи, опции, предизвици и многу други појави се поврзани со вооружениот судир, сите се етикетирани како асиметрични.[[73]](#footnote-73)

Американската централна разузнавачка агенција асиметричните закани ги дефинира како „употреба на иновативни стратегии, тактики и технологии од страна на послаба држава или недржавен противник, кои се наменети за да се избене моќта на на посилните и да се искористи потенцијалната ранливост на поголем и технолошки супериорен противник“.[[74]](#footnote-74)

Асиметричното војување е нетрадиционално војување кое што се води помеѓу воено супериорна сила и една или повеќе инфериорни сили, што ги опфаќа следните аспекти: евалуација и победа на асиметричните закани, водење на асиметрични операции, разбирање и оценување на културната асиметричност и цената на асиметричната закана.[[75]](#footnote-75)

Глобалниот тероризам, транснационалниот организиран криминал и информатичките опции не се нови поими. Денес тоа се трите основни средства што непријателот ќе се обиде да ги искористи за поткрепа на своите конвенционални капацитети против нивниот супериорно посилен противник. Послабите сили се обидуват да се вклучат во овие нетрадиционални пристапи, со цел да се добие „неконвенционална победа“. [[76]](#footnote-76)

Ал Каеда е совршен пример за асиметрични закани. Ал Каеда користи модерни методи на докажани модели на војување, преку кои остварува политичко движење за пораз на легитимните, демократски влади од сиот свет. Фундаментално правило на Ал Каеда е дека со правилно користење на супериорна политичка волја и стратегија, може да се порази поголема економска и воена сила. Против групи како Ал Каеда и случни на нив е тешко да се води борба, бидејќи тие се организирани најпрво да обезбедат политички, а потоа воен успех.[[77]](#footnote-77)

Асиметричниот конфликт претставува долга борба. Времето е сојузник на асиметричниот борец. Виетнамските комунисти се бореле триесет години, а Палестинците се борат речиси шеесет години против Израел, без догледен крај на конфликтот.[[78]](#footnote-78) Асиметричните непријатели времето го гледаат низ декади или низ генерации, а не во денови, недели, месеци или во години.[[79]](#footnote-79)

### 4.1. Тероризам – терминолошко определување на поимот тероризам

Со настаните од 11 септември 2001 година, американската и светската заедница станаа експлозивно свесни за моќта на тероризмот, како алатка на војната. Иако тероризмот не е нова алатка на војната и нагорната магнитута на нападот на Светскиот трговски центар, им осигура признанние на терористичките групи дека стојат позади тој грозоморен настан. Овој напад силно ја потресе владата на САД, колективната психологија и националната безбедносна индустрија. Денес, речиси не постои организација, агенција или трговско претпријатие во САД во кое нема на еден или друг начин безбедносен план за евентуален терористички напад. На национално ниво постојат илјадници агенции и институции, центри за обука, универзитети, колеџи и интернет страници кои обезбедуваат информации, истражувања, образование и препораки кои се поврзани со теористичките инциденти и соодветни начини на обезбедување. Сето ова бара огромно зголемување на инвестициите во борбата против тероризмот, на индивидуални, локални и државни нивоа.[[80]](#footnote-80)

Западниот свет во голема мера инвестира во т.н. „војна против тероризмот“, во најголем дел, со нејасни и претежно контроверзни резултати. Од идеолошка гледна точка минатиот век главно се соочуваше со децентрализирани терористички групи, конвергирани во антизападни и антихристијански движења, кои не бараа постојани оперативни комуникации, туку произведуваа неограничени струи на индивидуални, терористички подмладоци и ќелии со помош на само-индоктринација и радикализација, преку напредни комуникациски канали. Геополитички САД од фирма - сојузник на муслиманскиот свет, се трансформираа во дефинитивен непријател на многу муслимански држави. Ирак од неодамна стана нов епицентар на џихад против западните сили. Две последователни инвазии од христијанските велесили, со различни политички системи го осигураа јавното мислење на муслиманите дека овие агресии се религиозно мотивирани. Тактички, теорористичкото движење се премести од таргетирање на владини претставници и војска, на убивање на цивили во невидени размери, со користење на ефикасниот, прецизниот и флексибилниот потенцијал на самоубиствената мисија. Ал Каеда и нејзините лидери не само што го преживејаа најраспространетиот и најдобро подготвен лов, тие станаа идеолошки и тактички лидери и икони за илјадници и илјадници следбеници. Вистинскиот проблем произлегува од симпатизерите на терористите. Повеќето од овие групи имаат поддршка од многу влади и на тој начин имаат пристап до автоматски оружја. Денес, тероризмот е многу лесно остварлив метод на привлекување, не само на локалното, туку и на националното или светското внимание преку масовните медиуми. [[81]](#footnote-81)

Во академските кругови постои една општоприфатена дефиниција која гласи: „Тероризмот е метод инспириран со немир (страв) од насилство на (полу) тајни личности, групи или држави, заради идеолошки, криминални и политички причини, каде за разлика од погубувањето, директната цел на насилството не е и главната мета на насилството. Непосредните жртви на насилството обично се бираат случајно или како симболична цел и тие исклучиво служат како средство на пренесување на пораката. Заканата и насилството се темелни средства на комуникација помеѓу терористите (организацијата) државата и жртвата (загрозените). Таа директна цел се користи како средство за манипулација со главната цел (јавност, публиката), а сè со цел да се шири терор, да се постави барање или да се здобие со внимание, зависно од целта која е поставена, а тоа е сеење страв, насилство и пропаганда.“[[82]](#footnote-82)

Според Брајан Џекинс тероризмот е составен од непринципиелна употреба на сила заради постигнување на политички цели во случај кога невини луѓе претставуваат цел, и притоа го дефинира како насилство за остварување на одреден ефект, кој најчесто не е првостепена цел, а понекогаш се случува актот да не е насочен кон постигнување на политички цели во случај кога невини луѓе претставуваат цел, или актот да не е насочен кон постигнување на одреден физички ефект на поставената цел. Насилството најмногу е насочено кон предизвикување на драматичен ефект врз набљудувачката публика.[[83]](#footnote-83)

Според дефиницијата на Европската Унија, прифатена од земјите членки, нагласено е дека терористичкото дело претставува намерен акт во кое по својата природа и содржина сериозно загрозува одредена земја или пак дури и меѓународна организација преку заплашување на популацијата, нелегално прислушкување на влада, или пак организација, напад на личен живот и интегритет, дестабилизација на сите политички, уставни или социјални структури, киднапирање на заложници, уништување на јавни добра, институции и инфраструктура, сè со цел да се загрози човечкиот живот или да се нанесе економска штета, потоа кинапирање на луѓе во јавен транспорт (авиони, возови и слично), производство на оружје за масовно уништување и негова употреба, прекин на водоснабдување, енергија и слично, како и учеството во тие терористички групи, нивно финансирање и слично.[[84]](#footnote-84)

Тероризмот, во суштина, претставува криминална повреда на речиси секој национален или меѓународен правен кодекс. За таа цел неопходно е да се детерминираат најзначајните основи врз кои ќе се прави разлика на силните акти и неприфатливите криминални активности. За таа цел од суштинско значење е да се расветли феноменот на тероризмот и како кривично дело:

* Тероризмот претставува кривично дело против одреден државен поредок и против легитимно избраната власт на конкретната држава,
* Тероризмот претставува кривично дело што во описот на своето битие ги содржи следните елементи: насилство, терор, застрашување, уцени, земање заложници, киднапирање, закани, итн.
* Тероризмот претставува кривично дело што е насочено кон граѓаните и кон претставниците на воено-безбедносните формации на државата,
* Тероризмот претставува кривично дело што е поврзано со политиката,
* Тероризмот претставува кривично дело што се финансира и е тесно поврзано со блиските и сродни инкриминации, кои во суштина, ги претставуваат и основните извори за нивно финансирање: трговија со дрога, трговија со оружје, нуклеарна хемиска и биолошка пролиферација, трговија со луѓе, поврзаност со феномените на транснационалниот организиран криминал, а посебно со финансискиот криминал и рекетирањето,
* Мотивацијата на терористичкиот чин може да има социјална, политичка, филозофска, идеолошка, културна и етничка основа, и
* Тероризмот претставува сосема идентичен облик на криминалитет со воените злосторства (честопати е тешко да се направи разлика помеѓу тероризмот и воениот криминал).[[85]](#footnote-85)

### 4.2. Видови на тероризам

Сите тоталитарни општества се базираат врз страв, оттука тоталитаризмот како државно уредување може да послужи и како споредба во однос со тероризмот. Во тоталитаристичките државни уредувања или режими, стремежот е во насока на преуредување на општествениот поредок согласно политичката или религиозната идеологија преку настојување на комплетна мобилизација на населението и нетолеранција кон сите оние кои не се согласуваат со идеологијата. Кога станува збор за тоа какви видови на тероризам постојат, класификацијата се прави врз основа на тоа какви средства користи напаѓачот.

* **Државен тероризам** – државниот терор претставува форма на институционализирано насилство извршено од страна на владата врз сопственото население. Целта не е да се создаде немир со кој ќе се принуди променацво политичкиот поредок, туку одржување или консолидирање на моќта. Тероризмот, од друга страна, бара промена. Иако исходот врз жртвата на крајот останува ист, целта и сторителот се фундаментално различни. Државниот терор претставува класификација за катогоризирање на тактиката преку нејзиниот извршител. Домашниот тероризам се случува во рамките на една земја, вклучува и странци и не е ниту поддржан, ниту оркестриран од ниту една странска влада. Меѓудржавниот терор се однесува на терористичките акции кои вклучуваат повеќе држави и се контролирани или управувани од страна на владата. Често како синоними се користат термините „меѓународен“ или „транснационален“ тероризам, кој ги вклучува оние акции во кои се инволвирани државјани од повеќе држави, како меѓу жртвите, така и меѓу сторителите, се извршуваат од страна на недржавни актери и не се ниту контролирани ниту управувани од страна на државата. Ал Каеда спаѓа во оваа класификација. [[86]](#footnote-86)
* **Биотероризам** – се однесува на намерно ослободување на токсични биолошки агенси за да им наштети и да ги тероризира цивилите, во име на политичка или друга причина. Американскиот центар за контрола на болестите ги класифицираше вирусите, бактериите и токсините кои би можеле да се употребат во нападот. Категорија А биолошки болести се оние кои најверојатно ќе ја направат најголемата штета. Тие вклучуваат: антракс, ботулизам, чума, голема сипаница, туларемија, и сл. [[87]](#footnote-87)
* **Сајбер тероризам** – секој оној кој користи интернет може да пренесе приказни за проблеми со вируси, кражби на идентитети и други проблеми, но повеќето не се свесни за можноста на терористите да ги употребат вирусите или физичките напади за да го оневозможат интернетот[[88]](#footnote-88), а со тоа да извршат и низа на напади, сè со цел да се влее страв кај корисниците на интернетот, и да се остварат поголеми цели како што се крадење на значајни информации за сторителите.
* **Глобален тероризам –** глобализацијата создаде значајни претпоставки терористичките организации да дејствуваат на меѓународен план, им понуди механизми со кои се зголемува нивното влијание врз многубројни популации и ги оспособи за напад на определени влади на други држави.[[89]](#footnote-89) Глобалните терористички организации успешно оперираат и функционираат на глобално ниво со помош на мрежи инсталирани насекаде низ светот. Колективно, тие поседуваат капацитети и располагаат со оперативни можности да ги остварат своите крајно радикални цели во било која држава. Реализацијата на нивните идеолошки цели ја загрозува безбедноста на државите надвор од границите на нивните матични територии. Во време на модерна комуникациска технологија, интернет и способности за слободно и неограничено движење, се создава еден вид виритуелна нација, која поседува огромен квантум на средства за моќ, вклучувајќи ги информациите, вооружените сили и економската моќ. Најзначајната кохезивна сила што ги поседува овие моќни организации се изразува преку радикалните исламски верувања и силното заедничко спротивставување на вредностите на западната култура.[[90]](#footnote-90) Глобализацијата на тероризмот се согледува преку дејствувањето на тероризмот во функција на интернационализација на војната, можноста за легализација на тероризмот, односно оправдување на тероризмот како облик на војување за „праведни“ цели, формирање меѓународни терористички групи и етаблирање (позиционирање) на тероризмот како нуклеарна, биолошка и хемиска безбедносна закана. [[91]](#footnote-91)

### 4.3. Фактори кои влијаат врз појавата на тероризмот

Сè со цел подобро да се разбере тероризмот и неговите следбеници, потребно е да се идентификуфаат факторите кои влијаат врз неговата појава. Па така издвоени се следните фактори:

* **Личен, општествен и културен идентитет во етничко-религиозниот тероризам** – идентитетот има големо значење во идентификацијата на едно лице, посебно кога станува збор за припадник на терористичка организација. Идентитетот се состои од три елементи: културен идентитет, социјален идентитет и личен идентитет. Културниот идентитет ги објаснува културните вредности кои му се водилка на едно лице и врз кои ги базира сопствените навики и однесувања во општеството. Социјалниот идентитет, пак, всушност е претставувањето во општеството или групата на лицето на која што припаѓа, додека пак личниот идентитет е спој на културниот и социолошкиот идентитет на едно лице преку кои се идентификува и ги искажува сопствените ставови во секојдневието и во општеството. Верскиот идентитет од друга страна, пак, е најсилен, бидејќи сè што се прави е за божјата правда, затоа верскиот тероризам е длабоко вкоренет во индивидуалната и колективната идентификација, и е суров во извршувањето на активностите.
* **Религијата како идентификатор за тероризмот –** низ историјата, религијата одиграла голема улога во сузбивањето на насилството, сузбивање на агресијата како и промовирање на помирување и разбирање помеѓу спротивставените групи. Меѓутоа како што нè учи историјата, религијата може да биде и посредно или непосредно причинител на војни, тероризам и други форми на насилство. Под религија се подразбира духовен облик на поврзаност на една група на луѓе со виша сила, или Господ Бог. Односно тоа е облик на социјална свест во која природните и социјалните сили се прикажуваат како натприродни, независни од човекот, природата и историјата. Религијата помалку или повеќе подразбира учење кое се однесува на суштината и потеклото на сè што постои, како и одреден облик на верски заедници, одредени обреди, ритуали кои се извршуваат на осветени места односно во одредени институции.[[92]](#footnote-92) Изразот фундаментализам и употребата на овој израз е од христијанско потекло. Во раните години од дваесетиот век во Америка фундаментализмот претставувал став дека постои основно фундаментално одредиште и незаменлив собир на традиционални христијански доктрини. Во периодот кога теолошкиот либерализам бил во подем, новиот израз овозможил нова идеја која треба да се идентификува и промовира. Постоел став за потребата од борба за основите на верата, и во тој контекст гордо се носела титулата фундаменталист. Подоцнежните употреби на овој израз не поминале без проблеми, истиот не се преведува буквално во други религиозни контексти, и неговата употреба е непрецизна, дури и во христијанството. Сепак терминот останал во употреба. Фундаментализмот е фокусиран врз специфичен збир на ставови, одреден тип на тесен поглед на светот, начин на дејствување кој може да се примени во било која област на човековата активност, особено во религијата и политиката, бидејќи и двете се занимаваат со контекстот и целите на човековото постоење. Терминот „религиозен фундаментализам“ се однесува на зголемување на свеста од релативно безопасен, релативно застарен, ултрарелигиозен систем на верување, до подготвеност за агресивно наметнување на другите.[[93]](#footnote-93) Денес фундаментализмот претставува религиско-политичка перспектива која се наоѓа во повеќето, ама не и во сите религии. Често се поврзува со различни форми на верски екстремизам, посебно, но во никој случај не е исклучено и со исламистите. Движењата од фундаменталистички тип се евидентни во исламот, но истите ги има и во христијанството, хиндуизмот, јудаизмот и другите верски заедници. Современиот фундаментализам не е белег на само една религија. Сепак исламистичкиот фундаментализам на тероризмот му даде бруталност и фанатизам, апотеоза на жртвувањето со верувањето во инкарнацијата на животот. Ова се поставува секојдневно во случаите „бомбаш – самоубиец“ , „автомобил – бомба“ и во несвесноста кон невини жртви на лице место.[[94]](#footnote-94) Тероризмот сè повеќе влијае врз т.н. неразвиени земји. Оваа околност може да биде појдовна точка за сите понатамошни, социолошки и други анализи на овој светски феномен. Една особеност е религиозниот фактор, бидејќи религијата во тие земји е споена со етничката припадност, при што верските постулати вклучуваат и некои општествено-политички и идеолошки импланти, како во слоганот „прочисување на светот“. Во Русија, поточно во Киргистан, постои движење „вахабизам“. И движењето Хизб во Тахрир со слоганот „слобода, правда, обновување на калифатот“ (како замена за политичкиот деспотизам на компромитираниот социјалистички поредок). Дел од оваа идеолошка рационализација е застапена и во римокатолистичката религија која се стреми кон светски примат. [[95]](#footnote-95)

## . Теорија на игра и проценка на ризик од тероризам во критичната инфраструктура

Сè повеќе се зголемуваат истражувањата во насока на користење на теорија на игра како алатка за проценка на ризикот од терористички напади по критичната ифраструктура. Во ова поглавје ќе се обидеме да ги објасниме моделите на теоријата на игра кои се фокусирани во насока на оптимизација на заштитните стратегии во критичната инфраструктура.

Кокс го набљудува проблемот со ранливоста на критичната инфраструктура од терористички напади со фокус на веројатноста за напад. Прегледот предложува четири алтернативни техники: анализа на стеблото на одлуки, мрежа на веројатности за активност и/или модели на планирање на проекти за терористички напади и хиерархиска оптимизација. Без оглед на техниките кои се користат, третирањето на напаѓачите како интелигентни опортунисти, наместо како носители на одлуки со случајни променливи, се чини ветувачко за сигурно предвидување на веројатноста за настан. Заклучокот на истражувањето е дека фокусирњето на отпорноста на критичните инфраструктури на оптимизирање на заштитините решенија, под претпоставка дека напаѓачите потоа соодветно ќе ги оптимизираат своите стратегии, е ветувачка тема. Овој пристап не ги зема предвид информациите кои им се познати на напаѓачите кои можат да влијаат врз нивната стратегија.[[96]](#footnote-96)

Биер и Косаноглу развија модел на одвраќање на напаѓачите користејќи теорија на корисност ориентирана кон целта – функциите Виебул и Рејли и експоненцијали беа користени за изразување на заштитна инвестиција во функција на загуба поради успешен напад. Ефективните заштитни решенија придонесуваат за оптимална распределба на ресурсите или преку подобрување на заштитата кога економичноста на одбраната е ниска. Критичните објекти со повисоки приоритети ќе добијат дополнителни заштитни ресурси, што ќе ги натера напаѓачите да размислуваат за цели со помала вредност. Моделот претпоставува дека во добро заштитени критични објекти, доколку има напади, успешните напади ќе бидат на големи цели, а повеќе настани на мали цели – ова е забележано во Израел во периодот 2000-2012 година.[[97]](#footnote-97) Фенг и соработниците развија теорија на игри заснована врз Нешовата рамнотежа со целосни информации, статична игра со нулта сума. Методот беше развиен и имплементиран за оптимизирање на распределбата на ограничените одбранбени ресурси за ублажување на ризикот од тероризам на повеќе хемиски постројки. Како пример за верификација и примена на овој метод се тестирани осум погони за складирање на хемиски експлозивни материјали во Кина. Хемиските постројки со високи почетни внатрешни ризици добија приоритет на ограничени заштитни ресурси, а нивните првични внатрешни ризици можеа да се ублажат на исто ниво, нивото зависи од вкупниот износ на одбранбени ресурси. Спротивно на тоа, постројките со ниски иницијални внатрешни ризици не добија дополнителни заштитни ресурси, а нивните првични внатрешни ризици останаа исти. Главен недостаток на овој модел е недостатокот на анализа и оптимална распределба на ниво на фабрика.[[98]](#footnote-98) Хаускен и Хе пак развија модел на теоретски игри на заштита на Х цели со дадена инхерентна заштита од терористички закани со дадена почетна стратегија. Резултатот од оваа стратегија го зема предвид нивото на заштитата и инвестицијата, но не ги зема предвид смртните случаи, повредите како идиректните и индиректните загуби. [[99]](#footnote-99)

Јасперсен и Монтиблер развија модел на однесување кој ги предвидува целите на терористите како стохастички процес на учење користејќи засилен процес на учење. Моделот беше имплементиран на примерок од деловни, воени, владини, приватни и инфраструктурни објекти. Моделот покажа дека однесувањето на терористите е приспособливо на целната средина во рана фаза од животот, и помалку приспособливо потоа, бидејќи инфраструктурните активности продолжуваат со текот на времето. Тоа значи дека заштитните активности треба да се прилагодат на променливата околина. Моделот беше имлементиран за да се предвидат нападите на ослободителните игри од Тамил Елам (LTTE) во нивното активно време на работа по 2004 година и беше откриено дека ги предвидува веројатностите за напади 0-0,6. Овој модел укажува на потребата од оптимална стратегија во единствениот објект како клучен чекор за оддржување на трошоците за ублажување под буџетски ограничувања. [[100]](#footnote-100)

Горенаведените модели за заштита на критичната инфраструктура ни ја укажува важноста од постоење на ефикасна стратегија како основна компонента на заштитата на секторите на критичната инфраструктура од терористички напади.

Еден од главните предизвици кои се поврзани со моделирањето на терористичките напади е тоа што тие немаат значителна фреквенција или локација на појавување. Наместо тоа изборот на критичната инфраструктура од страна на терористите најверојатно ќе биде резултат на серија пресметки вклучувајќи, но не ограничувајќи го нивото на заштита на таа цел, нејзиното значење како критична инфраструктура, нивоата на заштита на другите потенцијални цели, последиците од успешен напад и способностите на напаѓачот.[[101]](#footnote-101)

Изборот на методот за напад се фокусира врз зголемување на целокупната последица од самиот напад. Теоријата на игра се користи за идентификација на оптималната стратегија за заштита од напад. Инфраструктурата пак се перцепира како мрежен систем кој вклучува различни компоненти, а последицата е губење на функционалноста на системот.

## Импликциите на тероризмот врз критичната инфраструктура

Критичната инфраструктура е моделирана како поврзана графика, во кој секоја функционална компонента се смета како јазол во мрежата додека компонентите во мрежата се дефинирани како рабови. Во теоријата на мрежата нивото на меѓусебност ја претставува и глобалната ефикасност на мрежниот систем, додека ранливоста на мрежата е замислена како ниво на намалување на глобалната ефикасност што произлегува од неуспехот на јазлите и/или рабовите во мрежата.[[102]](#footnote-102)

Терористичките напади можат да влијаат врз функционалноста на системот на два начина: прво, кога функционалната компонента од критичната инфраструктура ќе се оштети, нивото на отпорност на врските во сите рабови што се поврзани со оштетената компонента ќе се зголемат. Второ, со оштетување на еден поврзувачки раб, нивото на отпорност на поврзувањето на оштетениот раб може да се зголеми. Во двата случаи ќе дојде до намалување на функционалноста на целиот систем. Зад секој терористички напад во дадена инфраструктура, загубите можат да се поделат на два главни типа: директна загуба која се проценува врз основа на трошоците за санирање на оштетената опрема, и лекување на повредени пред враќање на инфраструктурата во првобитна состојба, и индиректна загуба проценета врз основа на нето економскиот прекин предизвикан од недостатокот на функционалност на целта. [[103]](#footnote-103)

Во продолжение на ова поглавје следи студија на случај, анализа на стратегија за заштита на критичната инфраструктура од асиметрични закани со користење на теоријата за игри, па така согласно анализата, претпоставка е дека и напаѓачите и бранителите имаат целосно познавање на критичната инфраструктура. Во таа насока процесот на заштита е моделиран како игра со нулта сума, што значи дека додека бранителите се обидуваат да ја минимизираат потенцијалната загуба по нападот, напаѓачите имаат за цел да ја максимизираат штетата со додавање на ограничени ресурси. Стратегиите кои што се користат од секоја страна се врз основа на нивната ефикасност и трошоците. Поточно беа разгледани два методи на заштита на секоја од компонентите на критичната инфраструктура. Првиот се состои од подобрување на робусноста на одредени компоненти, на пр., со изградба на бетонски ѕидови или засолништа кои ја опкружуваат компонентата, што ќе имаат тенденција да го намалат нивото на оштетување доколку се случи напад. Кога ќе се додаде нивото на робусност на целната компонента на инфраструктурата, факторот на намалување на штетата ќе се примени на првичната последица од нападот поврзана со таа компонента, и го намалува нивото на оштетување на поврзаните рабови во нападот, така што потенцијалната загуба се намалува. Вториот метод на заштита се состои од подобрување на вишокот, што значи дека дадената инфраструктурна компонента ќе се реплицира, со специфична цел да се овозможи таа компонента да ја оддржува функционалноста и покрај тоа што е оштетена во напад. Кога одредено ниво на вишок се применува на целната компонента, оштетувањето на таа целна компонента во рамките на нивото на вишок ќе има само мали последици врз неговата функционалност, а исто така ќе го задржи неговото ниво на потпирање на другите релативни компоненти во мрежа за време на нападот, што резултира со намалување на вкупната потенцијална загуба.[[104]](#footnote-104) Историски гледано, оружјето кое се користело во терористичките напади се експлозиви ТНТ со тежина која не е поголема од 20 килограми.[[105]](#footnote-105) Во равенките на Кингери – Булмаш, мерниот критериум за оштетување е познат како ниво на инцидентен прекумерен притисок при експлозија кој може да се пресмета врз основа на тежината на ТНТ експлозивот и растојанието до центарот на експлозијата.[[106]](#footnote-106)

Заштитата на критичната инфраструктура треба да биде во насока на интеграција на раниливоста на критичната инфраструктура со користење на тополошка мрежна анализа, со која што ќе се анализираат различни сценарија, закани и последици од евентуален терористички напад по инфраструктурата, земајќи ги предвид сите можни дректни и индиректни последици од истиот. Доколку зборуваме само за терористички напади кои се закана за критичната инфраструктура, заштитната стратегија која ќе е во насока на подобрување на робусноста на критичната инфраструктура резултира со поголема ефикасност и ефективност.

Терористичките напади со својата моќ и цел имаат влијание и врз електроенергетската инфраструктура, транспортот на нафта и природен гас како ранливи сегменти на критичната инфраструктура, кои се од исклучителна важност во насока на непречено функционирање на целокупното општество, а нивната десктрукција има негативно влијание врз целокупната инфраструктура и населението на една држава. Во продолжение ќе се елаборираат ризиците и заканите по енергетската инфраструктура, нафтените деривати и гасоводите, и какво е влијанието на тероризмот врз нив.

Заканите за енергетската инфраструктура на нацијата продолжуваат да растат и се движат од природни катастрофи до сајбер и физички напади. Енергијата е критичниот инфраструктурен сектор кој им овозможува на другите критични инфраструктурни сектори да работат, што ја прави атрактивна цел за злонамерните актери.[[107]](#footnote-107) Зголемувањето на потрошувачката на енергијата е директно поврзано со индустријализацијата и економскиот раст повеќе од еден век. Со ескалацијата на прекините во снабдувањето со енергија, дискусиите за енергетската безбедност се проширија за да ја вклучат општата доверливост на електричната енергија, гасот и нафтените продукти, како и целокупниот синџир на снабдување со енергија, вклучително и рецидивите. Неколку различни настани и феномени го нарушија снабдувањето, како што се политичката нестабилност на Блискиот Исток и Источна Европа, природни катастрофи, спорови за гас со Русија - кои ги дестабилизираа енергетските пазари во Европа, и прекини на струја слични на оние што се случија во САД во 2003 година. Исто така, ураганите Катрина и Рита во 2005 година меѓу другото предизвикаа катастрофи, и ја погодија мрежата за снабдување со енергија од сите извори (нафта, гас, електрична енергија). Клучни фактори за ризик по енергетсктата инфраструктура се природните опасности (т.е. физичка безбедност), безбедноста на информатичката и комуникациската технологија (ИКТ), човечките фактори (на пр. небрежност, намерни напади врз инфраструктура) и некои организациски аспекти, како што е интеракцијата помеѓу јавните и приватните тела за одговор при итни случаи или негативното влијание на надворешната задача за одржување на енергетската инфраструктура.[[108]](#footnote-108)

Од друга страна нафтената инфустрија се карактеризира како индустрија со висок ризик поради значителното ниво на инвестиции, геолошките несигурности кои се директно поврзани со фискалните политики на една земја. Управувањето со ризиците кои се поврзани со нафтениот сектор вклучува идентификување на ризиците почнувајќи од синџирот на снабдување, проценка на веројатноста и сериозноста на влијанијата, приоризирање на ризичните настани како и развивање активности и ублажување на ризиците. Терористичките напади кои досега беа извршени врз нафтената инфраструктура, ги фатија производителите на нафта неподготвени. На пример, нападот на Ал Каеда на 24 февруари 2005 година врз објектот Арамко во Абкаик и Саудиска Арабија, испрати шокантни бранови низ светските финансиски пазари. Истиот ден, цената на нафтата на меѓународните пазари скокна речиси 2,00 долари за барел, и покрај целосниот неуспех на нападот. Повеќето аналитичари се согласуваат дека нападот во февруари, дополнителен обид на 28 март 2005 година и нападот во стилот на 11 септември во април 2007 година, од кои сите беа успешно избегнати, беа само пробни работи во многу подолга кампања дизајнирана да ја наруши глобалната економија воопшто, а особено нафтената индустрија. Ризикот од снабдување со нафта е главно прашање на безбедносната политика уште од 1970-ти години, бидејќи зависноста на поголемиот дел од економиите на ОЕЦД од увезената нафта од Блискиот Исток се зголеми со растот на политичката нестабилност на главните земји извознички на нафта, зголеменото влијание на ОПЕК, арапското ембарго за нафта од 1973-1974 година (САД Стејт департмент, 1976 година) и национализацијата на синџирот на снабдување со нафта нагоре. За жал, сето ова може да доведе до непредвидлив ризик за снабдување со нафта. Заканата од безбедноста на снабдувањето со нафта може да се анализира или во однос на побарувачката за земјата производител, или понудата за земјата потрошувач. За земјата производител на нафта безбедноста значи сигурност на побарувачката, додека за земјата потрошувач значи сигурност на понудата. Блум и Легеј, исто така, тврдат дека безбедноста на нафтата е клучен елемент на економскиот развој, затоа мора да се гарантира континуитетот, адекватноста и достапноста на снабдувањето со енергија. Хатиб, исто така, ја дефинира безбедноста на нафтата како континуирана достапност на нафта во различни форми, во доволни количества, и по достапни нивоа на цени. Јергин ја дефинира енергетската безбедност како „достапност на доволно залихи по пристапни цени“. Калицки и Голдвин на сличен начин ја дефинираат енергетската безбедност во смисла на „обезбедување прифатливи, сигурни, разновидни и обилни резерви на нафта и гас и нивните идни еквиваленти, и соодветна инфраструктура за испорака на овие залихи на пазарот“. Прашањата за безбедноста на нафтените деривати не се нови грижи, напротив се прашања од национален интерес. На земјите производители на нафта, како што е ОПЕК, потребна им е сигурност на побарувачката на нивната нафта, бидејќи опстанокот на таквите нации директно зависи од приходите од изводот на нафта во странски валути кои пак се користат за увоз на стоки и услуги потребни за развој на земјите. Секое намалување на побарувачката за извоз на нафта, а со тоа и намалување на приходите, има директно економско и политичко влијание врз овој тип на земји. Според низа на истражувања, нафтата може да има сè поголемо негативно влијание врз земјите призводители кои имаат ниски примања, чијшто ефект е изразен во низок или негативен економски раст на земјата, лоши јавни услуги, слабо државно владеење, сиромаштија и нестабилност. Рос потврдува дека слабо развиените земји кои имаат нафтени деривати, односно се производители и продавачи на нафта, често доживуваат побавен екоомски раст, високо ниво на корупција, неписменост, сираомаштија, невработеност, како и поголема ранливост на економски шокови.[[109]](#footnote-109)

Следствено на сето ова е дека асиметричните закани имаат директно влијание врз критичната инфраструктура и нејзините ранливи сегменти. Ниту еден сектор од критичната инфраструктура не е имун на ризици закани и напади, но можеби нападите кои директно влијаат врз електроенергетскиот сектор, нафтените деривати и гасоводите, може да придонесат за значителни и масовни економски проблеми на одредена држава која е засегната со овој проблем, кој пак се продлабочува и влијае дирекнто на сите останати потсектори на критичната инфраструктура. Според многумина аналитичари за непречено функционирање на критичната инфраструктура со нејзините сектори и потсектори кои се различно утврдени во секоја земја поединечно согласно нејзините законски регулативи, потребата од систем за заштита на критичната инфраструктура од закани се нужност за намалување на потенцијалните ризици кои по себе носат негативи импликации по целокупното општество и жителите на една земја.

### 5. Огранизиран криминал

### 5.1. Дефинирање на поимот организиран криминал и облици на организиран криминал

За дефинирањето на организираниот криминал и при определување на поимот организиран криминал, во теоријата постојат голем број спротивставени сфаќања. Одредени теоретичари сметаат дека поимот организиран криминал датира од многу одамна, додека други сметаат дека тој датира од поново време. Сепак, и покрај многубројните ставови во врска со поимното определување, истражувањата потврдуваат дека почетоците на теоретското дискутирање околу концептот за организираниот криминал е од релативно нов датум. Некаде во почетокот на шеесетите години од ХХ век, во САД почнуваат теоретските дискусии околу оваа проблематика, додека во Европа се развива подоцна, некаде околу осумдесеттите години на ХХ век. Тоа е периодот кога се издвојуваше порастот на организираниот криминал, па токму поради тоа почнува и заинтересираноста кај повеќе истражувачи, темата за организираниот криминал да биде главна преокупација. Организираниот криминал, како криминална појава претставува најконтроверзна проблематика на денешницата, еден од најкомплексните поими во своето битие. Неговата комплицираност при поимното определување произлегува од неговите карактеристики, поточно противречноста на организираниот криминал се согледа во трансцедентниот карактер. Условно кажано, многу кривични дела можат да се вбројат во областа на организираниот криминал. Од самиот поим може да се согледа дека не постои една и единствена дефиниција за тоа што всушност претставува организираниот криминал, како единствен генерички поим во меѓународни размери. За дефинирањето на организираниот криминал во литературата постојат голем број на дефиниции кои можат да се поделат во неколку групи: теоретски дефиниции, дефиниции на меѓународните тела и организации (меѓународни дефиниции), дефиниции од националните законодавства на одделни држави (службени дефиниции).[[110]](#footnote-110)

Во Република Македонија многу малку автори даваат дефиниции во однос на организираниот криминал, па така според професорот д-р Владо Камбовски организираниот криминал се дефинира како: „Извршување на кривични дела од страна на злосторнички здруженија заради остварување на профит и/или постигнување на моќ со употреба на насилство или со користење на посебната положба во општеството со намалување на ризикот преку вклучување во легалните економии, политички и други активности, како и однапред направен систем на заштита од гонење“.[[111]](#footnote-111) Професорот Камбовски вели дека постојат различни дефиниции на поимот организиран криминал во зависност од нивната цел, како и догматско-јуридичките и криминално-политичките функции на дефинирањето на поимот организиран криминал.[[112]](#footnote-112)

Според српскиот теоретичар Миќо Бошковиќ, под организиран криминал се подразбира: „активност на добро организирана криминална организација, со строга хиерархија, дисциплина, одговорност, лојалност и поделба на задачите, чијашто цел е остварување на што поголем профит и легализација на незаконски стекнат имот, благодарение на достигнатот степен на општествен углед, било врз основа на пробив во структурите на власта или во воспоставените врски со државните органи, легалните деловно стопански структури и влијателни политички партии и странки“.[[113]](#footnote-113)

Во однос на облиците на организираниот криминал во литературата како најчести облици на организиран криминал се јавуваат: трговија со луѓе и трговија со деца, недозволена трговија со оружје, трговија со дрога, перење на пари, и сл.

* **Трговија со луѓе и трговија со деца –** Во македонското законодавство во Кривичниот законик според глава триесетичетврта – Кривични дела против човечноста и меѓународното право, согласно член 418-а, став 1, трговијата со луѓе се дефинира на следниот начин: тој што со сила, сериозна закана доведува до заблуда и други форми на присилба, грабнување, измама, со злоупотреба на својата положба или состојбата на бременост, немоќ или физичка или ментална неспособност на друг, или со давање или примање пари или друга корист заради добивање согласност на лице кое нема контрола на друго лице или на друг начин врбува, превезува, пренесува, купува, продава, засолнува или прифаќа лица за експлоатација по пат на проституција или други форми на сексуална експлоатација, порнографија, принудна работа или слугување, ропство, присилни бракови, присилна фертилизација, незаконито посвојување или нему сличен однос, или недопуштено пресадување делови од човековото тело, ќе се казни со казна затвор најмалку четири години.[[114]](#footnote-114) Под поимот трговија со луѓе се подразбира една од формите на транснационален организиран криминал кој се состои од противправно остварување на економска или друг вид корист од продажба на мигранти, која се остварува по пат на закана, врбување, транспорт, криење, преселување од едно во друго место, и сл., од страна на посредниците, како и разни видови на нивната експлоатација од страна на оние кои ги држат во одредена зависност и потчинетост.[[115]](#footnote-115) Постои тесна поврзаност помеѓу трговијата со луѓе и проституцијата. Лошата социо-економска состојба, невработеноста и лошите животни услови и животот во сиромаштија и невработеноста како главен економски проблем кај пооделни држави тера сè поголем број на жени и млади девојки да ја напуштат сопствената држава и да заминат во странство со надеж за подобар живот и услови, како и за заработка. Неретко се случува истите тие да влезат во замка, и наместо ветената добра заработувачка и добри услови за живот, да завршат како предмет за сексуална експлоатација. Трговијата со органи е исто така облик на организиран криминал кој во поново време зема замав. Напредокот на медицината и технологијата како и пресадувањето на органи овозможува овој т.н „бизнис“ да работи со полна пареа. Побарувачката за трансплантација на органи кај лица чија здравствена состојба е премногу лоша, скептицизмот на доброволно донирање на органи по смртта на човекот е сè уште табу тема, придонесува побарувачката да се зголеми, а понудата не е задоволителна, затоа се активираат нелегалните пазари на трговија со органи, кои пак се прибавуваат на повеќе начини. Примораност на сиромашно население да продаде бубрег за пари е најчест начин, бидејќи човекот може да живее и да функционира со еден бубрег, или со киднапирање на луѓе и искористување на нивните органи. Сторителите на овој вид криминалитет речиси секогаш се членови на организирани криминални групи, од што произлегува и сиситематизацијата на трговијата со луѓе во рамките на организираниот криминал. Се работи за структурална група од три или повеќе лица која постои одреден временски период, и дејствува во согласност со цел за извршување на едно или повеќе сериозни кривични дела и прекршувања, со цел директно или индиректно да се стекнат со финансиска или друга материјална корист.[[116]](#footnote-116) Овој вид криминалитет е олеснет поради лесната проодност на граничните премини и од брзниот развој на технологијата, строителите на овој вид криминалитет се стекнуваат со огромна финансиска добивка, моќ и богатство, а истовремено овој вид на криминалитет се поврзува и со трговија со дрога и наркотични супстанци, оужје, и сл.
* **Недозволена трговија со оружје –** согласно законот за оружје на Република Македонија, член 3 став 1 од истоимениот закон, дава јасна дефиниција што значи оружјето, па така „Оружје е секој предмет или уред дизајниран на начин да исфрла проектили во форма на куршуми, сачми, гас, течности, стрели, под притисок на гасови со цел да предизвика физичка или психолошка штета“.[[117]](#footnote-117) Постојаната потреба од оружје беше наметната од воените жаришта ширум светот, терористичките организации, загрозената лична безбедност, граѓанските конфикти, и слично, и се едни од виновниците кои влијаат директно врз потребата од легалната или нелегалната трговија со оружје. Сведоци сме дека по Втората светска војна беше направен обид да се регулира трансферот на оружје, затоа што голем број на држави беа согласни дека производството на оружје мора да биде регулирано. За жал, финансиската корист ги надвладеа моралните принципи, и трговијата со оружје се комерцијализира. Пазарот на оружјето, легалното и нелегалното, долго време беше раздвоено на два сегмента, пазар за лесно и тешко вооружување, со претпоставка дека тешкото вооружување е многу поопасно, поради што мора да биде построго регулирано. Во поново време оправдано се потенцира дека треба да се посвети поголемо внимание и на лесното вооружување.[[118]](#footnote-118) Следствена логика на ова е дека лесното оружје е најзастапено во вооружените конфликти, лесното оружје е она со кое најлесно се убива, а истовремено многу лесно е достапно за набавување по илегални канали. Што претставува нелегалната трговија со оружје? Тоа е пренос на оружје по илегален пат преку граница, кој се извршува од страна на организирани криминални групи, кои пак, се јавуваат како фирми што се занимаваат со трговија, компании кои се занимаваат со увоз-извоз, но неретко како илегални трговци со оружје се јавуваат и самите држави. Кога станува збор за начинот на кој се извршува трговијата, може да биде по патен односно земјен сообраќај, поморски, а исто така и воздушен. Најчесто се користи патниот сообраќај, а од возила се користат автомобили, комбиња или големи камиони во со кои се превезува друга стока, сè со цел да се скрие кримогената активност, односно да се срие овој вид на криминалитет од евентуално откривање.
* **Трговија со дрога –** под поимот нарко криминалитет се подразбира илегално производство и промет со дроги, психотропни супстанци и прекурзори, и со нив поврзаните илегални активности.[[119]](#footnote-119) Криминалниот аспект на производство и промет на наркотични дроги, се однесува на злоупотребата односно користењето на различни психоактивни супстанци, надвор од нивната органичена и дозволена употреба за научни медицински цели, додека пак предмет на злоупотреба - производство, промет, дистрибуција и користење, се различните дроги и психотропни супстанци.[[120]](#footnote-120) Трговијата со дрога преку мрежи позната како криптомаркет или „темна мрежа“ започна во 2009 година со неколку интернет страници кои функционираа тивко. Денес, трговијата со дрога преку интернет е значителна, а користењето на криптомаркетите подразбира и поделба на улогите и можност за различни начини за плаќање.[[121]](#footnote-121) Во таа насока една студија која ја истражува продажбата на 16 големи криптомаркети помеѓу 2011 и 2015 година, проценува дека на продажбата на дроги оптаѓаат повеќе од 90% од вкупните приходи од глобалните криптомаркети. Речиси половина (46%) од вкупната продажба на овие маркети потекнува од продавачи со седиште во Европа, од кои како главни продавачи се јавуваат Германија, Холандија и Велика Британија.[[122]](#footnote-122) Во однос на транспортот на дрога покрај класичниот транспорт, трговците со дрога почнаа да ги употребуваат новите технолошки пронајдоци, сè со цел да пренесуваат дрога, па така во Северна Колумбија трговците на дрога се свртеа кон употреба на беспилотни летала или дронови за да пренесуваат дрога преку границите. Еден дрон има капацитет да пренесе 10 килограми дрога на секое патување, и да помине 100 километри пат.[[123]](#footnote-123)

### 5.2. Фактори кои ги олеснуваат активностите на организираниот криминал

Според извештајот на Европол од 2006 година, фактори кои ги олеснуваат активностите на организираниот криминал се: глобализација, границите, злоупотреба на финансискиот сектор, техничко-технолошки фактор, злоупотребата на транспортниот сектор, измама со фалсификувани документи.[[124]](#footnote-124)

* **Измама и фалсификување на документи –** се идентификува како употреба на лажни идентификатори, лажни документи или украден идентитет при извршување на кривично дело. Фалсификуваните документи се незменлив олеснувач за кривични дела како што е трговијата со украдени возила. Фалсификувањето на документи и идентитет можат да бидат профитабилни злосторства за специјалисти како што се фалсификатори, фалсификатори експерти за графика и и типографија и хакери.[[125]](#footnote-125)
* **Техничко-технолошки фактор –** Технологијата сè повеќе станува главен олеснувач на организираниот криминал. Во последните години се појавија нов вид на измами како што е преносот на податоци за деталите на платежните картички, а традиционалните форми на криминал како што се перењето на пари, продажбата на дрога, ширењето на малолетнички порнографски материјал на интернет и проституција, еволуираа како резултат на технолошкиот развој. Интернетот имаше особено големо влијание врз криминалот. Предностите што ги нуди интернетот во однос на информатичката и комуникациската технологија се исклучително корисни за организираниот криминал. Подземните структури изградени околу некои од високотехнолошките феномени, како што е хакирањето, се совршени за поддршка, контакти, регрутирање, совети и клиенти. Комуникацијата помеѓу структурите на организираниот криминал и нејзините членови треба да биде или целосно тајна или тешка за откривање од страна на органите на прогонот. Структурите на организираниот криминал се потпираат врз брзи и сигурни средства за комуникација. Електронската пошта, собите за разговор на интернет, и инстант пораките, нудат нови можности за брза комуникација, а во комбинација со алатките за шифрирање, нудат безбедност за податоците кои ги складираат и разменуваат.[[126]](#footnote-126)
* **Злоупотреба на транспортниот сектор –** петте главни сектори во транспортната индустрија се воздушниот, патниот, железничкиот, поморскиот и цефководниот транспорт. Околку 44% од сите стоки се транспортираат по пат, од кои 41% по краткоморски превоз, 8% со железница и 4% со внатрешни водни патишта. Во однос на организираниот криминал, преферирано средство за транспорт на хероин и канабис во рамките на Европската Унија е парниот транспорт, особено преку трансконтиненталните возачи на камиони. Патниот транспорт се користи како канал за олеснување на различен асотриман на кривични дела кои бараат транспорт на стоки или луѓе. Ова е потпомогнато со проширувањето на Европската Унија. Пристапот на организираниот криминал кон секторот вклучува идентификување, таргетирање и последователна корупција на клучниот персонал, и инфилтрација, купување или формирање на транспортни компании кои работат на легалниот пазар, но со криминална намера.[[127]](#footnote-127)
* **Злоупотреба на финансиски сектор –** Злоупотребата на финансискиот сектор се однесува на следните категории: кредитни институции, финансиски институции како што се менувачниците, канцеларии за трансфер на пари или дознаки, осигурителни компании или посредници, и инвестициски фирми, ревизори, надворешни сметководители, даночни советници, нотари и други независни правни професионалци, даватели на услуги од доверба, агенти за недвижности, казина и коцкарници, други правни или физички лица кои тргуваат со стоки или услуги.[[128]](#footnote-128)
* **Глобализација –** миграциските текови кои се шират во Европската Унија придонесуваат за промена на социјаната средина. Се чини дека заедниците на државјаните од третите земји се зголемуваат поради легалната и илегалната имиграција. Овој тренд го води миграциското прашање во центарот на политичката агенда на Европската Унија. Од друга страна глобализацијата ги трансформира криминалните пазари со цел да доминираат купувачите наместо продавачите. Станува сè полесно да се дојде до нелегални стоки или производи потребни за криминал. Овој фактор, еден вид глобализација на понудата, може да ги фаворизира и домородните групи на организиран криминал, бидејќи треба да ги еродира или спречи монополските позиции на одредени недомородни групи на организиран криминал. Најсилна закана на ниво на Европската Унија ја претставуваат групите за организиран криминал кои дејствуваат надвор и имаат влијание врз Европската Унија. Понатаму, развојот на значајни заедници на државјани на трети земји може да претставува можност за недомородните групи на организиран криминал во нивната борба да стекнат стабилно упориште на криминалите пазари во Европската Унија, а истовремено да имаат и целосна корист од нивните транснационални врски.[[129]](#footnote-129)
* **Граници –** ерозијата на границите може да се надополни со дискусија за границите кои постојат и се подложни на злоупотреба од криминални групи. Слободното движење на лица и стоки со административни бариери речиси целосно исчезнува, и е предност што ја користат структурите на организираниот криминал. Границите ќе продолжат да им обезбедуваат можности за криминал на организациите на организираниот криминал. Главната закана се административните граници кои ги попречуваат меѓународните активности за спроведување на законот, додека организираниот криминал продолжува да функционира. Во однос на политичките граници и намалените гранични патроли, целосната интеграција на земјите членки во заедничкиот простор на Европската Унија има олеснителен ефект врз активностите на организираниот криминал, иако се предвидува дека ќе има негативен ефект врз организираниот криминал на долг рок.[[130]](#footnote-130)

### 6. Заштита на критичната инфраструктура од асиметрични закани

Општата заложба е дека заштитата на критичната инфраструктура треба особено да биде апострофирана, бидејќи се знае дека овој сегмент е есенцијален, односно суштински дел на националната безбедност на секоја држава, па оттука нејзината заштита е врвна цел и приоритет на секоја земја, особено ако се знае дека секоја земја е изложена на општествени девијации, природни катастрофи, техничко-технолошки несреќи, човечките пропусти, итн., сите може да предизвикаат големи човечки загуби и материјални штети. Ако на овие елементи се надоврзат и одредени специфични облици на загрозување, во чии рамки спаѓа и употребата на современите оружја и напредни технологии, вклучувајќи го и нуклеарниот материјал, хемиските и биолошките оружја и слично, сето тоа е јасен сигнал дека имаме сериозен безбедносен ризик кој надополнет со веројатноста таквото оружје да биде употребено во акти на незаконско постапување и врз критичната инфраструктура, ја наметнува потребата од создавање соодветни механизми за заштита на критичната инфраструктура.[[131]](#footnote-131) Заштитата на критичната инфраструктура и отпорноста на критичните субјекти се од витално значење за модерните општества. Без сигурни залихи на енергија, безбедна вода за пиење, здравствени услуги, банкарски и финансиски услуги или предвидлив транспорт меѓу другото, нашиот живот не би бил возможен. Поради тоа Европската Комисија долго време беше ангажирана во поддршката на заштитата на критичната инфраструктура и отпорноста на критичните субјекти од природни и вештачки ризици.[[132]](#footnote-132)

Критичната инфраструктура станува базичен елемент во современите општества и начин на живот, така што функционирањето на сите текови силно зависи од стабилното и сигурно фунцкионирање на овие системи. Системите на критична инфраструктура – физички и виртуелни, се витални за сите држави, така што нивното онеспособување или деструкција би имало особено негативен ефект врз безбедноста, економијата, националното јавно здравје и јавната безбедност, или пак комбинација од овие аспекти.[[133]](#footnote-133)

Во тековниот период очевидна е и оправданата интензивирана загриженост и дебата околу заштита на критичната инфраструктура, особено во доменот на нивната ефективна заштита, имајќи ја предвид нивната витална позиција во социо-економските односи. Покрај оваа оправдана загриженост, се истакнува и зголемениот акцент кој се става на потребата за подобрена ефикасност, изведба и продуктивност на системите за критичната инфраструктура, како и импликациите кои произлегуваат од реалната состојба дека системите на критичната инфраструктура речиси никогаш не функционираат и егзистираат одвоено и во изолација. Напротив, тие меѓусебно се сумплементарни. Тенденцијата е овие системи да се трансформираат во тесно поврзани системи на (меѓу)зависни инфраструктури, ковергентни со информатичките и комуникациските технологии и интернетот. Критичната инфраструктура станува базичен елемент во современите општества и начин на живот, така што функционирањето на сите текови силно зависи од стабилното и сигурно функционирање на овие системи. Системите на критичната инфраструктура – физички и виртуелни, се витални за сите држави, така што нивното онеспособување или деструкција би имало особено негативен ефект врз безбедноста, економијата, националното јавно здравје и јавната безбедност, или пак комбинација од овие аспекти. Критичната инфраструктура може да биде ефективно заштитена преку процена на заканите и ранливостите. Откако ќе се спроведе таа фаза, се развива и креира план со кој се елиминираат или минимизираат и ублажуваат заканите и ранливостите. Во тој процес потребно е да се спроведат неколку фази на активности во насока на заштита на критичната инфраструктура, и тоа:

1. Проценување на ранливостите на критичната инфраструктура од физички и сајбер напади;
2. Развивање на планови за елиминација на значителни ранливости;
3. Предлог на системи за идентификација и превенција на обиди за напад;
4. Развој на планови за предупредување, задржување и отфрлање напади во тек;
5. Брза реконструкција на минималните и основни капацитети во случаи на извршен напад.[[134]](#footnote-134)

Европските критични субјекти сè повеќе се меѓусебно поврзани и меѓусебно зависни, што ги прави посилни и поефикасни, но и поранливи во случај на инцидент. Воената агресија на Русија врз Украина донесе нови ризици, физички и сајбер напади, често комбинирани како хибридни закани. Саботажата на гасоводoт „Северен тек“ и другите неодамнешни инциденти, јасно ставија до знаење дека отпорноста на критичната инфраструктура на Европската Унија е под закана. Итно е потребна акција за да се засили капацитетот на Европската Унија за заштита од напади врз критичната инфраструктура. Како клучен дел од работата на Европската Унија за изградба на безбедносна Унија, комисијата во 2022 година предложи ажурирани правила за зголемување на отпорноста на критичните субјекти. Со неодамна договорената Директива за отпорност на критичната инфраструктура (CER Directive) и Ревидираната директива за безбедност на мрежата и информацискиот систем (NIS2 Directive), Европската Унија наскоро ќе има ажурирана и сеопфтна правна рамка за зајакнување и на физичката и на сајбер отпорноста на критичната инфраструктура.[[135]](#footnote-135)

Директивата за отпорност на критичните субјекти стапи во сила на 16 јануари 2023 година. Земјите членки имаат рок до 17 октомври 2024 година да усвојат национално законодавство за применување на директивата. Целта на директивата е да ја зајакне отпорноста на критичните субјекти против низа закани, вклучувајќи природни опасности, терористички напади, внатрешни закани или саботажа, како и итни случаи на јавното здравје. Според новите правила:

* Земјите членки ќе треба да усвојат наионална стратегија и да вршат редовни проценки на ризикот за да ги идентификуваат ентитетите кои се сметаат за критични или витални за општеството и економијата. Комисијата усвои список на основни услуги во сите сектори опфтени со Директивата. Ќе се спроведат проценки на ризик во однос на овие суштнски услуги за да може да се идентификуваат критичните субјекти во секоја земја членка.
* За возврат, критичните субјекти ќе треба сами да спроведат проценки на ризик и да преземат технички, безбедносни и организациски мерки за да ја подобрат нивната отпорност и да известуваат за инциденти.
* Критичните субјекти во ЕУ кои обезбедуваат основни услуги во шест или повеќе земји членки, ќе имаат корист од дополнителни совети за тоа како најдобро да ги исполнат своите обврски за да ги проценат ризиците и да преземат мерки за подобрување на отпорноста.
* Земјите членки ќе треба да обезбедат поддршка за критичните субјекти во зајакнувањето на нивната отпорност. Комисијата ќе обезбеди дополнителна поддршка за земјите членки и критичните субјекти, преку развивање преглед на ниво на Унијата за прекуграничните и меѓусекторските ризици, најдобрите практики, материјалот за насоки, методологиите, активностите за прекугранична обука и вежбите за тестирање на отпорноста на критичните субјекти, меѓу другите.[[136]](#footnote-136)

## 6.1. Импликациите на организираниот криминал врз критичната инфраструктура

Иако организираниот криминал не е нов феномен, ширењето, влијанието и формите на организираниот криминал во современиот свет се без преседан. Ефектите од организираниот криминал се чувствуваат подеднакво во неразвиените и развиените земји, а во многу делови од светот, организираниот криминал ги создава токму условите што му овозможуваат да напредува, што резултира со самоовековечен циклус на несигурност и пренасочен развој.[[137]](#footnote-137)

Почнувајќи од економски пад и невработеност до климатските промени и дезинформации, предизвиците со кои може светот да се соочи во иднина се во голем број. Како големи ризици кои може да се случат во следните две до десет години се следните: дезинформациите, екстремните временски услови, општествената поларизација, сајбер несигурноста, недостигот на природни ресурси на Земјата и промени во екосистемот. Организираниот криминал е во пораст на глобалното ниво, и иако моментално се смета за фактор со релативно низок ризик, со ранг на 28 и 31 место, сепак анализите укажуваат на фактот дека истиот има директна врска со највисоко рангираните ризици. Економскиот пад, недостатокот на економски можности, сајбер несигурноста, миграциите, се повисоко рангирани ризици кои се потенцијални двигатели на недозволената економска активност. Доколку не може да се најде легитимно вработување поради причини поврзани со главните ризици, криминалот може да стане атрактивна алтернатива. Сето ова може да има дестабилизирачко влијание врз поширок опсег на земји во наредните години. Се идентификуваат три клучни области кои ќе ги поттикнат криминалните синдикати и незаконските пазари: политичка и економска нестабилност, технолошкиот напредок што овозможува поголема поврзаност меѓу криминалците, и распадот на владеењето. [[138]](#footnote-138)

Во неразвиените држави и во ситуации на градење мир и консолидација на државата, организираниот криминал е сè поголема закана. Во голем број држави, криминалните групи и недозволените текови се докажани дека го финансираат конфликтот, и ги продолжуваат насилството и несигурноста. Нашироко е признато, на пример, дека незаконската трговија и организираниот криминал играат клучна улога во намалувањето на кредибилитетот на владата и финансирањето на вооружените групи кои го поттикнаа колапсот на државата во Мали во 2011 година. Во поново време во Либија, организираниот криминал и вооружените групи што го вршат имаат одлучувачко влијание врз развојот на земјата, ја поткопуваат транзицијата кон стабилност, го попречуваат функционирањето на централните државни институции, го држат демократскиот процес во заложништво, ги обесправуваат граѓаните, и ја зголемуваат несигурноста и животните шанси на заедниците.[[139]](#footnote-139)

Во контекст на невидените предизвици за глобалниот мир и безбедност, особено континуираното влијание на криминалот и нестабилноста во Европа и на глобално ниво, Европската Унија и Канцеларијата на Обединетите Нации за дрога и криминал (UNDOC) се состанаа во Брисел на 23 мај 2024 година да разговараат за заедничките приоритети, и да ја зајакнуваат нивната соработка. Клучните области кои беа опфатени беа: шверцот на мигранти, трговијата со луѓе, незаконските финансиски текови, заштитата на критичната инфраструктура и незаконитостите поврзани со критичните синџири на снабдување со суровини. Во последните години, организираните криминални групи ги искористија можноштвото конфликти и кризи за да ги прошират своите мрежи и приходи. Пример, само криумчарењето на мигранти како криминална индустрија се проценува на сума од 5 до 7 милијарди американски долари со многу низок ризик за казнување на инволвираните криминалци. Малопродажниот пазр на дрога во Европската Унија чија проценка е повеќе од 30 милијарди евра годишно, го прави главен извор на приход за организиран криминал и ја прави Европа пресек за зголемено насилство и други злосторства, како што се корупцијата и трговијата со огнено оружје. Криминалните перачи на пари најдоа нови начини да ги скријат своите криминални приходи во легитимни бизниси, недвижнини и луксузни стоки, вклучително и во Европската Унија.[[140]](#footnote-140)

Во Соединетите Американски Држави, директорот на ФБИ Кристофер Вреј, на 31 јануари сведочеше пред Конгресот, објаснувајќи како хакерите на кинеската влада се обидуваат „да најдат и да се подготват да ја уништат или деградираат цивилната критична инфраструктура што нè одржува безбедни и просперитетни“. Овие хакери се позиционираат на американската инфраструктура, и се спремни да направат хаос, со што ќе предизвикаат штета во реалниот свет на американските граѓани и заедници, ако или кога Кина ќе одлучи дека е време за напад. Креаторите на политиките мора да почнат да го зајакнуваат приватниот сектор и локалната подготвеност за овие тековни напади, како и да ја развиваат и да ги искористат ресурсите на федералната меѓуагенција за сложени итни случаи, со акцент на општествената отпорност.[[141]](#footnote-141)

Сè повеќе се препознава дека третирањето на организираниот криминал како прашање на безбедност е недоволно и дека сеопфатната стратегија за соочување со овој феномен треба да го земе предвид одржливиот развој во согласност со човековите права. Со други зборови, за успешна борба против криминалните организации, на луѓето и на заедниците треба да им се овозможат можности за достоинствен економски, социјален и политички живот. Затоа, спречувањето на организираниот криминал повеќе не се сфаќа како единствена одговорност на агенциите за спроведување на законот. Организираниот криминал има повеќе причини и многу сектори од општеството може да имаат влијание врз нивоата на криминалот, а со тоа и одговорност да дејствуваат за да помогнат во негово спречување. Само преку мултисекторски, мултидисциплинарен и интегриран пристап може да се спречи и ефикасно да се справи со организираниот криминал. Предложената типологија претставува три главни „нетрадиционални“ пристапи: пристапи на заедницата; пристапи на регулаторни, нарушувања и неправедни системи, и вклучување на приватниот сектор.

* **Пристап на заедницата** - Фокусот на овој тип на превенција на криминалот е на зајакнување на заедниците преку обезбедување услуги кои градат врски меѓу членовите на заедницата и ги поврзуваат со надворешни ресурси и услуги, кои можат да им помогнат во борбата против криминалот генерално, а конкретно против организираниот криминал. Овој пристап се фокусира врз станбените заедници и населби и се обидува да ги промени социјалните услови поврзани со криминалот. Затоа бара да се решат сите сложени причини зошто населението се врти кон незаконитост, вклучително и недостатоците во спроведувањето на законот, како и физичката и економската несигурност и социјалната маргинализација.
* **Пристапи на регулаторни, нарушувања и неправедни системи** - Оваа категорија вклучува широк опсег на активности, од кои сите вклучуваат државни агенции на различни нивоа кои не се дел од формалниот кривично-правен систем. За полесно изложување и земајќи ја предвид категоризацијата на Леви и Мегваер, ваквите пристапи се анализираат на следниов начин: прво, оние кои се фокусирани на фискалните и финансиските стратегии, и второ, оние фокусирани на употребата на регулаторните овластувања за нарушување на „криминалниот бизнис“. **Фискални и финансиски стратегии:** Работењето на легитимните пазари може да биде попречено од организираните криминални групи и нивните активности, како што се перење пари и корупција. Овие злосторства се мешаат во економските политики, ги нарушуваат пазарните услови и на крајот создаваат сериозни системски ризици. Проактивното следење на криминалните средства е клучна компонента во борбата против организираниот криминал, и игра важна улога во секоја ефикасна стратегија за спречување на организираниот криминал. Враќањето на приходите од криминал може да даде значаен придонес за намалување на криминалот, бидејќи ги спречува криминалците да финансираат понатамошни операции и пренесува порака на одвраќање до оние кои инаку би можеле да се обидат да се вклучат во организирана криминална активност. Сепак, идентификацијата и враќањето на криминалните приходи е тежок процес, бидејќи тие често се скриени од нивните нелегитимни сопственици, на пример, на сметки во странски банки. **Употреба на регулаторни овластувања за нарушување на „криминалниот бизнис“ -** Овластувањата на регулаторните агенции се широко користени за да им се отежне на организираните криминални групи да се основаат и да се организираат, како и да дејствуваат во одредени области. Широкиот опсег на мерки што може да се преземат во овој контекст, вклучуваат посебно законодавство, како и процедури за проверка и/или мониторинг.
* **Вклучување на приватниот сектор -** Приватниот сектор може да игра фундаментална улога во спречувањето на организираниот криминал и корупцијата. Ова е особено точно во денешното општество, во кое глобализацијата и револуцијата во комуникациите предизвикани од технологијата резултираа со зголемена моќ и значење на корпоративниот сектор ширум светот. Според една студија, приватниот сектор е значително засегнат од организираните криминални групи на различни начини, било како цел или како олеснувач на организираната криминална активност. Неодамнешните студии, исто така, го нагласуваат високото економско влијание врз профитабилноста на фирмата, перформансите и инвестициите од постоењето на друга компанија на истиот пазар поврзана со криминална организација. Организациите од приватниот сектор се жалат дека комуникацијата со органите за спроведување на законот е често еднонасочна и дека товарот на регулаторното известување може да дејствува како пречка за соработката наместо да ја олеснува. Со оглед на екстремно високата цена на организираниот криминал за приватниот сектор, не е изненадувачки што компаниите и приватните организации ширум светот се подготвени да играат улога во справувањето со овој феномен. Навистина е точно дека многу корпорации, големи и мали, имаат широки комерцијални понуди дизајнирани за безбедност, и организирано спречување на криминалот. Оваа тенденција се рефлектира и во зголеменото значење на пазарот за приватно обезбедување, кој во последните децении презеде значителен дел од одговорностите на јавниот сектор, и се етаблира како лидер во анализата на организираниот криминал и развојот на стратегии. Зголемените притисоци врз заедницата за спроведување на законот резултираа во многу места низ светот во „приватизација“ на некои полициски функции, при што цивилната приватна безбедносна индустрија ги пополнува празнините што ги остави пренатрупаната полиција, и игра сè поголема улога во општата превенција на криминалот и заедницата.[[142]](#footnote-142)

Организираниот криминал е дефиниран како „незаконски активности, спроведени од групи или мрежи кои дејствуваат заедно, со вклучување во насилство, корупција или сродни активности со цел да се добие, директно или индиректно, финансиска или материјална корист“. Транснационалниот организиран криминал се јавува кога овие активности или овие групи или мрежи дејствуваат во две или повеќе земји. Транснационалниот организиран криминал може да има многу форми и постојано се развива. Вклучените групи и мрежи се флуидни, а каналите за трговија со една стока често се користат за други. Некои од типичните активности што ги спроведуваат транснационалните криминални организации се трговијата со луѓе, оружје, дрога, минерали и диви животни; производство и трговија на фалсификувана стока; измама и изнуда; перење пари и компјутерски криминал. Глобализацијата, дигитализацијата и другиот напредок во технологијата дополнително ја менуваат природата на незаконските пазари и начините на дејствување на транснационалниот организиран криминал, неодамна вклучително и појавата на употреба на криптовалути кои го отежнуваат следењето на недозволените финансиски текови.[[143]](#footnote-143)

Организираниот криминал како форма на нелегална активност за жал е сè повеќе присутна во секојдневието, импликациите на организираниот криминал врз критичната инфраструктура дејствуваат во насока на разнишување на инфраструктурната поставеност на целокупниот државен апарат, започнувајќи од јавното здравје (глобално јавно здравје), економските системи на државите или глобалната економија, односно директно влијае врз стабилните економски текови, безбедноста, и сл.

Организираниот криминал може негативно да влијае врз глобалното јавно здравје преку широко распространето и зголемено производство и трговија со фалсификувани лекови. Проблемот особено ги погодува земјите со низок и среден приход, каде според Светската здравствена организација се проценува дека еден од десет медицински производи е или супстандарден или фалсификуван. Трговијата со фалсификувани лекови често има транснационален елемент, бидејќи лековите се произведуваат во една земја (Кина, Индија и Сингапур се главните земји извор) и потоа се дистрибуираат до многу други и се вметнуваат во легитимните глобални синџири за снабдување со лекови. Фалсификуваните лекови може да бидат неефикасни во лекувањето на целната болест, а во најлош случај може сериозно да им наштетат или да ги убијат оние што ги земаат. СЗО проценува дека над 1 милион смртни случаи годишно во светот се резултат на супстандардни или фалсификувани лекови, а најголемиот број случаи (200 000) се случуваат во Африка. Фалсификуваните антибиотици се водечки тип на фалсификувани лекови, и се директно поврзани со зголемувањето на стекнатата бактериска отпорност на антибиотици, вклучувајќи го и глобалниот пораст на туберкулозата отпорна на лекови. Транснационалниот организиран криминал директно влијае врз капацитетите за јавно финансирање на државите, и може да го попречи економскиот развој преку даночно затајување и незаконски финансиски текови. Ова е особено корозивно за земјите во развој, лишувајќи ги државните каси од финансии кои се многу потребни за инвестиции во јавни добра, како што се здравството, образованието и инфраструктурата. Транснационалниот организиран криминал, исто така, може да ја поткопа економската стабилност на една земја преку трошење на девизните резерви и влијание врз цените на средствата. Перењето пари вклучува разновиден опсег на финансиски, правни и комерцијални актери кои намерно им помагаат на криминалците да ги претворат приходите од криминалниот приход во средства кои не можат да се проследат наназад до основниот криминал, и канализираат незаконски средства во легитимната економија. Организираниот криминал ги поткопува меѓународниот мир и безбедност преку одржување на насилство и вооружени конфликти. Незаконската трговија со оружје е рангирана како трет најраспространет нелегален пазар на глобално ниво. Незаконскиот проток на оружје го ескалира конфликтот и го зголемува ризикот од конфликт, и го олеснува насилниот криминал и другите организирани криминални активности.[[144]](#footnote-144)

Критичната инфраструктура е столбот на секое општество чија цел е оддржување на глобалната економија, јавното здравје и болниците, финансиските институции, информациските и коминикациските системи, и сл.

Критичните инфраструктури формираат комплексна мрежа на меѓузависни средства, системи и процеси. Поради оваа причина, тие се исто така екстремно ранливи на „каскадни ефекти“, што се случуваат кога нарушувањето во една инфраструктура предизвикува дефект на втора инфраструктура и потенцијално на други. Како што растеа напорите за обезбедување критичната инфраструктура во изминатата деценија, проценките на заканите се фокусираа врз ризиците од природните катастрофи, климатските промени и тероризмот. Меѓутоа, до денес, овој пристап не успеа соодветно да ја објасни сложената закана од организираниот криминал. Во текот на изминатите неколку години, многу земји се разбудија со потребата да се засили заштитата на сè поранливите критични инфраструктури. Владите, претежно во развиениот свет, имплементираа национални стратегии околу идентификацијата на голем број сектори кои се сметаат за критични, како што се енергијата, транспортот, здравјето и храната, меѓу другото. Во овој контекст, специфичните инфраструктури потоа беа издвоени и одговорностите беа подложени на идентификуваните сектори, со координативни улоги распоредени низ владините агенции. Клучно за овој пристап е разбирањето дека заштитата на критичната инфраструктура е одговорност на повеќе засегнати страни, почнувајќи од операторите на терен. Поради оваа причина, воспоставени се голем број јавно-приватни партнерства за да се обезбеди течна размена на информации на сите нивоа.[[145]](#footnote-145)

### 7. Заштита и пристапот на Република Северна Македонија во однос на критичната инфраструктура

По распадот на Југославија и осамостојувањето на Република Северна Македонија, беше започнат процес на водење на автономна политика во целокупното општество на Република Северна Македонија. Беа започнати реформи на целокупниот државен апарат, односно се напушти стариот начин на функционирање, со што се рефрмираше економскиот и банкарскиот систем, јавното здравство, образованието, правото и политичкото уредување на државата, безбедноста, одбраната и сите сегменти на општеството. Секако реформите беа направени етапно со постепено напуштање на стариот начин на функционирање, но со поставување на постулати што беа преземени, но адаптирани на „новосоздадената држава“ согласно новите политики и државно уредување на истата. Република С. Македонија стана самостоен и рамноправен меѓународен субјект, градеше и сè уште гради свои принципи како во надворешната, така и во безбедносната политика.

Република Северна Македонија е земја членка на НАТО. Таа е држава што опфаќа површина од 25.713 км², со вкупен број на население од 1.836.713 жители (Државен завод за статистика, 2022 г.). 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.[[146]](#footnote-146)

Во Република Северна Македонија, критичната инфраструктура не е дефинирана, односно нејзиното значење и потребата од заштита не е ставено во правна рамка во позитивните законски прописи, а со тоа нема определено кои сè субјекти можат да се третираат како критична инфраструктура и да ја уживаат посебната правна заштита. Потребата од нејзино законско уредување се појави со технолошкиот развој, глобалните промени во животната средина во последните неколку години и елементарните катастрофи кои укажаа на потребата за сериозно преиспитување на заштитата на критичната инфраструктура во контекст на опасноста од елементарни непогоди и други видови загрозување типични за современото живеење, како што се тероризам, шпионажа, и сл. Критичната инфрастурктура е од витално значење за функционирањето на една држава, а доколку дојде до нејзино оштетување, унишутување или загуба, доведува до губење на испоракта на услугите кои зависат од нејзино непречено функционирање. Критичната инфраструктура се системи, мрежи и објекти кои пружаат основни услуги во едно општество, па претставуваат поддршка за успешено функционирање на стопанството, сигурност и заштита на здравјето, и благосостојбата во државата. Сигурноста и заштитата на здравјето и благосостојбата во државата зависи од сигурноста и отпорноста на критичната инфраструктура. Бројни се причините поради кои инфраструктурата мора да биде добро обезбедена и заштитена. Некои од причините се терористички напади. Критичните информациски инфраструктури може да бидат особено ранливи на напади од страна на хакери, криминалци и терористи. Електроенергетската инфраструктура, транспортот на нафта и природен гас, се најранливи сегменти од енергетската инфраструктура, и претставуваат цели на напад.[[147]](#footnote-147)

Во редот на најважните активности, врз чија основа понатаму се надоврзува и заштитата на критичната инфраструктура, спаѓаат: дефинирање на објекти како критична инфраструктура; дефинирање на мерки за нивна заштита и безбедност; и дефинирање на задолженија и одговорности. Од овој аспект, особено е значајно да се забележи дека детерминирањето на критичната инфраструктура во Република Северна Македонија не е во согласност со насоките на Европската Унија. Во таа насока, недостасува јасно конкретизирање на поимот критична инфраструктура.[[148]](#footnote-148)

За да може оперативно, стручно и ефикасно да се заштити критичната инфраструктура во Република С. Македонија, дефинирано е задолжително приватно обезбедување на правните лица, и тоа кога е во интерес остварување на безбедноста на Република С. Македонија. Конкретно дефинирани се неколку дејности, и тоа: енергетиката (производство, пренос и дистрибуција на енергија), водоснабдувањето, животната средина, македонската радиотелевизија, електронските и печатените медиуми, Народната Банка на Република С. Македонија, и други правни лица регистрирани за вршење на банкарски работи.[[149]](#footnote-149)

Заштитата и обезбедувањето на критичната инфраструктура во Република С. Македонија треба да бидат насочени кон неколку клучни дејности, и тоа: енергетски сектор, информатичките технологии, водните системи и воздушниот сообраќај.[[150]](#footnote-150) Енергетскиот сектор во Република С. Македонија е регулиран согласно Законот за енергетика, во кој се изрично утврдени регулативите за производство, пренос и дистрибуција на струјата на територија на Република С. Македонија во домаќинствата и правните субјекти. Обезбедувањето на информатичките технологии треба да се акцентира на обезбедување на целокупната информатичка инфраструктура, односно заштита на мобилната и фиксната мрежа, оптичката мрежа како и заштита на телекомуникациските врски. Водните системи се регулирани со законот за води. Во овој контекст треба да се прецизира што се подразбира под обезбедување на водите, односно акцентот треба да биде ставен на обезбедување и достапност на здрава и чиста вода за пиење за граѓаните на државата, и во случај на контаминација на истата, да се обезбедат соодветни мерки за нејзино деконтаминирање преку забрани или ограничувања. Воздушниот сообраќај е регулиран со законот за воздухопловство. Според истоимениот закон, член 5 став 1 за регулирање и спроведување на работите од областа на цивилното воздухопловство, надлежни се: Министерството за транспорт и врски и Агенцијата за цивилно воздухопловство. Според член 5 став 2 за регулирање и спроведување на работите утврдени со овој закон, за потребите на државните воздухоплови, надлежни се: Министерството за одбрана, за воздухопловите кога вршат воени активности преку воено-воздухопловниот авторитет, кој е функционално одвоен од операторот на воздухопловите, командите и единиците кои се под негова контрола; Министерството за внатрешни работи, односно Агенцијата за национална безбедност за воздухопловите, кога вршат полициски активности; и Министерството за финансии – Царинската управа за воздухопловите, кога вршат царински активности. Според член 5 став 3, за спроведување на безбедносно истражување на воздухопловни несреќи и сериозни инциденти, во смисла на овој закон, Владата на Република Северна Македонија формира Комитет за истрага на воздухопловни несреќи и сериозни инциденти (во натамошниот текст: Комитет за истражување) како независно истражно тело со својство на правно лице.[[151]](#footnote-151)

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.[[152]](#footnote-152) 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).[[153]](#footnote-153)

**Првата фаза** опфаќа дефинирање на објекти кои ќе бидат нотирани како дел од критичната инфраструктура, како и дефинирање на мерки на заштита на истоимените објекти 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 процената 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 ад хок 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.[[154]](#footnote-154)

Втората 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 е потребно да се утврди список 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. 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 врз 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 што 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. Во Законот за критична инфраструктура треба да се назначи безбедносен координатор кој ќе претставува клучна фигура која во сите тела и органи, и ќе биде задолжен 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 што ќе ја определи динамиката на активностите.[[155]](#footnote-155)

### 7.1. Креирање на ефикасна стратегија на енергетско–критичната инфраструктура на Република С. Македонија

Прецизното дефинирање на енергетската инфраструктура на Република Северна Македонија е дел од потенцираните реформски зафати. Како еден од структурните елементи и составен дел на критичната инфраструктура, енергетската инфраструктура подлежи на бројни мерки и активности за нејзина заштита. Она што мораме да го предочиме е фактот што активностите кои се преземаат за обезбедување на енергетската инфраструктура, претставуваат посебен концепт, различен од концептот на енергетска безбедност, кој првенствено се фокусира врз политички и економски мотивираните прекини на снабдувањето со соодветните енергетски ресурси. Современиот концепт за заштита на енергетската инфраструктура на развиените држави е релативно нов и поразличен од традиционалниот – одбранбено фокусиран начин на обезбедување на енергетската инфраструктура. Тој е сеопфатен и интегриран во концептот за заштита на критичната инфраструктура, и има нераскинлива врска со националната безбедност. Тоа значи, дека покрај државните институции, вклучени се сите релевантни структури од приватниот сектор кои стопанисуваат со енергетската инфраструктура. Како резултат на тоа, современиот концепт има сериозен потенцијал да се развие во систем кој драстично ќе го редуцира ризикот од современите безбедносни закани. Гернерално гледано, и покрај фактот што во нашата држава нема позитивно законодавство за критична инфраструктура, сепак постои своевидна заштита на објектите и системите кои спаѓаат во категоријата критична инфраструктура. За жал, таквите парцијални решенија, кои најчесто се и неконсолидирани, не се преточени во систем, па во пракса може да се случи одредени институции да се преклопуваат во надлежностите или паралелно, а различно да постапуваат. Оттука се гледа важноста оваа област која сама по себе е и важно безбедносно прашање, да биде соодветно регулирана. Со донесување на соодветно законодавство (закон, подзаконски акти) прво, конечно би се воспоставил јасен систем според кој би биле дефинирани клучните поими во оваа област, би се утврдиле основните сектори или области од сферата на критичната инфраструктура, би била јасно детерминирана и доделена улогата на централно тело за координација, со што ќе дојде до креирање на оптимален систем во кој адекватно би биле лоцирани и соодветно искористени сите потребни, особено човечки ресурси, затоа што заштитата на критичната инфраструктура нужно бара планирање и спроведување на безбедносни мерки и брза и соодветна реакција на опасностите и можните штети. Во нив треба да се вклучени не само државните капацитети, кои се сепак ограничени, туку и огромните ресурси кои ги нуди приватниот безбедносен сектор.[[156]](#footnote-156)

Заштитата на енергетската инфраструктура од асиметрични закани е од исклучително значење за безбедноста на демократските држави. Република С. Македонија како земја членка на НАТО и со аспирации да се приклучи на земјите членки на ЕУ, како земја со важна геополитичка и геостратешка положба во Европа, не е имуна на асиметричните закани. Иако Република С. Македонија сè уште се нема соочено со закани и оштетувања на енергетската инфраструктура, недостатокот на правни регулативи за превенција и заштита на критична инфраструктура може да предизвика сериозни последити по економијата на државата и нејзините граѓани како резултат на асиметрични закани.

### 7.2. Законодавно и нормативно регулирање на безбедноста во Република Северна Македонија и пристапот кон асиметричните закани

Почнувајќи од 1991 година, т.е. од осамостојувањето на Република Северна Македонија и донесувањето на Уставот од 1991 година, Република Северна Македонија е дефинирана како самостојна, суверена и независна држава, а со тоа започнува и нормативното регулирање на воено-безбедносната сфера на државата. Процесот на изградбата и воспоставувањето на автономен систем за безбедност беше процес кој бараше соодветно знаење, средства и ресурси. Република Северна Македонија и покрај тоа се одлучи да изгради сопствен воено-безбедносен систем, кој во исто време ќе ги штити интересите на граѓаните и нема да загрозува туѓа безбедност.

Покрај Уставот на Република Северна Македонија, прв и основен документ во областа на безбедноста и одбраната е националната концепција за безбедност и одбрана, која е заснована врз процената за меѓународното опкружување и положба на Република Северна Македонија, загрозувањата по нејзината безбедност, и врз таа основа усогласени цели и насоки за водење на националната безбедносна политика. Националната концепција ја сочинуваат четири главни делови, и тоа: интереси на РСМ, безбедносно опкружување, политика на нацонална безбедност, и одбрана.

Следен документ кој е од важно значење од областа на безбедноста на Република Северна Македонија е стратегијата за одбрана која дава насоки за функционирањето и развојот на системот за одбрана, и произлегува од Уставот на Република Северна Македонија, трајните определби од Концепцијата за безбедност и одбрана, Законот за одбрана, и стратегиската определба на Република Северна Македонија за интеграција во евро-атлантските структури. Усогласена со обврските и одговорностите кои ќе произлезат од членството на Република Северна Македонија во колективните системи за безбедност, Стратегијата дава насоки за:

* зголемување на отпорноста на системот во справувањето со ризиците и заканите;
* унапредување на постојните и развивање нови способности неопходни за ефективно и ефикасно функционирање на системот;
* обезбедување поголема транспарентност кај сите субјекти и одговорност во заштитата на одбранбените интереси, и во остварувањето на одбранбените цели;
* синхронизирање и унапредување на одбранбеното планирање во согласност со стандардите на НАТО и на ЕУ;
* поголема ефективност и рационална искористеност на човечките, материјалните, и на финансиските ресурси;
* зголемување на свесноста и довербата кај населението за важноста на системот за одбрана во развојот на демократското општество.[[157]](#footnote-157)

Основниот елемент во процесот на формирање на стратегија за одбрана на современите држави е проценката на заканите по безбедноста. Секоја држава се соочува со закани, а природата на заканите во било која држава вклучително и на Република С. Македонија е предмет на континуирана дебата без крај. Република С. Македонија е последната земја-членка која се приклучи на НАТО алијансата, и со самото приклучување придобивките кои нашата држава ги има се во поглед на гаранциите за зголемената безбедност, со капацитетите на армијата на Република Северна Македонија и другите безбедносни актери кои имаат изградено ресурси и капацитети достојни за партнерство со другите држави земји членки. Што се однесува до членството во Европска Унија, нашата држава континуирано добива позитивни извештаи за преговори со што прашањето за преговори за членство во Европска Унија останува отворено, но самото и покрај тоа што државата ја гради политиката според европските стандарди, сепак членството навидум е надежно, но и далеку достижно.

Голем број научни и политички експерти по завршувањето на Студената војна сметале дека конвенционалните закани и натаму ќе претставуваат причина за конфликтите кои би се случиле во иднина. Меѓутоа овие мислења биле само на една група експерти, другата група сметала дека светот по Студената војна ќе се соочи со нови безбедносни закани каде ќе се војува со употребата на нови неконвенционални методи и средства.

Екстремниот национализам, расната и верската нетрпеливост помеѓу македонското и албанското население, која во голема мера е резултат на лошите политики на политичките партии од македонскиот и албанскиот блок, и континуираната борба против обесправеноста на албанското население, може да биде една од причините за појава на граѓански конфликт кој директно влијае врз стабилноста и безбедноста на државата, корупцијата која е длабоко навлезена во сите пори на општеството, нелегалната трговија со оружје и дрога, компјутерскиот криминал преку ширањето на лажни вести на интернет просторот влева страв и недоверба на граѓаните во безбедносниот сектор е дестабилизатор на безбедноста без да се употреби ниту едно средство за војување, тероризмот и сл, се само дел од заканите и ризиците по безбедноста на Република С. Македонија.

Промените во безбедносното опкружување кои се предизвикани од нови методи и начини на војување наметнаа и промени во начинот на кој се перцепираат заканите, како и заштита на општеството и граѓаните од истите. Република С. Македонија мора да воспостави функционален систем, почнувајќи од превенција до заштита преку минимизирање на ризиците и заканите кои директно влијаат врз целокупната безбедност на државата и населението. Во контекст на горенаведеното, Република С. Македонија мора да обезбеди комплетна меѓусекторска соработка на институциите преку искористување на сите можни ресурси и институции, вклучително и приватниот безбедносен сектор со кои располага, сè со цел обезбедување на безбедна средина и оддржување на тој континуитет.

### ЗАКЛУЧОК:

Природата на војувањето во текот на годините низ историјата претрпе многу промени. Првата и Втората светска војна беа војни каде околу 57 милиони луѓе ги загубија своите животи. Овие војни беа тотални, а посебно Втората светска војна беше тотална војна во која беа бомбардирани и цивили. Во модерниот начин на војување постои страв од тоталните војни поради брзата ескалација на воениот конфликт, како и неможноста истиот да се контролира. Улогата на обичниот граѓанин беше во насока на подгревање и провокации, за подоцна да биде главна цел на масовно насилство.

Периодот по 1945 година, глобализацијата го измени начинот и текот на војувањето. Со глобализацијата се појавија нови техники и методи на војување, па така војните се водат внатре во државите каде етничките и религиозните разлики се многу поважни од политичката идеологија, што е причинител за ескалација, немири и конфликти во државите. Новите војни се водат преку герилски техники и контраразузнавање, затоа што се избегнуваат судири, а територијата се контролира преку политички манипулации на населението. Всушност глобализацијата го забрза темпото на војување, појавата на асиметричните закани и другите воени и невоени закани ги зголемија безбедносните проблеми.

Со завршувањето на Студената војна беа започнати позитивни процеси, но сè уште не е изнајден соодветен начин да се воспостави мир и да се регулираат конфликтите меѓу државите, па така се наметна потребата од промена во безбедносните системи на државите. Глобалните закани како што се тероризмот, организираниот криминал, корупцијата, перењето на пари, нелегалната трговија со дрога, луѓе и човечки органи, и хибридните закани, ја наметнаа потребата од изградба на заедничка стратегија на глобално ниво за одговор на овие закани.

Заканите делуваат негативно директно на државите, како на безбедносниот систем така и на критичната инфраструктура. Безбедносниот систем и критичната инфраструктура во идеални услови на безбедност прават синергија од сектори кои се од суштинско значење за нормално институционално функционирање. Критичната инфраструктура како поим не е нов, и се појавува како поим во списите на Римската Империја, Кина, колонијална Шпанија, итн. Она што е значајно за критичната инфраструктура е фактот што таа ја опфаќа целокупната инфраструктура на една држава. Критичната инфраструктура е организациска целина која е составена од подсектори кои се меѓусебно поврзани, а се потребни за негово непречено функционирање. Генерално критичната инфраструктура е поделена на неколку сектори кои со текот на развојот на општествата станале критични, чие што нарушување може да доведе до колапс и трајна економска штета на државата. Согласно Европската комисија, енергетскиот сектор, информациските и комуникациските технологии, храната, водата, финансискиот и банкарскиот сектор, транспортот и сообраќајот, здравствениот систем и сл., се апострофирани како сектори од витален и значаен интерес на критичната инфраструктура. Имено системот на критичната инфраструктура, постојано се соочува со потенцијални безбедносни закани, чијшто ефект може да предизвика помали или поголеми проблеми, кои пак, може да доведат до нарушувања или дефекти на нејзините потсистеми.

Заканите од друга страна пак, се дефинирани од многу теоретичари на различни начини, но генерално е дека истите може да предизвикаат повреда на одреден субјект, и истите ја користат ранливоста на послабиот субјект. Заканите кон критичната инфраструктура можат да бидат поделени на природни непогоди, како што се поплави, земјотреси и пожари, но и закани кои се предизвикани со намера да нанесат штета. Доколку се анализираат природните закани, заклучокот е дека истите може да се случат во било кое време и на било кое место, предизвикувајќи последици од широки размери. Овде се поставува прашањето дали природните закани може да се превенираат и да се контролираат? Доколку се работи за фактор човек кој може да предизвика пожар и поплава, истите може да се исконтролираат да се спречи ескалација, но доколку говориме за земјотрес, науката вели дека земјотресите не може да се предвидат ниту да се превенира, затоа што тие се резултат на тектонско поместување на плочите со разорна моќ на деструкција која не може ниту да се детектира, а уште помалку да се спречи. Природните непогоди се случуваат и поради промена на климатските услови чиј фактор причинител е човекот со неговото несмасно однесување кон природата.

Заканите по системите на критичната инфраструктура се изменети во поглед на современата безбедносна слика и воочено е дека закани со конвенционално оружје се помалку веројатни, но паралелно на нив е зголемена опасноста од закани со употреба на неконвенционално оружје. Заканите доаѓаат од државни и недржавни актери, кои сè повеќе користат инструменти на моќ за да ги ослабнат институциите, а со тоа и да ја загрозат нивната безбедност. Следствено, современите држави својот стремеж треба да го насочат кон создавање на ефикасен концепт за справување со предизвици како што се тероризмот, пролиферацијата на оружје за масовно уништување, корупција, хибридни закани, итн. Комплексноста на овие закани ја наметна потребата од градење на национални капацитети за унапредување на отпорноста кон овие закани на национално ниво.

Брзиот напредок на технологијата донесе и нов вид на закани, хибридни закани кои се комбинација од субверзивни и злонамерни активности, преку употреба на конвенционални и неконвенционални методи за да се постигне посакуваната цел. Тие се комбинација од воени и невоени средства, вклучително и ширење на дезинформации, сајбер напади и слично, чија што брзина и интензитет постојано се менува.

Асиметричните закани се појавуваат нејасно и невообичаено од послабата страна од таргетираната цел, дејствувајќи преку неутрализирање на предностите на големата сила. Асиметричните закани користат широк спектар на заплашувања како што се дестабилизација, заплашувања, бунтови, и сл. Разликата помеѓу водењето војна со асиметрични закани од стандардниот тип на водење на војна, е да се влијае врз политичкиот естаблишмент со создавање на притисок кој ќе доведе до негова капитулација. Постојат повеќе видови на асиметрични закани, и тоа: тероризам, организиран криминал, хибридни закани и сајбер напади. Тероризмот како асиметрична закана е непријател број еден на државите кој позади себе сее ужас, страв и шок. Дефиниран од многу автори на различни начини, но со едноставно објаснување, тероризмот е намерен акт кој загрозува одредена земја преку дестабилизација на нејзините политички, правни, економски и социјални структури, со јасна цел да уништи нечие достоинство, да загрози нечиј живот или да нанесе економска штета. Организираниот криминал е активност на организирана криминална група со строго утврдена хиерархија и поделеност на задачите на нејзините припадници, со единствена цел стекнување на голем профит. Постојат повеќе видови на организиран криминал како што се недозволена трговија со луѓе, оружје, дрога и човечки органи, фалсификување и перење на пари, компјутерски криминал, и сл. Организираниот криминал како нелегална активност постои во современите држави, и поради неговата навлезеност во институциите честопати се случува истиот да биде прикриен и тешко откриен. Видовите на организираниот криминал директно влијаат врз безбедносниот, правниот и политичкиот систем на една држава, а оттука ја загрозуваат и критичната инфраструктура на државата.

Кога станува збор за Северна Македонија од нејзиното осамостојување беше започнат реформски процес на формирање на безбедносен систем, кој ќе одговори на предизвиците со кои Северна Македонија се соочува и ќе се соочува и во иднина. Ниту една држава, па ни Северна Македонија не е имуна на потенцијалните закани. Она што е симптоматично за Северна Македонија е честото непочитување на правниот поредок на државата и нефункционалност на системот. Кога станува збор за критичната инфраструктура, за жал во Северна Македонија критичната инфраструктура, нејзиното значење и потребата од нејзина заштита од асиметрични закани, не е ставена во правна рамка, а со тоа не е определено кои субјекти можат да се дефинираат и да се третираат како критична инфраструктура. Во последните неколку години елементарните непогоди, лажните дојави за бомби во училиштата, трговските центри, шпионажата, можни терористички напади кои се карактеристични во современите општества на живеење, укажаа на фактот од итно и сериозно преиспитување на заштитата на критичната инфраструктура. Покрај тоа што нема законодавство со кое се регулира критичната инфраструктура, во Северна Македонија постои заштита на системите кои се дел од критичната инфраструктура. Во идеален случај, кога би постоел закон, со тој закон концизно би била дефинирана критичната инфраструктура, секторите кои се дел од критичната инфраструктура, како и јасно утврдени органи кои се задолжени за заштита на критичната инфраструктура од асиметрични закани. Ова нè води до еден генерален заклучок: Северна Македонија мора да создаде систем кој ќе функционира во насока на заштита на критичната инфраструктура од асиметрични закани, вклучувајќи ги расположливите ресурси, создавајќи образовен систем кој ќе продуцира кадар кој соодветно ќе одговори на задачата и ќе работи во насока на подобрување на заштитата на населението и државата од потенцијални ризици и закани по нејзината безбедност.

### Библиографија:

Albanese, J. S.: The causes of organized crime, Yournal of Conteporary Criminal Justice,Thousand Oars, 2000.,

Alibabić V. Mujić I., Pravilna prehrana i zdravljе, Veleučilište, Rijeka, 2016,

Army War College, 2000,

Berakovic.M , Voda-Vjecna tajna prirode , Zagreb Antibarbarus, 2015

Bier,V.M.;Kosanoglu,F.Target-orientedutility theory for modeling the deterrent effects of counterterrorism. *Reliab. Eng. Syst. Saf.* 2015,

Bompard, E.; Wu, D.; Xue, F. Structural vulnerability of power systems: A topological approach. *Electr. Power Syst. Res.* 2011, 81, No 7,

Brian, Ј. “International Terrorism”, A New Mode of Conflict, Crescent Publications, Los Angeles, 1975

Bruce W. Bennett, Christopher P. Twomey, and Gregory F. Treverton, What Are Asymmetric Strategies? “Santa Monica, CA: Rand Corporation, 1998; Steven Metz, Armed Conflict in the 21st Century: The: TheInformation Revolution and Post-Modern Warfare, Carlisle Barracks, PA: Strategic Studies Institute, U.S.Army War College, 2000

C.Chen, C.Li, G.Reniers, F.Yang, Safety and security oil and gas pipeline transportation: “A systematic analysis of research trends and future needs using Wos”, Delt University of Technology, 2021

C.A.Briggs, Global Oil dependency and security risk: “The scramble oil resurce”, Southern University New Orleans LA, April, 2020

* Central Intelligence Agency, Statement of Work for Asymmetric Warfare Threads to US Interests: Expert panel support , Washington , D.C: DIA, 1997

Convention against transnational organized crime, United Nations, 2002

David L. Buffaloe. “Defining Asymmetric Warfare,” Land Warfare Papers, no.58, September, 2006:

David W. Bamo. “Challenges in Fighting a Global Insurgency,”.

Dawson, M., Omar, M. ,New Threats and Countermeasures in Digital Crime and Cyber Terrorism Information Science Reference, 2015

Edward G. Amoroso, Cyber Attacks Protecting National Infrastructure, Elsevier Inc, USA, 2011

Elkabets, S.M.; Shohet, I.M. Resilience Modeling (TRA) for critical infrastructures to withstand extreme events-sensitivity analyses. In Proceedings of the Creative Construction Conference, Krakow, Poland, June 2015

Energy Sector – Specific Plan, 2015

EU and UNDOC enhance cooperation to address increasing organized crime and violence within and beyond the EU, Brussels, February,6.2024

European Drug Report: Trends and Developments, European Monitoring Centre for Drugs and Drug Addiction Publications Office of the European Union, Luxembourg, 2017,

Europol – European Union Organized crime threat assessment, Public Version, The Hague, 2006

European Defence Agency, “Protection of critical energy infrastructure (PCEI) conceptual Paper”, Brussels, October, 2017

Feng, Q.; Cai, H.; Chen, Z.; Zhao, X.; Chen, Y. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. *J. Loss Prev. Process Ind.* 2016,

Financial Services Sector – Specific plan 2015

Franklin. B. Miles, Asymmetrical Warfare: An Historical Perspective, USAWC Class Of 1999

George Loukas., Cyber-Physical Attaks- A Growing Invisible Threat, Elsevier Inc, USA, 2015

Green Paper on a European Programme for Critical infrastructure protection Brussels, 17.11.2005, COM , 576 final Anne II, 2005

Hausken, K.; He, F. On the Effectiveness of Security Countermeasures for Critical Infrastructures. *Risk Anal.* 2016

Information Revolution and Post-Modern Warfare, Carlisle Barracks, PA: Strategic Studies Institute, U.S.

Interagency Security Committee: Annual Report. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency CISA, 2019 https://www.cisa.gov/sites/default/files/publications/ISC\_2019\_Annual\_Report\_508.pdf (посетена на 03.06.2024)

Јаspersen, J.G.; Montibeller, G. On the learning patterns and adaptive behavior of terrorist organizations. *Eur. J. Oper. Res.* 2020

Jeffrey Record. “Why the Strong Lose,” Parameters 35, no. 4, Winter 2005

Jeon, D., Kim, K. and Han, S.,Modified equation of shock wave parameters. *Computation*, *5*(3), 2017

Kravcov, A., *et al*. Durability of Critical Infrastructure, Monitoring and Testing: Proceedings of the ICDCF 2016. SpringerNature Singapore, 2017, преземенаод:<https://books.google.mk/books?id=1f6qDQAAQBAJ&pg=PA249&dq=critical+infrastructure>

Lambakis, S.,, Kiras J., Kolet K., *Understanding “Asymmetric” Threats to theUnited States*, Fairfax:National Institute for Public Policy, 2002

Lambakis,S. , Kiras J., Kolet K., Understanding “Asymmetric” Threads to the United States, Fairfax: National Institute for Public Policy, 2002

Lennart S, Threat Politics, New perspectives on security, risk and crisis management, Ashgate, 2001

Li-Wei, Frederick Teo, “Rethinking Western Vulnerabilities to Asymmetric Warfare,” Journal of theof theSingapore Armed Forces, April-June 2002

Mann Paul “Asymmetrical Threads”, New Military watchworld, Aviation Week and Space Technology, 27 April, 1998

M.Chalaris. “Security of Energy Infrastructure”, Academia Letters, Article 1116, June, 2021

Milan Vrsec, Managing Corporate Security in the Energy Sector: Energy as Vital (Critical) Infrastructure for the Functioning of a State, Economy and Civil Society, во Denis Caleta and Paul Semella, “*Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection*”, Center for Civil – Military Relations, Monterey, USA, 2011

Miletiħ S., *Policijsko pravo*, Policijska akademija, Beograd, 1997

Moteff Ј., Parfomak P., Critical Infrastructure and Key Assets:Definition and Identification, Congresional Research Service - The Library of Congress, 2004

Mounteney, J., Oteo, A., Griffiths, P., European Monitoring Centre for Drugs and Drug Addiction, The internet and drug markets, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016

Naylor, R.T.: The rise of the modern arms black market and the fall of supply – side control- U:combating transnational crime concept, activities and response, London – Portland, O.R, 2001

Pavlicevic.V. Sociologija religije, Beograd:BIGZ, 1988

Philip P. Purpura, Security An Introduction, CPP, 2011

Pratt. D, Terrorism and Religious Fundamentalism Prospects for a Predictive Paradigm, Marburg Journal of Relligion, Volume 11, No.1, 2006

Radvanovski, R., McDougall, A: *Critical Infrastructure: Homeland Security and Emergency Preparedness,* Third Edition. CRC Press, Taylor and Francis Group, 2013

RAND Objectiv analysis, effective solutions, “Threats to America’s critical infrastructure are now a terrifying reality, 12 February,2024

Rankovic. M: Savremeni/Globalni teorirzam Socioloski pristup, Sociologija, Vol XLVI No4,

Remennikov, A.M., A review of methods for predicting bomb blast effects on buildings. *Journal of battlefield technology*, *6*(3),2003

Richardson, L., „Terrorist Rivals: Beyond the State – Centric Model” Harvard International Review, XXXIX (1), Spring, 2007

Sage P. Andrew, Systems Engineering for Risk Management, Norwel MA, 1995

Sage, C., “Food security in: Page, A.E. Redclift, M (eds.) Humman Security ans the Environment – International comparisons. Cheltenham UK: Edward elgar, 2002

Sheehan, I “When terrorism and counterterrorism clash”, New York 2007,

Singapore Armed Forces, April-June 2002

Stallings. W. Network and Internetwork Security – Principles and Practices, New Yersey 1995

Terorizam i liberalno-demokratska drzava, Izmijenjena i nadopunjena verzija predavanja održanog na simpoziju Svjetski dan filozofije održanog u Zadru 16. i 17. studenog 2006

The global inititatice against transnational organized crime, “Organized crime: A Cross-cutting thread to susteinable development”, A research Report, January 2015

The global inititatice against transnational organized crime, “Organized crime: A Cross-cutting thread to susteinable development”, A research Report, January 2015

US Senate, An Oversight Hearing on the Planning and Conduct of the War in Iraq, 109 Cong., 3 sess.2006

Vaughan J. Emmett, Risk Management, John Wiley & Ins Inc, New York, 1996

Water and wastewater Sector – Specific Plan – 2015,

World economics forum, Global Risks Report: “Three risks we aren’t talking enough about”, Febr.6.2024

Бакрески О., Милошевска Т. Алчески Ѓ., ,, Заштита на критичната инфраструктура“ Комора на Република Македонија за приватно обезбедување, 2017,

Бакрески О., Милошевска Т., ,,Безбедноста на информациите и критичната инфраструктура“, Дирекција за безбедност на класифицирани информации, Скопје, 2021

Бошковиќ,М., Транснационален организиран криминал, Полициска академија, Београд, 2003

Георгиева Л, Менаџирање на ризици, Филозофски факултет, Скопје 2006,

Закон за воздухопловство, Службен весник бр.14, член 5. 22 јануари 2024,

Закон за оружје на РМ,

Закон за просторно и урбанистичко планирање, пристапено на 31.07.2023

Здравковски.Б, Сообраќајна инфраструктура, Скопје 2010

Камбовски, В., Казнено право – општ дел, ПРавен факултет, Скопје, 2011

Камбовски, В., Организиран криминал, 2 август С - Штип, Скопје, 2005

Камбовски, В., Правна држава и организиран криминалитет, Правен Факултет, Јустинијан Први, Скопје, 1996

Котовчевски М., Национална безбедност на Република Македонија, прв дел, Македонска Цивилизација, Скопје, 2000

Котовчевски М., Современ тероризам, Македонска Цивилизација, Скопје,2002

Котовчевски.М, Полемологија, Скопје: Филозофски факултет, 2011

Кривичен законик на РМ, стр.

Кронин, Курт Одри., Лудс, М. Џејмс. Напад на тероризмот:Елементи на грандиозна стратегија, НАМПЕРС, 2009

Лабовиќ, М., Николовски, М., Организиран криминал и корупција – нови теоретски димензии и практични консеквенции, методика на откривање и докажување, Скопје, 2009

Милески Т. Еколошка безбедност, одржлив развој – одржлива безбедност, Скопје, Филозофски факултет 2015

Милошевска.Т, „Глобален Тероризам”, Скопје:Филозофски Факултет, 2018

Митревска. М, Микац, Р, Прирачник за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Скопје, 2017

Митревска.М, Милески.Т, Кон отпорност и заштита на Критичната инфраструктура: Студија на случај на Република Северна Македонија, Фондација Фридрих Еберт, Канцеларија Скопје, 2022

Митревска.М, Милески.Т, Микац. Р, Критична Инфраструктура: Концепт и безбедносни предизвици, Фондација Фридрих Еберт, Канцеларија Скопје, Скопје, 2019

Парламентарното собрание на Советот на Европа на 24.01.2002 год. ја усвои Резолуцијата 1271(2002) за борба против тероризмот и почитување на човековите права.

Платон 427-437 п.н.е

Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016

Предлог закон за критична инфраструктура, Скопје, 2022

Роберт Ј. Фишер, Едвард.Х и Гион.Г, „Вовед во безбедноста”, 2008

Стратегија за градење отпорност и справување со хибридни закани, Влада на Р.Македонија, Април 2021,

Сулејманов, З., Криминологија, Скопје, 2007.

Сулејманов. З, Криминологија (четврто издание), Графохартија, Скопје, 2009

## Интернет страници

[https://ec.europa.eu/commission/presscorner/detail/fr%C2%A0/ip\_22\_6238 посетено на 12.08.2024](https://ec.europa.eu/commission/presscorner/detail/fr%C2%A0/ip_22_6238%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.08.2024)

[https://faktor.mk/shto-e-vsushnost-zemjotresot-i-kako-se-meri посетена на 04.06.2024](https://faktor.mk/shto-e-vsushnost-zemjotresot-i-kako-se-meri%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%B0%20%D0%BD%D0%B0%2004.06.2024)

[https://hom-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience\_en пристапено на 12.08.2024](https://hom-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.08.2024)

[https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience\_en посетено на 12.08.2024](https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.08.2024)

<https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/>

<https://mk.eferrit.com/%D1%80%D0%B0%D0%B7%D0%B1%D0%B8%D1%80%D0%B0%D1%9A%D0%B5-%D0%BD%D0%B0-%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D1%87%D0%BD%D0%B8-%D0%B2%D0%B8%D0%B4%D0%BE%D0%B2%D0%B8-%D0%BD%D0%B0/>

[https://sherloc.unodc.org/cld/en/education/tertiary/organized-crime/module-12/key-issues/organized-crime-approaches.html пристапено на 12.09.2024](https://sherloc.unodc.org/cld/en/education/tertiary/organized-crime/module-12/key-issues/organized-crime-approaches.html%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.09.2024)

<https://shoc.rusi.org/blog/critical-infrastructures-the-threat-from-organised-crime/>

<https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Michael%20N.%20Schmitt&eventCode=SE-AU>

<https://www.cisa.gov/supporting-policy-and-doctrine>

<https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookCyberThreats_MK_web_Jan2023.pdf>

<https://www.inst-antonatrstenjaka.si/gerontologija/slovar/1029.html>,

[https://www.mdpi.com/2076-3417/10/20/7162 посетено на 10.08.2024](https://www.mdpi.com/2076-3417/10/20/7162%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2010.08.2024)

[https://www.mdpi.com/2076-3417/10/20/7162 посетено на 11.08.2024](https://www.mdpi.com/2076-3417/10/20/7162%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2011.08.2024)

[https://www.mdpi.com/2076-3417/10/20/7162 пристапено на 11.08.2024](https://www.mdpi.com/2076-3417/10/20/7162%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2011.08.2024)

<https://www.merriam-webster.com/dictionary/critical>

[https://www.osce.org/files/f/documents/6/0/282436.pdf посетена на 04.06.2024](https://www.osce.org/files/f/documents/6/0/282436.pdf%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%B0%20%D0%BD%D0%B0%2004.06.2024)

[https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods пристапено на 12.09.2024](https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.09.2024)

[https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods пристапено на 13.09.2024](https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2013.09.2024)

<https://www.vodostopanstvo.mk/index.php/mk/osj/soopstenija/645-22>,

<https://zdravstvo.gov.mk/wp-content/uploads/2018/01/ZAKON-ZA-ZDRAVSTVENATA-ZASHTITA-zakluchno-so-br.-37-od-2016.pdf>

<https://pretsedatel.mk/%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%98%D0%B0-%D0%B7%D0%B0-%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0-%D0%BD%D0%B0-%D1%80%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0-%D1%81%D0%B5/>

<https://www.businessinsider.com/colombian-cocaine-drug-smuggler-using-drones-2016-11>

<https://www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure>

1. Бакрески О., Милошевска Т. и Алчески Ѓ., Заштита на критична инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 9. [↑](#footnote-ref-1)
2. Исто., стр. 9-10. [↑](#footnote-ref-2)
3. Central Intelligence Agency, Statement of Work for Asymmetric Warfare Threads to US Interests: Expert panel support , Washington , D.C: DIA, 1997, стр. 2. [↑](#footnote-ref-3)
4. Milan Vrsec, Managing Corporate Security in the Energy Sector: Energy as Vital (Critical) Infrastructure for the Functioning of a State, Economy and Civil Society, во Denis Caleta and Paul Semella, “*Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection*”, Center for Civil – Military Relations, Monterey, USA, 2011, стр.107-130. [↑](#footnote-ref-4)
5. Kravcov, A., *et al*. Durability of Critical Infrastructure, Monitoring and Testing: Proceedings of the ICDCF 2016. SpringerNature Singapore, 2017, преземенаод:<https://books.google.mk/books?id=1f6qDQAAQBAJ&pg=PA249&dq=critical+infrastructure> [↑](#footnote-ref-5)
6. Котовчевски М., Национална безбедност на Република Македонија, прв дел, Македонска Цивилизација, Скопје, 2000, стр.21 [↑](#footnote-ref-6)
7. Miletiħ S., *Policijsko pravo*, Policijska akademija, Beograd, 1997. [↑](#footnote-ref-7)
8. Moteff Ј., Parfomak P., Critical Infrastructure and Key Assets:Definition and Identification, Congresional Research Service - The Library of Congress, 2004,стр. 5. [↑](#footnote-ref-8)
9. https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Michael%20N.%20Schmitt&eventCode=SE-AU [↑](#footnote-ref-9)
10. Mann Paul “Asymmetrical Threads”, New Military watchworld, Aviation Week and Space Technology, 27 April 1998 – стр 55-56 [↑](#footnote-ref-10)
11. Lambakis, S.,, Kiras J., Kolet K., *Understanding “Asymmetric” Threats to the United States*, Fairfax:
National Institute for Public Policy, 2002. [↑](#footnote-ref-11)
12. Кронин, Курт Одри., Лудс, М. Џејмс. Напад на тероризмот:Елементи на грандиозна стратегија, (2009).НАМПЕРС [↑](#footnote-ref-12)
13. Парламентарното собрание на Советот на Европа на 24.01.2002 год. ја усвои Резолуцијата 1271(2002) за борба против тероризмот и почитување на човековите права. [↑](#footnote-ref-13)
14. Albanese, J. S.: The causes of organized crime, Yournal of Conteporary Criminal Justice,
Thousand Oars, 2000., стр. 23 [↑](#footnote-ref-14)
15. Radvanovski, R., McDougall, A: *Critical Infrastructure: Homeland Security and Emergency Preparedness,* Third Edition. CRC Press, Taylor and Francis Group, 2013, стр. 23-77. [↑](#footnote-ref-15)
16. Закон за просторно и урбанистичко планирање, пристапено на 31.07.2023 [↑](#footnote-ref-16)
17. <https://www.merriam-webster.com/dictionary/critical> (посетена на 03.06.2024) [↑](#footnote-ref-17)
18. <https://www.cisa.gov/supporting-policy-and-doctrine> (посетена на 03.06.2024) [↑](#footnote-ref-18)
19. Dawson, M., Omar, M. New Threats and Countermeasures in Digital Crime and Cyber Terrorism Information Science Reference, 2015, стр.97 [↑](#footnote-ref-19)
20. Interagency Security Committee, Annual Report. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency CISA, 2019 https://www.cisa.gov/sites/default/files/publications/ISC\_2019\_Annual\_Report\_508.pdf (посетена на 03.06.2024) [↑](#footnote-ref-20)
21. Бакрески О., Милошевска, Т., Алчески Ѓ., ,,Заштита на Критична инсфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр.17 [↑](#footnote-ref-21)
22. Green Paper on a European Programme for Critical infrastructure protection Brussels, 17.11.2005, COM , 2005, 576 final Anne II [↑](#footnote-ref-22)
23. Energy Sector – Specific Plan, 2015стр. 7 [↑](#footnote-ref-23)
24. Препис стр.11 [↑](#footnote-ref-24)
25. Препис стр.13 [↑](#footnote-ref-25)
26. <https://www.inst-antonatrstenjaka.si/gerontologija/slovar/1029.html>, пристапено на 09.09.2023 [↑](#footnote-ref-26)
27. Stallings. W. Network and Internetwork Security – Principles and Practices, New Yersey 1995 стр 29-30 [↑](#footnote-ref-27)
28. Здравковски.Б, Сообраќајна инфраструктура, Скопје 2010 ,стр.11 [↑](#footnote-ref-28)
29. Препис. Стр.11 [↑](#footnote-ref-29)
30. Платон 427-437 п.н.е [↑](#footnote-ref-30)
31. <https://www.vodostopanstvo.mk/index.php/mk/osj/soopstenija/645-22>, пристапено на 09.09.2023 [↑](#footnote-ref-31)
32. Water and wastewater Sector – Specific Plan – 2015, стр.2 [↑](#footnote-ref-32)
33. Препис стр.2-3 [↑](#footnote-ref-33)
34. Berakovic.M , Voda-Vjecna tajna prirode , Zagreb Antibarbarus, 2015, стр. 205 [↑](#footnote-ref-34)
35. Alibabić V. Mujić I., Pravilna prehrana i zdravljе, Veleučilište, Rijeka, 2016, стр. 3 [↑](#footnote-ref-35)
36. Милески Т. Еколошка безбедност, одржлив развој – одржлива безбедност, Скопје, Филозофски факултет 2015, стр. 115 [↑](#footnote-ref-36)
37. Препис,стр. 115 [↑](#footnote-ref-37)
38. Sage, C “Food security in: Page, A.E. Redclift, M (eds.) Humman Security ans the Environment – International comparisons. Cheltenham UK: Edward elgar, 2022, стр.132. [↑](#footnote-ref-38)
39. Financial Services Sector – Specific plan 2015, стр. 6 [↑](#footnote-ref-39)
40. Препис стр.6 [↑](#footnote-ref-40)
41. Препис стр.6 [↑](#footnote-ref-41)
42. Препис стр.8 [↑](#footnote-ref-42)
43. Препис стр. 8 [↑](#footnote-ref-43)
44. <https://zdravstvo.gov.mk/wp-content/uploads/2018/01/ZAKON-ZA-ZDRAVSTVENATA-ZASHTITA-zakluchno-so-br.-37-od-2016.pdf> член 2 [↑](#footnote-ref-44)
45. Philip P. Purpura, Security An Introduction, CPP, 2011, стр. 522 [↑](#footnote-ref-45)
46. Бакрески О., Милошевска Т. Алчески Ѓ., ,, Заштита на критичната инфраструктура” Комора на Република Македонија за приватно обезбедување, 2017, стр.85 [↑](#footnote-ref-46)
47. Vaughan J. Emmett, Risk Management, John Wiley & Ins Inc, New York, 1996, стр.23 [↑](#footnote-ref-47)
48. Sage P. Andrew, Systems Engineering for Risk Management, Norwel MA, 1995, стр.4 [↑](#footnote-ref-48)
49. Георгиева Л, Менаџирање на ризици, Филозофски факултет, Скопје 2006, стр. 79 [↑](#footnote-ref-49)
50. Препис, стр. 79 [↑](#footnote-ref-50)
51. Препис, стр. 80 [↑](#footnote-ref-51)
52. Lennart S, Threat Politics, New perspectives on security, risk and crisis management, Ashgate, 2001, стр. 21 [↑](#footnote-ref-52)
53. Бакрески О., Милошевска Т., ,,Безбедноста на информациите и критичната инфраструктура”, Дирекција за безбедност на класифицирани информации, Скопје, 2021 стр.87 [↑](#footnote-ref-53)
54. Препис, стр.87 [↑](#footnote-ref-54)
55. <https://faktor.mk/shto-e-vsushnost-zemjotresot-i-kako-se-meri> посетена на 04.06.2024 [↑](#footnote-ref-55)
56. Бакрески О., Милошевска Т., Безбедноста на информациите и критичната инфраструктура”, Дирекција за безбедност на класифицирани информации, Скопје, 2021 стр.89 [↑](#footnote-ref-56)
57. <https://www.osce.org/files/f/documents/6/0/282436.pdf> посетена на 04.06.2024 [↑](#footnote-ref-57)
58. Стратегија за градење отпорност и справување со хибридни закани, Влада на Р.Македонија, Април 2021, стр.2 [↑](#footnote-ref-58)
59. Препис, стр.2 [↑](#footnote-ref-59)
60. Препис, стр.4 [↑](#footnote-ref-60)
61. <https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookCyberThreats_MK_web_Jan2023.pdf> пристапено на 04.06.2024 [↑](#footnote-ref-61)
62. Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016 [↑](#footnote-ref-62)
63. <https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/> пристапено на 05.08.2024 [↑](#footnote-ref-63)
64. George Loukas., Cyber-Physical Attaks- A Growing Invisible Threat, Elsevier Inc, USA, 2015 [↑](#footnote-ref-64)
65. Edward G. Amoroso, Cyber Attacks Protecting National Infrastructure, Elsevier Inc, USA, 2011 [↑](#footnote-ref-65)
66. Бакрески.О, Милошевска.Т, Алчески.Ѓ, Заштита на критична инфраструктура,Комора на Република Македонија за приватно обезбедување, Скопје, 217, стр.126 [↑](#footnote-ref-66)
67. European Defence Agency, “Protection of critical energy infrastructure (PCEI) conceptual Paper”, Brussels, October, 2017, стр. 18-19 [↑](#footnote-ref-67)
68. Препис стр.19-21 [↑](#footnote-ref-68)
69. Препис стр.23-24 [↑](#footnote-ref-69)
70. C.Chen, C.Li, G.Reniers, F.Yang, Safety and security oil and gas pipeline transportation: “A systematic analysis of research trends and future needs using Wos”, Delt University of Technology, 2021, стр.1-9 [↑](#footnote-ref-70)
71. Mann Paul “Asymmetrical Threads”, New Military watchworld, Aviation Week and Space Technology, 27 April 1998 – стр 55-56 [↑](#footnote-ref-71)
72. Lambakis,S. , Kiras J., Kolet K., Understanding “Asymmetric” Threads to the United States, Fairfax: National Institute for Public Policy, 2002 [↑](#footnote-ref-72)
73. Bruce W. Bennett, Christopher P. Twomey, and Gregory F. Treverton, What Are Asymmetric Strategies? ”

Santa Monica, CA: Rand Corporation, 1998; Steven Metz, Armed Conflict in the 21st Century: The

Information Revolution and Post-Modern Warfare, Carlisle Barracks, PA: Strategic Studies Institute, U.S.

Army War College, 2000, стр. 40-41 [↑](#footnote-ref-73)
74. Franklin. B. Miles, Asymmetrical Warfare: An Historical Perspective, USAWC Class Of 1999, стр.3 [↑](#footnote-ref-74)
75. David L. Buffaloe. “Defining Asymmetric Warfare,” Land Warfare Papers, no.58,September,2006стр. 27 [↑](#footnote-ref-75)
76. Li-Wei, Frederick Teo, “Rethinking Western Vulnerabilities to Asymmetric Warfare,” Journal of the

Singapore Armed Forces, April-June 2002. [↑](#footnote-ref-76)
77. Jeffrey Record. “Why the Strong Lose,” Parameters 35, no. 4, Winter 2005. стр.19. [↑](#footnote-ref-77)
78. 26 US Senate, An Oversight Hearing on the Planning and Conduct of the War in Iraq, 109 Cong., 3 sess.,

2006, стр. 3. [↑](#footnote-ref-78)
79. David W. Bamo. “Challenges in Fighting a Global Insurgency,” стр. 23. [↑](#footnote-ref-79)
80. Richardson, L., „Terrorist Rivals: Beyond the State – Centric Model” Harvard International Review, XXXIX (1) Spring 2007 стр. 66-68 [↑](#footnote-ref-80)
81. Роберт Ј. Фишер, Едвард.Х и Гион.Г, „Вовед во безбедноста”, 2008година, стр. 394 [↑](#footnote-ref-81)
82. Terorizam i liberalno-demokratska drzava, Izmijenjena i nadopunjena verzija predavanja održanog na simpoziju Svjetski dan filozofije održanog u Zadru 16. i 17. studenog 2006. [↑](#footnote-ref-82)
83. Brian, Ј. "International Terrorism", A New Mode of Conflict, Crescent Publications, Los Angeles, 1975 [↑](#footnote-ref-83)
84. Парламентарното собрание на Советот на Европа на 24.01.2002 год. ја усвои Резолуцијата 1271(2002) за борба против тероризмот и почитување на човековите права [↑](#footnote-ref-84)
85. Котовчевски М., Современ тероризам, Македонска Цивилизација, Скопје,2002, стр.82-83 [↑](#footnote-ref-85)
86. Sheehan, I “When terrorism and counterterrorism clash”, New York 2007, стр.37 [↑](#footnote-ref-86)
87. <https://mk.eferrit.com/%D1%80%D0%B0%D0%B7%D0%B1%D0%B8%D1%80%D0%B0%D1%9A%D0%B5-%D0%BD%D0%B0-%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D1%87%D0%BD%D0%B8-%D0%B2%D0%B8%D0%B4%D0%BE%D0%B2%D0%B8-%D0%BD%D0%B0/> посетено на 01.12.2023година [↑](#footnote-ref-87)
88. Роберт Ј. Фишер, Едвард.Х и Гион.Г, „Вовед во безбедноста”, 2008, стр. 424 [↑](#footnote-ref-88)
89. Милошевска.Т, „Глобален Тероризам”, Скопје:Филозофски Факултет, 2018, стр.39 [↑](#footnote-ref-89)
90. Котовчевски.М, Полемологија, Скопје: Филозофски факултет, 2011, стр 293-294 [↑](#footnote-ref-90)
91. Милошевска.Т, „Глобален тероризам”, Скопје:Филозофски Факултет, 2018, стр.39 [↑](#footnote-ref-91)
92. Pavlicevic.V., Sociologija religije, Beograd,1988, BIGZ [↑](#footnote-ref-92)
93. Pratt. D, Terrorism and Religious Fundamentalism Prospects for a Predictive Paradigm, Marburg Journal of Relligion, Volume 11, No.1, 2006 стр 56-57 [↑](#footnote-ref-93)
94. Rankovic. M: Savremeni/Globalni teorirzam Socioloski pristup, Sociologija, Vol XLVI No4, стр.323 [↑](#footnote-ref-94)
95. Препис, стр.324 [↑](#footnote-ref-95)
96. [https://www.mdpi.com/2076-3417/10/20/7162 посетено на 10.08.2024](https://www.mdpi.com/2076-3417/10/20/7162%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2010.08.2024) [↑](#footnote-ref-96)
97. Bier,V.M.;Kosanoglu,F.Target-orientedutility theory for modeling the deterrent effects of counterterrorism. *Reliab. Eng. Syst. Saf.* 2015, стр.*136*, 35–46. [↑](#footnote-ref-97)
98. Feng, Q.; Cai, H.; Chen, Z.; Zhao, X.; Chen, Y. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. *J. Loss Prev. Process Ind.* 2016, стр. *43*, 614–628 [↑](#footnote-ref-98)
99. Hausken, K.; He, F. On the Effectiveness of Security Countermeasures for Critical Infrastructures. *Risk Anal.* 2016, стр. *36*, 711–726 [↑](#footnote-ref-99)
100. Јаspersen, J.G.; Montibeller, G. On the learning patterns and adaptive behavior of terrorist organizations. *Eur. J. Oper. Res.* 2020, стр. *282*, 221–234 [↑](#footnote-ref-100)
101. Elkabets, S.M.; Shohet, I.M. Resilience Modeling (TRA) for critical infrastructures to withstand extreme events-sensitivity analyses. In Proceedings of the Creative Construction Conference, Krakow, Poland, June 2015 стр. 21–24 [↑](#footnote-ref-101)
102. Bompard, E.; Wu, D.; Xue, F. Structural vulnerability of power systems: A topological approach. *Electr. Power Syst. Res.* 2011, 81, No 7, стр. 1334–1340 [↑](#footnote-ref-102)
103. <https://www.mdpi.com/2076-3417/10/20/7162>посетено на 11.08.2024 [↑](#footnote-ref-103)
104. [https://www.mdpi.com/2076-3417/10/20/7162 пристапено на 11.08.2024](https://www.mdpi.com/2076-3417/10/20/7162%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2011.08.2024) [↑](#footnote-ref-104)
105. Jeon, D., Kim, K. and Han, S., 2017, Modified equation of shock wave parameters. *Computation*, *5*(3), стр.41. [↑](#footnote-ref-105)
106. Remennikov, A.M.,A review of methods for predicting bomb blast effects on buildings. *Journal of battlefield technology*, *6*(3), 2003,стр.5-10. [↑](#footnote-ref-106)
107. <https://www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure>пристапено на 27.09.2024 [↑](#footnote-ref-107)
108. M.Chalaris. “Security of Energy Infrastructure”, Academia Letters, Article 1116, June, 2021, стр.1-2 [↑](#footnote-ref-108)
109. C.A.Briggs, Global Oil dependency and security risk: “The scramble oil resurce”, Southern University New Orleans LA, April, 2020, стр. 1-7 [↑](#footnote-ref-109)
110. Лабовиќ, М., Николовски, М., Организиран криминал и корупција – нови теоретски димензии и практични консеквенции, методика на откривање и докажување, Скопје, 2009 стр. 50-51 [↑](#footnote-ref-110)
111. Камбовски, В., Правна држава и организиран криминалитет, Правен Факултет, Јустинијан Први, Скопје, 1996г. Стр 8 и 9 [↑](#footnote-ref-111)
112. Камбовски, В., Казнено право – општ дел, ПРавен факултет, Скопје, 2011, стр.396 [↑](#footnote-ref-112)
113. Бошковиќ,М., Транснационален организиран криминал, Полициска академија, Београд, 2003 [↑](#footnote-ref-113)
114. Кривичен законик на РМ, стр. 179 – 180 [↑](#footnote-ref-114)
115. Сулејманов, З., Криминологија, Скопје, 2007. Стр 147 [↑](#footnote-ref-115)
116. Convention against transnational organized crime, United Nations, 2002 [↑](#footnote-ref-116)
117. Закон за оружје на РМ, стр 2 [↑](#footnote-ref-117)
118. Naylor, R.T.: The rise of the modern arms black market and the fall of supply – side control- U:combating transnational crime concept, activities and response, London – Portland, O.R, 2001 стр.344 [↑](#footnote-ref-118)
119. Сулејманов. З, Криминологија (четврто издание), Графохартија, Скопје, 2009, стр.137 [↑](#footnote-ref-119)
120. Камбовски, В., Организиран криминал, 2 август С - Штип, Скопје, 2005, стр. 273 [↑](#footnote-ref-120)
121. Mounteney, J., Oteo, A., Griffiths, P., European Monitoring Centre for Drugs and Drug Addiction, The internet and drug markets, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016, стр.13 [↑](#footnote-ref-121)
122. European Drug Report 2017: Trends and Developments, European Monitoring Centre for Drugs and Drug Addiction Publications Office of the European Union, Luxembourg, 2017, стр.20 [↑](#footnote-ref-122)
123. Види повеќе на: <https://www.businessinsider.com/colombian-cocaine-drug-smuggler-using-drones-2016-11> [↑](#footnote-ref-123)
124. Europol – European Union Organized crime threat assessment, Public Version, The Hague, 2006стр. 17 [↑](#footnote-ref-124)
125. Препис стр.18 [↑](#footnote-ref-125)
126. Препис стр. 18-19 [↑](#footnote-ref-126)
127. Препис стр. 19 [↑](#footnote-ref-127)
128. Препис стр 19-20 [↑](#footnote-ref-128)
129. Препис стр.21 [↑](#footnote-ref-129)
130. Препис стр.22 [↑](#footnote-ref-130)
131. Бакрески.О, Милошевска.Т, Безбедноста на информациите и критичната инфраструктура, Скопје, 2021 стр.119 [↑](#footnote-ref-131)
132. <https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en> посетено на 12.08.2024 [↑](#footnote-ref-132)
133. Бакрески.О, Милошевска.Т, Безбедноста на информациите и критичната инфраструктура, Скопје, 2021, стр.121 [↑](#footnote-ref-133)
134. Бакрески.О, Милошевска.Т, Безбедноста на информациите и критичната инфраструктура, Скопје, 2021 стр.120-122 [↑](#footnote-ref-134)
135. [https://ec.europa.eu/commission/presscorner/detail/fr%C2%A0/ip\_22\_6238 посетено на 12.08.2024](https://ec.europa.eu/commission/presscorner/detail/fr%C2%A0/ip_22_6238%20%D0%BF%D0%BE%D1%81%D0%B5%D1%82%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.08.2024) [↑](#footnote-ref-135)
136. [https://hom-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience\_en пристапено на 12.08.2024](https://hom-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BF%D0%B5%D0%BD%D0%BE%20%D0%BD%D0%B0%2012.08.2024) [↑](#footnote-ref-136)
137. The global inititatice against transnational organized crime, “Organized crime: A Cross-cutting thread to susteinable development”, A research Report, January 2015, стр.3 [↑](#footnote-ref-137)
138. World economics forum, Global Risks Report 2024: “Three risks we aren’t talking enough about”, Febr.6.2024 [↑](#footnote-ref-138)
139. The global inititatice against transnational organized crime, “Organized crime: A Cross-cutting thread to susteinable development”, A research Report, January 2015, стр. 3-4 [↑](#footnote-ref-139)
140. EU and UNDOC enhance cooperation to address increasing organized crime and violence within and beyond the EU, February,6.2024, Brussels [↑](#footnote-ref-140)
141. RAND Objectiv analysis, effective solutions, “Threats to America’s critical infrastructure are now a terrifying reality, February, 12.2024 [↑](#footnote-ref-141)
142. <https://sherloc.unodc.org/cld/en/education/tertiary/organized-crime/module-12/key-issues/organized-crime-approaches.html> пристапено на 12.09.2024 [↑](#footnote-ref-142)
143. <https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods> пристапено на 12.09.2024 [↑](#footnote-ref-143)
144. <https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods> пристапено на 13.09.2024 [↑](#footnote-ref-144)
145. <https://shoc.rusi.org/blog/critical-infrastructures-the-threat-from-organised-crime/> пристапено на 14.09.2024 [↑](#footnote-ref-145)
146. Митревска.М, Милески.Т, Кон отпорност и заштита на Критичната инфраструктура: Студија на случај на Република Северна Македонија, Фондација Фридрих Еберт, Канцеларија Скопје, 2022, стр.135 [↑](#footnote-ref-146)
147. Предлог закон за критична инфраструктура, Скопје, 2022, стр.2 [↑](#footnote-ref-147)
148. Митревска.М, Милески.Т, Микац. Р, Критична Инфраструктура: Концепт и безбедносни предизвици, Фондација Фридрих Еберт, Канцеларија Скопје, Скопје, 2019, Стр.158 [↑](#footnote-ref-148)
149. Препис.стр.158 - 159 [↑](#footnote-ref-149)
150. Митревска. М, Микац, Р, Прирачник за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Скопје, 2017, Стр.50 [↑](#footnote-ref-150)
151. Закон за воздухопловство, Службен весник бр.14, 22 јануари 2024, член 5, стр.5 и 6 [↑](#footnote-ref-151)
152. Митревска.М, Милески.Т, Кон отпорност и заштита на Критичната инфраструктура: Студија на случај на Република Северна Македонија, Фондација Фридрих Еберт, Канцеларија Скопје, 2022, стр.135-136 [↑](#footnote-ref-152)
153. Препис стр.137 [↑](#footnote-ref-153)
154. Препис стр. 137-139 [↑](#footnote-ref-154)
155. Препис 150-152 [↑](#footnote-ref-155)
156. Митревска.М, Милески.Т, Микац. Р, Критична Инфраструктура: Концепт и безбедносни предизвици, Фондација Фридрих Еберт, Канцеларија Скопје, Скопје, 2019, Стр.160-161 [↑](#footnote-ref-156)
157. Преземеноод: <https://pretsedatel.mk/%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%98%D0%B0-%D0%B7%D0%B0-%D0%BE%D0%B4%D0%B1%D1%80%D0%B0%D0%BD%D0%B0-%D0%BD%D0%B0-%D1%80%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0-%D1%81%D0%B5/> [↑](#footnote-ref-157)