

ПРОФ. Д-Р ОЛИВЕР БАКРЕСКИ
ПРОФ. Д-Р ТАЊА МИЛОШЕВСКА

**ПРИВАТНАТА БЕЗБЕДНОСТ
ВО ГРАДЕЊЕ ОТПОРНОСТ И ЗАШТИТА
НА КРИТИЧНАТА ИНФРАСТРУКТУРА**

проф. д-р Оливер БАКРЕСКИ
проф. д-р Тања МИЛОШЕВСКА

**ПРИВАТНАТА БЕЗБЕДНОСТ ВО
ГРАДЕЊЕ ОТПОРНОСТ И ЗАШТИТА
НА КРИТИЧНАТА ИНФРАСТРУКТУРА**

ПРИВАТНАТА БЕЗБЕДНОСТ ВО ГРАДЕЊЕ ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Автори	проф. д-р Оливер Бакрески проф. д-р Тања Милошевска
Истражувачки тим	д-р Лета Барџиева Миовска м-р Благојчо Спасов
Рецензенти	проф. д-р Јасмин Ахиќ проф. д-р Желимир Кешетовиќ
Издавач	Комора на Република Северна Македонија за приватно обезбедување
За издавачот	Седиште: ул. 50-та Дивизија бр. 34 1000 Скопје м-р Верица Милеска Стефановска
Уредник	м-р Верица Милеска Стефановска
Ликовен уредник	Билјана Иванова
Лектор	д-р Лилјана Пандева
Тираж	1000
Печати	Попе КОМПАНИ ДОО Скопје Седиште: ул. Горно Лисиче бр.210, 1000 Скопје
Година на издавање	2025 г.
Седиште на издавање	Скопје

© Сите права се заштитени. Ниту еден дел од оваа книга не може да биде репродуциран или пренесен во која било форма или со кои било средства, електронски или печатени, вклучувајќи фотокопирање, преснимување или чување во информациски системи без претходна писмена дозвола на авторот или на издавачот.

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

351.746.3:351.78
351.759.5:351.78
351.746.3:351.78(497.7)(047.31)
351.759.5:351.78(497.7)(047.31)

БАКРЕСКИ, Оливер

Приватната безбедност во градење отпорност и заштита на критичната инфраструктура /
Оливер Бакрески, Тања Милошевска. - Скопје : Комора на Република Северна Македонија
за приватно обезбедување, 2025. - 210 стр.
: илустр. ; 21 см

Фусноти кон текстот. - Библиографија: стр. 177-210

ISBN 978-608-66545-7-3

1. Милошевска, Тања [автор]

а) Приватна безбедност -- Критична инфраструктура -- Заштита б) Приватна безбедност --
Критична инфраструктура -- Македонија -- Истражувања

COBISS.MK-ID 66053637

СОДРЖИНА

ПРЕДГОВОР	9
------------------------	----------

ГЛАВА I

ПРИВАТНА БЕЗБЕДНОСТ – ТЕОРИЈА И КОНЦЕПТ	13
--	-----------

1. Приватната безбедност како концепт	15
2. Значење на приватната безбедност	17
3. Историска генеза на приватната безбедност	20
4. Терминолошки дивергенции околу поимот и употребата на терминот приватна безбедност	23
5. Детерминирање на опсегот на приватната безбедност	28
6. Регулмирање и стандардизација на дејноста приватно обезбедување	31
7. Приватното обезбедување во функција на националната безбедност	37
8. Новите безбедносни трендови во приватното обезбедување	42
9. Предвидени решенија како одговор на новите безбедносни трендови	50
10. Предизвици и перспективи во развојот на приватната безбедност	54
11. Предизвиците на приватната безбедност во заштита на критичната инфраструктура	62
12. Идни правци на развој на приватната безбедност	67

ГЛАВА II

КРИТИЧНА ИНФРАСТРУКТУРА – РАНЛИВОСТ, ОТПОРНОСТ И ЗАШТИТА	75
1. Терминолошки дивергенции околу поимот и употребата на терминот критична инфраструктура	77
2. Процес на заштита и градење отпорност на критичната инфраструктура	80
3. Концептуализација на транснационалните предизвици во заштита на критичната инфраструктура	87
3.1. Транснационални размислувања за заштита на критична инфраструктура	89
3.2. Влијанието на транснационализмот во процесот на заштита на критична инфраструктура	92
4. Фундаментални концепти	93
4.1. Ранливост	93
4.2. Меѓузависност	95
4.3. Управување	98
5. Пристапи/модел за идентификација и анализа на меѓузависноста и каскадните ефекти помеѓу системите на критичната инфраструктура	100
5.1. Моделирање на меѓузависности помеѓу секторите на критичната инфраструктура: пристап/модел на системска динамика	108
5.2. Заштита на критичната инфраструктура – Примери на каскадни ефекти	111
6. Својства и способности на критичната инфраструктура	115
6.1. Отпорност, ризик и ранливост	116
6.2. Отпорност на критичната инфраструктура	120
6.3. Сценарио за временски фази на отпорност	123
6.4. Процена заснована на индикатори	125

7.	Европската Унија и отпорноста на критичната инфраструктура	128
7.1.	Предизвици за примена на Директивата за отпорност на критичните ентитети	130
7.2.	Мерки за отпорност на критичните ентитети	132
8.	Актери на примарна закана насочена кон критичната инфраструктура	134
8.1.	Општ профил на ризици и закани во регионот на Западен Балкан	135
9.	Предизвици за донесување одлуки во заштита на критичната инфраструктура	138
9.1.	Концептуализација на перцепцијата на ризикот и хеуристиката за донесување одлуки и предрасуди	138
9.2.	Хеуристика за донесување одлуки и предрасуди во литературата за заштита на критична инфраструктура	141
10.	Анализа за перспективноста на приватната безбедносна индустрија во контекст на заштита на критичната инфраструктура	145
10.1.	Предизвици за приватната безбедносна професија	145

ГЛАВА III

ИНТЕРПРЕТАЦИЈА НА РЕЗУЛТАТИТЕ

ОД ЕМПИРИСКОТО ИСТРАЖУВАЊЕ

1.	Методолошка рамка	153
2.	Интерпретација на резултатите	154

Дефинициско-поимен речник	173
---------------------------------	-----

Библиографија	177
---------------------	-----

Закони, подзаконски акти и други правни прописи	209
---	-----

ПРЕДГОВОР

Сегментот прашања што се поврзуваат со безбедноста, со приватната безбедност, со критичната инфраструктура итн., се постојано отворени прашања за кои се бараат нови одговори, а колку приватната безбедност и критичната инфраструктура се значајна, комплексна, специфична и сложена тема најдобро говори податокот дека ова прашање ги заинтересирало повеќе истражувачи, но и државата во целост бидејќи се нераскинливо ткиво од општественото милје.

Во основа, повеќедимензионалноста и комплексноста на приватната безбедност може да се симплифицира со метаморфозата дека таа е една видлива манифестација на заштита на граѓаните што е повеќе од неопходна, а заради комплементарноста на функциите со јавната безбедност таа стои рамо до рамо со јавната безбедност за да се обезбеди потребната заштита за имотите, инфраструктурните објекти, граѓаните итн. Оттука денес основното прашање не е: „Дали има потреба од обезбедување на потребната заштита?“, туку прашањето: „Каква заштита е обезбедена и од кого?“, и уште поважно е прашањето: „Како да се обезбедат објектите од витално значење за државата, односно како да се заштитат бидејќи се ресурс важен од критичната инфраструктура?“ Ова е особено важно ако се има предвид фактот дека новите безбедносни закани што се појавуваат во различни сложени околности и под одредени специфични услови имплицираат потреба за обезбедување синхронизиран одговор и приспособувања на новите безбедносни трендови.

Во контекст на оваа студија, идентификацијата на безбедносните трендови што влијаат на приватниот безбедносен сектор се врши преку примена на методологија на статистички и аналитички калкулации, при што тие категоријално се диференцираат.¹ По-

1 Hasbrouck, J. (1993) Assessing the Quality of a Security Market: A New Approach to Transaction-Cost Measurement, *The Review of Financial Studies*, Volume 6, Issue 1, January 1993, стр. 191–212.

датоците што се преземени за анализа потекнуваат од релевантни примарни, секундарни и терцијарни извори што се третираат на глобално, но и на национално ниво.²

Во согласност со интегрираните и холистички анализи на пазарот на приватни безбедносни услуги, во контекст на предвидувањата за големината на пазарот, трендовите, двигателите на раст и предизвиците, како и анализа на давателите на услуги, но и аранжманите во критичните инфраструктурни објекти се предвидува дека глобалниот пазар за приватна безбедност, во согласност со податоците на Меѓународната организација на трудот од Женева (International labor organization) и Меѓународната стандардна индустриска класификација (International Standard Industrial Classification) вработува околу 20 милиони луѓе ширум светот, а ќе се зголеми експоненцијално со значителна стапка од 6 % во текот на периодот помеѓу 2023 и 2030 година.³

Врз основа на статистичките податоци на глобално ниво, од вкупниот број лица вработени во приватната безбедносна индустрија, за потребите на своите работни задачи, речиси 50 % се вооружени. Околу 66 % од вкупниот број вработени во приватната безбедносна индустрија се вработени во Европа, во САД и во Азија.⁴ Податоците говорат дека поголем број лица се вработени во приватната безбедносна индустрија отколку во државните полициски сили. Ваков тренд се бележи во НР Кина, во Индија, додека соодносот службеници на јавната безбедност (полиција) и вработени во приватниот безбедносен сектор е највисок во Латинска Америка

2 Cunningham, V.C., Strauchs, J.J., Van Meter, C.V. (1990) The Hallcrest Report II Private Security Trends (1970 to 2000) Chapter 6: Security Market Analysis. Hallcrest Systems Inc.

3 Fortune Business Insights. Key market Insights, достапно на: <https://www.fortunebusinessinsights.com/private-security-market-107006>

4 Private Security Market by Qualitative Analysis [2023-2030], достапно на: <https://www.marketwatch.com/press-release/private-security-market-by-qualitative-analysis-2023-2030-by-360marketupdatescom-2023-06-10>

1:4,6.⁵ По стабилизација на општествата од налетот на пандемијата, пазарот на приватна безбедносна индустрија има тенденција на пораст со стабилна стапка и со зголемено ниво на усвојување стратегии од страна на клучните играчи, при што се очекува пазарот да го престигне проектираниот приходен праг во текот на 2023-2030 година, со раст од 4,81 % во текот на предвидениот период.⁶

Во контекст на актуелните случувања, порастот на побарувачката за приватно обезбедување на пазарот е придвижена од неколку фактори. Овие фактори се од политичка, од економска, од општествена, од безбедносна и од еколошка природа и претставуваат двигатели на трендовите што ја одбележуваат функцијата на приватната безбедносна индустрија.⁷ Значи приватната безбедносна индустрија еволуира и зазема форма што е условена од трендовите на пазарот, кои пак се дериват на низа комплексни процеси и релации што имаат општествен, политички, безбедносен, економски и еколошки карактер и што ги диктираат стандардите во постапките, во процедурите и во протоколите во работата на приватната безбедносна индустрија.⁸

Пред да се соочи студијата со јавноста треба да нагласиме дека во оваа студија се содржани резултатите од истражувач-

5 Y. Hu, S. Liu, T. Abdelzaher, M. Wigness and P. David, “On Exploring Image Resizing for Optimizing Criticality-based Machine Perception,” *2021 IEEE 27th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, Houston, TX, USA, 2021, стр. 169-178, достапно на: 10.1109/RTCSA52859.2021.00027.

6 Private Security Market Growth | 2030. Published: June 16, 2023 “Private Security Market” [2023-2030] Research Report Analysis and Outlook Insights

7 Economics of Security: Facing the Challenges. A Multidisciplinary Assessment. European Network and Information Security Management. Report 2012.

8 Schepers, D., Ranganathan, A., Mathy Vanhoef M. (2021) Let numbers tell the tale: measuring security trends in wi-fi networks and best practices. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21). Association for Computing Machinery, New York, NY, USA, стр. 100–105, достапно на: <https://doi.org/10.1145/3448300.3468286>

киот предлог што го поддржа Комората на РСМ за приватно обезбедување, а го реализираше тим во состав: проф. д-р Оливер Бакрески, проф. д-р Тања Милошевска, д-р Лета Барчиева Миовска и м-р Благојчо Спасов. Студијата немаше да биде сеопфатна без ангажманот на м-р Сања Керметчиева во дистрибуција на истражувачкиот материјал до членките на Комората, а особено благодарност изразуваме за ангажманот на рецензентите проф. д-р Јасмин Ахиќ и проф. д-р Желимир Кешетовиќ при рецензирање на оваа студија и за изнесените позитивни оценки за квалитетот на трудот.

Скопје, септември 2024

Од авторите

Глава I

ПРИВАТНА БЕЗБЕДНОСТ – ТЕОРИЈА И КОНЦЕПТ

1. ПРИВАТНАТА БЕЗБЕДНОСТ КАКО КОНЦЕПТ

Во денешниот свет чија клучна карактеристика е брзиот развој, и е евидентна комодификацијата на безбедноста како јавно добро и улогата на државата во нејзината традиционална улога да се фокусира на обезбедување на потребното ниво на безбедност за нејзините граѓани, сепак важноста на приватната безбедност не може да не биде земена предвид. Од заштита на корпоративните средства до обезбедување настани, обезбедување на критичната инфраструктура итн., приватната безбедност игра клучна улога во современото општество. Овие приватни безбедносни актери служат како проактивни ентитети, пополнувајќи ги празнините во безбедноста што јавните безбедносни субјекти за спроведување на законот можеби не ги покриваат сеопфатно. Нивната улога опфаќа мноштво аспекти што значително придонесуваат за остварување безбедност и заштита во заедниците, бизнисите, настаните и други поставки.⁹

Несомнено, една од клучните предности на приватната безбедност е нејзината приспособливост. Приватните безбедносни компании нудат низа услуги приспособени на уникатните потреби на нивните клиенти. Без разлика дали се работи за заштита на компании, обезбедување лична заштита за поединци од висок профил или обезбедување специјални настани, приватната безбедност може да се приспособи за да се исполнат специфичните барања, што е доказ за професионалноста на секторот и сериозноста на предизвиците што ги решава.¹⁰

9 Deatherage, R. H. (2021). *Security operations: an introduction to planning and conducting private security details for high-risk areas* (Second edition). CRC Press, достапно на: <https://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9781000387438>

10 Contemporary Threats to National and International Security, and Appropriate Security Measures. Slovenia in NATO, достапно на: <http://nato.gov.si/eng/topic/threats-to-security/>

Професионалноста на приватниот безбедносен сектор се мери низ призмата на клучните индикатори за изведба, што се мерат преку: заштита на јавноста од неговото работење, заштита на јавноста преку ефективни активности за усогласување со регулативата и нејзиното спроведување, ефикасно и ефективно лиценцирање, но и организација фокусирана на потребите на клиентите.¹¹

Суштината на приватните безбедносни субјекти не е само во зголемување на постоечката безбедносна структура, туку и проактивно идентификување и ублажување на потенцијалните ризици и закани по безбедноста. Услугите што ги нуди приватниот безбедносен сектор се во насока на обезбедување дополнителен слој на заштита на органите за спроведување на законот, специјализирани за проактивен и превентивен пристап.¹²

Имајќи ја предвид големата разновидност на специфични безбедносни услуги што ги нуди приватниот безбедносен сектор, останува да се заклучи дека во рамките на овие безбедносни услуги се вградени актуелните и современи безбедносни барања, што диктираат модификација на „полициските“ активности, односно функциите на приватното обезбедување се многу слични на оние на јавната, односно државната полиција при управување со безбедносните ризици.¹³

Со проширувањето надвор од конвенционалните мерки за спроведување на законот, приватното обезбедување ги пополнува клучните празнини, особено во областите каде што јавните безбедносни институции и органи на државната управа можат да се соочат со ограничувања во физичката покриеност на терен или времето на одговор.¹⁴

11 Бела книга за приватното обезбедување. (2019). *Комора на PCM за приватно обезбедување*. Скопје.

12 Abrahamsen R., Leander A. (2015) *Routledge Handbook of Private Security Studies*. Routledge, Taylor & Francis Group London ^ New York.

13 Williams B. (2022). *Private Security: An Effective Method to Prevent Being a Crime Victim*. Mises Institute. Austrian Economics, Freedom and Peace.

14 Cook P. J. (2009). *Crime Control in the City: A Research-Based Briefing on Public and Private Measures*. Duke University and National

Значи приватното обезбедување го олицетворува овој проактивен став со поттикнување чувството на безбедност преку видливо одвраќање, но и со обученост и опременост за брзо справување со новите закани. Овој проактивен пристап е клучен за справување со огромен број безбедносни предизвици со кои се соочува модерното општество, а со тоа значително придонесува за севкупната безбедност и благосостојба на заедниците и институциите.¹⁵

2. ЗНАЧЕЊЕ НА ПРИВАТНАТА БЕЗБЕДНОСТ

Значењето на приватната безбедност може да се согледа во низа аспекти на нејзиното дејствување како дејност, при што дејноста приватно обезбедување се етаблира како есенцијална компонента во севкупниот безбедносен систем на општеството.¹⁶

Значењето на приватната безбедност се лоцира примарно во капацитетот да ја подобри целокупната безбедносна состојба во современото живеење, да обезбеди специјализирана заштита и да ги надополни напорите за остварување на јавната безбедност, придонесувајќи за побезбедно и поуредено општество. Клучните точки што го истакнуваат значењето на приватната безбедност таксативно се наведуваат во согласност со идентификуваните придобивки и се идентификуваат преку:

- *Надодолнување на јавниот систем за спроведување на законот*, што подразбира дека приватните безбедносни фирми често работат заедно со јавните безбедносни институции за спроведување на законот, нудејќи дополнителни ресурси и специјализирани услуги. Оваа соработка помага да се решат недостатоците во полицијата, особено во обла-

Bureau of Economic Research. *Cityscape: A Journal of Policy Development and Research*, Volume 11, Number 1.

¹⁵ Eser A. (2024.) Global Private Security Industry Statistics: \$257 Billion Market Projection. Worldmetrics.org Report 2024.

¹⁶ Buzatu, A. (2024). *Towards an international code of conduct for private security providers : a view from inside a multistakeholder process*. Ubiquity Press.

стите со ограничено полициско присуство, најчесто предизвикано од буџетски ограничувања.¹⁷

- *Превенција и спречување криминал* што се согледува преку присуството на персонал за приватно обезбедување што се перцепира како когнитивна бариера во интенцијата за извршување криминални активности. Физичкото присуство на персоналот, системите за надзор и патролите можат значително да ја намалат веројатноста за злосторства како што се кражби, вандализам и неовластен пристап.¹⁸
- *Обезбедување специјализирани услуги за заштита* приспособени на потребите на различни сектори, вклучувајќи корпоративно обезбедување, заштита на станови, обезбедување настани итн. Ова приспособување осигурува дека специфичните безбедносни проблеми се соодветно адресирани.
- *Брза реакција и управување со инциденти*, што се согледува преку ангажманот на персоналот на приватното обезбедување во хронологијата на настаните каде често претставува прв одговор на инцидентите што настануваат во просториите што тие ги штитат. Нивната способност брзо да управуваат и да ги ублажат ситуациите може да спречи ескалација и да ја намали штетата или опасноста.¹⁹
- *Технолошката интеграција* подразбира дека приватните безбедносни фирми во својата работа користат напредни технологии интегрирани во системите за надзор CCTV, системите за контрола на пристап, алармните системи и мерките за сајбер-безбедност. Овие технологии го подобруваат надзорот, следењето и целокупното управување со безбедноста.²⁰

17 Wiśniewski, R. (2018). Notion of strategic national security management. *Security and Defence Quarterly*, 20(3), стр. 18-41, достапно на: <https://doi.org/10.5604/01.3001.0012.4887>

18 Bureš, O. (2015). *Private security companies : transforming politics and security in the Czech Republic*. Palgrave Macmillan, достапно на: <https://doi.org/10.1057/9781137477521>

19 Clarno A. (2017). *Neoliberal Apartheid*. The University of Chicago Press, Chicago, 2017.

20 Galaby, A. A. R., & Abdrabo, A. A. (2021). *Handbook of research on creative cities and advanced models for knowledge-based urban*

- *Економски придобивки* што ги создава приватната безбедносна индустрија овозможува бројни можности за вработување, придонесувајќи за економијата. Исто така, им овозможува на бизнисите да работат во побезбедни средини, што потенцијално ќе доведе до зголемена продуктивност и економски раст.
- *Заштита на средства и информации.* Приватното обезбедување помага да се заштитат вредните средства, вклучувајќи ја и физичката сопственост, интелектуалната сопственост и чувствителните информации. Оваа заштита е од клучно значење за бизнисите, владините институции и поединците.²¹
- *Приспособено управување со ризик* значи дека приватните безбедносни фирми што нудат услуги за проценка и управување со ризик, им помагаат на клиентите да ги идентификуваат потенцијалните закани и ранливости. Овој проактивен пристап овозможува развој на приспособени безбедносни планови за ублажување на ризиците.²²
- *Поддршка за организирање големи настани на јавни простори* значи дека обезбедувањето на големи настани, како што се концерти, спортски настани и јавни собири, често е управувано од приватното обезбедување. Нивната експертиза гарантира безбедност на присутните и непречено функционирање на настанот.²³

development. IGI Global, Engineering Science Reference, достапно на: <https://doi.org/10.4018/978-1-7998-4948-3>

21 Miyazawa Koichi. (1995). *Crime prevention in the urban community*. Brill Nijhoff; Kluwer law and taxation publishers, достапно на: <https://brill.com/view/title/10986>

22 Delgado G. V., Castro-Toledo F. J. (2020). Urban security and crime prevention in smart cities: a quantitative systematic review. *International E-Journal of Criminal Sciences*.

23 Bergin, A., William, D., & Dixon, C. (2018). SECURITY OFFICERS. In *Safety in numbers: Australia's private security guard force and counterterrorism* (pp. 10–19). Australian Strategic Policy Institute., достапно на: <http://www.jstor.org/stable/resrep23117.6>

- *Регулаторната усогласеност и професионалните стандарди* придонесуваат приватната безбедносна индустрија да е сè повеќе регулирана, при што од фирмите се бара да се придржуваат до строгите стандарди и барањата за лиценцирање. Оваа професионализација обезбедува повисок квалитет на услуги и одговорност.²⁴

3. ИСТОРИСКА ГЕНЕЗА НА ПРИВАТНАТА БЕЗБЕДНОСТ

Потребата за безбедност е суштинска за човековиот опстанок и е присутна од почетокот на настанокот на човештвото. Како што еволуирало човековото постоење, паралелно се јавувала потреба од развивање одредени форми на заштита со што постепено се развивала и безбедноста што ја остварувале човековите заедници.²⁵

Археолошките ископувања и историските докази покажуваат дека и најпримитивниот човек бил загрижен за неговата безбедност и дека развил рудиментарни безбедносни техники. Пештерните цртежи и други докази јасно демонстрираат дека заштитата и примената на првобитни општествени норми навистина постоела од почетокот на човештвото. Со задоволување на овие потреби, оттогаш па натаму, човекот ја развил наједноставната модерна јавна безбедност и приватна безбедност. Развојот на овие форми на безбедност, денес со различни и одделни функции, покажува дека во минатото често биле испреплетени, дури и неразделни.²⁶

Значи појавата на приватната безбедност е обликувана од различни историски, социјални и економски фактори. Клучните случувања што придонесуваат за подемот на приватната безбед-

24 Wakefield A. (2002) The Public Surveillance Functions of Private Security. Surveillance and Society.

25 Churchill, D., Janiewski, D., Leloup, P., & Stenning, P. C. (2020). *Private security and the modern state historical and comparative perspectives*. Routledge, Taylor & Francis Group, ESSHC Valencia.

26 Бакрески, О., Ахик Ј., и Наѓ И., оп. цит.

ност се поделени во согласност со историските околности, каде се детектираат раните форми на приватна безбедност и современите трендови, што подразбираат урбанизација на општествата, подем и пораст на корпорациите и аналогно на тоа, потребата од комерцијална безбедност наспроти зголемувањето на стапките на криминал во сите негови форми.²⁷

Според историската фактографија, тоа што се нарекува приватна безбедност како форма на организирање и дејствување е всушност постар облик на организација од јавната полиција. Имено, првите полициски оддели како формални владини органи во функција на спроведување на законот со територијални надлежности се формирани во XIX век. Првата полициска станица е основана во Обединетото Кралство, со актот за основање на полициската служба Метрополитен во Лондон во 1829 година.²⁸

Првите пишани историски наоди потекнуваат од Антички Египет. Таму, големите фараони и нивните дворски службеници ангажирале приватно обезбедување за да се заштитат себеси и својот имот. Фараонот Рамзес II, во 1300 п.н.е., приватно ангажирал Нубијски Мецаи, Сиријци, либиски и сардински војни за да ги надополнат неговите официјални воени и полициски сили, како еден конкретен пример.²⁹

Античките Грци развиле софистициран систем на безбедносни сили за да ги заштитат офисијалните лица од никакви и криминалци што ги пљачкале и нив и патниците по јавните патишта што воделе во големите градови. Раните форми на приватно обезбедување и концептот на приватно обезбедување од

27 George, B., Kimber, S. (2014). The History of Private Security and Its Impact on the Modern Security Sector. In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, London, достапно на: https://doi.org/10.1007/978-1-349-67284-4_2

28 The establishment of the Metropolitan Police. 2024 BBC, достапно на: <https://www.bbc.co.uk/bitesize/guides/z9f4srd/revision/4>

29 Clark, R. (2019). *Securing eternity : ancient Egyptian tomb protection from prehistory to the pyramids*. The American University in Cairo Press, достапно на: <https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2518978>

периодот на античко време се карактеризира кога богатите поединци и трговци вработувале чувари за да ги заштитат своите имоти. За разлика од античките Грци, римските императори имале преторијанска гарда, а римските владетели од источното византиско Римско Царство најмувале чувари да ги штитат нивните семејства и имоти, додека средновековните трговци ангажирале приватни милиции.³⁰

Со текот на времето постепено доаѓа до раст и развој на приватната безбедност. Првенствено, периодот на индустриската револуција и рапидната индустријализација од XVIII и XIX век довела до значителна урбанизација и раст на целокупното производство. Поради тоа, фабриките, магацините и транспортните мрежи имале потреба од заштита од кражби, што довело до создавање приватни безбедносни сили.³¹

Во контекст на генезата на приватната безбедност, првите примери на дејноста приватно обезбедување каква што се одвива во денешни услови се забележуваат во средината на XIX век. Националната агенција за детективи основана од страна на Алан Пинкертон во 1850 година во Чикаго во Соединетите Држави, што обезбедувала низа безбедносни услуги, вклучувајќи приватна полиција и истражна работа е прва од овој вид,³² додека пак, регулацијата на приватната безбедносна индустрија се бележи дека официјално започнала во 1915 година, кога станало задолжително лиценцирањето на приватните истражители во сојузната држава Калифорнија.³³

Останува да заклучиме дека од самите почетоци на развојот на човештвото се развива и се истакнува улогата на приватна безбедност за подоцна во современото општество да говориме

30 Schreier, F. and Caparini, M. (2004). *Privatising Security*. Geneva: DCAF.

31 Draper, H. (1978). *Private Police*. Brighton: Harvester.

32 Percy, S. (2007). *Mercenaries: The History of a Norm in International Relations*. Oxford: Oxford University Press.

33 Blackstone, E. A., Hakim, S., & Meehan, B. J. (2023). *Handbook on public and private security*. Springer, достапно на: <https://doi.org/10.1007/978-3-031-42406-9>

за приватната безбедност што обезбедува различни потреби и претставува суштинска компонента на севкупната безбедносна структура, суплементарна на јавната безбедност и олицетворена во државно финансираните полициски сили.³⁴

4. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ ОКОЛУ ПОИМОТ И УПОТРЕБАТА НА ТЕРМИНОТ ПРИВАТНА БЕЗБЕДНОСТ

Добра аналогија за приватната безбедност е познатиот брег со високопрофитабилниот униформиран сектор малку над површината и остатокот од индустријата долу под површината. Значи има многу различни перцепции околу тоа што опфаќа приватната безбедност што во основа го прави нејзиното дефинирање многу потешко. Исто така, има многу сиви области на маргините, што може, а и не мора да бидат земени предвид од различни поединци и организации во опсегот на приватната безбедност. Оттука има многу пречки за да се создаде прифатлива дефиниција за приватна безбедност.³⁵

За да дојдеме до вистинската дефиниција за приватната безбедност треба најнапред да се исцрта линија што ќе покаже каде завршува приватната безбедност, а каде почнуваат другите области. Дали извршителите како агенциите за кредитни референци и инсталаторите на противпожарните аларми ќе бидат вклучени, на пример? Оваа листа може да биде проширена на неколку страници и може да направи еднакво убедливи случаи за да ги вклучи и нив, или да ги исклучи од приватната безбедност. Предизвикот е да се најде лепеза на зборови што е доволно широка за да ги опфати сите релевантни сектори, без притоа да биде толку широка за да ја уништи прецизноста на дефиницијата. Според тоа,

34 Krahmann, E. (2010). *States, Citizens and the Privatisation of Security*. Cambridge: Cambridge University Press.

35 Bruce G. and Button Mark, *Private Security*, Palgrave Macmillan, New York, 2004, стр. 7-10.

зборот приватна безбедност е употребуван во широк контекст и токму оваа поширока употреба создава потешкотии околу обидите за негово дефинирање. Како дополнителен проблем во неговото дефинирање се јавуваат терминолошките дивергенции околку поимот и употребата на приватната безбедност и на приватната безбедносна индустрија. По правило, приватната безбедносна индустрија значи исто што и приватната безбедност. Сепак, можеби би било покорисно во овој момент да правиме одредена разлика меѓу „приватна безбедносна индустрија“ и „приватната безбедност“, затоа што првата ги опфаќа сите оние поединци и организации што произведуваат и обезбедуваат „приватно-безбедносни продукти“, додека втората се состои од самите производи и услуги.³⁶

Експертите и теоретичарите во оваа област немаат постигнато консензус околу дефинирањето на приватната безбедност и околу тоа што претставува приватно обезбедување, па оттука, се среќаваат бројни различни дефиниции користени во претходните истражувања. Разликите во дефинициите имаат тенденција да го елаборираат фокусот на работните задачи, влијанието на профитот и клиентот, како и производство, дистрибуција и монтажата на безбедносната опрема и технологија.³⁷

Со цел поимно определување на приватната безбедност, понудени се релевантни дефинициски пристапи во насока на теориската експликација на приватната безбедност во однос на колокацијата, дејноста, функцијата и регулацијата на лицата што вршат приватна безбедност и субјектите што нудат услуги од приватната безбедност.³⁸ Оттука приватната безбедност може да биде разбрана и како независна или сопственичка комерцијална

³⁶ Исто., стр. 7-19.

³⁷ Hansen Löfstrand, C. (2021). The everyday reality of private security work in Sweden: negotiations at the front line of public order maintenance. *Policing and Society*, 34(1-2), 59-74, достапно на: <https://doi.org/10.1080/10439463.2021.1998049>

³⁸ Avant, D. D., & Sigelman, L. (2006). *Globalization, private security, and democratic processes : implications for the democratic peace*. Research Group in International Security = Groupe d'étude et de recherche sur la sécurité internationale.

организација чии активности вклучуваат обезбедување на имотот на коминтентот што ги ангажирал, потоа заштита на човечки животи до итен одговор на инциденти, вршење истраги за минатото на вработените, изведба на функциите, детекција и истражување криминал и криминалци, како и изнесување престапници на распит,³⁹ односно приватната безбедност ги опфаќа концептите и техниките што можат да се применат во различни истраги вклучувајќи измама, осигурување, приватност и криминал. Тоа се детали на собирање и зачувување докази, начин на постапување на сведоците, техники на надзор, истраги во заднина.⁴⁰ Значи приватната безбедност во себе ги содржи сите видови приватни организации и поединци што нудат услуги поврзани со безбедност, вклучувајќи истраги, распоредување на клучни позиции, патроли, извршна заштита, алармен мониторинг и одговор, како и вооружен транспорт. Во споредба со ваквата аргументација, Бирн смета дека приватната безбедност е конституиент на масовен ресурс што содржи ветувачки потенцијал во доменот на поддршка на државата во превенцијата и редукцијата на криминалот, додека припадниците на приватното обезбедување се на „првата линија“ заедно со полицијата во заштита на имотот и сопственоста. Приватната безбедност не е финансирана од јавни средства, туку остварува профит со давање на своите услуги.⁴¹

Во аргументацијата на Ли во контекст на криминолошката дефиниција и кривичното право, приватно обезбедување значи обезбедување од лице што не е јавен службеник за заштита или чување луѓе и/или имот,⁴² додека за австралискиот автор и експерт Вилијамс, работниците за приватно обезбедување се „очите и

39 <https://www.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary..>

40 Nemeth P. Ch., *Private Security and the Investigative Process*, Taylor&Francis, 2010, pp.5-25.

41 Report of the Task Force on Private Security. National Advisory Committee on Criminal Justice Standards and Goals. Washington 1976.

42 Lee, S.(. (2021). Security: Private. In: Shapiro, L.R., Maras, M.H. (eds) *Encyclopedia of Security and Emergency Management*. Springer, Cham. https://doi.org/10.1007/978-3-319-70488-3_242

ушите“ на терен; тие се во секојдневен контакт со заедницата и, кога ќе се случи инцидент, тие се вистинските први одговорни: во оддалечување на случајните минувачи, набљудување, известување, примена на прва помош и информирање на службите за итни случаи, пријавување сомнителни активности и обезбедување вредни информации што можат да помогнат во спречувањето на криминалот. Исто така, тие често играат клучна улога во истрагите, обезбедувајќи снимки од надзор или изјави на сведоци, што можат да бидат клучни во решавањето на злосторствата. Владиниот сектор, приватниот сектор, како и јавноста се потпираат на овие лица за да ги заштитат нив и нивните средства.⁴³

Ханс-Херман Хоп смета дека приватната безбедност го има потребниот примат и дека е најдобро осигурувањето на безбедноста да му се довери на приватниот безбедносен сектор. Тој тврди дека приватните фирми за обезбедување имаат посилен поттик да ги заштитат своите клиенти, бидејќи нивната репутација и континуиран бизнис зависи од тоа. Спротивно на тоа, државната полиција не е одговорна пред поединците што треба да ги заштити и затоа има помала стимулација да ги заштити ефективно.⁴⁴

За Немет, приватната безбедност претставува состојба на заштита од опасности, закани, ризици и загуби од екстерни извори, односно состојба не само на безбедност, туку и обезбеденост.⁴⁵

Во тој контекст се размислувањата и на глобалната заедница на безбедносни практичари АСИС (ASIS) од 2023 година, според кои приватната безбедност подразбира одржување на редот, на економски заштитни системи, заштита на бизниси, технолошка безбедност, информатичка и сајбер-безбедност, како и персона-

43 Williams, D. (2018) The Role of Private Security in Counter Terrorism. Security Solutions, достапно на: <https://www.securitysolutionsmedia.com/2018/12/10/role-private-security-counter-terrorism/> [27.07.2024]

44 Hoppe, H. H. (2009) The Private Production of Defense. Ludwig von Mises Institute.

45 Nemeth, C.P. (2022). Private Security: An Introduction to Principles and Practice (2nd ed.). CRC Press, Boca Raton, достапно на: <https://doi.org/10.4324/9781003217299>

лот во оваа индустрија,⁴⁶ додека извештаите на РАНД (RAND) за 2024 година, ја карактеризираат приватната безбедност како сите видови активности за заштита и превенција на загуба и штета што не се извршувани од страна на органите за спроведување на законот.⁴⁷ Истовремено, во концептот за стратегиско управување со безбедноста, приватната безбедност се перцепира како градивен елемент во контурирањето на националната безбедност, односно оваа дејност е неизоставна и интегрално дејствува во комбинација со силите за јавна безбедност во гарантирањето на националната безбедност.⁴⁸

Постојат дефиниции што не се изненадувачки, а се базирани врз листа на услуги што ги дава приватната безбедност, затоа што приватната безбедност подразбира овозможување услуги поврзани во безбедносната сфера од страна на невладини економски субјекти што овие услуги ги вршат за профит. Современиот тренд на инкорпорирање на приватниот безбедносен сектор во владините договори за одржување на безбедноста отвора место за нивна понатамошна експанзија на пазарот. Се добива впечаток дека потребата за безбедност постојано расте.⁴⁹

Од презентираниите дефиниции јасно се гледа дека одредени автори го фаворизираат поимот приватна безбедност што се покажа дека е или премногу широк или премногу тесен. Други автори го нудат концептот на приватна безбедност што го поврзуваат со давање безбедносни услуги и производи, а трети сметаат дека приватната безбедност значи обврска да се извршуваат одредени задачи на начин што ќе му овозможи на клиентот да има доверба дека нема да биде загрозувана неговата безбедност или дека ќе треба овој сектор да плати значителни штети поради однесувањето на

46 ASIS International 2023 Annual Report. <https://www.asisonline.org/>

47 Private Military and Security Companies Newsletter Latest Issue: June 2024. RAND National Security Research Division.

48 National Security Strategy of the Republic of Serbia. Belgrade, October 2009, достапно на: <http://www.voa.mod.gov.rs/documents/national-security-strategy-of-the-republic-of-serbia.pdf>

49 <http://www.cops.usdoj.gov/Default.asp?Item=2034>

приватното обезбедување.⁵⁰ Одредени размислувања одат во насока дека приватната безбедност преку компаниите за приватно обезбедување се чувари на луѓето, имотот и информациите, додека други се осврнуваат на проучување и анализа на нормативните, етичките и регулаторни димензии на приватните компании за обезбедување,⁵¹ а во дефинициите преовладува и грижата за превенција на криминалот, за превенција на загубата, за редукција на загубата, за сигурноста, за редукција на ризикот. Има ставови со кои се менува фокусот на примарната активност и функција на приватната безбедност во насока на идентификација на пристапите за обезбедување што, исто така, придонесува во одредена мера за да го подобри нашето разбирање од што е конституирана приватната безбедност.

Општата констатација е дека приватната безбедносна индустрија бележи раст на побарувачката и софистицираноста во последните неколку децении. Ова се должи на зголемената употреба на технологијата, како што е затворено коло на телевизија и ласерската технологија, како и обуката на безбедносниот персонал за искористување на овие технологии. Приватните станбени и деловни случувања се дизајнирани имајќи ја предвид безбедноста.⁵²

5. ДЕТЕРМИНИРАЊЕ НА ОПСЕГОТ НА ПРИВАТНАТА БЕЗБЕДНОСТ

При детерминацијата на опсегот на приватната безбедност, методологијата за нејзиното утврдување опфаќа широк спектар на услуги што се сведуваат на активности за заштита

⁵⁰ *Corrections, Public Safety and Policing: Private Investigator and Security Guard Training Manual*, Ministry of Justice and Attorney General of Canada, 2008, стр. 5-10.

⁵¹ Krahmann E. and Leander A., *Private Military and Security Companies: Transforming Security Governance?* 2003, стр. 1.

⁵² Restitution in Theory and Practice. in Volume 12, Number 1 (1996) of the *Journal of Libertarian Studies*

на луѓето, имотот и информациите.⁵³ Тоа подразбира заштита на вработените, видеонадзор, контрола на пристап, процена на ризик и мерки за сајбер-безбедност. Притоа наведените услуги не се ограничени на традиционално обезбедување, туку се прошируваат на специјализирани области како што се безбедност на настани, консултантски услуги за управување со ризик, како и симулации за обука.⁵⁴ Со видоизменувањето на криминалот и софистицираноста на прекршоците и кривичните дела, каде, на пример, спаѓаат заканите како сајбер-нападите и тероризмот, се потенцира потребата на личната безбедност на високопрофилни личности (ВИП-личности, политичари, државници, итн.).⁵⁵ Понатаму, приватното обезбедување дејствува како клучен суплемент на јавните органи за спроведување на законот. Тие честопати се првите што реагираат во итни ситуации, играјќи витална улога во спречувањето и давањето соодветен одговор на криминалот.⁵⁶

Неопходно е да се напомене и аспектот на технолошка интеграција во приватното обезбедување. Интеграцијата на технологијата ја зајакнува приспособливоста на приватниот безбедносен сектор. Како илустративен пример ќе ги земеме меѓународните саеми и конференции за приватно обезбедување на кои може да се согледа видлива трансформација во нивните понуди, каде паметните технолошки решенија сè повеќе ги заменуваат продуктите на физички бариери за заштита од упад, како што се оградите, бариерите, капиите и сл. Во таа насока, важно е да се забележи дека воведувањето на новите технологии и способности веројатно нема да биде униформно во регионите

⁵³ Williams, K. (L. I. C. (2017). *Criminology*. Oxford University Press.

⁵⁴ Lee A. (2023) Private Security: Trends and Innovations. AGS Inc., достапно на: <https://www.agsprotect.com/blog/private-security-trends-and-innovations>

⁵⁵ Crime, Justice and the Law. Security Industry Authority, достапно на: <https://www.gov.uk/browse/justice>

⁵⁶ Bernard V. (2024) *How Technology is Changing Private Security*. Private Security Conversations. ICoCa

или во земјите поради различни фактори и пречки.⁵⁷ Одредени земји, како Кина, се далеку понапред во согласност со статистиката, бидејќи домашните технологии станаа широко достапни и за домашна употреба и за извоз. Во други земји се забележуваат одредени политичко-општествени бариери за усвојувањето на технологијата: компаниите често не сакаат или не се во можност да ги задолжат своите вработени со опрема како таблети, паметни телефони и сл., како резултат на трошоците за имплементација, ниската дигитална писменост меѓу вработените во приватното обезбедување или неподготвеноста на клиентите да платат повеќе за безбедносни услуги овозможени со технологијата итн.⁵⁸

Современите безбедносни решенија комбинираат работна сила и технолошки алатки, како што се: системите за видеонадзор, дигитални системи за контрола на пристап и софистицирани алармни системи. Пристапот на приватните безбедносни актери за инкорпорирање напредни технологии во нивните услуги го илустрира овој тренд. Користењето дигитални алатки ја подобрува ефикасноста на безбедносните операции и обезбедува робустен механизам за превенција, следење и одговор на безбедносни инциденти.⁵⁹

Значи дигиталните решенија како автоматизиран надзор и аналитика на податоци нудат значителни подобрувања, овозможувајќи подинамични и поактивни безбедносни мерки. Оваа промена не само што го одразува технолошкиот напредок, туку и промената на пејзажот на заканите, каде брзото приспособување и технолошката интеграција стануваат клучни за ефективна безбедност.⁶⁰ Како што се наведува во хрватскиот

57 Bakreski O., Bardjieva M. L. (2023) The Need for an Integrated Approach in the Operation of Private Security Companies, *Security Dialogues* / Vol. 14, No. 1, 2023.

58 Blackstone, E. A., Hakim, S., & Meehan, B. J. (2023). *Handbook on public and private security*. Springer, достапно на: <https://doi.org/10.1007/978-3-031-42406-9>

59 Benedict A. B. (2023) Private Guards and National Security: Issues, Challenges and Opportunities/Prospects. Author House, UK.

60 Meurant, G. (2014). *CCTV Surveillance : Video Practices and Technology*. Elsevier Science. <http://qut.eblib.com.au/patron/FullRecord.aspx?p=1838151>

магазин „Заштита“, глобалниот пазар на видеонадзор покажува значителен раст и се карактеризира со висок степен на иновација и бројни производители на технологија. Новиот извештај дава клучни сознанија за овој пазар и обезбедува вредни насоки и за купувачите и за корисниците. Во согласност со анализите на овој водечки магазин, според новиот извештај на ИДК (IDC), водечки снабдувач на глобални ИТ- истражувања и консалтинг, мултинационалната компанија „аксис“ (Axis), основана во 1984 година со седиште во Лунд, Шведска, е прогласена за „водечки снабдувач на камери за видеонадзор во светот“ со вкупна продажба од 1,6 милијарди долари во 2023 година.⁶¹

6. РЕГУЛИРАЊЕ И СТАНДАРДИЗАЦИЈА НА ДЕЈНОСТА ПРИВАТНО ОБЕЗБЕДУВАЊЕ

Приватната безбедност несомнено станува неопходност, и оттука паралелно се развива и потребата за соодветно регулирање на оваа дејност и утврдување на професионалните стандарди во оваа сфера.⁶²

Во таа насока, важно е да се истакне дека постои генерален универзално акцептиран консензус околу фактот дека активностите на приватните безбедносни субјекти мора да се целосно регулирани и се вршат напори на национално и на меѓународно ниво со кои до крај се утврдуваат нивните активности, овластувања и санкции при лошо постапување. Овој вид супранационална регулатива што ги инкорпорира овие сегменти треба да содржи пропис на ангажманот на приватното обезбедување и нивна контрола од

61 AXIS Communications. Improving security and business performance. For a smarter, safer world, достапно на: <https://www.axis.com/about-axis>

62 Born H., Caparini M. Cole E. (2007) Regulating Private Security in Europe: Status and Prospects. Geneva Centre for the Democratic Control of Armed Forces (DCAF) Policy Paper – №20, достапно на: https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf

извршната власт, законодавен надзор и правна ревизија. Понатаму, одредени законски рамки што се однесуваат на државните безбедносни органи и тела, треба да се мандаторни и за приватниот безбедносен сектор.⁶³

Во основа, регулативата е од суштинско значење во поглед на законското работење на фирмата/компанијата и соодветното регулирање значи дека ќе се покрие една премногу чувствителна област во оваа сфера. Регулативата, исто така, може да помогне за подобро да се согледаат одредени состојби со што би се обезбедило што е можно подобро и порационално да се стават во функција сите ресурси. Од ова произлегува дека регулативата е клучен и корисен елемент во работењето на самата фирма/компанија што им помага на раководните тимови да воспостават соодветен баланс меѓу остварените и планираните активности. Без соодветна регулатива тие ќе се претворат во слепи набљудувачи на процесот што може да доведе до отстапувања на планираните цели и задачи и ќе бидат ограничени без можност да го коригираат, а со тоа и да го подобрат своето работење, како и работењето на приватниот субјект. Со други зборови, прописот може да се толкува како обичен формален механизам на контрола што е воспоставен со цел да се насочува однесувањето и да се обезбеди универзална примена на законот. Во принцип, поголема регулатива може да доведе до зголемена одговорност.⁶⁴

Постојната национална регулатива варира во квалитетот и ефикасноста во многу земји. Повеќето земји имаат донесено закони со многу недостатоци, а во некои земји законска регулатива воопшто и не постои. Во многу случаи легални се т.н. „сиви зони“ што вклучуваат и екстериторијални прашања и проблеми што се однесуваат на мешање на државните и на приватните актери што

63 Smith, R (2013). Supply and Demand: the Paradox of Private Security Companies in Libya. *Open Democracy*, [online], достапно на: <https://www.opendemocracy.net/en/supply-and-demand-paradox-of-private-security-companies-in-libya/> (28.03.2019)

64 O'Connor Lippert, Greenfield & Boyle, 'After the "Quiet Revolution": The Self-Regulation of Ontario Contract Security Agencies', *Policing & Society*, Vol. 14, No. 2, June 2004, стр. 153.

работат заедно. Ова значи дека секоја држава која на кој било начин е замешана во регулирање на приватната безбедност и на нејзините активности има потреба да ги развива законите што се релевантни за фирмите за обезбедување како и законите што би ги регулирале нивните активности.⁶⁵

Оттука важен елемент на регулацијата е да се утврди што е тоа што приватните компании за обезбедување можат или не смеат да го направат. Често овие одредби веќе постојат во други закони. На пример, во многу држави, граѓаните можат да бидат лишени од слобода. Тие права обично се дадени во општото законодавство. Важно е да се напомене дека, иако во повеќето држави, работниците за обезбедување не поседуваат никакви дополнителни посебни овластувања од пропишаните со закон, сепак тие се фигури на авторитетот облечени во униформа, што значи дека многу луѓе ќе ги исполнат нивните барања на кој било начин. Исто така, тие имаат предности во однос на обичните граѓаните на следните начини: во земји каде работниците за обезбедување го имаат граѓанското право да уапсат и да употребат сила за да спречат кривично дело, тие често се обучени и од нив се очекува да ги користат овие овластувања во одредени околности; работникот за обезбедување што работи на приватни простори често може да ги користи правата на сопствениците на земјиштето, на исклучување, и може да става услов за влез и да наметнува санкции поради прекршување на условите за влез; постои услов договорот за вработување на работникот за обезбедување што работи на места каде што ги заштитува вработените, во којшто се предвидуваат санкции за непочитување на процедурите за безбедност и тој често е *de facto* овластен да запира и да пребарува.⁶⁶

Генерално, регулативата може да придонесе за подобрување на професионализмот на приватните компании за обезбедување, но може да придонесе и кон зголемување на довербата на

65 Ahić J.: *Sistemi privatne sigurnosti*, Sarajevo, 2009, стр.20-42.

66 Button Mark, *Introductory Handbook on State Regulation concerning Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety*, United Nations Office on Drugs and Crime, New York, 2014.

јавноста.⁶⁷ Исто така, многу е важно во работата и во работењето приватното обезбедување да настојува да работи според строгите етички и професионални стандарди. Приватните безбедносни стандарди се однесуваат на упатствата, протоколите и најдобрите практики воспоставени за да се обезбеди ефикасност, доверливост и интегритет на приватните безбедносни компании и агенции.⁶⁸ Овие стандарди се дизајнирани да обезбедат рамка според која ќе работат приватните безбедносни компании, обезбедувајќи постојан квалитет, етичко однесување и отчетност и опфаќаат оперативни стандарди, стандардни оперативни процедури (СОП), што се однесува на развивање и имплементирање детални стандардни оперативни процедури за различни безбедносни сценарија, вклучувајќи контрола на пристап, одговор при итни случаи, известување за инциденти и патролни операции.⁶⁹ Тука спаѓаат и прописите и упатствата за употреба на сила, што подразбира воспоставување јасни правила и протоколи за соодветна употреба на сила, гаранција дека таа е пропорционална, неопходна и законски оправдана, како и стандарди за опремата што се користи, што подразбира гаранција дека целата безбедносна опрема и нејзината примена (на пример, камери за надзор, аларми, комуникациски уреди) ги исполнува индустриските стандарди за квалитет и доверливост и неопходноста од поседување на потребните лиценци, дозволи, обука на персоналот и ветинг при вработувањето и за време на вршење на дејноста.⁷⁰ Во стандардните оперативни

67 *Sourcebook on Security Sector Reform*, Fluri P., Hadžić M. (eds.) Geneva Centre for the Democratic Control of Armed Forces/Centre for Civil-Military Relations, Belgrade, Geneva/Belgrade, 2004, стр. 236-237.

68 Security Industry Authority, достапно на: <https://www.gov.uk/government/organisations/security-industry-authority/about>

69 Public or private security forces are not bound by rules of engagement or standard operating procedures. UNDP Business and Human Rights in Asia Bangkok Regional Hub United Nations, достапно на: <https://hrdd-assessment.org/public-or-private-security-forces-are-not-bound-by-rules-of-engagement-or-standard-operating-procedures/>

70 Commitments, Policies and Standards. Health, Security, Safety, the Environment (HSSE) and Social Performance (SP), достапно на: <https://>

процедури спаѓаат и протоколите за сајбер-безбедност, што подразбира усвојување сеопфатни мерки за сајбер-безбедност за заштита на чувствителните податоци и одржување на интегритетот на дигиталните системи што ги користи безбедносната агенција.

Сите наведени аспекти на стандардизирањето на дејноста приватно обезбедување во 2012 година се усвоени од страна на Организацијата на обединетите нации во рамки на нивните операции и претставуваат „цврсти“, односно обврзувачки елементи во договорите за ангажман на приватните безбедносни агенции/компаниј. ⁷¹ Понатаму, стандардот ANSI/ASIS PSC.1-2012 се надоврзува на документот од Монтре и Меѓународниот кодекс на однесување (ICoC) за давателите на приватни безбедносни услуги за да обезбеди барања и насоки за систем за управување за поддршка на квалитетна испорака на безбедносни операции и управување со поврзаните ризици, во согласност со почитувањето на човековите права, законските обврски и добри практики во услови на влошено општествено и административно владеење, каде владеењето на правото е поткопано поради човечки или природно предизвикани настани. ⁷² Меѓународната организација за стандардизација (ИСО – ISO) го воведува стандардот ISO 18788:2015 што претставува систем за управување со приватни безбедносни операции — барања со упатства за употреба. Овој меѓународен стандард обезбедува принципи според кои организациите што спроведуваат или склучуваат договори за безбедносни операции се обврзани да покажат: соодветен деловен капацитет и капацитет за управување со ризик за да се исполнат професионалните барања на клиентите и другите засегнати страни; како и процена и управување со влијанието на

www.shell.com/sustainability/our-approach/commitments-policies-and-standards.html

⁷¹ The Montreux Document on Private Military and Security Companies, достапно на: <https://www.montreuxdocument.org/about/montreux-document.html>

⁷² Management System for Quality of Private Security Company Operations Standard (PSC.1), достапно на: <https://www.asisonline.org/publications--resources/standards--guidelines/management-system-for-quality-private-security-company-operations/>

нивните активности врз локалните заедници; одговорност пред законот и почитување на човековите права; доследност со доброволните обврски на кои организацијата се потпишува.⁷³ На овој стандард се надоврзува и амандманот објавен во февруари 2024 година, ISO 18788:2015/Amd 1:2024 – Систем за управување со приватни безбедносни операции — барања со упатства за употреба/ Амандман 1: Промени во климатските активности, што подразбира дека релевантните чинители може да постават барања поврзани со климатските промени.⁷⁴ Исто така, стандардот BS 7499 – што е и британски стандард дава препораки за управување, екипирање и работење на организација што обезбедува услуги за обезбедување статична локација, со кој се наведуваат најдобрите практики за управување и испорака на овие услуги, ги дефинира признатите процедури, како и условите и предиспозициите што се однесуваат на безбедносните служби. Тоа им помага на приватните субјекти да ги применат своите ресурси со гаранција дека се поставени вистинските безбедносни мерки. Овој стандард не се однесува на сите безбедносни услуги, како на пример, услуги за заштита на готовина во транзит и други вредни пратки, блиска заштита, услуги за контрола на пристап, управување со настани и управување и функционирање видеонадзор.⁷⁵

Во изминатите три децении, приватното обезбедување забележува развој на програми за професионална обука и сертификати за унапредување и понатамошно подобрување на вештините и професионалноста на безбедносниот персонал. Како конкретен пример, организацијата АСИС интернешенел (ASIS International), основана во 1955 година, обезбедува сертификати, како што е сертифициран професионалец за заштита (Certified Protection

73 Management system for private security operations — Requirements with guidance for use, достапно на: <https://www.iso.org/obp/ui/en/#iso:std:iso:18788:ed-1:v1:en>

74 Институт за стандардизација на Република Северна Македонија, достапно на: <https://isrsm.gov.mk/mk/project/show/iso:proj:88403>

75 BS7499 – Static site guarding and mobile patrol service. Code of Practice, достапно на: <https://assets.publishing.service.gov.uk/media/5a7f8c08e5274a2e8ab4cd4e/BS7499.pdf>

Professional –CPP). Овој сертификат се доделува на менаџери за безбедност на повисоко ниво, со пет до седум години работно искуство во сферата, признат на меѓународно ниво, наречен и „златен стандард“ во управувањето со безбедноста. Сертификатот за професионалец за физичка безбедност (Physical Security Professional – PSP) ја докажува експертизата за процени кај физичката безбедност, примена, дизајн и интеграција на системот за физичка безбедност.⁷⁶ АСИС (ASIS) претставува глобална заедница на безбедносни практичари, од кои секој има улога во заштитата на средствата – луѓето, имотот и/или информациите и вбројува 34 600 членови во 155 земји и претставува најголемата европска заедница на професионалци за безбедност.⁷⁷

7. ПРИВАТНОТО ОБЕЗБЕДУВАЊЕ ВО ФУНКЦИЈА НА НАЦИОНАЛНАТА БЕЗБЕДНОСТ

Приватното обезбедување игра значајна улога во заштитата на националната безбедност преку дополнување и поддршка на работата на јавните органи за спроведување на законот. Во многу случаи, приватното обезбедување има тесна соработка со националните безбедносни органи, особено во областите на сајбер-безбедноста, заштитата на критичната инфраструктура и одговорот во итни случаи.⁷⁸ Тука првенствено се издвојуваат активностите во заштитата на критичната инфраструктура, при што приватните безбедносни актери често управуваат и заштитуваат критична инфраструктура, како што се електрани, системи за водоснабдување, транспортни мрежи итн. Нивната улога вклучу-

⁷⁶ Latest News from Security Management. <https://www.asisonline.org/>

⁷⁷ Buzatu, A.M. and Buckland, B. (2010). Private Military and Security Companies: Future Challenges in Security Governance. Geneva: DCAF.

⁷⁸ Czop, A. (2017). Genesis, development and importance of private security companies in the provision of public safety in Poland. *Security and Defence Quarterly*, 17(4), стр. 100-118, достапно на: <https://doi.org/10.5604/01.3001.0011.7856>

чува следење и одговор на потенцијални закани, што помага да се спречат нарушувања што можат да влијаат на националната безбедност.⁷⁹ Понатаму, во контекст на најновите тенденции, приватните безбедносни актери можат да обезбедат разузнавачки информации и процени на ризик поврзани со специфични закани или ранливости. Тие често имаат специјализирано знаење и алатки за да ги проценат ризиците што можеби не им се достапни на јавните институции.⁸⁰ Во областите каде што постои висок ризик од терористички активности, приватното обезбедување може да спроведе напреден надзор во поддршка на контратерористичките напори, системи за контрола на пристап и стратегии за одговор при итни случаи за да ги ублажи ризиците.⁸¹ Понатаму, настаните од големи размери, вклучувајќи меѓународни самити, политички конвенции и спортски настани, бараат силни безбедносни мерки. Приватните безбедносни актери често се справуваат со логистиката и безбедноста на теренот за вакви настани, работејќи заедно со јавните институции за да се осигури безбедноста.⁸² Исто така, многу компании во чувствителните индустрии (како одбранбените изведувачи или фирмите за висока технологија) користат приватно обезбедување за да ги заштитат своите средства и интелектуална сопственост. Ова може да помогне да се спречи шпионажа и кражба што може да има импликации за националната безбедност.⁸³

79 Heino, O. (2022). Intelligent terrorism as a security threat to critical infrastructure. *Security and Defence Quarterly*, 39(3), стр. 33-44, достапно на: <https://doi.org/10.35467/sdq/152422>

80 Lizzo S. (2024) Intelligence Redefined: The Interplay of Private Companies and National Security. *Journal of International Affairs*. Columbia University.

81 Private Security Market Research 2032. Allied Market Research, достапно на: <https://www.alliedmarketresearch.com/private-security-market-A06346>

82 Sage-Passant, Lewis (2023). The security intelligence services of the private sector. Loughborough University. Thesis, достапно на: <https://doi.org/10.26174/thesis.lboro.24050421.v1>

83 Private Security Governance and National Action Plans on Business and Human Rights (2019). The Danish Institute for Human Rights & DCAF

Имајќи ги предвид масовните мигрирачки струи во изминатата декада како резултат на меѓународните конфликти, станува евидентно дека државно-центричното гранично дихотомно управување засновано на безбедност и мобилност нема доволно капацитет да ги опслужува комплексните двигатели и да ја сноси одговорноста за миграцијата, интеграцијата, капацитетот за прифаќање и политиките за почитување на човековите права што произлегуваат од политиките за гранично управување. Во Европската Унија, приватните безбедносни компании се вклучени во управувањето со граничната безбедност и царинските операции, помагајќи да се следи и да се контролира движењето на стоки и луѓе.⁸⁴ Во безбедносната архитектура поставена на граничното управување, преку трансформативни процеси на екстернализација и информализација, приватните безбедносни агенции го одржуваат своето присуство во граничните зони, со цел поддршка на соработката и брзо споделување информации помеѓу граничната полиција и колегите од соседните земји.⁸⁵

Нема дилема дека приватната безбедност може да ги подобри напорите за зачувување и унапредување на сите аспекти на националната безбедност, при што особено е важно да се осигури дека нивните активности се соодветно регулирани и координирани со јавните власти, за да се избегнат потенцијални конфликти или празнини во безбедносното покривање.⁸⁶ Сепак, несомнено покрај активностите на приватната безбедност во остварување на националната безбедност, таа има и одредено значење во придонесот на меѓународната безбедност. Така, приватните безбедносни актери се инволвирани во обезбедување обука и консултантски услуги на организациите од јавниот сектор, зголемувајќи ја нивната способност да одговорат на различни закани преку организирање обуки (примерот со одвраќање на нелегална миграција во Средоземно Море за Либиската крајбрежна

84 Private Sector Partners. Interpol, достапно на: <https://www.interpol.int/en/Our-partners/Private-sector-partners>

85 Border Management. OSCE, достапно на: <https://www.osce.org/border-management>

86 SITA Border Control, достапно на: <https://www.sita.aero/>

служба под менторство и финансиска поддршка на Италија и на Европската унија), работилници и подигање на свеста за службениците за морнарица и граничната безбедност, царинскиот персонал и персоналот за воздухопловната и аеродромската безбедност во однос на процедурите на патролирање, техниките на надзор, протоколите за поморска безбедност, управување со безбедноста на аеродромите, спротивставување на трговијата со дрога, зајакнување на безбедноста на патните исправи, техники за меѓународно профилирање, борба против транснационалниот организиран криминал, нелегална трговија со дрога и хемиски прекурсори, состаноци за рано предупредување со граничните служби, локалните власти и локалното население, обезбедување технички совети и помош за спречување и реагирање на гранични инциденти во согласност со новите безбедносни наративи (како примерот на соработката на ИНТЕРПОЛ со приватниот безбедносен сектор во насока на премостување на празнините и обезбедување витални услуги или експертиза што инаку не би биле достапни за земјите членки на ИНТЕРПОЛ). Оваа соработка може да има форма на финансирање, но често вклучува испраќање персонал, лиценцирање софтвер, употреба на опрема и објекти, како и други донации).⁸⁷

Современите меѓународни конфликти сè повеќе ја вклучуваат употребата на приватни безбедносни компании што играат различни улоги во конфликтните зони и нестабилните региони и нивното поле на активности се проширува низ различни географски зони. Емпириските примери добиени преку преглед и анализа на пресекот помеѓу меѓународните конфликти и приватната безбедност идентификува различни улоги на приватното обезбедување во меѓународните конфликти.⁸⁸ Тие генерално гравитираат околу поддршка на изведувањето воени операции, и тоа

87 Public-private partnerships INTERPOL, достапно на: <https://www.interpol.int/en/Crimes/Cybercrime/Public-private-partnerships>

88 White, N. D., & Henderson, C. (2013). *Research handbook on international conflict and security law : jus ad bellum, jus in bello and jus post bellum*. Edward Elgar Pub. Ltd. <http://www.elgaronline.com/abstract/9781849808569.xml>

како логистика и поддршка, вклучувајќи транспорт, управување со синџирот на снабдување и други специјализирани услуги за одржување воени операции. Приватните безбедносни компании нудат вооружени безбедносни услуги за заштита на воени бази, конвои за снабдување и критична инфраструктура.⁸⁹

Во услови на конфликт, приватните безбедносни агенции понекогаш обезбедуваат воена обука за локалните сили или сојузничкиот воен персонал. Како и на национално ниво, неизоставно е нивното присуство и во заштита на критичната инфраструктура во конфликтните зони. Агенциите или фирмите за приватно обезбедување се ангажирани за да се обезбеди критична инфраструктура како што се нафтени полиња, гасоводи и рударски операции. Овие локации често се мета на бунтовници, терористички организации и/или други непријателски сили.⁹⁰

Од аспект на меѓународната безбедност, во меѓународните конфликти и во политички и безбедносно нестабилните региони, правните лица што вршат услуги за приватно обезбедување ги штитат амбасадите, конзулатите и другите дипломатски мисии, ја одржуваат безбедноста на хуманитарната помош преку одржување на безбедноста за хуманитарните организации што работат во конфликтните зони, обезбедувајќи безбедно доставување помош до погодените популации, како во случајот со достава на хуманитарна помош во појасот Газа во 2024 година.⁹¹ Во тој контекст, тие вршат процена на ризик и управување со кризи, конкретно во поддршка на невладините организации и меѓународните орга-

89 The Business of War – Growing risks from Private Military Companies. Council of the European Union. General Secretariat. 31 August 2023.

90 Ashley K. (2014) Security in a Globalized World. Understanding the Paradigm Shift of Contending Dynamics. GRIN Verlag. Open Publishing GmbH

91 Dall'Asta G. (2024) The Impact of Private Security Companies Employed by INGOs on Humanitarian Operations. Private Security Conversations. IcoCA, достапно на: <https://blog.icoca.ch/the-impact-of-private-security-companies-employed-by-ingos-on-humanitarian-operations/>

низации со процени за ризик, управување со кризи и планирање на евакуација.⁹²

Државите се обраќаат кон приватните безбедносни компании за обезбедување од различни причини, при што овој тренд е дел од поширокиот процес на демонтирање и реконфигурација на некои од традиционалните алатки на државниот суверенитет како одговор на рапидно еволуирачкото безбедносно опкружување (контрола на граници/територија, заштита на инфраструктурата, хибридни закани, пропаганда).⁹³

Во некои региони, работните места за приватно обезбедување обезбедуваат важни економски можности, особено во области со висока невработеност или ограничени економски перспективи. Локална експертиза и културно разбирање, културни и јазични вештини. Локалните регрути носат вредно културно знаење и јазични вештини, што се клучни за навигација во сложената социјална динамика и ефективна интеракција со локалното население.⁹⁴

8. НОВИТЕ БЕЗБЕДНОСНИ ТРЕНДОВИ ВО ПРИВАТНОТО ОБЕЗБЕДУВАЊЕ

Трендовите во приватната безбедносна индустрија можат да се идентификуваат преку примена на соодветна методологија, со што се обезбедува макровизура за создавање соодветни правни и

92 Michalski, D., Radomyski, A. (2019). Modern aspects of the development of security in air transport under the conditions of air terrorism. *Security and Defence Quarterly*, 26(4), стр. 51-66, достапно на: <https://doi.org/10.35467/sdq/110553>

93 Report on the role of private military and security companies in immigration and border management and the impact on the protection of the rights of all migrants. Working Group on the use of mercenaries. 09 July 2020, достапно на: <https://www.ohchr.org/en/calls-for-input/report-role-private-military-and-security-companies-immigration-and-border>

94 Davidov G., Langille B., Lester G. (2024) *The Oxford Handbook of the Law of Work*. Oxford University Press.

нормативни рамки, стратегии и програми за работа во контекст на обезбедување соодветен одговор на истите, при што се мери нивната димензија, обем, влијание итн.⁹⁵

Трендовите во приватната безбедносна индустрија се поттикнати од различни фактори, вклучувајќи ја појавата на нови технолошки достигнувања и зголемената побарувачка за максимизирање на производниот потенцијал.⁹⁶

Трендовите, како генерална насока на промена и развој, се предусловени од предизвиците со кои се соочува безбедносната индустрија.⁹⁷ Мегатрендовите, пак, се долгорочни движечки сили кои може да се забележат во моментот, но кои ќе продолжат да имаат глобално влијание во наредните години.⁹⁸

Анализата на трендовите во индустријата за приватна безбедност се спроведува по пат на индукција на карактеристиките на пазарните сегменти и подсегментации.⁹⁹ Во пазарните сегменти се препознаваат приватните безбедносни актери, додека потсегментациите се вршат во согласност со услугите за обезбедување што може да бидат кон: владини институции и институции на јавната администрација, образовни институции, здравствени институции, финансиски институции, безбедност на производство, големопродажба и малопродажба, безбедност на транспорт, безбедност на

95 Abbaszadeh M. & Zemouche A. (2022). *Security and resilience in cyber-physical systems : detection estimation and control*. Springer, достапно на: <https://doi.org/10.1007/978-3-030-97166-3>

96 MacDonald, J., Klick J., Grunwald B. (2012) The Effect of Privately Provided Police Services on Crime: Evidence from a Geographic Regression Discontinuity Design. *Journal of the Royal Statistical Society (Series A)* 179:831–46.

97 Dempsey, J. S. (2010) *Introduction to Private Security*. Wadsworth, Cengage Learning.

98 Prior, T., Hagmann, J. (2014) Measuring resilience: methodological and political challenges of a trend security concept, *Journal of Risk Research*, 17:3, 281–298, достапно на: 10.1080/13669877.2013.808686

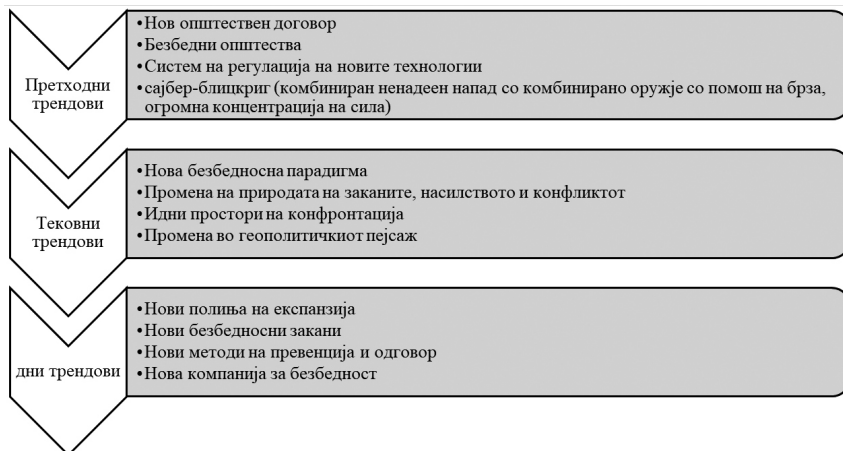
99 Cook, Philip J., and John MacDonald. (2011). Public Safety through Private Action: An Economic Assessment of BIDS. *Economic Journal* 121:445–62.

културни настани, спортски натпревари, објекти за игри на среќа, безбедност на информации, итн.¹⁰⁰

Сè поголемата потреба за услугите и производите од приватната безбедносна индустрија, како и потребата за инвестирање во безбедносни решенија се детерминирани од низа безбедносни предизвици.¹⁰¹ Нивната идентификација има за цел ефективна валидација, приоритизирање и одговор на ризиците што се највлијателни во приватната безбедносна индустрија. Оттука со елаборирање на сите овие факти, станува јасно дека од наведените предизвици произлегуваат новите безбедносни трендови.¹⁰²

Слика 1: Нови безбедносни трендови и мегатрендови.

Извор: Европска комисија, 2023



Според податоците на годишниот Извештај за безбедносни репери (The Security Benchmark Report) за 2022 година, објавен од

100 Statistical profile - Private Security Services Sector. International Labour Association. 22.February.2022, достапно на: https://ilo.org/global/docs/WCMS_837788/lang--en/index.htm (Посетена на 20.07.2023)

101 Private Security Companies. (2020). Toolkit for Security Sector Reporting: Media, Journalism and Security Sector Reform. DCAF.

102 Smith, F. C. (2013) Current and Emerging Trends in the Private Security Industry: The need for Continuing Education and Training of the Security Professional. ASIS.

страна на „Секјурити магазин“ (Security magazine), предизвиците со кои се соочуваат правните лица што обезбедуваат услуги и производи на приватно обезбедување и нивните вработени, ги диктираат новите безбедносни трендови, што генерално се поделени во овие домени:

- тероризам и насилство;
- Ковид-19 и други видови пандемии;
- деловен континуитет и деловна отпорност;
- Сајбер-безбедност на уреди и услуги (злоупотреба на податоци, напади за откуп, пробивање безбедносни протоколи, напади базирани на социјален инженеринг, DDoS напади на образовни ресурси);
- граѓански протести, насочени протести, немири, насилен активизам;
- управување со кризи;
- персонал и обука;
- модернизација на технологија и опрема;
- хибридни закани (државно-спонзорирани хакерски напади, државно-спонзорирано сајбер-војување, ранливост на облак);
- инсајдерски закани;
- ризици и закани што произлегуваат од деловно разузнавање;
- природни непогоди.¹⁰³

Врз основа на ефикасноста во справување во наведените домени, се мери степенот на способност и зрелост на индустријата да ги оствари своите програмски цели, преку анализа на нивните буџети, приходи и расходи, како и структурата и организациската поставеност, носењето одлуки и менаџментот/управувањето со процесите и процедурите и персоналот.¹⁰⁴ Овие наоди се добиени

¹⁰³ The Security Benchmark Report 2022. Security Magazine.

¹⁰⁴ Shein, M. (2022) The 2022 Security Benchmark. Security Magazine, достапно на: <https://www.securitymagazine.com/articles/98528-the-2022-security-benchmark-methodology> (посетена на 18.07.2023)

во согласност со програмите за работа на правните лица што се занимаваат со дејноста приватно обезбедување, во контекст на задачите и одговорностите на приватното обезбедување, од кои се обезбедуваат параметри за компарирање принцип на секторска поделеност.¹⁰⁵

Следствено на тоа, овие набројани предизвици ги диктираат трендовите што содржински го обликуваат соодветниот одговор на приватната безбедносна индустрија.¹⁰⁶ Трендовите во приватното обезбедување во доменот на физичко обезбедување на глобално ниво се поделени според следните категории:

- Контрола на пристап и движење со термални камери (термичкото скенирање е тип на технологија што се користи за откривање на инфрацрвената енергија што ја емитува некој објект и создавање детална термичка слика. Во однос на физичката безбедност, ова може да открие невообичаени топлински движења што укажуваат на пожар или дури и сокриено лице. Технологијата станува сè поприсутна бидејќи може да се користи во различни услови, од аеродроми до деловни згради).¹⁰⁷
- Биометриска проверка на автентичност (предноста на биометриската автентикација е тоа што е многу потешко да се измами од другите форми на идентификација, како што се лозинка или пин, бидејќи биометриските податоци се единствени за секој поединец и многу потешко се реплицираат или се фалсификуваат). Дополнително, биометриската автентикација може да се користи заедно со други форми на идентификација, како што се лични

105 Emerging Trends, Drivers and Challenges in the Private Security Services Market 2019-2023. Business Wire, London.

106 Private Security Governance Challenges and the Relevance of International Norms and Best Practices. A Guide for Civil Society and Media. Private Security Governance Observatory. DCAF.

107 Park, H., Cho, J.T. Global trends in the standardization of the burglary-resistance testing of security hardware. *Secur J* 31, стр. 247-264 (2018), достапно на: <https://doi.org/10.1057/s41284-017-0097-y>

идентификациски картички или безбедносни токени, за да се обезбеди дополнителен слој на безбедност.¹⁰⁸

- Видеоаналитика со вештачка интелигенција (апликации-те за откривање закани користат алгоритми со вештачка интелигенција за да ги анализираат видеоснимките и да ги идентификуваат потенцијалните безбедносни закани. Тие можат да се користат за следење широк спектар безбедносни ризици, вклучувајќи упади, пожари и други еколошки опасности.¹⁰⁹ Во примената кај физичкото обезбедување во откривање аномалии, снимките преку видеоаналитика може да анализираат движења возила или лица, формирање толпа; предвидување инциденти, каде аналитиката на податоци служи за предвидување кога и каде ќе се случи инцидент, преку анализа на шемите и трендовите од минатите инциденти, со што овие информации може да се користат за соодветно распоредување безбедносни мерки и за подобрување на времето на одговор, особено корисно во ситуации на одговор во итни случаи и во создавање подобри планови за евакуација.).¹¹⁰
- Интернет на нештата во физичката безбедност (виртуелна детекција на кражба, виртуелна ограда, следење температура, влажност и други физички параметри во периметарот на обезбедување).¹¹¹
- Преминување на хибридни решенија во облак (сè повеќе компании усвојуваат хибридни облак решенија, спој на

108 Global Risks Report 2022. Chapter 3. Digital Dependencies and Cyber Vulnerabilities. World Economic Forum.

109 Ariel B, Bland M, Sutherland A. 'Lowering the threshold of effective deterrence'-Testing the effect of private security agents in public spaces on crime: A randomized controlled trial in a mass transit system. PLoS One. 2017 Dec 6;12(12):e0187392. достапно на: [10.1371/journal.pone.0187392](https://doi.org/10.1371/journal.pone.0187392). PMID: 29211735; PMCID: PMC5718484.

110 Bernat, L. (2021), "Enhancing the digital security of critical activities", Going Digital Toolkit Note, No. 17, достапно на: https://goingdigital.oecd.org/data/toolkitnotes/No17_ToolkitNote_DigitalSecurity.pdf.

111 A Trend Report of IFSEC Global | The 2022 State of Physical Access Control Report.

системи за безбедност во периметарот на обезбедување и облак. Привлечноста на овие видови системи е што тие можат да се приспособат на потребите на секој клиент.).¹¹²

Од аспект на новите трендови во технологијата што се применува за потребите за остварување физичка безбедност, интенцијата е таа да придонесува, или додава, таканаречени слоеви на заштита што се вклопуваат во структурата и ги дополнува кадровските способности.¹¹³

Кога се гледа употребата на приватно обезбедување од хронолошки аспект, евидентна е тенденцијата на зголемено потпирање на новоразвиената технологија за да се одржат безбедни субјектите што се предмет на заштита.¹¹⁴ Сè покомплексните безбедносни потреби на клиентите создаваат побарувачка за комплементарни решенија, како што се предвидливите (антиципативните) безбедносни услуги, нагласувајќи ја важноста да се има нова и соодветна технологија, податоци во облак и низа други способности кај давателите на безбедносни услуги.¹¹⁵ Овие нови безбедносни трендови им овозможуваат на компаниите за безбедносни услуги да им понудат на клиентите поефикасни и уште поквалитетни безбедносни решенија.¹¹⁶ Најзастапен тренд во доменот на техничкото обезбедување е примената на автоматизација во безбедносните процеси.¹¹⁷ Автоматизираниите безбедносни процеси можат да

112 Heaton, P., *et al.* (2018) *The Short- and Long-Run Effects of Private Law Enforcement: Evidence from University Police*. University of Chicago Press.

113 Fennelly L. J. & Perry M. A. (2017). *Physical security: 150 things you should know* (Second). Butterworth-Heinemann. достапно на: <http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4730474>.

114 Fennelly, L. J. (2017) *Effective Physical Security* (Fifth Edition), Butterworth-Heinemann. P.347-385, достапно на: <https://doi.org/10.1016/B978-0-12-804462-9.00020-8>.

115 Lippert R. K. & Walby K. (2019). *A criminology of policing and security frontiers*. Bristol University Press.

116 Bearpark, A., Schulz, S. (2007) *The Private Security Challenge in Africa: Problems and Options for Regulation*. Chapter 5. Institute for Security Studies.

117 Private Security Service Market Size 2023 to 2031 | Global Insights and Outlook with Top Players. <https://www.digitaljournal.com/pr/news/>

помогнат да се намали времето потребно за откривање и одговор на заканите и да се подобри точноста на откривањето закани. Автоматизацијата, исто така, може да го намали потпирањето на мануелните процеси, што може да одземаат време и да бидат склони кон човечки грешки.¹¹⁸ Во доменот на техничкиот аспект на безбедносните услуги и производи, предничат алармните мониторинг системи и системите за надзор со камери. Како конкретен пример, во 2021 година, бројот на инсталирани безбедносни камери на глобално ниво надминал една милијарда парчиња, што одговара на зголемување од над 50 проценти во споредба со 2018 година.¹¹⁹ Најголемиот сооднос по број на поставени безбедносни камери изнесува 439 камери на 1 000 луѓе во НР Кина, или речиси една камера на секои двајца луѓе. НР Кина доминира по својата огромна тактика за надзор.¹²⁰ Како што забележува Британската асоцијација за безбедносна индустрија, бројот на безбедносни камери во функција се зголемува во последните пет години, бидејќи достапноста на овие производи се подобрува.¹²¹ Достапноста и прифатливата цена на овие производи доведува до пораст на оние што инвестираат во видеонадзор во станбените објекти, како дел од најновиот тренд, концептот *паметен дом*, како и професионални системи за видеонадзор за канцелариски комплекси и други комерцијални имоти.¹²²

theexpresswire/private-security-service-market-size-2023-to-2031-global-insights-and-outlook-with-top-players- (Посетена на 20.07.2023).

118 Vijay Singh Rathore, Vincenzo Piuri, Rosalina Babo, Marta Campos Ferreira (2023) Emerging trends in expert applications and security: proceedings of 2nd. ICETEAS 2023, Volume 2. Springer Verlag Singapore.

119 Thomas J. Rzymek, Chapter 10 - Biometrics in the Criminal Justice System and Society Today, Editor(s): Lawrence J. Fennelly, Effective Physical Security (Fifth Edition), Butterworth-Heinemann, 2017, стр. 249-254, <https://doi.org/10.1016/B978-0-12-804462-9.00010-5>.

120 Lemieux F. (2018). *Intelligence and state surveillance in modern societies: an international perspective*. Emerald Group Publ.

121 White, S. (2023) CCTV Cameras by Countries & Cities (2023 Guide). Upcoming Security. [article]

122 Wildhorn, S. (1975) Issues in Private Security. Santa Monica, CA. RAND Corporation

Слика бр. 2: Трендови во техничкото обезбедување.

Извор: Gartner, 2023.



9. ПРЕДВИДЕНИ РЕШЕНИЈА КАКО ОДГОВОР НА НОВИТЕ БЕЗБЕДНОСНИ ТРЕНДОВИ

Во согласност со концептот на четвртата индустриска револуција, или синонимизирана како ера на дигиталната еволуција, процес со кој настанува спојување на физичкиот, биолошкиот и дигиталниот свет, владите, општествата и компаниите сè повеќе се потпираат на технологијата за управување со сè она што претставува антропогена активност: од јавните услуги до деловните процеси, дури и рутинското купување намирници.¹²³ Конвергираните техно-

¹²³ Security trends to watch for in 2023. Security Info Watch. <https://www.securityinfowatch.com/home/article/21291956/security-trends-to-watch-for-in-2023>

лошки платформи, програми и апликации поврзани преку интернет во децентрализирана верзија, истовремено создаваат покомплексен пејзаж на сајбер-закани и растечки број на ранливи точки.¹²⁴ Притоа, приватните безбедносни агенции се среќаваат со безброј потенцијални закани во ерата на дигиталната трансформација, каде што настанува модификација и развој на нови техники за напад врз заштитените субјекти.¹²⁵ Оттука, во контекст на наведената фактографија и во согласност со методолошката рамка за анализа, може да се констатира дека безбедносните системи, што се соочуваат со сè поинтелигентни задачи, стануваат сè подлабоко интегрирани и сеопфатни, проширувајќи ги своите способности како и оперативните функции, со цел да ја подобрат ефикасноста во безбедноста, напоредно низ многу различни индустрии и типови на организации.¹²⁶

Од општествен аспект, овие наоди произлегуваат од фактот дека во изминатите три децении се забележува директната каузалност помеѓу присуството на приватното обезбедување и отстранување или ублажување на појавата и последиците од разни форми на насилство, како семејно насилство, кражби, вооружени грабежи, несреќи во сообраќајот, нарушувања на јавниот ред и мир, напади и слични криминогени феномени, што влегуваат во сферата на суплементарност помеѓу јавната и приватната безбедност, каде приватното обезбедување има функција на детерент (одвраќач).¹²⁷

124 Neufeind M. O'Reilly J. & Ranft F. (2018). *Work in the digital age: challenges of the fourth industrial revolution*. Rowman & Littlefield International.

125 Emerging trends and methods in international security (Workshop) Townsend E. Keck Center National Academies of Sciences Engineering and Medicine (U.S.). Board on Behavioral Cognitive and Sensory Sciences & National Academies of Sciences Engineering and Medicine (U.S.). Division of Behavioral and Social Sciences and Education. (2018). National Academies Press, Washington, DC, 2018.

126 Craig McQuate. (2017). Chapter 19 - Security Officers and Equipment Monitoring, Editor(s): Lawrence J. Fennelly, *Effective Physical Security* (Fifth Edition), Butterworth-Heinemann, стр. 343-346, достапно на: <https://doi.org/10.1016/B978-0-12-804462-9.00019-1>.

127 Brian Meehan & Bruce L. Benson (2017) Does private security affect crime?: a test using state regulations as instruments, *Applied Economics*, 49:48, стр. 4911-4924, достапно на: 10.1080/00036846.2017.1296551

Значи сè пософистицираните непријатели и вектори на закани во современиот безбедносен пејзаж ја налагаат потребата за пософистициран одговор и одбрана.¹²⁸ За заштитно-одбранбени, како и превентивни и проактивни ефикасни безбедносни операции, безбедносните професионалци имаат на располагање голем број технологии, каде приматот несомнено ѝ припаѓа на вештачката интелигенција (ВИ – AI), применета во интегрираните безбедносни технологии во видеонадзорот, во употребата на беспилотните летала и решенијата што применуваат автономни системи на автоматизација и роботика.¹²⁹

Интегрираните безбедносни технологии се еден од најпопуларните нови трендови во безбедносната технологија.¹³⁰ Со нив се надоместува недостатокот на деноноќна физичка безбедност со интегрирање на апликациите за сајбер-безбедност, како што се системи за далечински видеомониторинг, робусни мерки за контрола на пристап, алармни системи и патроли.¹³¹ Технолошките решенија за безбедносна интеграција, како што е поврзувањето на видеомониторингот со вештачката интелигенција и аналитиката (IVC) може да ја подобрат безбедносната ефикасност и да реагираат на закани со минимална, како и без човечка интервенција.¹³² Видеонадзорот е незаменливо средство во вршењето на дејноста при-

128 Khando, K., Shang, G., Sirajul M. I., Salman, A. (2021) Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, Volume 106, достапно на: <https://doi.org/10.1016/j.cose.2021.102267>.

129 Drone technology: security threats and benefits for police focus of INTERPOL forum <https://www.interpol.int/ar/1/1/2018/Drone-technology-security-threats-and-benefits-for-police-focus-of-INTERPOL-forum>. (посетена на 21.07.2023).

130 Бакрески, О., Ѓуровски, М., Барџиева М., Л. (2021). „Јавната и приватната безбедност - координација и соработка“ Комора на РСМ за приватно обезбедување.

131 S. Subashini *et al.* (2011). A survey on security issues in service delivery models of cloud computing. *J Network Comput Appl*.

132 Schwab K. (2017). *The fourth industrial revolution*. Penguin, достапно на: <http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9780241980538>. (посетена на 22.07.2023).

ватно обезбедување од повеќе аспекти. Правилно поставените камери можат да обезбедат тактичка предност во позиционирањето и нивна стационираност на клучни места, додека ги следат другите области на локацијата за сомнителна активност.¹³³

Кога се говори за видеонадзорот, новитетите во технологијата за безбедносни камери ги претставуваат беспилотните летала како тренд што предничи и претставува безбедносна алатка за повеќекратна употреба, што им овозможува на надлежните поглед од високо за следење големи области и настани со потенцијално сомнителни активности, притоа со ангажирање минимална работна сила.¹³⁴

Во практика, од аспект на меѓуинституционалната соработка и концептот на јавно-приватно партнерство, операторите на беспилотни летала во приватната безбедносна индустрија можат брзо да ги насочат припадниците на полицијата таму каде што се најпотребни, зголемувајќи ги ефектите на заштита и времето на одговор на безбедносните тимови со помалуброен персонал.¹³⁵ Беспилотните летала обезбедуваат проширен видеонадзор надвор од типичните линии на хоризонтот и се применуваат во остварување на периметарската безбедност, заштитата на критичната инфраструктура, следењето толпи, крајбрежните операции и операциите за пребарување и спасување итн., на земја, во вода и во воздух, со прецизно и ефикасно извршување на задачите што би биле од висок ризик ако би ги извршувал човечки пилот.¹³⁶ Употребата на дронови и другите видови беспилотни возила се, исто така, конзистентни со новата парадигма во приватната безбедност, така наречената *нова компанија за безбедност*, при што безбедносните службеници и технологијата се комбинираат во *безбедносни*

133 Slone, M. (2022) Drones as Security Tools. *Security Magazine*, достапно на: <https://www.securitymagazine.com/articles/98699-drones-as-security-tools> (21.07.2023).

134 Staff H. (2020). *The political economy of private security: how European states privatize regulate and produce domestic security*. Lit Verlag.

135 The Use of UA in Private Security. March 2017. Confederation of European Security Services.

136 Global Market Trends, 2023. Securitas.

решенија, со цел да се оптимизира услугата за клиентите и да се обезбеди зголемена безбедност.¹³⁷

10. ПРЕДИЗВИЦИ И ПЕРСПЕКТИВИ ВО ИНДУСТРИЈАТА ЗА ПРИВАТНА БЕЗБЕДНОСТ

Појавата на приватното обезбедување е повеќеслоен процес поттикнат од историски преседани, општествено-економски промени, технолошки напредок и глобални случувања. Покрај општествените и економските фактори, изворите на загрозување и заканите со предзнак на тероризам и политичка нестабилност ја зголемуваат потребата за специјализирани безбедносни услуги. Приватните безбедносни фирми често обезбедуваат заштитни услуги во области со висок ризик каде што јавното спроведување на законот може да биде недоволно или недостапно.¹³⁸

Во денешни услови, приватното обезбедување е составен дел од поширокиот безбедносен пејзаж, надополнувајќи го системот за спроведување на законот, што обезбедува специјализирани услуги за задоволување на различните потреби на поединци, бизниси и заедници.¹³⁹ Работниците за приватно обезбедување, исто така, се одговорни за безбедноста и заштитата на индустријата и производството, комуналните услуги, транспортот, здравствените и образовни објекти, итн. Главната функција на униформираниот работник за обезбедување е намалување на ризикот и обично се постигнува преку принципот на видливост и внимателност, каде генерално мото на оваа индустрија е: „откривање, одвраќање, набљудување и пријавување“.¹⁴⁰

137 Changing Security Paradigm. Knowledge for Policy. European Commission. 12 Jul 2023.

138 Private Security Governance and National Action Plans on Business and Human Rights. The Danish Institute for Human Rights (DIHR), DCAF – Geneva Center for Security Sector Governance, 2019.

139 Nemeth P. C. (2023) *Private Security: An Introduction to Principles and Practice*. 2nd Edition. CRC Press.

140 Nalla, M. K., & Crichlow, V. J. (2017). Have the standards for private security guards become more stringent in the post-9/11 era? An assessment of

Приватното обезбедување е, исто така, одговорно за заштита на многу од институциите и системите на критична инфраструктура на нацијата, но и за заштита на интелектуалната сопственост и чувствителните корпоративни информации. Општествата ширум светот, покрај ова, во голема мера се потпираат на приватната безбедност за широк спектар на функции, вклучувајќи и заштита на вработените и имотот, спроведување истраги, вршење скрининг пред вработувањето, обезбедување безбедност на информатичката технологија и многу други функции.¹⁴¹

Приватната безбедносна индустрија се соочува со бројни предизвици, од закани што се развиваат и технолошка интеграција до регулаторна усогласеност и проблеми со човечките ресурси. Сепак, таа исто така претставува плејада на можности преку напредок во технологијата, услугите за сајбер-безбедност, иновативни решенија за физичка безбедност и глобална експанзија.¹⁴² Со справување со овие предизвици и капитализирање на овие можности, приватните безбедносни фирми можат да ја подобрат нивната ефикасност и подобро да ги заштитат своите клиенти во сè покомплексниот пејзаж на закани.¹⁴³

Во оваа насока се идентификуваат предизвиците во приватната безбедност што е неопходно да се детерминираат со цел соодветно да се управуваат (менаџираат). Тука, пред сè, спаѓаат законите што се развиваат постојано, а првенствено се дефинираат како закани во доменот на сајбер-безбедноста, односно зголемување на софистицираноста во сајбер-нападите како што се откуп, фишинг

security guard regulations in the U.S. from 1982 to 2010. *Security Journal*, 30(2), стр. 523–537.

141 Strom, K., Berzofsky M., Shook-Sa B., Barrick K., Daye C., Horstmann N., Kinsey S. (2010) The Private Security Industry: A Review of the Definitions, Available Data Sources, and Paths Moving Forward. RTI International, The Bureau of Justice Statistics (BJS)

142 Berg, J. (2023). Private Security. *obo in Criminology*. достапно на: 10.1093/obo/9780195396607-0329

143 Churchill, D., Janiewski, D., & Leloup, P. (Eds.). (2020). *Private Security and the Modern State: Historical and Comparative Perspectives* (1st ed.). Routledge., достапно на: <https://doi.org/10.4324/9780429060991>

и протекување на податоци, но и класичните физички закани, дефинирани во согласност со дефиницијата за физичка безбедност, што подразбира обезбедување и заштита на организациски средства од оштетување како резултат на физички настани, каде се набројуваат ризиците како што се кражба, вандализам, организиран криминал, вооружено насилство и тероризам.¹⁴⁴

Во контекст на современите предизвици со кои се соочува приватната безбедност, заканите во доменот на сајбер-безбедноста котираат високо на листата и налагаат потреба од технолошка интеграција, односно примена на современи системи за надзор, паралелно со балансирањето на примената на напредните технологии за надзор со консидарацијата за почитувањето на приватноста; како и контрола на пристап, преку употреба и одржување на биометриски и други напредни системи за контрола на пристап.¹⁴⁵

Неизоставно е да се наведе и аспектот на соодветното управување со човечки ресурси, односно потребата од континуирана и соодветна обука и гаранција дека безбедносниот персонал е соодветно обучен за најновите технологии и техники за откривање и спречување безбедносни закани и нивно долгорочно задржување на работните позиции за континуитет на одржување на квалификувана работна сила.¹⁴⁶

Од аспект на менаџментот и управувањето, во согласност со дефиницијата за водењето кон ефикасно и ефективно остварување на целите, еден од предизвиците во сферата на приватната безбедност се поврат на инвестицијата, односно оправдување на трошоците за безбедносните мерки кај засегнатите страни (клиентите), трошоците и буџетските ограничувања, односно балансирање на

144 Katz, D. S. (2020). *Executive's guide to personal security*. Wiley & Sons Canada, Limited, John.

145 65% of organizations cite data loss as top risk of unauthorized tools. Security Staff. Security, достапно на: <https://www.securitymagazine.com/articles/keyword/479-private-security>

146 Security operations : an introduction to planning and conducting private security details for high-risk areas (Second). (2021). CRC Press. July 12, 2024.

потребата од напредни безбедносни мерки со буџетските можности.¹⁴⁷

Како еден од тековните предизвици во сферата на приватното обезбедување е и јавната перцепција, односно генерираната општествена слика што јавноста ја има за приватното обезбедување како засебна дејност од аспект на давање на услугата во сегментот безбедност, покрај јавните органи на државната управа задолжени за безбедноста.¹⁴⁸ Во оваа насока, на ниво на одделни држави, перцепцијата варира,¹⁴⁹ при што во одредени географски региони и политички контексти приватното обезбедување се перцепира како инсуфициентно средство на осигурување на безбедност поради низа предизвици како што се недоволната и несоодветна обука (Јужна Азија), немањето кредибилитет и легитимитет (Источна Африка); додека во одредени региони се перцепира како достоин суплемент на јавната безбедност (Источна Азија) поради високото ниво на професионализам и имплементирани стандарди во работата и претставува гарант на стабилноста во критичните региони (Северна Америка).¹⁵⁰ Овие тенденции се поттикнати од повеќе социоекономски фактори. На пример, Јужна Африка, иако е најразвиената земја во африканскиот континент, ја бележи една од највисоките стапки на насилан криминал во светот, при што се бележи експанзија на индустријата за приватно обезбедување. Во контекст на овој пример, Јужна Африка има помалку од 150 000 полицајци за население од 62 милиони луѓе, што ја потврдува хипотезата дека јавните служби

147 South Africa: private security industry booming. Africa /news , достапно на: <https://www.africanews.com/2024/01/05/south-africa-private-security-industry-booming/>

148 Aitken, A. 2021. Community Perceptions of Private Security at a Mega-Event. *Security Journal*, достапно на: <https://doi.org/10.1057/s41284-021-00309-y>.

149 White, A. (2023) Critical workers? Private security, public perceptions and the Covid-19 pandemic. *Secur J* 36, стр. 317–332, достапно на: <https://doi.org/10.1057/s41284-022-00339-0>

150 Wright R. (2024) Surge in maritime violence boosts demand for private security forces, достапно на: <https://www.ft.com/content/5175a8b4-41cc-4b60-913f-dc6f2f68307d>

за осигурување на безбедноста, односно полицијата, во современи услови нема доволно реален капацитет физички да се распореди во насока на превенција и одвраќање на криминалот, особено во мега урбанизираните центри, но и во руралните средини.¹⁵¹

Во тој контекст, потребата за заштита на трговските пловила, што е во тенденција на пораст поради зголемените непријателства во географските региони со значителна стратешка важност, каде што се одвива меѓународната поморска трговија, како што се Хормуз, Гибралтар и Малака, што претставуваат витална точка на глобално ниво. Интеракцијата помеѓу оперативното право на меѓународна територија и во меѓународните води и улогата на приватната безбедност вклучува балансирање на слободата на навигација, како и на безбедносните грижи на државите и комерцијалните интереси на бродската индустрија. Во таа насока се истакнуваат неколку принципи што се во поддршка на изградба на доверба помеѓу засегнатите страни, каде што се вбројуваат прашањата на доверба, односно континуирано градење и одржување доверба со јавноста и клиентите.¹⁵²

Овие тенденции повикуваат на зголемена потреба од приватно обезбедување во одржувањето на меѓународниот мир и безбедност и гарантирањето на безбедноста на меѓународната слободна трговија, од разните форми на вооружени напади, грабеж, пиратство и сл., па оттука, од аспект на регулативата, се наметнува потребата за примена на Оперативното право во меѓународните теснеци и улогата на приватната безбедност вклучува сложена интеракција на меѓународното право, поморската безбедност и националните регулативи.¹⁵³

Кога станува збор за перспективите во дејноста приватно обезбедување, правецот што го диктираат тековните трендови и

151 Eski, Y. (2019) Maritime security and piracy: Effects of armed guards on board. *Encyclopedia of Security and Emergency Management*

152 Schildknecht, J., Dickey, R., Fink, M. D., & Ferris, L. (2018). *Operational law in international straits and current maritime security challenges*. Springer.

153 Magunna, A. (2024). Charting waters: the private sector's evolving governance role in Southeast Asian maritime security. *Australian Journal of International Affairs*, 78(3), стр. 306–325, достапно на: <https://doi.org/10.1080/10357718.2024.2337013>

идните проекции предвидуваат неминовно усвојување напред-на технологија, односно примена на вештачка интелигенција и машинско учење. Примената на вештачката интелигенција за откривање закани, предвидувачка анализа и подобрување на процесите на донесување одлуки, интеграцијата на концептот *Интернет на нештата* (IoT) преку имплементирање на уреди и апликации со IoT, за следење во реално време и паметни безбедносни решенија.¹⁵⁴

Слика 3: Перспективи во приватното обезбедување.

Извор: Bretschneider, Wolfgang; Freytag, Andreas; Rieckmann, Johannes; Stuchtey, Tim (2022) : State or private security supply? An analysis from the institutional economics perspective, Jena Economic Research Papers, No. 2022-009, Friedrich Schiller University Jena, Faculty of Economics and Business Administration, Jena

Перспективи во приватното обезбедување

Јавно-приватно партнерство

Соработка со владини агенции за подобрување на севкупните безбедносни мерки

Работа со заедниците за изградба на побезбедни средини и подобрување на односите со јавноста

Меѓународна соработка

Партнерство со меѓународни безбедносни фирми и агенции за справување со глобалните безбедносни закани

Глобална експанзија

Проширување на услугите на пазарите во развој со растечки безбедносни потреби

¹⁵⁴ Global Market Trends. Securitas, достапно на: <https://www.securitas.com/en/about-us/global-market-trends/>

Перспективите за понатамошниот развој на приватното обезбедување неодминливо вклучуваат понуда на услуги во доменот на сајбер-безбедноста, што подразбира сеопфатен пристап во управувањето со безбедносните услуги и проактивно и анти-ципативно следење закани и одговор на инциденти.¹⁵⁵

Овој аспект подразбира тековно усогласување со развојот на технологијата и практичната примена, обезбедување експертиза и стратегии за сајбер-безбедност и усогласеност со регулативата.¹⁵⁶

Во контекст на перспективите, се предвидуваат иновации и во физичката безбедност во доменот на мониторинг обезбедувањето како постојан физички надзор над вградени технички системи и уреди за обезбедување лица и имот и телекомуникациски пренос на алармни сигнали во центар за обезбедување и надзор. Тука се предвидува и унапредување на преносната технологија, односно користење уреди за носење, за следење и комуникација во реално време меѓу безбедносниот персонал.

Програмите за физичка безбедност се првиот слој на заштита од злонамерни активности врз лицата, средствата и физичкиот имот што се обезбедува. Програмите и технологиите за физичка безбедност што ги користат повеќето организации не смее да се занемаруваат и да го изгубат водството во ефикасноста во откривањето и реагирањето на заканите.¹⁵⁷

Иновациите во надзорот предвидуваат подобрени системи за видеонадзор и имплементирање системи за видеонадзор со висока дефиниција и интелигентни видеонадзор со препознавање лице и други напредни функции. Иновациите во физичката безбедност,

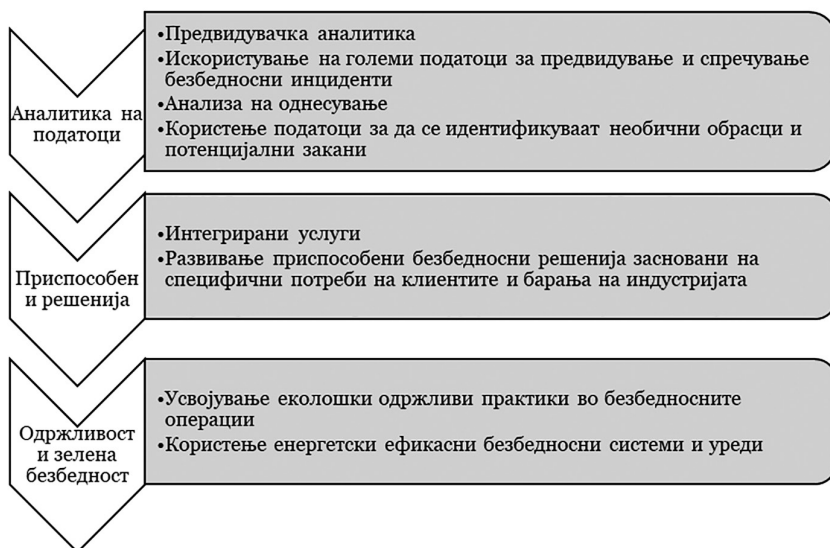
155 The Role of Private Security in Today's Society. Security Guarding 12 February 2024, достапно на: <https://theconstellation-group.com/role-of-private-security/>

156 Бернард В. (2024) How Technology is Changing Private Security. Private Security Conversations. [article] Feb. 6th 2024, достапно на: <https://blog.icoca.ch/how-technology-is-changing-private-security-and-why-it-matters/>

157 Forcht K., A., Kruck S., E. (2001) Physical Security Models, Philosophies and Context. Journal of International Information Management. Volume 10, Issue 2

првенствено сè поизразената примена на дронови и роботика, во практика значи користење дронови за надзор и работи за патрола и тие претставуваат зголемен тренд.¹⁵⁸

Слика 4: Перспективи за развој на приватно обезбедување.
Nalla M., Prenzler T. (2020) Regulating the Security Industry.
Global Perspectives. 1st Edition. Routledge



¹⁵⁸ Водич за вршење видеонадзор. “Поддршка во спроведувањето на модернизираната правна рамка за заштита на личните податоци“, финансиран од Европската Унија [chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://azlp.mk/wp-content/uploads/2024/01/](https://efaidnbmnnnibpcajpcgclefindmkaj/https://azlp.mk/wp-content/uploads/2024/01/)

11. ПРЕДИЗВИЦИТЕ НА ПРИВАТНАТА БЕЗБЕДНОСТ ВО ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Приватните безбедносни актери ангажирани како даватели на приватни безбедносни услуги играат важна, односно сериозна улога во заштитата на државните и недржавните клиенти во напорите за помош, закрепнување и реконструкција, комерцијални деловни потфати, воени операции и дипломатски активности.¹⁵⁹

Имајќи предвид дека дејноста приватно обезбедување законски е вrameна како дејност од јавен интерес, правните лица што имаат дозвола за приватно обезбедување се одговорни за заштита на многу од институциите и системите на критичната инфраструктура на нацијата, каде спаѓаат објектите на индустријата и производството, комуналните услуги, транспортот и здравствените и образовните објекти итн.

Синтагмата критична инфраструктура се синонимизира и со поимот објект од посебен интерес, односно инфраструктура што е суштествено, животно неопходна, а нарушувањето на нејзиното нормално функционирање може да доведе до загрозување на најзначајните вредности и добра врз коишто почива државата, општеството, економијата, благосостојбата и воспоставениот начин на живот и е неопходна нејзина задолжителна заштита.¹⁶⁰

Државата претставува централна точка во регулацијата на системот за заштита на критичната инфраструктура. Оттука, од најголем, односно витален интерес е непреченото функционирање на системите на критичната инфраструктура, без разлика на сопственичката структура на објектите од критичната инфраструктура или мрежа, со што се обезбедува непрекинато функционирање на заедницата.

¹⁵⁹ Cusumano E., Kinsey C. (2019) Diplomatic Security. A Comparative Analysis. Stanford University Press, достапно на: <https://www.sup.org/books/title/?id=24211>

¹⁶⁰ Предлог на закон за критична инфраструктура, Скопје 2022 година, достапно на: <https://mod.gov.mk/storage/2022/12/predlog-Zakon-za-krivicna-infrastruktura.pdf>

Во согласност со податоците на Меѓународната безбедносна лига (International Security Ligue), приватниот сектор поседува и заштитува приближно 85 % од инфраструктурата на земјата, додека органите за спроведување на законот имаат пристап до разузнавачки информации во врска со заканите по инфраструктурата.¹⁶¹ Како логичен след на фактичката состојба, најрационалниот механизам за заштита на критичната инфраструктура претставуваат јавните-приватни партнерства меѓу органите за спроведување на законот и приватните безбедносни агенции. Придобивките од овие партнерства се прифатени како најефективни и се дискутираат пречките што ја спречуваат ефективната со цел да се надминат. Примарните бариери вклучуваат недоверба што произлегува од природата на самите институции што се инволвирани, (не)спodelување информации поради различните методи на комуницирање и дезинформации, што можат да бидат намерни и/или ненамерни. Оттука, произлегуваат иницијативите и предлозите за формализација на партнерствата со меморандуми за соработка и формални договори за координација во кои ќе се прецизираат механизмите преку кои ќе се спodelуваат информациите.¹⁶²

Од оваа перспектива неопходно е да се подигне свеста и правилното поимање на важноста на критичната инфраструктура во рамките на стратeгиското управување на државата и нејзините институции. Приватното обезбедување игра клучна улога во заштитата на критичната инфраструктура, што вклучува средства од суштинско значење за функционирањето на општеството, како што се електрани, системи за водоснабдување, телекомуникациски мрежи, транспортни системи и финансиски институции. Вклучувањето на приватната безбедност во овој домен е одговор на зголемената сложеност и софистицираност на заканите, што се

161 International Security Ligue. Critical Infrastructure, достапно на: <https://www.international-security-ligue.org/>

162 Information Sharing. A Vital Resource. Cyber Security and Infrastructure Security Agency CISA, достапно на: <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/information-sharing-vital-resource>

движат од тероризам и сајбер- напади до природни катастрофи и инсајдерски закани.¹⁶³

Генезата на приватната безбедност во заштитата на критичната инфраструктура е длабоко вкоренета во еволуцијата и на концептот на самата критична инфраструктура и на пошироката историја на приватното обезбедување. Почетоците на развој на критичната инфраструктура се детектираат во индустриската револуција. Индустриската револуција го означува почетокот на голем развој на инфраструктурата, вклучувајќи железници, телекомуникациски системи и комунални услуги, како вода и електрична енергија. Овие инфраструктурни системи биле од витално значење за функционирањето на општеството и економијата. Како почетен фокус, во раните фази, улогата на приватното обезбедување во заштитата на критичната инфраструктура била ограничена и првенствено фокусирана на физичката безбедност, што вклучувало активности како што се чување објекти, следење на пристапните точки и патролирање во одредени периметри, додека критичната инфраструктура примарно подразбирала објекти, како што се: електрани, системи за водоснабдување, транспортни центри и комуникациски мрежи. Првично, владите и приватните корпорации биле основните заштитници на овие инфраструктури. Корпорациите, особено оние во индустриите како што се железницата, нафтата и комуналните претпријатија, развивале свои безбедносни сили за да ги заштитат своите средства. Заканите биле претежно од физичка природа, како кражба, вандализам или саботажа од поединци или мали групи. Како што се менувал пејзажот на заканите, така се модифицирале и оперативните методи и средства за заштита. Со текот на времето, дефиницијата за критична инфраструктура се прошири за да ги вклучи секторите: здравство, финансии, информатичка технологија и телекомуникациите. Овој проширен опсег наложи повеќе специјализирани

163 Pöyhönen, J. ; Nuojua, V. ; Lehto, M. & Rajamäki, J. (2019) Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. *Information & Security: An International Journal* 43:2, 236-256. достапно на: [10.11610/isij.4318](https://doi.org/10.11610/isij.4318)

безбедносни мерки. Меѓузависноста меѓу различните сектори стана поочигледна, што бара холистички пристап кон безбедноста. Понатаму, појавата на нови закани по безбедноста, како што се подемот на глобалниот тероризам, особено по настаните како нападите на 11 септември 2001 година, ја истакна ранливоста на критичната инфраструктура на пософистицирани и организирани закани. Исто така, сајбер-безбедноста се појави како критична грижа, при што инфраструктурата сè повеќе се потпира на дигиталните системи и интернетот, што ги прави ранливи на сајбер-напади, хакирање и упад во базите на податоци.¹⁶⁴

Следствено на тоа, улогата на приватната безбедност во заштитата на критичната инфраструктура значително еволуира со текот на времето, поттикната од промените во природата на заканите, технолошкиот напредок и промените во регулаторните и политичките рамки. Па така, приватните безбедносни фирми почнуваат да нудат повеќе специјализирани услуги, вклучувајќи мерки за сајбер-безбедност, процена на ризик и управување со кризи. Интеграцијата на технологијата, како што се системите за надзор, биометриските контроли за пристап и алармните системи, стануваат стандардна практика во заштитата на критичната инфраструктура и се зголемува соработката со органите за спроведување на законот и владините агенции, при што приватните фирми за обезбедување често обезбедуваат експертиза и ресурси.¹⁶⁵

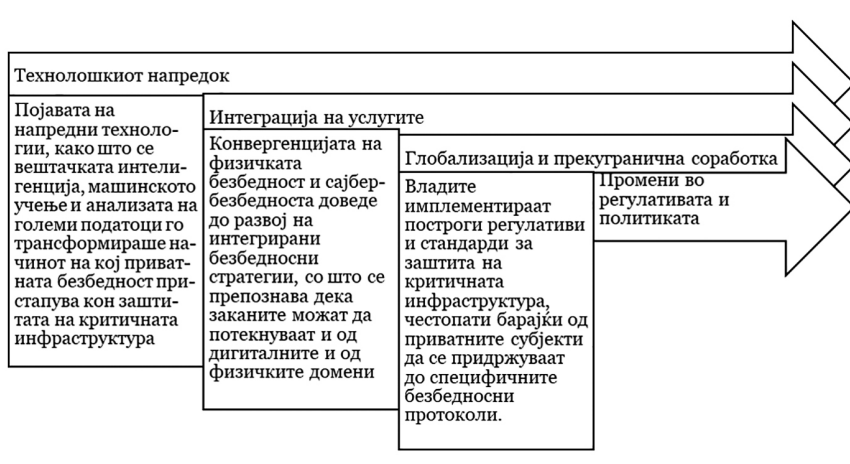
Во тековното безбедносно опкружување и системска поставеност, улогата на приватната безбедност во заштитата на критичната инфраструктура е незаменлива, особено во ера каде заканите се повеќеслојни и постојано се развиваат. Со обезбедување специјализирани услуги за физичка безбедност, сајбер-безбедност, управување со ризик и одговор при итни случаи, приватните

164 Bakreski O., Bardjieva M. L. (2023). The Need for an Integrated Approach in the Operation of Private Security Companies, Безбедносни дијалози. Issue No: 1 14, стр. 95-107.

165 Resilience of Critical Infrastructure Protection, European Commission - Directorate-General for Humanitarian Aid and Civil Protection, достапно на: <http://ec.europa.eu/echo>.

безбедносни фирми помагаат да се обезбеди издржливост и континуитет на основните услуги што го поткрепуваат современото општество.¹⁶⁶

Слика 5: Современи случувања и трендови во заштитата на критичната инфраструктура и ангажманот на приватната безбедност



Нема дилема дека глобалната природа на заканите, како што се сајбер-нападите и тероризмот, доведе до зголемена меѓународна соработка и размена на информации. Приватните безбедносни фирми често работат преку границите, поради што е потребно разбирање на различни правни и регулаторни средини. Во оваа насока, алокацијата на ограничените ресурси, утврдувањето каде да се распределат безбедносните инвестиции е постојан предизвик, особено кога се појавуваат нови закани. Оттука, јавно-приватните партнерства претставуваат императив во стопанисувањето со добратата од општ интерес.¹⁶⁷

¹⁶⁶ Bakreski, O. (2019) The Role of Private Security in the Protection of Critical Infrastructure in Urban Areas, Security Dialogues.

¹⁶⁷ Закон за концесии и јавно приватно партнерство („Службен весник на Република Македонија“ бр. 6/12, 144/14, 33/15, 104/15 и 215/15 и

Од аспект на карактеристиките, еластичноста и приспособливоста се атрибутите што се припишуваат на денешните концепции во доменот на заштитата на критичната инфраструктура од страна на приватното обезбедување. Тука фокусот е сè повеќе на градење на отпорност во системите и инфраструктурата, со што ќе се осигури дека тие можат брзо да се опорават од одредени прекин и нарушувања. Ова вклучува не само технички мерки туку и стратегии за кризна комуникација и континуитет на операциите. При обезбедувањето на овие услуги, активностите на приватните безбедносни агенции/компаниии може да имаат потенцијално позитивни последици за нивните клиенти, локалното население во областа на дејствување, општата безбедносна средина, уживањето на човековите права и владеењето на правото, имајќи предвид дека како што мерките за безбедност стануваат понаметливи, се наметнува потребата за рамнотежа помеѓу обезбедувањето безбедност и заштитата на индивидуалната приватност и граѓанските слободи.¹⁶⁸

12. ИДНИ ПРАВЦИ НА РАЗВОЈ НА ДЕЈНОСТА ПРИВАТНО ОБЕЗБЕДУВАЊЕ

Во насока на детерминирање на понатамошните правци на развој на дејноста приватно обезбедување, идентификувани се идните тенденции во приватното обезбедување, што се обликувани од комбинација на технолошки, на општествени, на економски и на регулаторни фактори. Овие фактори колективно го обликуваат идниот пејзаж на приватното обезбедување, влијаејќи врз стратегиите и врз технологиите што компаниите ќе ги усвојат во наредните години.¹⁶⁹

„Службен весник на Република Северна Македонија“ бр.153/19, 261/19, 89/22 и 65/23).

¹⁶⁸ The Physical Protection of Critical Infrastructures and Key Assets. The White House Washington, 2003.

¹⁶⁹ Report Summary. Security 2025. A Roadmap for the Future. Australian Security Industry Association Limited., достапно на: <https://>

Меѓу нив се издвојуваат:

- Регулаторни и правни предизвици во уредување и дезигнација на нивните надлежности и улога во рамки на националната и на меѓународната регулатива.
- Лиценцирање и акредитација, што всушност значи дека државите имаат различни барања за лиценцирање и акредитација на приватните фирми и персоналот за обезбедување. Ова може да претставува предизвик за компаниите кои работат на меѓународно ниво.
- Употреба на сила и одговорност – примената на сила од страна на персоналот за приватно обезбедување е чувствително прашање, особено во однос на одговорноста и правната одговорност. Во таа насока се вршат значителен број експертски дебати за соодветните регулаторни рамки за регулирање на овие аспекти.¹⁷⁰
- Обука и професионализација: постои тренд кон поригорозни програми за обука на безбедносниот персонал, што опфаќаат области, како што се: решавање конфликти, прва помош, сајбер-безбедност и културна чувствителност.¹⁷¹
- Професионални стандарди и сертификација: здруженијата на индустријата и регулаторните тела промовираат повисоки професионални стандарди и програми за сертификација за да го подобрат кредибилитетот и доверливоста на приватните безбедносни субјекти.¹⁷²

asial.com.au/common/Uploaded%20files/ASIAL_Public/Security%202025%20Summary.pdf

170 Meehan, B., & Benson, B. L. (2017). Does private security affect crime?: a test using state regulations as instruments. *Applied Economics*, 49(48), стр. 4911–4924, достапно на: <https://doi.org/10.1080/00036846.2017.1296551>

171 Ruddell, R., Thomas, M. O., & Patten, R. (2011). Examining the Roles of the Police and Private Security Officers in Urban Social Control. *International Journal of Police Science & Management*, 13(1), стр. 54-69, достапно на: <https://doi.org/10.1350/ijps.2011.13.1.210>

172 Prenzler, T., Sarre, R. (2023). Public Space Crime Prevention Partnerships: Reviewing the Evidence. In: Blackstone, E., Hakim, S., Meehan,

- Глобални безбедносни закани и одговор – тука првенствено се вбројуваат тероризмот и организираниот криминал. Тековните закани од тероризмот и организираниот криминал продолжуваат да ја поттикнуваат побарувачката за приватни безбедносни служби, при што од агенциите за приватна безбедност се наметнува императивот да останат понапред од тактиките и заканите што се развиваат. Во оваа категорија спаѓаат и пандемиите и јавното здравје, што беше потврдено со појавата на пандемијата КОВИД-19, што ја истакна улогата на приватната безбедност во кризите во јавното здравје, вклучувајќи ги и задачите како што се спроведување мерки за карантин и управување со пристап до објекти. Ова го прошири опсегот на услуги што ги нудат многу приватни безбедносни фирми.¹⁷³

Приватната безбедност стана критична компонента во добавувањето на безбедноста во глобални рамки, приспособувајќи се на различни предизвици и промени во меѓународниот пејзаж. Најзначајните и клучни глобални тенденции во приватната безбедносна индустрија се:

- Раст и експанзија, пред сè раст на пазарот, што подразбира дека приватната безбедносна индустрија бележи значителен раст ширум светот, поттикнат од зголемената побарувачка за безбедносни услуги и во јавниот и во приватниот сектор. Ова вклучува традиционална физичка безбедност, сајбер-безбедност и специјализирани консултантски услуги.¹⁷⁴

B.J. (eds) Handbook on Public and Private Security. Competitive Government: Public Private Partnerships. Springer, Cham, достапно на: https://doi.org/10.1007/978-3-031-42406-9_3

173 Walby, K. and Joshua, C. (2021), “Community crime prevention and crime watch groups as online private policing”, *Safer Communities*, Vol. 20 No. 4, стр. 237-250, достапно на: <https://doi.org/10.1108/SC-05-2021-0016>

174 Stoddard A., Harmer A., DiDomenico V. (2008) The use of private security providers and services in humanitarian operations. Humanitarian Policy Group Overseas Development Institute 111 Westminster Bridge Road London.

- Глобален дофат. Многу приватни безбедносни компании сега работат на меѓународно ниво, обезбедувајќи услуги преку границите. Оваа експанзија е олеснета од глобализацијата и меѓународната природа на модерниот бизнис и трговија.¹⁷⁵
- Диверзификација на услугите и понудата на сеопфатни безбедносни решенија. Компаниите сè повеќе нудат интегрирани безбедносни решенија што ги опфаќаат и физичките и дигиталните аспекти. Ова ги вклучува услугите како сајбер-безбедност, управување со ризик и разузнавачка анализа.¹⁷⁶
- Специјализација. Постои тренд кон специјализација, при што компаниите се фокусираат на специфични области како што се блиска заштита, поморска безбедност или безбедност на настани.
- Технолошка интеграција: напредно надгледување и следење. Употребата на напредни технологии како ВИ, машинско учење и препознавање лица во системите за надзор станува сè поприсутна. Овие технологии ја подобруваат способноста за откривање и одговор на заканите.
- Сајбер-безбедност. Со порастот на сајбер-заканите, приватните безбедносни фирми сè повеќе се вклучени во обезбедувањето услуги за сајбер-безбедност. Ова вклучува откривање закани, одговор на инциденти и консултации за најдобрите практики за заштита на дигиталните средства.
- Јавни-приватни партнерства. Приватните безбедносни компании често соработуваат со владини агенции, особено во области како што се заштитата на критичната инфраструктура, контратероризмот и јавната безбедност.¹⁷⁷
- Усогласеност со регулативата. Постои зголемена потреба приватните фирми за обезбедување да се усогласат со

175 NATO-Private Sector Dialogues focus on NATO 2030 initiative, достапно на: https://www.nato.int/cps/en/natohq/news_184601.htm.

176 Button, M. (2019) *Private policing*. 2d ed. London: Routledge. достапно на: 10.4324/9781351240772

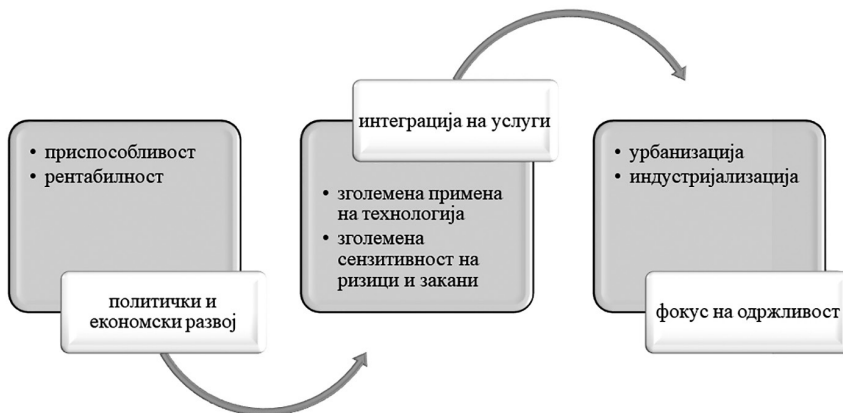
177 Welsh, B. C., Farrington, D. P., & Gowar, B. R. (2015). Benefit-cost analysis of crime prevention programs. *Crime and justice*, 44(1), стр. 447-516.

- меѓународните регулативи и стандарди, што може значително да се разликува во различни јурисдикции.¹⁷⁸
- Фокус на корпоративната општествена одговорност и етички стандарди. Постои зголемена контрола на етичките практики на приватните безбедносни фирми, особено во однос на употребата на сила, почитувањето на човековите права и приватноста на податоците. Притоа, иницијативите за општествената одговорност се евидентни преку вклучување на приватната безбедносна индустрија и нејзините субјекти во ангажмани за подобрување на заедниците, концепти на одржливост и транспарентни деловни практики.
 - Зголемена побарувачка за лична безбедност – блиска и ВИП заштита. Побарувачката за лични безбедносни услуги порасна, поттикната од фактори како што се зголемувањето на разликите во богатството, експонираноста на јавните личности и зголемената загриженост за безбедноста.¹⁷⁹
 - Безбедност за области со висок ризик: компаниите и поединците што работат во области со висок ризик, како што се конфликтните зони или регионите со висока стапка на криминал, честопати се потпираат на приватни безбедносни служби за заштита;
 - Зголемување на побарувачката. Како што продолжуваат меѓународните конфликти и нестабилноста, побарувачката за приватни безбедносни служби, вклучително и локално регрутирање, најверојатно ќе продолжи да расте.
 - Технолошка интеграција. Употребата на технологија во обуката и операциите може да помогне да се ублажат некои предизвици поврзани со локалното регрутирање, како што се стандардизирана обука и подобрена комуникација.

178 Schiller E., Aidoo A., Fuhrer J., Stahl J., Ziörjen M., Stiller B. (2022) Landscape of IoT security, Computer Science Review, Volume 44, 2022.

179 Alexandra A., Baker D. P., Caparini M. (2009) Private Military and Security Companies. Ethics, Policies and Civil-Military Relations. 1st Edition. Routledge.

Слика бр. 6. Еволуција на глобалниот пазар на приватно обезбедување и придвижувачки фактори
Извор: Global Market Trends. Interim report Jan-June 2024, Securitas.



Во согласност со статистичките предвидувања, пет милијарди луѓе ќе се преселат во градовите до 2030 година. Како што ќе расте населението во градовите и ќе се зголемува притисокот врз предвидените јавни ресурси, се менува начинот на управување со градовите, со цел тие да бидат поефикасни, но и побезбедни и, според тоа, попаметни во однос на примената на новите технологии и користењето на расположливите ресурси.¹⁸⁰

Во тој контекст, конвенционалното управување со мегалополисите и големите градови се движи кон примената на концепт на управување таканаречен „паметни градови“. Тоа е концепт што започнува да се користи во 1990-тите како резултат на развојот на новите технологии во модерните градски инфраструктури, главно во Соединетите Американски Држави.¹⁸¹ Сепак, имајќи предвид

¹⁸⁰ Deloitte. (2015). Smart Cities. How rapid advances in technology are reshaping our economy and society, достапно на: <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf>

¹⁸¹ Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., & Walker, S. (2012). Building understanding of smart

дека како концепт своите најрани почетоци во рудиментирани облици ги бележи веќе еден век, постојат многу дефиниции за концептот на паметен град, како и тоа дека е модификуван со одредени варијанти и синтагми како што се „интелигентен град“ или „дигитален град“.¹⁸²

Безбедноста и доброто функционирање на паметен и безбеден град се потпираат на меѓусебно поврзани, сложени и меѓусебно зависни мрежи и системи: јавни транспортни мрежи, енергија, комуникација, трансакциска инфраструктура, цивилна безбедност и агенции за спроведување на законот, патен сообраќај, мрежи и услуги од јавен интерес понудени од јавни и приватни оператори.¹⁸³

Оттука, паметните градови се дефинираат со способноста да се создадат или да се усвојат решенија за предизвиците и можностите за трансформирање на градовите во попродуктивни и попогодни места за живеење за нивните граѓани, со искористување на новите технологии во безбедноста и хипер-поврзаноста на интернет на нештата.¹⁸⁴ Таков е примерот со градот Истанбул во Република Турција, кој преку градската општинска управа на Истанбул (İMM) во 2015 година започна сеопфатна иницијатива за трансформација во паметен град. Визијата паметен град (Smart City Vision) на Истанбул развиена во рамките на овој проект за трансформација е до 2029 година да биде еден од најпаметните градови во светот, каде најголем акцент се става во подобрување на квалитетот на животот во градот, преку планирање, координација

city initiatives. In *Electronic Government: 11th IFIP WG 8.5 International Conference, EGOV 2012, Kristiansand, Norway, September 3-6, 2012. Proceedings 11* (pp. 40-53). Springer Berlin Heidelberg.

¹⁸² McCrie, R. D. (2016). *Security operations management* (3rd ed.). Waltham: Butterworth-Hernemann.

¹⁸³ Security for smart and safe cities, including for public spaces. CORDIS - EU research results. European Commission https://cordis.europa.eu/programme/id/H2020_SU-INFRA02-2019

¹⁸⁴ Zanella, A., Bui, N., Castellani, A.P., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 1, стр. 22-32.

и исполнување кратки, среднорочни и долгорочни стратешки цели, што се идентификувани во осум фокусни области: мобилност, животна средина, енергија, управување, економија, живот, луѓе и безбедност.¹⁸⁵

¹⁸⁵ Smart Cities and the Role of Defense [online., достапно на: <https://www.defenceturkey.com/tr/icerik/smart-cities-and-the-role-of-defense-2475>

Глава II

КРИТИЧНА ИНФРАСТРУКТУРА – РАНЛИВОСТ, ОТПОРНОСТ И ЗАШТИТА

1. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ ОКОЛУ ПОИМОТ И УПОТРЕБАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Концептот и важноста на критичната инфраструктура се здобива со значење во државите во последните децении на XX век. Светскиот интерес за заштита на критичната инфраструктура беше поттикнат од главните настани како што се нападите врз кулите на Светскиот трговски центар во Њујорк во февруари 1993 година, потоа сајбер-нападите врз системите на американските воздухопловни сили во Римските лаборатории од 1994 година, како и нападите на Ал Каеда врз сообраќајната критична инфраструктура во Мадрид во 2004 година, Шпанија.¹⁸⁶ Критичните инфраструктурни системи се карактеризираат со нивната сложена структура и нивното силно влијание врз сите аспекти на општеството.

Првата формална дефинициска поставеност на концептот се појавил во 1996 година со Извршниот налог 13.010 на претседателот Клинтон.¹⁸⁷ Оттогаш се смета дека термилолошките дивергенции околу поимот и употребата на концептот поврзан со критичната инфраструктура се во постојан режим на унапредување и подобрување. Во одредени земји или контексти, термините: *системи за спасување, витални општествени функции или критични ентитети* се користат и може да се разгледуваат како тесно поврзани концепти.¹⁸⁸ Затоа што има различни контексти, тради-

186 Sachs, M. (2022). Reflections on executive order 13010, достапно на: <https://mccrary.auburn.edu/work/insights/reflections-on-executive-order-13010>

187 US Election Assistance Commission. (2017). History of critical Infrastructure designation, достапно на: <https://www.eac.gov/ci-scoop-history-of-criticalinfrastructure-designation>

188 Pursiainen, C., & Kytomaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What

ции и вредности низ земјите и не постои вистински меѓународен консензус, ниту политички ниту академски, околу прашањето кои општествени системи е потребно да се сметаат за критични инфраструктури. Сепак, има доближувања и сличности дека тоа се: системите за телекомуникации, електрична енергија, здравствена заштита, гас и нафта, транспорт, банкарство и финансии, водоснабдување, итните служби и континуитет на владата што се разгледуваат како критична инфраструктура.¹⁸⁹

За целите на дискусијата претставени во оваа книга, усвоена е приспособена верзија на дефиницијата за европска критична инфраструктура (ECI), исполнета со специфики на ниво на средства од Патриотскиот акт.¹⁹⁰ Конкретно, критичните инфраструктурни системи се дефинирани како „Системи и средства или дел од нив, без разлика дали се физички или виртуелни, лоцирани во која било група на нации или држави чие нарушување или уништување би имало значително влијание врз најмалку две нации или држави членки на групите“. Во тој контекст, инфраструктури што претставуваат значајна јавна инвестиција и каде што дури и мали нарушувања можат да го намалат функционирањето на системите и предизвикуваат значителна општествена штета може да се наречат критични инфраструктури.¹⁹¹

Барока и соработниците ја перцепираат инфраструктурата (т.е. збир на објекти што обезбедуваат услуги неопходни за

does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), стр. 85–101, достапно на: <https://doi.org/10.1080/23789689.2022.2128562>

189 European Commission. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L333, стр. 164–197.

190 US Congress. (2021). Public law 107-56 uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, достапно на: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>.

191 Brown, G. At all. (2006). Defending critical infrastructure. *Interfaces* (Providence), стр. 530–544, достапно на: <https://doi.org/10.1287/inte.1060.0252>.

функционирање на еден град), како критична ако нејзиното не-исправно функционирање ја загрозува безбедноста, економијата, начинот на живот или јавноста, здравјето на еден град, регион или дури и држава.¹⁹²

За одделот за внатрешна безбедност на САД, инфраструктурен систем, „чија неспособност или уништување би имал ослабено влијание врз одбраната и економската безбедност“, би можел да биде и да се смета за критичен.¹⁹³

Европската комисија ги идентификува системите на критичната инфраструктура како физички и информатички капацитети, мрежи, услуги и средства кои, доколку бидат нарушени или уништени, би имале сериозно влијание врз здравјето, безбедноста или економската благосостојба на граѓаните или ефективно функционирање на владите во земјите на Европската Унија.¹⁹⁴

Разбирањето на сложеноста и значењето на заштитата на критичната инфраструктура е најважно, не само за економскиот просперитет и јавната благосостојба, туку и за заштитата на националната безбедност. Затоа функционирањето на системот на критична инфраструктура е под постојана закана од широк спектар безбедносни закани. Во справување со потенцијалните закани, системот на критична инфраструктура вклучува мноштво елементи со различно ниво на важност, категоризирани во неколку нивоа и поврзани меѓусебно преку врски од разни видови и интензитет.¹⁹⁵ Ваквиот структурен аранжман води кон широка корелација помеѓу

192 Barroca, B., Serre, D., Youssef, D. (2012). Le concept de r´esilience `al’`epreuve du g´enie urbain Le concept de r´esilience `al’`epreuve du g´enie urbain, достапно на: <https://doi.org/10.4000/vertigo.12469>.

193 U.S Department of Homeland and Security. (2022). Critical Infrastructure Security & Resilience Research (CISRR) Fact Sheet, достапно на: <https://www.dhs.gov/science-and-technology/publication/critical-infrastructure-security-resilience-research-fact-sheet>

194 EUR-Lex. (2010), достапно на: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum%3A33259>, 2010.

195 Good Progress on Tackling Hybrid Threats. European Commission Press Release, достапно на: [A_Europe_that_protects_good_progress_on_tackling_hybrid_threats.pdf](https://ec.europa.eu/pressroom/content/2022-05-11-good-progress-on-tackling-hybrid-threats.pdf).

поединечните потсистеми, што го утврдува методот и интензитетот на ширење на влијанието од дефектите во системите на критична инфраструктура врз зависните потсистеми и општеството.

2. ПРОЦЕС НА ЗАШТИТА И ГРАДЕЊЕ ОТПОРНОСТ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Претходните анализи и објавени публикации повеќе акцент ставаат на заштитата. Меѓутоа, во текот на последната деценија, дојде до промена кон употреба на концептот за *отпорност*, движејќи се од начинот на размислување на заштита од антагонистички закани кон поширок концепт што вклучува доверливост, ранливост, безбедност и обновување на критичните инфраструктури.¹⁹⁶

На 30 април 2024 година, Советот за национална безбедност на Белата кука го објави Меморандумот за национална безбедност за безбедност и отпорност на критичната инфраструктура. Овој меморандум се надоврзува на активностите што Агенцијата за сајбер-безбедност и безбедност на инфраструктурата (ЦИСА – CISA) како и агенциите ширум федералната влада ја преземаат во партнерство со критичните инфраструктурни заедници во Америка повеќе од една деценија. Меморандумот, исто така, ја заменува Директивата за претседателска политика 21 (ППД-21 – PPD-21) за безбедност и отпорност на критичната инфраструктура, што беше издадена пред повеќе од една деценија за да се воспостави национална политика за безбедност и отпорност на критичната инфраструктура. Безбедносното опкружување значително се промени откако беше издаден ППД-21, преминувајќи од контратероризам на стратегиска конкуренција, напредок во

196 Pursiainen, C., & Kytomaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), 85–101., достапно на: <https://doi.org/10.1080/23789689.2022.2128562>

технологијата, како што е вештачката интелигенција, малициозни сајбер-активности од актери на националните држави и потребата за зголемена меѓународна координација. Оваа промена во пејзажот на заканите, заедно со зголемените федерални инвестиции во критичната инфраструктура на САД, ја поттикна потребата да се ажурира ППД-21 и да се издаде новиот меморандум.¹⁹⁷

Следен пример е промената на името во програмите на Европската Унија од Директива за идентификација и означување на европските критични инфраструктури и процената на потребата од подобрување на нивната заштита (или директивата ЕЦИ – ECI) во Директивата за отпорност на критичните ентитети (или директивата ЦЕР – CER) во 2022. Критичен ентитет е концепт воведен со новата директива и дефиниран како „даватели на основни услуги“.¹⁹⁸ За оваа публикација критичните субјекти може да се поистоветат со операторите на критична инфраструктура. За порамнување со новата номенклатура на ЕУ користиме отпорност на критичната инфраструктура во оваа публикација.

Во современата литература не постои единствена дефиниција за тоа што е ризик. Одредени автори сметаат дека ризик претставува ситуација во која постои можност од отстапување во однос на посакуваниот резултат,¹⁹⁹ за други тоа е мерка на веројатност дека последиците штетни за животот, здравјето, сопственоста и/или животната средина може да се појават како резултат на некои одредени опасности,²⁰⁰ додека трети сметаат

197 America's Cyber Defense Agency (2024). National Coordinator for critical infrastructure security and resilience, достапно на: <https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience>

198 European Commission. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L333, стр. 164–197.

199 Vaughan J. Emmett, *Risk Management*, John Wiley & Ins Inc, New York, 1996, стр. 23.

200 Sage P. Andrew, *Systems Engineering for Risk Management*, Norwel MA, 1995, стр. 4.

дека ризик е комплексна особина со која се опишува веројатност од настанување штетни настани и очекувана големина на последици од тие настани за сиот систем и за време на утврдената должина на временскиот интервал или за време на одредена мисија.²⁰¹ Исто така, според некои дефиниции ризикот претставува неможност да се предвиди резултатот од идните случувања со целосна сигурност.

Процесот на управување со ризик се однесува на капацитетот на субјектот соодветно да се подготви и да одговори на сериозни инциденти што вклучуваат критична инфраструктура на регион или нација²⁰² и најчесто се идентификува како Процес за заштита на критичната инфраструктура (ЦИП – CIP). Процената на ризикот е круцијална во процесот заштита на критичната инфраструктура со оглед на нејзината улога во идентификацијата на заканите, процената на ранливостите и евалуацијата на влијанието врз средствата и системите.²⁰³ Карактеристичен пример за таков процес е Рамката за управување со ризик на Националниот план за заштита на инфраструктурата (НИПП – NIPP) развиена од Одделот за домашна безбедност во САД, како што е прикажано на Слика 7.²⁰⁴

201 Бакрески О., Триван Д. и Митевски С., *Корпоративски безбедносен систем*, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012.

202 European Council. (2008). Directive 2008/114 - Identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

203 Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. *JRC Technical Notes*, 1(1), стр. 1–53.

204 Homeland Security. (n.d.). National infrastructure protection plan - risk management framework, достапно на: https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf.

Слика 7: Процеси на заштита на критичната инфраструктура²⁰⁵



При изработка на методологија за процена на заканата, подобро е да се користи систематски и мерлив пристап за да се оцени кои се специфичните закани за одредена држава и критична инфраструктура. Структурата на овој методолошки пристап има три основни принципи на безбедност:

1. идентификација,
2. имплементација и
3. одржливост.

Кога се прави процена за закана, аналитичарите главно го користат првиот принцип, идентификација, а другите два принципа имаат значајна улога во процесот на управување со ризиците. Првиот чекор е да се идентификува заканата или заканите врз критичната инфраструктура, а следната задача е да се спроведе соодветна безбедносна реакција пропорционална со таквата закана.

За целите на дискусијата и анализата презентирани во овој труд, можеме да ги категоризираме овие предизвици во два главни типа:

1. Предизвици засновани на домени (заштита на критична инфраструктура). Околината во која се одвива секој

²⁰⁵ Critical Infrastructure Protection Process. Source: Homeland Security, ndFigure 2. ISO 31,000 risk management process. Source:Pursiainen and Rød (2021), стр. 368.

процес на процена на ризик е уникатна по природа и е значително засегната од карактеристиките на домениот на разгледуваниот случај за заштита на критична инфраструктура. Иако овие предизвици варираат во голема мера помеѓу секој поединечен случај, регионот на ЕУ претставува одличен пример за предизвиците со кои потенцијално би можеле да се соочиме: отсуство на влада и постоење мноштво граници и правни рамки и полабави контроли на рамковната имплементација и преглед.²⁰⁶ Иако беа направени конкретни обиди да се обезбеди хармонизирана рамка за националните процени на ризик на европско ниво²⁰⁷, тие не беа во можност да дадат значителни резултати поради аверзијата на земјите членки да споделуваат чувствителни информации и недостатокот на ентитет или процес да служи како „медиум“ за споделување.²⁰⁸

2. Хоризонтални методолошки предизвици и прашања за процена на ризик. Познати се хоризонтални прашања поврзани со имплементацијата на процес за процена на ризик во кој било вид домен. Ваквите прашања може да вклучуваат нецелосно дефинирање на контекстот на процената на ризик и нејзините цели²⁰⁹, несоодветен избор на алатки за процена на ризик, недостаток на

206 Pursiainen, C., & Rød, B. (2021). National disaster risk assessments in Europe. How comparable are they and why? *Risk, Hazards & Crisis in Public Policy*, 12(2), стр. 194–214, достапно на: <https://doi.org/10.1002/rhc3.12215>

207 Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Scientific and Technical Research Reports, Report EUR 27332 EN, достапно на: <https://doi.org/10.2788/621843>

208 Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, 39(10), стр. 6100–6119, достапно на: <https://doi.org/10.1016/j.enpol.2011.07.010>

209 Lyon, B. K., & Hollcroft, B. (2012). Risk Assessments. *Professional Safety*, 57(12), стр. 28–34.

објективност,²¹⁰ потенцијален неуспех да се идентификуваат опасностите и да се приоритизираат ефективно²¹¹ и неефикасна комуникација помеѓу засегнатите страни во процесот на процена на ризик.²¹²

Методологијата на процесот на заштита на критичната инфраструктура може да ги содржи следните елементи:

- ✓ прецизна идентификација на критичните инфраструктури и нивна дефиниција;
- ✓ утврдување на опасностите што се закануваат на идентификуваната критична инфраструктура;
- ✓ анализа на ранливост/чувствителност на оние инфраструктури на кои им се заканува ризик и оние што придонесуваат за прекин во случај на намерен напад и во случај на природни или случајни настани;
- ✓ процена на ризик од деградација или губење на критичната инфраструктура и приоритет на оние што се ризични и се ранливи;
- ✓ примена на контрамерки каде што не постои прифатлив ризик, со цел да се заштитат инфраструктурните капацитети за ефикасно извршување на активностите во итни ситуации.²¹³

210 Hermansson, H. (2012). Defending the conception of “objective risk”. *Risk Analysis: An International Journal*, 32(1), стр. 16–24, достапно на: <https://doi.org/10.1111/j.1539-6924.2011.01682.x>

211 Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 152, 137–150, достапно на: <https://doi.org/10.1016/j.res.s.2016.02.009>

212 Andersson, M. G at all. (2020). Communication inside Risk Assessment and Risk Management (COMRISK). EFSA Supporting Publications, 17(7), 1891E, достапно на: <https://doi.org/10.2903/sp.efsa.2020.EN-1891>

213 Ribeiro, S.L., Bezerra, E.K., Nakamura, E.T., (2005). “Critical Infrastructure in Brazil“, *1st IEEE International Workshop on Critical Infrastructure Protection*, 3-4th, Darmstadt, Nov 2005, достапно на: <http://www.cpqd.com.br> и достапно на: <http://www.cpqdusa.com>

Дополнителните предизвици вклучуваат различна перцепција за сериозноста на ризикот проценета од различни поединци, неефикасното толкување на информациите што произлегуваат од процесот на проценка на ризик²¹⁴ и неусогласеноста во процената на ризикот за прифаќање.²¹⁵ Клучен хоризонтален предизвик за време на имплементацијата на генеричкиот процес на проценка на ризикот се однесува на таканаречениот „човечки агол“, со други зборови, аспектите на донесување одлуки што критично влијаат врз спроведувањето на процесот на заштита на критична инфраструктура и се суштински поврзани со претходните предизвици.²¹⁶

Главната цел на овој труд е да обезбеди теоретски придонес кон подобро разбирање на некои од предизвиците со кои се соочуваат за време на спроведувањето на процесот на проценка на ризик во контекст на целокупниот процес на заштита на критична инфраструктура. Очигледно е дека критичката анализа (во соодветна широчина и длабочина) на сите можни параметри што влијаат на овој процес би била невозможна задача во контекстот и ограничувањата на една студија. Поради оваа причина, нашето истражување експлицитно е насочено кон специфичен предизвик од секоја од категориите наведени погоре, врз основа на следните критериуми:

- ✓ Предизвик заснован на домен (Заштита на критична инфраструктура) за кој практичарите сметаат дека е критичен за успешното спроведување на процесот на

214 Fairbrother, A. at all. (1995). Risk assessment in practice: Success and failure. *Human and Ecological Risk Assessment: An International Journal*, 1(4), стр. 367–375, достапно на: <https://doi.org/10.1080/10807039509380021>

215 Reid, S. G. (2000). Acceptable risk criteria. *Progress in Structural Engineering and Materials*, 2(2), стр. 254–262, достапно на: [https://doi.org/10.1002/1528-2716\(200004/06\)2:23.O.CO;2-K](https://doi.org/10.1002/1528-2716(200004/06)2:23.O.CO;2-K)

216 Lazari, A. (2014). *European critical infrastructure protection*. Springer International Publishing.

процена на ризик во контекстот на заштита на критична инфраструктура (транснационални предизвици).

- ✓ Хоризонтален предизвик за кој има перцепција дека неакадемската литература е критична за успешното имплементирање на процесот процена на ризик во кој било домен, но не е детално проучен во контекст на домениот заштита на критична инфраструктура (донесување одлука –хеуристика и предрасуди).

Посебните цели поврзани со нашата студија се следните:

Цел 1: Истражување како транснационалните предизвици влијаат врз спроведувањето на процесот на процена на ризик во контекст на заштита на критична инфраструктура.

Цел 2: Истражување како хеуристиката и предрасудите при одлучувањето влијаат врз спроведувањето на процесот на процената на ризикот во контекст на заштита на критична инфраструктура.

Цел 3: Идентификација на специфични силни страни, празнини и можности во врска со предизвиците идентификувани во претходните цели и формулирање прашања што ќе ја поттикнат идната истражувачка работа во овој домен.

3. КОНЦЕПТУАЛИЗАЦИЈА НА ТРАНСНАЦИОНАЛНИТЕ ПРЕДИЗВИЦИ ВО ЗАШТИТА НА КРИТИЧНА ИНФРАСТРУКТУРА

Разликите во концептуализацијата и во дефинирањето на критичната инфраструктура во различни земји се резултат на различната перцепција на заканите и безбедносните ризици и разлики во географските и во историските услови, но влијаат и социополитичките фактори.

Имало многу обиди да се согледа карактеристиката на ризикот што се однесува на преминувањето на националните и другите граници во контекст на критичната инфраструктура.

Термините „транснационален“²¹⁷ и „прекуграничен“²¹⁸ се широко користени во литературата за оваа цел. Иако поимите „транснационален“ и „прекуграничен“ може да се сметаат дека се еквивалентни до некоја линија,²¹⁹ нивната употреба како дел од целокупниот процес на заштита на критичната инфраструктура треба да се разгледува преку следните констатации:

- Терминот „транснационално“ конкретно алудира на државата или на границите на нацијата што е во согласност со ставот изразен дека мултинационалната средина, како што е случајот со ЕУ, ќе обезбеди значителен увид во студијата.

- Се смета дека што се однесува до процена на ризикот, терминот „прекуграничен“ често се користи во контекст на ризикот за животната средина или јавното здравје и на ресурсите што ги преминуваат националните граници, како, на пример реките, што се надвор од опсегот на овој труд.²²⁰

Врз основа на претходните размислувања, може да се каже дека терминот „транснационален“ претставува валидна основа за водење на дискусијата што следи, но сепак, треба да се каже дека алтернативните термини, исто така, беа експлицитно земени предвид во нашата анализа, секаде каде што се појавија во литературата во контекст на разгледуваната тема.

217 Van der Vleuten, E., & Lagendijk, V. (2010b). Transnational infrastructure vulnerability: The historical shaping of the 2006 European “blackout”. *Energy Policy*, 38(4), стр. 2042–2052, достапно на: <https://doi.org/10.1016/j.enpol.2009.11.047>

218 Borghetti, F., Marchionni, G., Gugiatti, E., Ambrosi, C., Czerski, D., & Melzi, C. (2020). Cross border critical infrastructure: A new approach for the protection evaluation. Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference ESREL 2020 PSAM (Vol. 15ed. стр. 21–26, Venice. June, 2020

219 Cambridge on-line Dictionary. (2021). *Transnational*, достапно на: <https://dictionary.cambridge.org/dictionary/english/transnational>

220 Linnerooth-Bayer, J., & Sjøstedt, G. (Eds.). (2010). Transboundary risk management. Routledge.

3.1. Транснационални размислувања за заштита на критичната инфраструктура

Општо земено, конкретно се тврди дека денешните ранливости на Европа се наоѓаат токму поради нивниот транснационален карактер.²²¹ И покрај неговата препознатлива важност, концептот на транснационални предизвици во контекст на процена на ризик за заштита на критичната инфраструктура не го привлече вниманието на истражувачите до некој значаен степен.²²² Некои примери го вклучуваат моделот ЕУРАМ (EURAM)²²³, рамката ЕУРАКОМ (EURACOM)²²⁴ и бројни мултинационални кризни вежби поврзани со критичната инфраструктура, управувани од ЕУ и од НАТО.²²⁵ Слично на тоа, регулаторните напори за справување со транснационалните размислувања преку подобрување на споредливоста на националните процени на ризик во ЕУ не станаа влијателни поради неуспех на самиот потфат.²²⁶ Друг таков пример

221 Högselius, P., Hommels, A., Kaijser, A., & Van der Vleuten, E. (Eds). (2013). *The making of Europe's critical infrastructure: Common connections and shared vulnerabilities*. Palgrave Macmillan, UK.

222 Pursiainen, C., & Rød, B. (2021). National disaster risk assessments in Europe. How comparable are they and why? *Risk, Hazards & Crisis in Public Policy*, 12(2), стр. 194–214, достапно на: <https://doi.org/10.1002/rhc3.12215>

223 Klaver, M., et al. (2008). *European risk assessment methodology for critical infrastructures*. 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA) (pp. 1–5). Rotterdam, Netherlands: IEEE, достапно на: <https://doi.org/10.1109/infra.2008.5439614>.

224 CORDIS. (2011). *European Risk Assessment and Contingency Planning Methodologies for Interconnected energy networks (EURACOM)*, достапно на: <https://cordis.europa.eu/article/id/89833-increasing-the-security-of-europes-energy-supply>

225 European Commission. (2016). VITEX 2016 беше првата EUWide вежба фокусирана на ефектите од големи дефекти на критичната (електрична) инфраструктура низ Европа. Види повеќе на: <https://erncip-project.jrc.ec.europa.eu/events/vitex-2016-was-first-eu-wide-exercisefocussed-effects-large-scale-failure-critical>

226 European Commission. (2022). Opening remarks by commissioner Johansson at the press conference on EU critical infrastructure resilience, достапно на: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_6265

е напорот да се реши проблемот со споредливоста помеѓу националните процени на ризик користејќи го моделот на критични инфраструктури и системски ризици и методологија за проценка на отпорноста (КРИСПРАМ – CRISRRAM)²²⁷, што, исто така, не привлече значајно внимание.

Потребно е да се потенцира дека концептот на транснационални предизвици навистина често се разгледува во контекст на литературата за критична инфраструктура, но не на директен начин. Особено, следните области на истражување се природно поврзани со транснационални размислувања:

- *Закани за критичната инфраструктура од странски противници.* Ова е вообичаено разгледување во анализите за критичната инфраструктура што се однесуваат на земји надвор од европскиот простор, почесто САД, Австралија и други географски простори со малку, доколку ги има, соседи на националните држави. Во овој случај, транснационалните закани и ризик се однесуваат на противници надвор од заднината на соодветната земја, што имаат за цел да ѝ наштетат на критичната инфраструктура на некој начин.
- *Сајбер-закани* што му пркосат на секој концепт на географска граница.²²⁸ Овој дел од активностите се однесува на вид сајбер-ризик што е инхерентно транснационален поради меѓусебно поврзаната, прекугранична природа на денешницата-инфраструктура на информатичка и комуникациска технологија. Критичните инфраструктури во својот развој сè повеќе користат информациски технологии, со оглед на тоа дека тие стануваат достапни на пошироката јавност. Како резултат на интензивното користење информатички технологии од страна на различни сектори, доаѓа до формирање голема меѓузависност

227 Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Scientific and Technical Research Reports, Report EUR 27332 EN, достапно на: <https://doi.org/10.2788/621843>

228 ENISA. (2021). European Union Agency for Cybersecurity, достапно на: <https://www.enisa.europa.eu/>

меѓу различните инфраструктурни сектори. Во тој контекст, особено е забележителна и значајната зависност на речиси сите инфраструктурни сектори од информациските технологии (што прераснаа во еден критичен, а најверојатно и најкритичен инфраструктурен сектор). Оттука постоењето голема меѓуповрзаност на инфраструктурата е еден од најголемите проблеми во управување со инфраструктурата.²²⁹

- *Закани против физичките елементи* на критичната инфраструктура што се протегаат низ границите на земјата.²³⁰ Истражувачката работа идентификувана во овој контекст почесто се гледа во однос на земјите членки на ЕУ и други земји.

Во контекст на овој труд, терминот „транснационализам“ во голема мерка „ќе се однесува на повеќекратни врски и интеракции што ги поврзуваат луѓето или во ситуации преку границите на националните држави“²³¹ со неговото значење засновано врз различните концептуални премиси на авенијата на капиталот и реконструкцијата на „местото“ или локалитетот. Изненадувачки, иако и покрај фактот дека транснационализмот е концепт заснован на домен што често се поврзува со проектите на заштита на критичната инфраструктура, тој не е директно опфатен во објавените студии како составен дел од процесот на ЗКИ. Конкретно, прегледот на литературата не идентификуваше рамки што експлицитно се однесуваат на постоењето на транснационална динамика и пропусти во просторната инфраструктура за време на спроведувањето на процесот на ЗКИ. Овој наод создава потреба за понатамошно истражување и анализа во однос на актуелната

229 Li, H., et al, *Strategic Power Infrastructure Defense*, Proceedings of the IEEE, 2005.

230 Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security. The transnational dimension. In A.D. Sofaer & S. E. Goodman (Eds), *The Transnational Dimension of Cyber Crime and Terrorism*, (стр. 1–34). Hoover Institution Press, достапно на: <https://onlinebooks.library.upenn.edu/webbin/metabook?id=hoovercyber>.

231 Vertovec, S. (1999). Conceiving and researching transnationalism. *Ethnic and Racial Studies*, 22(2), стр. 447–462, достапно на: <https://doi.org/10.1080/014198799329558>

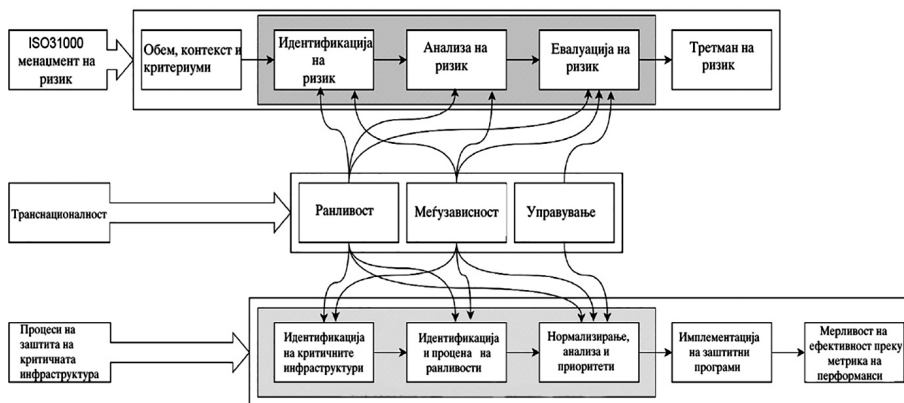
потреба од експлицитно адресирање на транснационализмот како дел од имплементацијата на процесот на заштита на критичната инфраструктура, како и потенцијалниот ризик од неговото неразгледување. Сепак академската литература дава значајни докази за оваа тема, како што ова е дискутирано во следниот поддел.

3.2. Влијанието на транснационализмот во процесот на заштита на критична инфраструктура

Потребата за експлицитно разгледување на параметрите на транснационализмот како дел од процесот на заштита на критична инфраструктура е интензивно нагласена во академската литература. Особено се тврди дека во контекст на заштита на критична инфраструктура, концептот на транснационализам влијае на имплементацијата на процена на ризикот во контекст на процесот на ЗКИ на повеќе нивоа.

Посебен фокус е даден на димензиите на ранливост, меѓузависност и владеење. Слика број 8 ја дава графичката рамка за олеснување на дискусијата во врска со потенцијалните ефекти на транснационализмот во контекст на процесот на заштита на критична инфраструктура.

Слика број 8: Влијанието на транснационализмот во процесот на заштита на критичната инфраструктура



Конкретно, сликата го илустрира процесот на генерички „златен стандард“ ISO31000:2018 за управување со ризик, како и генеричка рамка за имплементација на процесот на заштита на критична инфраструктура. Помеѓу нив се прикажани главните димензии на транснационализмот што се во фокусот на нашата дискусија. Помеѓу секој од овие аспекти и соодветните фази што потенцијално може да бидат засегнати за време на имплементацијата на процесот ISO31000:2018 (и следствено за време на имплементацијата на процесот ЗКИ) се повлечени стрелките на асоцијација, според академската литература. Слика број 8 покажува дека таму постои силна поврзаност помеѓу транснационалните димензии и сите фази од процесот на имплементација на проценка на ризикот во контекст на процесот на заштита на критична инфраструктура.

4. ФУНДАМЕНТАЛНИ КОНЦЕПТИ

4.1. Ранливост

Неусогласеноста во толкувањето на ранливоста не е невообичаена, како што беше прикажана во примерот на случајот „Европско затемнување“.²³² Доделувањето на проценета вредност на ранливоста за време на фазата на проценка на ризикот од процесот на заштита на критична инфраструктура, особено во транснационален контекст, е многу предизвикувачки пред да се случи вистински дефект. Дури и тогаш, големината на нарушувањето е под влијание на мерките за ублажување спроведени пред настанот. Примерот на спорната ранливост на производството на електрична енергија во ЕУ поттикна зголемување на регулатор-

²³² Van der Vleuten, E., & Lagendijk, V. (2010). Interpreting transnational infrastructure vulnerability: European blackout and the historical dynamics of transnational electricity governance. *Energy Policy*, 38(4), стр. 2053–2062, достапно на: <https://doi.org/10.1016/j.enpol.2009.11.030>

ните овластувања за ЕУ под изговор за економски и аргументи за одржливост. Сепак регулативата не е секогаш одговорот со оглед на парадоксот на понекогаш дополнителна ранливост на критичната инфраструктура што се произведува со самите мерки што се спроведуваат за да се намали ранливоста на прво место.²³³ Намерното узурпирање на функционирањето на мрежите за снабдување со електрична енергија може да има големо негативно влијание врз националната безбедност, националната економија и на животот на секој човек. Бидејќи дистрибутивната мрежа за електрична енергија е многу разгранета, голем предизвик е да се зачува нормалното функционирање на оваа инфраструктура.²³⁴ Саботажите како што се сајбер-нападите во голема мера може да го оштетат производството и дистрибуцијата на електрична енергија и да се спречи нормална комуникација и функционирање на информациските системи и не само на национално, туку и на транснационално ниво.

Поставениот линеарен пристап за решавање на ранливостите изолирано, под претпоставка дека резултатите ќе бидат збирни, исто така е предизвикан.²³⁵ Се предлага зајакнување на прекуграничните пристапи за намалување на ранливоста во препознавањето на појавата на просторни статистички жаришта како резултат на група опасности наместо влијание на поединечни опасности и национални пристапи, барем во Европа, што се резултат на нормална практика на позиционирање на поединечни земји во рамките на рангирањето на ранливоста што, пак, е поврзано

233 Van der Vleuten, E., & Disco, C. (2004). Water wizards: Reshaping wet nature and society. *History and Technology*, 20(3), стр. 291–309, достапно на: <https://doi.org/10.1080/0734151042000287014>

234 Massoud, A., “Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)”. *Computer* (IEEE computer society), 2002.

235 Birkmann, J., at all, (2021). Regional clusters of vulnerability show the need for transboundary cooperation. *Environmental Research Letters*, 16(9), 094052, достапно на: <https://doi.org/10.1088/1748-9326/ac1f43>

со линеарните модели на процена на ризикот што се користат.²³⁶ Ова сознание го дискредитира секој процес на процена на ризик што излегува надвор од границите на една нација, ако се претпостави дека резултатите од поединечниот пристап кон процената на ризикот и ранливоста би можеле да се зголемат, со што транс-националната консолидација на процената на ризикот за целите на заштита на критичната инфраструктура е неверојатна.

4.2. Меѓузависност

Поимите меѓузависност и зависност често се користат наизменично во литературата за заштита на критична инфраструктура. Зависност „...е еднонасочен однос на две инфраструктури преку кои состојбата на зависната инфраструктура е под влијание или е во корелација со состојбата на другиот“ и меѓузависноста е „...меѓусебна поврзаност помеѓу ентитетите (објекти, поединци, групи)“.²³⁷ Двата термина ќе се користат како што е споменато во соодветните референци заради конзистентност.

Критичните инфраструктурни системи се сложени, односно меѓусебно зависни системи, додека потенцијалниот дефект што се шири меѓу инфраструктурите може да влијае на целината на мрежата. Иако беше предложено дека владите во такви случаи треба да прифатат неопределен ризик, литературата за критична инфраструктура е богата со обиди да се следат модели и процеси што се справуваат со предизвикот за соодветно управување со меѓузависноста на критичната инфраструктура. Овие обиди во голема мера го разгледуваат предизвикот на меѓузависноста

236 Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Scientific and Technical Research Reports, Report EUR 27332 EN. <https://doi.org/10.2788/621843>.

237 Luijff, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, 35, 100471, достапно на: <https://doi.org/10.1016/j.ijcip.2021.100471>

исклучиво во националните граници. Типичен пример на САД е раната пионерска работа на Риналди, Пиренбум и Кели²³⁸, кои го воведоа концептот на инфраструктурата како сложени адаптивни системи и ги истакнаа предизвиците во развојот, примена и потврдување на методологиите за моделирање и симулација за анализа на меѓузависност на инфраструктурата. Потенцијалот за ширење на неуспехот на критичните инфраструктурни системи и поврзаните каскадни ефекти низ мрежата, исто така, беше дискутиран;²³⁹ сепак, очигледно е дека таквите каскадни ефекти може да се прошират и надвор од географските граници на една нација.

Главната цел на графикот на меѓузависност на критичната инфраструктура (КИ) е да се добие разбирање за глобалното однесување на мрежата на КИ врз основа на локалната динамика (т.е. локалното однесување или перформансите на КИ). Локалната динамика е опишана преку внатрешен модел во секој јазол. Јазлите ги претставуваат системите на критичната инфраструктура и рабовите на зависностите меѓу нив. Се користи квалитативна скала за да се карактеризира состојбата на секој јазол, што се движи од 1 (најдобро) до 5 (најлошо). Во зависност од типот на јазолот, нивоата ја претставуваат функционалноста или достапноста на компонентата. Некои можни толкувања се дадени во Табела 1:

238 Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), стр. 11–25.

239 Eusgeld, I., Nan, C., & Dietz, S. (2011). “System-of-systems” approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6), стр. 679–686, достапно на: <https://doi.org/10.1016/j.res.2010.12.010>

Состојба	Функционалност	Достапност	Загуба/штета
1.	Целосна функционалност	Нормално	Нема или е занемарлива
2.	Делумно намалена	Мало доцнење	Одредени мали оштетувања што може да се поправат
3.	Одредени ограничувања, но сè уште оперативна	Одредени прекини или доцнења, но сè уште достапна	Одредени сериозни оштетувања или повеќе помали проблеми, поправката бара значително време или финансии
4.	Големи ограничувања	Големи прекини или доцнења	Тешко или долготрајно оштетување, поправката одзема многу време или е скапа
5.	Нефункционална	Недостапна	Неуспех, треба целосно да се замени или барем привремено

Табела 1. Интерпретација на состојби на јазол²⁴⁰

Транзициите меѓу секоја состојба ја претставуваат внатрешната динамика на секоја КИ кога е под влијание на специфичен инцидент. Критично-инфраструктурните сектори се меѓусебно поврзани, а нивните широко распространети нарушувања предизвикуваат каскадни ефекти. Меѓузависните инфраструктури се ранливи на ризик од каскадна природа. Каскадните ефекти се користат за ажурирање на јазлите во КИ со менување на состојбата на јазолот. Транзициите меѓу функционалноста на секој јазол ја

²⁴⁰ Meisam Gordan (2024). Protecting critical infrastructure against cascading effects: The PRECINCT approach, Resilient Cities and Structures Volume 3, Issue 3, стр. 1-19, достапно на: <https://www.sciencedirect.com/science/article/pii/S277274162400019X>

претставуваат внатрешната динамика на секоја критична инфраструктура кога е погодена од специфичен тежок инцидент, на пример, бомбардирање или пожар.

Новите процени го преземаат предизвикот за разгледување на прашањето во многу пошироки рамки и спроведуваат анализа на единствена мултинационална база на податоци за закани, неуспеси, прекини и загубена инфраструктура. Резултатите беа конзистентни во тоа што анализата на трендовите, зависностите и феномените на неуспех од вообичаена причина, и подобреното разбирање на другите феномени поврзани со критичната инфраструктура во двете овие студии диктира дека распространетата мрежа на зависности има потенцијал да предизвика значителна штета и општествено нарушување и може да биде предизвик да се обезбеди и да се управува.²⁴¹ Имајќи предвид дека истражувачката работа во транснационален контекст би била зададена со методолошки размислувања како што е споредливоста на резултатите, двосмисленоста на термините што се користат во различните географии и соодветните сектори и потребата за анализа на зависноста,²⁴² ефективната процена на ризик за транснационален систем е уште попредизвикувачки.

4.3. Управување

Со оглед на сложеноста на проектите за критична инфраструктура, природно е да се претпостави дека управувањето со транснационална критична инфраструктура од националните „силоси“ потенцијално може да воведо проблеми со управувањето. Дополнително, вистинската испорака на управување за КИ може

241 Luijff, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, 35, 100471, достапно на: <https://doi.org/10.1016/j.ijcip.2021.100471>

242 Theocharidou, M., & Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. *Scientific and Technical Research Reports, Report EUR 27332 EN*, достапно на: <https://doi.org/10.2788/621843>.

да биде доведена во прашање кога националните процени на ризик не се усогласени и координирани. Се сугерира дека координираното владеење низ транснационалниот проект за КИ ќе се соочи со предизвици ако се спроведува само преку соодветните „национални“ алатки на секоја земја. ЕУ е истакната како карактеристичен пример за ваквите предизвици.²⁴³ Конкретно, се тврди дека и покрај појавата на секторски специфични генерални директорати и поддршката на Заедничкиот истражувачки центар (ЦПЦ – JRC), неговата сопствена истражувачка единица, управувањето со КИ останува фрагментирано. Беше предложено дека овие предизвици може да се припишат на тешкотиите во управувањето со програмите за меѓусекторска политика и значителните трошоци за усогласување поврзани со високото ниво на регулаторна и институционална различност.²⁴⁴ На ниво на проектот, транснационалните јавно-приватни партнерства остануваат поистакната платформа за финансирање и испорака на проекти за КИ иако „...феномени ... се движат од лабави форми за соработка до правно обврзувачки договори за имплементација на конкретни проекти“.²⁴⁵ Сепак, прашањата поврзани со одговорностите, ризикот, овластувањата во партнерството, разликите меѓу партнерите во методите на работа, како и недостатокот на посветеност од партнерите, создаваат значителни предизвици за управувањето со проектите поврзани со критичната инфраструктура.

Сумирајќи, анализата на литературата сугерира дека транснационализмот може да има силно влијание врз имплементацијата

243 Bossong, R. (2014). The European programme for the protection of critical infrastructures—meta-governing a new security problem? *European Security*, 23(2), стр. 210–226, достапно на: <https://doi.org/10.1080/09662839.2013.856307>

244 May, P. J., & Koski, C. (2013). Addressing public risks: Extreme events and critical infrastructures. *Review of Policy Research*, 30(2), стр. 139–159, достапно на: <https://doi.org/10.1111/ropr.12012>

245 Schäferhoff, M., Campe, S., & Kaan, C. (2009). Transnational public-private partnerships in international relations: Making sense of concepts, research frameworks, and results. *International Studies Review*, 11(3), стр. 451–474, достапно на: <https://doi.org/10.1111/j.1468-2486.2009.00869.x>

на процена на ризик во контекст на заштита на критичната инфраструктура, особено во однос на ранливоста на средствата, меѓузависноста помеѓу елементите и функциите на проектот преку националните граници, и управување, или негово отсуство, во однос на управувањето со транснационалните елементи.

5. ПРИСТАПИ/МОДЕЛИ ЗА ИДЕНТИФИКАЦИЈА И АНАЛИЗА НА МЕЃУЗАВИСНОСТА И КАСКАДНИТЕ ЕФЕКТИ ПОМЕЃУ СИСТЕМИТЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Неодамна сè повеќе студии за отпорност на критичната инфраструктура ги анализираат врските и меѓузависностите, кои се првенствено помеѓу системите на критичната инфраструктура, а понекогаш помеѓу секторите на КИ и нетехничките компоненти во човековата средина. Човечкото опкружување ги вклучува физичките, атмосферските, биолошките, социјалните, економските и политичките компоненти, услови и фактори кои влијаат на државата, состојбата и квалитетот на условите за живот, вработувањето и здравјето.²⁴⁶ Нан и Сансавини ја оценуваат отпорноста имајќи ја предвид инфраструктурната меѓузависност, што може да одговара на една инфраструктура (внатрешна меѓузависност) или на повеќе инфраструктури (надворешна меѓузависност).²⁴⁷

Одејќи подалеку од секторите на критичната инфраструктура, одредени анализи ја преиспитуваат отпорноста на интеракциите помеѓу инфраструктурите и социоеколошките компоненти.²⁴⁸ Во

246 National Academies of Sciences, Engineering, and Medicine. (1992). Assessment of the U. S. Outer Continental Shelf Environmental Studies Program: III. Social and Economic Studies. Washington, DC: The National Academies Press, достапно на: <https://doi.org/10.17226/2062>.

247 Nan, C., Sansavini, G., 2017. A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety* 157, 35–53.

248 Markolf, S. At all. (2018). Interdependent infrastructure as linked social, ecological, and technological systems (SETs) to address lock-in and enhance resilience. *Earth's Future* 6 (12), 1638–1659

современото општество, поради меѓузависност на сите изградени средини, штетата на еден единствен систем на КИ, како физичко нарушување или дисфункција, често влијае на другите урбани компоненти. Отпорноста на меѓузависноста помеѓу инфраструктурите бара секој систем да ја гарантира неговата функционалност кога се соочени со неуспехот на другите системи.²⁴⁹ Овој тренд на отпорност на критичната инфраструктура доаѓа од свесноста за каскадните ефекти поради меѓусебно поврзаните урбани компоненти. Зголемените опасности бараат урбан систем за справување со потенцијалните каскадни ефекти со негативни последици врз КИ. Понатаму, од пристап заснован на последици негативните ефекти предизвикани од искористените ресурси треба да се имаат предвид при анализата на меѓузависностите. Ова мислење е подеднакво поврзано со несаканите ефекти од спроведувањето на гореспоменатите дејства.²⁵⁰

Севкупно, отпорноста на критичната инфраструктура може да се опише преку различни својства, способности, фази и потенцијални ефекти (позитивни, негативни, несакани или каскадно) при размислување за спроведување акции и меѓузависност. Опсегот на урбаните компоненти е широк и може да се категоризира во социоекономски системи, владина организација, природа, енергетски системи и техничко-инфраструктурни системи.²⁵¹ Според некои историски настани, потеклото на катастрофалните влијанија врз системите на КИ (прекинувања, изградба, акција, итн.) веќе се случија на социоекономските системи, на владини организации, на природата и на системите за проток на енергија.

249 Serre, D., Heinzl, C., (2018). Assessing and mapping urban resilience to floods with respect to cascading effects through critical infrastructure networks. *Int. J. Disaster Risk Reduct.* 30, 235–243, достапно на: <https://doi.org/10.1016/j.ijdrr.2018.02.018>.

250 Robert, B., H'emon, Y., (2012). Organizational resilience: A multidisciplinary sociotechnical challenge. *Resilience and urban risk management* 119–125

251 Yang, Z., et al. (2022). Resilience of Social-Infrastructural Systems: Functional Interdependencies Analysis. *Sustain.* 14, достапно на: <https://doi.org/10.3390/su14020606>.

Разбирањето на меѓузависноста во и помеѓу инфраструктурните сектори е од клучно значење за зајакнување на отпорноста. На пример, потпирањето на енергетскиот сектор на „паметната технологија“ покажува како ранливостите во една област може да предизвикаат каскадни неуспеси кај другите. Покрај тоа, интегрирањето на ИТ, ОТ и ИОТ во енергетските системи, како што се паметните мрежи, ја подобрува ефикасноста и одговорноста, но исто така воведува нови пропусти. Овие напредни системи користат ИТ и ИОТ за да го оптимизираат производството, дистрибуцијата и потрошувачката на електрична енергија. Сепак нивната дигитална природа ги прави подложни на сајбер-напади што може да ја нарушат дистрибуцијата на енергија, што влијае на сè, од снабдување со електрична енергија во станбени простории до индустриски операции. Ефективноста на службите за итни случаи, вклучително и полициски, противпожарни и медицински тимови за одговор, зависи од доверливите комуникациски мрежи и напојувањето. Прекршување во енергетскиот или во комуникацискиот сектор може да ги попречи овие критични услуги, да го одложи времето на одговор и да ги загрози животите.

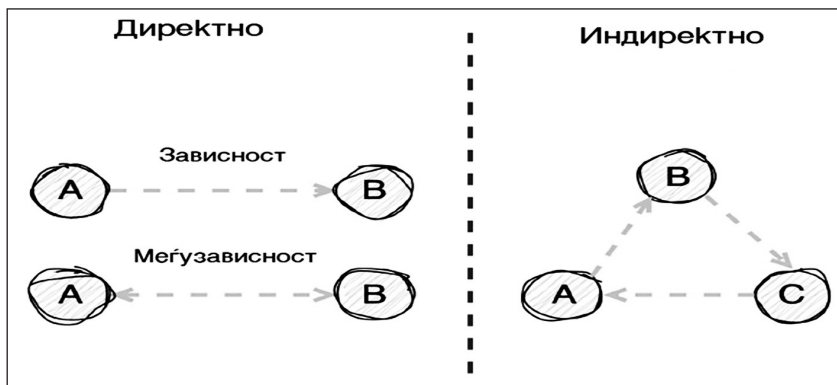
Во контекст на критичната инфраструктура, зависноста може да се дефинира како: „Поврзување или конектирање помеѓу две инфраструктури, преку кои состојбата на една инфраструктурата влијае или е во корелација со состојбата на другата“.²⁵²

Термините зависност и меѓузависност често се користат наизменично. Сепак, понекогаш има потреба да се прави разлика меѓу нив. Во оваа теза, зависноста се однесува на еднонасочна врска помеѓу системите (лево на слика број 9). Спротивно на тоа, меѓузависноста се однесува на двонасочна врска помеѓу системите или директно (лево на Слика број 9) или индиректно преку циклус за повратни информации (десно на Слика број 9).²⁵³

252 Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), стр. 11–25, достапно на: <https://doi.org/10.1109/37.969131>

253 Setola, R., & Theocharidou, M. (2016). Modelling Dependencies Between Critical Infrastructures. In *Managing the Complexity of Critical*

Слика број 9: Илустрација на зависноста и меѓузависноста и директната и индиректната меѓузависност



Зависностите, исто така, може да се класифицираат врз основа на видот на врската што постои помеѓу две инфраструктури²⁵⁴, каде што:

- *Физичката (меѓу)зависност* се однесува кога функционирањето зависи од физичкиот излез од друга критична инфраструктура (на пример, струја или вода).

- *Сајбер (меѓу)зависноста* се однесува на тоа кога зависи состојбата на инфраструктурата од информации што се пренесуваат преку информациската инфраструктура.

- *Географската (меѓу)зависност* се однесува кога елементи од повеќекратни инфраструктури се во непосредна просторна близина.

- *Логичката (меѓу)зависност* се однесува кога состојбата на една критична инфраструктура зависи од состојба на другата преку контрола, регулација или други механизми што не можат да се определат за физички, географски или сајбер.

Меѓузависноста помеѓу инфраструктурите може да доведе до последици што се шират од еден систем до друг. Во зависност

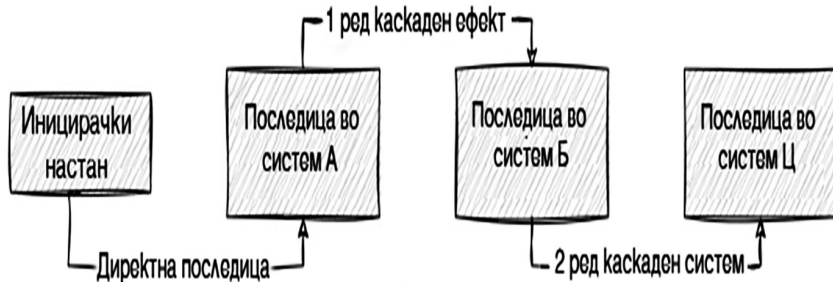
Infrastructures (стр. 19–41). Springer, Cham, достапно на: <https://doi.org/10.1007/978-3-319-51043-9>

²⁵⁴ Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), стр. 11–25, достапно на: <https://doi.org/10.1109/37.969131>

од контекстот, овие последици често се наречени индиректни или *каскадни ефекти*. На пример, индиректна последица е утврден концепт во управувањето со ризикот од поплави,²⁵⁵ додека каскадните ефекти почест о се користат во контекст на критичната инфраструктура.²⁵⁶ Овој труд ги претполага концептите за синоним, но се претпочита терминот „каскаден ефект“, бидејќи е поблиску поврзан со критичната инфраструктура и посоодветно ја образложува како динамична појава.

Бидејќи еден каскаден ефект може да доведе до друг, понекогаш е неопходно да се специфицира редоследот по кој се појавуваат. На пример, ако иницирачки настан, како што е природна катастрофа, неуспех или прекин, се случува и влијае на системот А, ова се смета за директен ефект.²⁵⁷ Ако влијанието врз системот А доведе до влијание на системот Б, ова се смета како каскаден ефект од прв ред итн. (види Слика број 10).

Слика бр. 10. Шематски преглед на редот на каскадни ефекти



255 Jha, A. K., Bloch, R., & Lamond, J. (2012). *Cities and Flooding: A Guide to Integrated Urban Flood Risk Management for the 21st Century*. The World Bank, достапно на: <https://doi.org/10.1596/978-0-8213-8866-2>

256 Hilly, G., at all. (2018). Methodological Framework for Analysing Cascading Effects from Flood Events: The Case of Sukhumvit Area, Bangkok, Thailand. *Water*, 10(1), стр. 81, достапно на: <https://doi.org/10.3390/w10010081>

257 Johansson, J., at all. (2015). *Cascading Effects in Past Events – A Database Structured Around Originators and Dependencies* (Research Report Casceff Deliverable 2.3). Division of Risk Management and Societal Safety, Lund University.

Во литературата за критична инфраструктура и за управување со ризик се користат три, главно, различни значења на каскадни ефекти.

1. Прво, каскаден ефект може да се однесува на настан каде што инфраструктурата (негативно) влијае на друга инфраструктура.
2. Второ, каскадните ефекти може да се однесуваат кога условите во инфраструктурата активираат повеќе или поголеми последици во рамките на истата инфраструктура, понекогаш наречени и каскадни неуспеси. Ова се случи, на пример, во затемнувањето во 2003 година во САД и во Канада, каде дефект на високонапонски далновод доведе до преоптоварување на дополнителни далноводи, што следствено предизвика откажување на повеќе линии до голем дел од Југоисточна Канада и осум држави во САД што биле погодени од затемнувањето.²⁵⁸
3. Трето, каскадните ефекти може да се однесуваат кога природна опасност предизвикува дополнителни опасности. На пример, поплава може да доведе до нестабилност на земјата и да предизвика лизгање на земјиштето.²⁵⁹ Во оваа теза се фокусираме на првиот вид каскадни ефекти, каде што инфраструктурата негативно влијае на друга инфраструктура и последователно влијае врз општеството.

²⁵⁸ OECD. (2011). *Future Global Shocks*. Organisation for Economic Co-operation and Development, достапно на: <http://www.oecd-ilibrary.org/content/book/9789264114586-en>.

U.S.-Canada Power System Outage Task Force. (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*.

²⁵⁹ Gill, J. C., & Malamud, B. D. (2014). Reviewing and visualizing the interactions of natural hazards: Interactions of Natural Hazards. *Reviews of Geophysics*, 52(4), стр. 680–722, достапно на: <https://doi.org/10.1002/2013RG000445>

Постојат три главни пристапи за да се идентификуваат и да се анализираат меѓузависноста и каскадните ефекти помеѓу критичната инфраструктура.

Еден пристап е консултација со експерти за критична инфраструктура за да се процени силата на меѓузависноста или последиците од каскадните ефекти. Ова, на пример, може да се направи преку анкети²⁶⁰, интервјуа²⁶¹ или работилници.²⁶² Овие методи главно идентификуваат меѓузависности и собираат податоци за понатамошна анализа.

Вториот пристап е да се разгледаат настаните од минатото што довело до каскадни ефекти помеѓу критичната инфраструктура за да се соберат емпириски докази и да се извлечат заклучоци за распространетоста или природата на меѓузависности.²⁶³

И на крај, се користат пристапи базирани на симулација на модели на критична инфраструктура и нивните меѓузависности за проучување како се појавуваат каскадни ефекти. Овој пристап е генерално доста баран и бара експертиза, на пример, инженерство, математика и компјутерски науки. Успехот на таквиот пристап, исто така, е многу зависен од достапните податоци за критична инфраструктура и меѓузависност. Сепак, тоа може да биде и најмоќниот пристап за проучување на каскадните ефекти

260 Lauge, A., Hernantes, J., & Sarriegi, J. M. (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, 8, стр. 16–23, достапно на: <https://doi.org/10.1016/j.ijcip.2014.12.004>

261 Chang, S. At all (2014). Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments: Toward Disaster-Resilient Cities. *Risk Analysis*, 34(3), стр. 416–434, достапно на: <https://doi.org/10.1111/risa.12133>

262 Deltares. (2023). *CIRCLE – Critical Infrastructures: Relations and Consequences for Life and Environment*, достапно на: <https://www.deltares.nl/en/software/circle-critical-infrastructure-relations-and-consequences-for-life-and-environment-2/>

263 Luijck, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, 35, 100471, достапно на: <https://doi.org/10.1016/j.ijcip.2021.100471>

бидејќи овозможува експериментирање со системи што инаку би биле премногу скапи, опасни или нарушувачки.²⁶⁴ Користењето на пристапот базиран на симулација може да помогне во откривањето на слабите точки или ранливости во системот што инаку не би биле можни.²⁶⁵

Неколку релевантни видови модели може да се користат за моделирање на критичната инфраструктура, како модели базирани на агенти²⁶⁶, модели на системска динамика,²⁶⁷ графикони модели²⁶⁸, национални економски модели²⁶⁹ и модели базирани на проток.²⁷⁰

264 Birta, L. G., & Arbez, G. (2007). *Modelling and simulation: Exploring dynamic system behaviour*. Springer.

265 Pursiainen, C., & Kytomaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), 85–101, достапно на: <https://doi.org/10.1080/23789689.2022.2128562>

266 Kaegi, M., Mock, R., & Kroger, W. (2009). Analyzing maintenance strategies by agentbased simulations: A feasibility study. *Reliability Engineering and System Safety*, достапно на: 94(9), 1416–1421. <https://doi.org/10.1016/j.ress.2009.02.002>

267 Min, H.-S. J., Beyeler, W., Brown, T., Son, Y. J., & Jones, A. T. (2007). Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions (Institute of Industrial Engineers)*, 39(1), стр. 57–71, достапно на: <https://doi.org/10.1080/07408170600940005>

268 Espada, R. Jr., Apan, A., & McDougall, K. (2015). Vulnerability assessment and interdependency analysis of critical infrastructures for climate adaptation and flood mitigation. *International Journal of Disaster Resilience in the Built Environment*, 6(3), стр. 313–346, достапно на: <https://doi.org/10.1108/IJDRBE-02-2014-0019>

269 Svegrupp, L., Johansson, J., & Hassel, H. (2019). Integration of Critical Infrastructure and Societal Consequence Models: Impact on Swedish Power System Mitigation Decisions. *Risk Analysis*, 39(9), 1970–1996, достапно на: <https://doi.org/10.1111/risa.13272>

270 Johansson, J., Hassel, H., & Svegrupp, L. (2017). Capturing societal interdependencies from a flow perspective—Part I: Method and model. In *European Safety and Reliability Conference (ESREL 2016)*, стр. 2152–2159. CRC Press.

5.1. Моделирање меѓузависности помеѓу секторите на критичната инфраструктура: пристап/модел на системска динамика

Критичните настани не само што предизвикуваат штета на критичната инфраструктура, туку поради нивната релевантност во социоекономскиот контекст имаат влијание врз целото општество. Поради оваа причина КИ претставува стратешки елемент за носителите на одлуки што треба да се има предвид при дефинирањето на акциите за прв одговор и поставувањето на општествените политики и инвестиции. Критичните настани, како што се временски екстремни настани, инциденти поврзани со човечки грешки, терористички напади што традиционално се сметаа за ретки настани, а процедурите за итни случаи беа насочени кон минимизирање на последиците и забрзување на закрепнувањето. Отпорноста се здоби со висока цена бидејќи пошироката надворешна средина почна да се менува. Всушност, тековниот процес на приватизација на многу критични инфраструктури, менувајќи го фокусот од успешен производ на услугата кон економската благосостојба на компанијата како целина, генерира за овие средства ефект на „темпирана бомба“, со намалување на одржувањето и одложување програми за замена.²⁷¹ Во исто време, климатските промени предизвикаа временските шеми да станат и понепредвидливи и поекстремни, а исто така се појави нова закана од тероризам и особено сајбер-тероризам, што генерира нов вид нарушувања со потенцијално многу големо влијание, имено оштетување поврзано со системот. Последно, но не и најмалку важно, како што секторите на критичната инфраструктура станаа посоефицицирани и покомплексни, нивните различни делови станаа помеѓузависни, што на крајот го зголемува ризикот од ширење на нарушувачките ефекти на настани низ различни критични инфраструктури, така наречен домино ефект.

271 Warren K., Thurlby R. (2012). “Understanding and Managing the Threat of Disruptive Events to the Critical National Infrastructure”, Proceedings of the 30th International Conference of the System Dynamics Society.

Глобалната поврзаност, што доколку се користи на соодветен начин може да обезбеди и целосна анонимност, ги зголемува можностите на злонамерните корисници за пристап, кражба и злоупотреба на чувствителни информации. Голем дел од злонамерните корисници и криминални организации го препознаа сајбер-просторот како можност за брза добивка, притоа овозможувајќи им намален ризик од нивно откривање. Глобализацијата и анонимноста им овозможуваат на злонамерните корисници полесни напади кон претходно точно дефинирани жртви, но воедно и реализирање на многу поголеми операции и напади од многу поголеми размери.

Сајбер-напад врз енергетскиот сектор, на пример, може да има далекусежни последици. Енергетските системи се основа за другите критични инфраструктури, обезбедувајќи ја потребната моќност за нивното функционирање. Ако електричната мрежа е загрозувана, може да ги наруши постројките за третман на вода, транспортните мрежи и комуникациските системи. Ова може да доведе до верижна реакција на неуспеси, предизвикувајќи широк хаос и значителни нарушувања во секојдневниот живот. Истото може да се случи и со постројките за третман на вода. Овие капацитети се потпираат на стабилно напојување за прочистување и дистрибуција на чиста вода. Прекилот во енергетскиот сектор може да го запре работењето, што ќе доведе до недостиг на вода и потенцијално небезбедна вода за пиење. Во оваа насока се и примерите со транспортните мрежи. Современите транспортни системи зависат од електричната енергија и дигиталните комуникациски мрежи за сообраќајни сигнали, железнички операции и контрола на воздушниот сообраќај. Сајбер-напад врз електричната мрежа може да ги доведе овие системи во застој, предизвикувајќи одложувања, несреќи и логистички кошмари. Дополнително и телекомуникациските мрежи бараат постојана моќност за да функционираат. Прекршувањето на енергетскиот сектор може да ги прекине услугите на интернет, мобилните мрежи и комуникациските системи за итни случаи, попречувајќи ја способноста да се координираат одговорите на инцидентот.

Во овој контекст, способноста за моделирање на социоекономските влијанија што произлегуваат од нарушувања на

критичната инфраструктура стануваат сè поважни за одредување на најефективната инвестиција – стратегии за заштитни мерки и ублажување на последиците во случај на критични настани. Иако многу мерки за ублажување може да изгледаат круцијални и потенцијално ефективни, повеќето владини агенции треба да ги рангираат овие алтернативи за ефективно да ги распределат нивните ограничени буџети. Понатаму, постои сè поголема потреба да се разберат трошоците за целото општество - надвор од оние на првично погодените инфраструктури - целосно да се разбере големината на настанот и да се донесат соодветни одлуки за распределба.²⁷²

Во последните неколку години, моделот на системска динамика често се користи за спречување и управување со безбедносни/одбранбени прашања. Оваа симулација е способна инхерентно да ги земе предвид случајноста и меѓузависноста, што го карактеризираат однесувањето на реални деловни средини. Понатаму, овозможува вклучување на оние „меки“ променливи/варијабли типични за меѓусебно поврзаните општествени системи, што генерално не се земаат предвид во повеќето техники за линеарно моделирање што сè уште се користат во денешно време. Идејата зад пристапот на системска динамика е дека ако „системската структура го дефинира нејзиното однесување“, ²⁷³ потоа со точноста во анализирањето и утврдувањето на меѓусебните односи меѓу различни делови од системот, би било можно прецизно да се дефинира структурата на проблемот што се проучува и тоа на крајот би довело до точно разбирање на динамиката на системот. Така, системската динамика ја реплицира динамичната деловна реалност со моќ да „погледне во иднината“ и да го разбере влијанието врз повеќекратните клучни метрики. Дополнително, симулацијата му овозможува на корисникот да ја долови специфичната варијабилност на повеќекратни процеси и на крајот

272 Warren K., Thurlby R. (2012). “Understanding and Managing the Threat of Disruptive Events to the Critical National Infrastructure”, Proceedings of the 30th International Conference of the System Dynamics Society.

273 Strman, J.D. (2000). “Business dynamics: systems thinking and modeling for a complex world”.

дава резултати, што се попрецизни поредоци на големина отколку детерминистичка анализа.

Со интегрирањето на различните аспекти добиени преку теоретската рамка, симулациите на системска динамика имаат моќ да ги претставуваат главните меѓусебни влијанија на различните параметри, дефинирајќи за секое влијание дали е позитивно (директна причинско-последична врска) или негативно (инверзна врска), со што се дефинираат и вредноста и времето на овие влијанија.

Холистичкиот пристап на моделот на системска динамика, од една страна, бара целиот контекст да биде земен предвид, а од друга страна, факторите што се перцепираат како слаби или недоволно поврзани на процесите од интерес не се вклучени, со цел да не се заврши со модел што потоа би било тешко да се управува и/или да се толкува. Идентификацијата на релевантните влијанија во рамките на рамката за динамика на системот овозможува длабоко разбирање на меѓузависноста меѓу критичната инфраструктура како и на можните влијанија во случај на критични настани, имајќи ја предвид динамиката на инфраструктурата како функција на операции во другите. Таквиот пристап овозможува процена на влијанијата врз социоекономскиот контекст претставен како динамичен систем без да се бараат претпоставки за рамнотежни решенија. Всушност, социоекономските влијанија што произлегуваат од критичните настани се подобро опишани како ефекти предизвикани од динамиката на нерамнотежа. Значи, со оглед на горенаведените карактеристики, пристапот на системска динамика се чини дека е изводливо и соодветно решение за справување со прашања поврзани со безбедноста, а особено во областа на заштита на критичната инфраструктура.

5.2. Заштита на критичната инфраструктура – примери на каскадни ефекти

Првиот пример за каскадни ефекти ќе се согледа низ призмата на данскиот енергетски критичен сектор од 2023 година. Според неодамнешниот извештај на „Форескоут“ (Forescout), вториот бран на сајбер-нападите во данскиот енергетски сектор

во 2023 година ги искористил незакрпените заштитни сидови користејќи ново „популарен“ CVE-2023-27881 и дополнителни ИП-адреси (IP). Доказите сугерираат дека вториот бран бил дел од посебна кампања за масовна експлоатација. По вториот инцидент, понатамошни напади беа насочени кон изложените уреди во критичната инфраструктура ширум светот во следните месеци. Истражувачите открија бројни ИП-адреси што се обидуваат да ја искористат ранливоста на Zyxel CVE-2023-28771, што опстојува дури до октомври 2023 година, на различни уреди, вклучително и дополнителни огнени сидови на Zyxel. Во моментот, шест различни електроенергетски компании во европските земји користат заштитен сидови на Zyxel и може да останат подложни на потенцијална експлоатација од страна на злонамерни актери.

Овој неодамнешен доказ го нагласува императивот за енергетските фирми и организации што ја надгледуваат критичната инфраструктура да стават поголем акцент на користењето на тековните разузнавачки информации за закани, вклучувајќи информации за малициозни (ИП) IP и познати експлоатирани пропусти. Владите сè повеќе преземаат проактивни мерки со доделување средства за иницијативи насочени кон зајакнување на безбедносната положба на критичната инфраструктура во енергетскиот сектор.²⁷⁴

Вториот пример е поврзан со Kill Net во периодот 2022-2023 година. Главната закана беше насочена кон нарушувања на секторите за здравство, енергија и одбрана, а осомничен сторител беше проруската хакерска група KillNet. KillNet водеше голем број постојани DDoS напади врз украинските сојузници од почетокот на конфликтот. Неодамна тие ги таргетираа американските и холандските болници за помош во одбраната на Украина од Русија и ја укинаа електричната мрежа на Литванија во невидени DDoS напади. Тие, исто така, погодија над десетина американски аеродроми, откажувајќи ги летовите и прекинувајќи ги операторите.

KillNet беше гласен поддржувач на руската војна во Украина, користејќи DDoS напади како нејзино основно оружје за да ги

274 <https://www.securitymagazine.com/articles/100319-cybercriminals-target-critical-infrastructure-in-2023-cyberattack>

попречи операциите во сојузничките земји. Додека самиот DDoS не е закана за многу системи, тој се користи како покритие за по-сериозни напади на малициозен софтвер.²⁷⁵

Следен пример е поврзан со Колонијалниот гасовод од 2021 година. На 7 мај 2021 година, еден од најразорните сајбер-напади на инфраструктурата беше нападот на Колонијалниот нафтовод во САД. Најголемиот гасовод во САД и оној што снабдуваше повеќе од 45 % од гасот, дизелот и авионското гориво на Источниот брег беше принуден целосно да ги затвори своите мрежи и операции. Иако успеаја да ја вратат функцијата на системот до 18 мај, речиси 11 000 бензински пумпи сè уште беа без бензин. Хакерската група Dark Side, исто така, украде повеќе од 100 GB податоци од серверите на компанијата пред нападот и ја предала контролата дури откако „Колонијал“ Colonial платила 5 милиони долари во криптовалути. Уште позначајно, просечната цена во САД за гас по галон се зголеми на национално ниво до највисоката цена во последните шест години. Векторот за напад засега е сè уште непознат.²⁷⁶ Инцидентот ги истакна ранливостите во енергетскиот сектор и потенцијалот за каскадни ефекти врз другите критични услуги.

Интересен е и примерот со нападот со откуп на JBS Foods (Ransomware Attack) од 2021 година. Во јуни 2021 година, JBS Foods, еден од најголемите преработувачи на месо во светот, претрпе напад со откупен софтвер што принуди да ги запре операциите во Северна Америка и во Австралија. Нарушувањето влијаеше на глобалниот синџир на снабдување со храна, што доведе до страв од недостиг на месо и зголемување на цените. Овој инцидент ја нагласи меѓусебно поврзаната природа на прехранбената индустрија и нејзиното потпирање на континуирано работење.

Нема дилема дека и нападот на електричната мрежа во Украина е сериозен за анализа. Украинскиот електроенергетски објект „Прикарпатија Обленерго“ (Prykarpattya Oblenergo) во 2016

²⁷⁵ Bahadar Candan (2023). Top 5 critical infrastructure cyberattacks, Анапаја.

²⁷⁶ Analysis of top 11 cyber attacks on critical infrastructure, 2021, достапно на: <https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attacks-on-critical-infrastructure>

година беше уште еден пример на намерен, потенцијално смртоносен сајбер-напад. Половина од населението (~ 700.000 поединци) во Ивано-Франковскиот регион во Украина, остана без струја во средината на декември поради напад на малициозен софтвер. Наводно од озлогласената руска хакерска група Sandworm, нападот користел опасен малициозен софтвер наречен „Black Energy 3“. Сепак, овој напад не бил толку јасен. Хакерите, исто така, користеле убиец на хард-дискови, Kill Disk, фишинг со копје, кражба на акредитиви, VPN, за далечински пристап, DoS телефонски напади и други тактики. Прво, за да се заштитат од такви повеќевекторски напади, мрежите мора да се сегментираат една од друга, а секој дел од мрежната опрема мора да има овозможено логирање каде што е достапно. Мониторингот на мрежата е, исто така, најважен во овој случај и задолжителен.²⁷⁷

Случајот со NotPetya од 2017 година го заслужува потребното внимание. Овој напад со откупни софтвери ги таргетираше бизнисите и инфраструктурата на глобално ниво, попречувајќи ги операциите во различни сектори, вклучително и превозот, логистиката и производството. Нападот покажа како еден сајбер-инцидент може да има широки последици низ меѓусебно поврзаните системи. Исто така, и примерот Саудиска Арамко од 2012 година потврди дека „Сауди Арамко“, како една од најголемите светски нафтени компании, беше цел на малициозен софтвер Shamoon, што ги бришеше податоците од приближно 30 000 компјутери. Овој напад имаше за цел да го наруши работењето на компанијата и имаше значителни импликации за глобалниот пазар на нафта. Сајбер-нападот врз Саудиска Арамко ги истакна ранливостите во енергетскиот сектор и нагласи како нарушувањата во еден критичен сектор може да имаат каскадни ефекти врз глобалните енергетски резерви, економската стабилност и геополитичката динамика.²⁷⁸

277 Analysis of top 11 cyber attacks on critical infrastructure, 2021, достапно на: <https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/>

278 Jonathon Gordon. (2024). Critical infrastructure protection in modern society, *Industrial Cyber*, достапно на: <https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/>

6. СВОЈСТВА И СПОСОБНОСТИ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Вредноста или нивото на отпорноста на критичната инфраструктура може да се опише преку својства (како безбедност, одржливост итн.) или способности на критичната инфраструктура од потесно толкување.

Способностите на системот може да бидат капацитети, карактеристики, можности, ресурси и знаења.²⁷⁹ И имотот и способноста често се користат за отпорност на критичната инфраструктура. Левесон²⁸⁰ се фокусира на безбедноста на социотехничкиот систем за процена на отпорноста. Брунеу и соработниците²⁸¹ ја нагласуваат важноста на пет својства (капацитет, робусност, вишок, снаодливост и брзина) во инженерските системи. Холнагел²⁸² спомнува способност за реагирање, следење, учење, предвидување, отпорност на изградената средина, вклучувајќи ги и инфраструктурите, додека Барока²⁸³ констатира дека когнитивната компетентност (т. е. имање доволно познавање на критичната инфраструктура и потенцијалните опасности) е еден од најсуштинските аспекти за отпорност на инфраструктурата.

Ранливоста и кривката се тесно поврзани со отпорноста, односно претставуваат карактеристики на критичната инфра-

279 Lindbom, H. at all. (2015). The capability concept - On how to define and describe capability in relation to risk, vulnerability and resilience. *Reliab. Eng. Syst. Saf.* 135, стр. 45–54, достапно на: <https://doi.org/10.1016/j.res.2014.11.007>.

280 Leveson, at all. (2017). Engineering resilience into safety-critical systems. In: *Resilience engineering*. CRC Press, стр. 95–123.

281 Bruneau, M. at all. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake spectra* 19 (4), стр. 733–752.

282 Hollnagel, E. (2014). Resilience engineering and the built environment. *Building Research & Information* 42 (2), 221–228.

283 Barroca, B., Serre, D. (2013). Behind the barriers: a resilience conceptual model. SAPI EN. S. *Surveys and Perspectives Integrating Environment and Society* 6.1

структура што ги опишуваат штетните ефекти на опасност.²⁸⁴ Понатаму, од организациски аспект, за системите на критичната инфраструктура што се изложени на природни опасности, отпорноста содржи карактеристики поврзани со ублажување, планирање и претходно искуство при катастрофи.²⁸⁵

Потенцирани се три капацитети за урбани инфраструктури:

1. отпорни,
2. апсорптивни и
3. ресторативни.²⁸⁶

Во врска со способноста за обновување, достапноста на ресурсите обично се споменува во системот на заштита на критичната инфраструктура.

6.1. Отпорност, ризик и ранливост

Управувањето со ризикот и ранливоста и градењето на отпорност се стратегии за решавање неизвесни и несакани настани во системите или општеството. Клучната разлика лежи во вид на несакани настани што ги таргетираат: *пристапот заснован на ризик* има тенденција да се фокусира на настани што се познати и следат познати обрасци, *пристапот базиран на ранливост* има тенденција да се фокусира на идентификување на слабостите на системот и *пристапот врз основа на отпорност* има тенденција да се фокусира на способноста на системот да одговори на кој било настан, дури и неочекувани или непознати.²⁸⁷

284 Argyroudis, S.A., at all. (2019). Fragility of transport assets exposed to multiple hazards: State-of-the-art review toward infrastructural resilience. *Reliability Engineering & System Safety* 191, 106567.

285 Cutter, S.L., Burton, C.G., Emrich, C.T., (2010). Disaster resilience indicators for benchmarking baseline conditions. *Journal of homeland security and emergency management* 7 (1).

286 Ouyang, M., Dueñas-Osorio, L., Min, X., (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Struct. Saf.* 36–37, стр. 23–31, достапно на: <https://doi.org/10.1016/j.strusafe.2011.12.004>.

287 Mentges, A. at all. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International*

Стратегиите за управување со ризик традиционално се фокусираат на спречување на опасностите и избегнување на изложеност, додека управувањето со ранливоста се фокусира на намалување на слабостите, а отпорноста се фокусира за изградба на робусни системи што можат да апсорбираат неочекувани удари, да ги обноват и да се приспособат на нови околности. Треба да се забележи дека овие концепти често се испреплетуваат; на пример, процените на ризик или ранливост се начини да се постигне отпорен систем, а управувањето со ризикот може да вклучи и похолистички пристап, што вклучува подобрување на способноста на системот да одговори на настани.

Постојат две вообичаени толкувања на ранливоста во контекст на критичната инфраструктура.

Првото толкување доаѓа од перспектива на ризик, каде што ранливоста се смета за придонесувач за ризикот, заедно со опасноста и изложеноста на опасноста.²⁸⁸ За ова толкување, ранливоста мора секогаш да има врска со нешто, на пр., одреден настан или опасност. Исто така, системот или општеството може да има висока ранливост на опасности од поплави, но ниска ранливост кон земјотреси. Оваа интерпретација најчесто се користи за процена на ризикот од природни опасности.²⁸⁹

Во второто толкување, ранливоста опишува пропуст или слабост во дизајнот или управување со систем што го прави подложен на уништување или онеспособување без разлика на видот на опасност или неуспех. Овој труд се фокусира исклучиво на втората перспектива на ранливоста.

Отпорноста е концепт што се користи во многу дисциплини, како што се екологијата, економијата и инженерство. Постојат

Journal of Disaster Risk Reduction, 96, 103893, достапно на: <https://doi.org/10.1016/j.ijdrr.2023.103893>

²⁸⁸ Aven, T. et al. (2018). *Society for Risk Analysis Glossary*. Society for Risk Analysis.

²⁸⁹ Tamaro, A. et al. (2018). Characterization of the expected seismic damage for a critical infrastructure: The case of the oil pipeline in Friuli Venezia Giulia (NE Italy). *Bulletin of Earthquake Engineering*, 16(3), стр. 1425–1445, достапно на: <https://doi.org/10.1007/s10518-017-0252-1>

неколку прифатени дефиниции за отпорност, но основната способност на еластичниот систем е да ја одржи и да ја обнови својата основна функционалност по нарушувачки настан.²⁹⁰ Иако отпорноста е концепт што опфаќа многу аспекти, ризикот и анализите на ранливост сè уште имаат централна улога во анализата на отпорноста.²⁹¹

Бидејќи критичната инфраструктура е контекстот на оваа публикација, отпорноста се дефинира како способност на критичната инфраструктура да ја одржува и да ја враќа основната функционалност по прекин.

Овој труд ја усвојува дефиницијата за управување со ризик од Белата книга на ИРГЦ за управување со ризик како „целост на актери, правила, конвенции, процеси и механизми што се занимаваат со тоа колку се релевантни информациите што се собираат, се анализираат за ризикот, се соопштуваат и се донесуваат менаџерски одлуки“.²⁹² Дефиницијата е вредна за истражување на критичната инфраструктура, обезбедување објектив за концептуализирање и решавање на сложеноста, двосмисленоста и несигурност на ризици и зависности на критичните инфраструктури.

Управувањето со ризикот е фокусирано на управување со системски ризици, што се сложени, несигурни и склони кон каскадни ефекти. Рамката ги адресира предизвиците како оние видени во глобалната финансиска криза во 2008 година или климатските промени.²⁹³ Управувањето со ризик има за цел да се прошири надвор од конвенционалниот ризик на проценка и управување,

290 Mentges, A. at all. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, 96, 103893, достапно на: <https://doi.org/10.1016/j.ijdr.2023.103893>

291 Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 152, стр. 137–150, достапно на: <https://doi.org/10.1016/j.res.2016.02.009>

292 IRGC. (2006). *White paper on risk governance: Towards an integrative approach*. Geneva: International Risk Governance Council.

293 IRGC. (2018). *Guidelines for the Governance of Systemic Risks*. Geneva: International Risk Governance Council.

нагласувајќи го колаборативното одлучување меѓу различни засегнати страни со различни цели и перспективи. Се интегрираат фактички димензии, како што се физички исходи и веројатности, и социокултурни димензии, вклучувајќи ги животните услови, вредностите и емоциите.²⁹⁴

Рамката за управување со ризик артикулира три основни принципи:

1. принципот на комуникација и вклучување,
2. принципот на интеграција и
3. принципот на размислување/рефлексија.

Принципот на комуникација и вклучување се залага за вклучување широк спектар на засегнати страни во процесите на одлучување поврзани со системски ризици, со инклузивност пропорционална на сложеноста на ризикот. Овој принцип има за цел да идентификува и да вклучи различни перспективи, инкорпорирање на извори на информации и подобрување на демократското одлучување за социјално робусни резултати.

Принципот на интеграција ја нагласува потребата да се интегрираат знаењата од различни дисциплини или извори.

Принципот на размислување/рефлексија промовира колективна рефлексија за несигурности, сложеност и двосмисленост, обесхрабрувајќи ги симплистичките пристапи кон справување со ризиците.²⁹⁵

Позитивните резултати поврзани со ефективно управување со ризик опфаќаат јасно дефинирани одговорности, правичност и транспарентност²⁹⁶

Отпорноста може да се дефинира како способност за апсорпција и приспособување на променливо опкружување.²⁹⁷

294 IRGC. (2006). *White paper on risk governance: Towards an integrative approach*. Geneva: International Risk Governance Council.

295 van Asselt, M. B. A., & Renn, O. (2011). Risk governance. *Journal of Risk Research*, 14(4), 431–449, достапно на: <https://doi.org/10.1080/13669877.2011.553730>

296 Andersen, T. J., Garvey, M., & Roggi, O. (2014). *Risk, Risk Management, and Risk Governance*, Oxford University Press.

297 ISO (2021), ISO 22300:2021-Security and resilience-Vocabulary, достапно на: <https://www.iso.org/fr/standard/77008.html>.

Меѓутоа, како што е терминот „отпорност“ широко користен во различни контексти, тој се однесува на различни аспекти, како на пример, капацитет да се управува со поврзаните системи, и да се подобри способноста за справување со идните ризици.²⁹⁸ Обединетите нации сè повеќе ја препознаваат важноста на урбаната отпорност при соочување со криза или катастрофа.²⁹⁹

Неодамна, процената на отпорноста стана клучна компонента на управување со катастрофи бидејќи тоа е распространет прифатен процес што се користи за разбирање на функционалноста и перформансите на сложениот систем изложен на катастрофи.³⁰⁰ „Отпорност“ е апстрактен концепт, додека процената на издржливоста е процес за познавање на неговата вредност или ниво со примена на соодветни чекори.³⁰¹

6.2. Отпорност на критичната инфраструктура

Терминот „отпорност“ е мултидисциплинарен и тежок за дефинирање поради неговата многу широка употреба. Етимолошки именката отпорност доаѓа од латинскиот, *resilio*, *resilire*, што значи враќање и способност за продолжување. Многу студии за издржливост тврдат дека Холинг³⁰² првпат го вовел концептот за изучување на еколошката наука и дефинираната „отпорност“ како

298 Yang, Z. at all. (2022). Resilience Indicator of Urban Transport Infrastructure. A Review on Current Approaches. Infrastructures 7, достапно на: <https://doi.org/10.3390/infrastructures7030033>.

299 United Nations. (2020). UN Common Guidance On Helping Build Resilient Societies 48.

300 CORDIS-IMPROVER Project. (2016). Report on Current Approaches for Defining, Evaluating and Implementing Resilience Concepts in Critical Infrastructure, достапно на: <https://cordis.europa.eu/project/id/653390/results>, 2016

301 Tang, J. (2019). Assessment of Resilience in Complex Urban Systems. In: Leal, F.W. at all. (Eds.), Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer, Cham, достапно на: https://doi.org/10.1007/978-3-319-71059-4_71-1.

302 Holling, C.S. (1973). Resilience and stability of ecological systems. Annual review of ecology and systematics 4 (1), 1–23.

упорна способност да се апсорбираат промените и нарушувањата и уште да се одржат истите променливи на состојбата.

Во областа на критичната инфраструктура, отпорноста нема широко прифатена дефиниција, но е многу поврзано со инженерството или социо-техничката наука.³⁰³ За инфраструктури изложени на катастрофи и меѓусебно зависни во современото општество, дефиницијата за отпорноста е проширена со повеќе аспекти и перспективи. Меѓу различните толкувања на отпорноста, оваа публикација го фаворизира она што е во согласност со високоприфатената перспектива во научната заедница, фокусирајќи се и на инженерска отпорност и социотехничка димензија.

Ефектите што произлегуваат од овие закани врз критичната инфраструктура и нејзините потсистеми може да предизвикаат помали или поголеми проблеми што можат да предизвикаат нарушувања и дефекти во различните потсистеми.³⁰⁴ Тука првенствено се мисли на нарушување на функционалните параметри што предизвикуваат пад на изведбата на одредени елементи, каде падот е директно пропорционален на интензитетот на вонредната ситуација и степенот на отпорност на дадениот елемент на критичната инфраструктура.

Пред несреќа	Фаза на менаџмент на ризик	За време на несреќа	Фаза на менаџмент на ризик	По несреќа	Фаза на менаџмент на ризик
исчекување ублажување	превенција подготвеност	апсорпција адаптација	одговор	обнова трансформација	обнова

Табела број 2: Фази на градење на отпорност на критичната инфраструктура

³⁰³ Mottahedi, A. at all. (2021). The resilience of critical infrastructure systems: a systematic literature review. *Energies* 14 (6), 1571.

³⁰⁴ Hybrid Conference: Critical Connections, Continuity and Supply – Assessing the Security of European Critical Infrastructure and Functions in a Hybrid Threat Context, достапно на: <https://eu2019.fi/en/events/2019-11-06/countering-hybrid-threats-critical-infrastructureprotection-security-of-supply>,

Следејќи ја оваа методолошка рамка, различните фази се накратко опишани како што следува: пред катастрофа, треба да се предвидат и да се ублажат потенцијалните нарушувања и негативните влијанија придонесувајќи за проактивно управување со ризикот: „Предвидување на потенцијалните последици од катастрофи може да помогне да се одредат активностите што треба да бидат започнати пред да се случи катастрофата за да се минимизира нејзиниот ефект.“³⁰⁵

Во рамките на фазата на превенција сопствениците/операторите на критични инфраструктурни системи можат да ги идентификуваат и да ги проценат сите потенцијални ризици и опасности на кои нивните системи се изложени и планираат и спроведуваат мерки и активности за ублажување на идните негативни влијанија, неуспеси и нарушувања на системите. Подготвеноста е вградена во суштинската текстура на овие превентивни активности за ублажување насочени кон избегнување потенцијални дефекти на инфраструктурата и сериозно нарушување на услугите. Како што споменавме погоре, елементот на снаодливост (на пример, вешто подготвување за одговор при катастрофи, како што е изразено во бизнисот: континуитет, обука, управување со синџирот на снабдување и повеќе) може да се идентификува во текот на оваа фаза на градење отпорност на критичната инфраструктура.

За време на катастрофа или за време на фазата на одговор, системите треба да ги апсорбираат ударите и притисоци, притоа прифаќајќи го неочекуваното и минимизирање на последиците од негативниот настан. Адаптивните способности на системите на критичната инфраструктура се однесуваат на континуитет во работењето, функциите и давање услуги во рамките на параметрите на новата ситуација, а терминот го нагласува елементот на робусност. Адаптација на потребите на системите на КИ да бидат поттикнати од преовладувачките, променливи и потенцијални

305 Lelisa Sena, Kifle Woldemichael. (2006). *“Disaster Prevention and Preparedness”*, Lectures for Health Science Students, Jimma University, стр. 2, достапно на: <https://tinyurl.com/m4kewued>

ризици и закани. Сите дејства што би биле преземени во оваа фаза треба да бидат навремени, ефективни и ефикасни.

По катастрофи или за време на фазата на закрепнувањето, системите на КИ треба брзо да закрепнат и да реконституираат нормалност што е можно побрзо, на пример, реконструкција и рехабилитација користејќи го принципот „да се изгради назад подобро“ (“Build Back Better”)³⁰⁶ и многу повеќе. Покрај тоа, овие системи треба да се трансформираат самите, предвидувајќи ги идните нарушувања, неуспеси и неповолни ситуации и да можат подобро да се справат со хроничните стресови и акутните шокови. Оваа трансформабилност се однесува и на структурите на овие системи и на нивното функционирање и управување. „Научени лекции“ и добри практики се меѓу најефикасните алатки што овозможуваат сите клучни актери да придонесат за зајакнување на отпорноста на инклузивен и на партиципативен начин.³⁰⁷

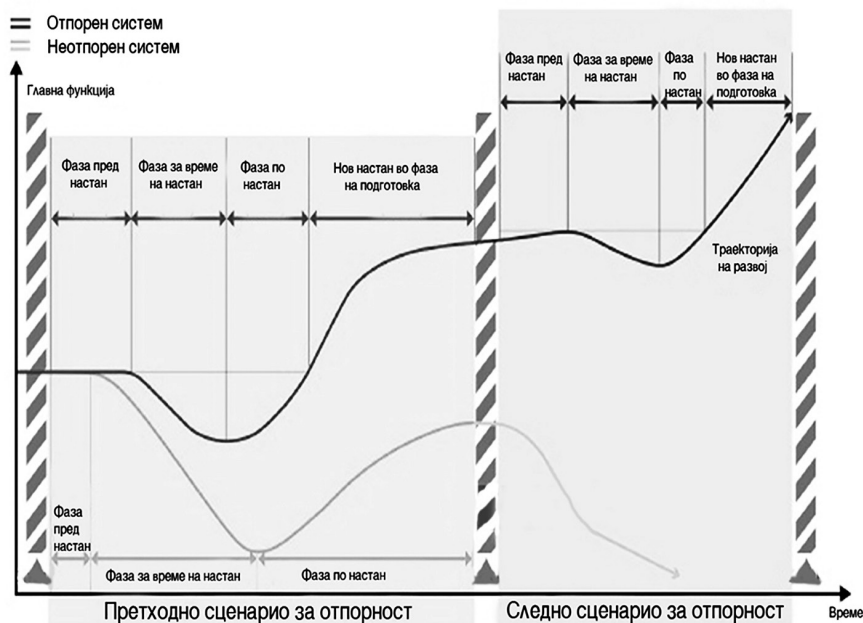
6.3. Сценарио за временски фази на отпорност

Отпорноста може да се опише и преку промената на перформансите или функциите со текот на времето. Како што е претставено низ сценариото за издржливост со различни временски фази. Врз основа на постоечките теории на отпорноста на критичната инфраструктура³⁰⁸ оваа публикација го дели сценариото за отпорност во четири фази (види слика број 11):

³⁰⁶ Означува идеален процес на реконструкција и обновување кој обезбедува отпорни, одржливи и ефикасни решенија за обновување на заедниците погодени од катастрофи.

³⁰⁷ Guidance notes on building critical infrastructure resilience in Europe and Central Asia. (2022). United Nations Development Programme, United Nations Plaza New York, NY, 10017, USA, достапно на: file:///C:/Users/User/Downloads/UNDP_Guidance%20notes_v4.pdf

³⁰⁸ Ouyang, M., Dueñas-Osorio, L., Min, X., (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Struct. Saf.* 36–37, стр. 23–31, достапно на: <https://doi.org/10.1016/j.strusafe.2011.12.004>.



1. Фаза пред настан (PrES): од појава на опасност до почеток на деградација на функцијата на системите на критичната инфраструктура;
2. Фаза за време на настан (DES): од почетокот на деградација до максималната деградација на функцијата на системите на критичната инфраструктура;
3. Фаза по настан (PoES): од максималната деградација на функција на системите на критичната инфраструктура до функцијата што се враќа на нивото на преднастанот фаза или закрепнување до идеална состојба, структура или својство (но сепак пониска од првобитната состојба) и
4. Нов настан во фаза на подготовка (NEPS): од функцијата што се враќа во нивото на фазата пред настан до појава на следниот шок на системите на критичната инфраструктура. Оваа фаза ја нагласува способноста за учење и подобрување од искуство.

Неопходно е да се нагласи дека способноста на подобрувањето може да влијае на различни следните фази и сценарија. Во секое сценарио, перформансите треба да се подобрат барем во една фаза

во споредба со претходните сценарија, благодарение на способноста за учење и подобрување од искуството.

6.4. Процена заснована на индикатори

Пристапите изградени за процена на отпорноста на критичната инфраструктура често се засноваат на индикатори.³⁰⁹ Индикатор претставува помалку апстрактен концепт од отпорноста и може да се користи за да се покажат позитивни или негативни промени во отпорноста. Затоа процената на отпорноста базирана на индикатори може да им помогне на засегнатите страни да ги анализираат критичните сектори на инфраструктура на практична и ситуацииска основа и да донесуваат ефикасни одлуки. Идентификацијата на индикаторите се сметаат за клучни пред да се процени отпорноста. Индикаторите се врз основа на основни податоци што се произведени под строг квалитет.³¹⁰ Друг предизвик за процена на отпорноста е да се трансформираат податоците во акциско знаење со помош на индикатори.³¹¹

Процената на отпорноста е популарен и вообичаен метод во студиите за отпорност што се проучува поради потребата за проценување и карактеризирање на карактеристиките на комплексен систем. Процената е процес со кој информациите (може да биде податок или индикатор) се добиваат во однос на некоја позната цел. Рамката изградена за процената на отпорност, без разлика дали е квантитативна, квалитативна или полукванти-

309 CORDIS-Smart Resilience Indicators for Smart Critical Infrastructures. (2018). Resilience indicators for SCIs based on big and open data. <https://cordis.europa.eu/project/id/700621/results>.

310 Eurostat. (2014). Getting messages across using indicators - A handbook based on experiences from assessing Sustainable Development Indicators, достапно на: <https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-gq-12-001>, 2014

311 CORDIS-Smart Resilience Indicators for Smart Critical Infrastructures. (2018). Resilience indicators for SCIs based on big and open data, достапно на: <https://cordis.europa.eu/project/id/700621/results>.

тативна, често се заснова на индикатори.³¹² Квантитативните пристапи нудат домен-агностички мерки за квантитативна вредност низ апликациите и пристапите за моделирање базирани на структура што се специфични за тој домен. Полуквантитативните пристапи обезбедуваат општ нумерички опис на класификацијата, без детални формули или модели. Квалитативните пристапи се поврзани на пристапите без нумерички дескриптор и врз основа на процените и анализите на луѓето, како анкетирани експерти или оператори. Понатаму, квалитативниот пристап вклучува и графики или илустрации што ја прикажуваат вредноста или промената на индикатор и податоци без нумерички пресметки.

За да се произведе знаење, што може да се користи за донесување одлуки и поставување политики, потребни се информациски системи да ги трансформираат податоците во информации. Покрај тоа, според Еуростат,³¹³ оценката заснована на индикатори се состои од поставување на очекуваната еволуција за индикаторот преку референца. Врз основа на индикатори процената на отпорност може да се дефинира како пристап знаејќи ја вредноста или нивото на отпорност со набљудување на индикаторите со множество референци. Во контекст на процената на отпорноста на КИ, апликативен е индикатор – информации за мерење или оценување на нивото на својства, функционалност или способности.

Индикаторот е мерлив, поврзан со критериум, наменет за набљудување на неговата еволуција во дефинирани интервали. Критериум е лик или знак со кој се разликува предмет, концепт или да се донесе став или процена. Индикаторот е објективна информација, чија процена, како и процената на отпорност, би можела да биде квантитативна, полуквантитативна или ква-

312 Cantelmi, R., Di Gravio, G., Patriarca, R., (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience, *Environment Systems and Decisions*. Springer US, достапно на: <https://doi.org/10.1007/s10669-020-09795-8>.

313 Eurostat (2014). Getting messages across using indicators - A handbook based on experiences from assessing Sustainable Development Indicators, достапно на: <https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-gq-12-001>

литативна.³¹⁴ На пример, температурата може да биде индикатор проценет преку објективни квантитативни методи, како што се отчитувањата на термометарот. Во меѓувреме, процената на индикаторот може да биде врз основа на многу субјективни судови, што ги нарекуваме квалитативно оценување. На пример, за индикатор „бројот на задоволни клиенти“ „бројот“ е објективна информација, но начинот на добивање на оваа информација се заснова на субјективните процени на клиентите. Полуквантитативната процена на индикаторот, на пример, го квантифицира бројот на задоволни клиенти, што е категоризиран по ниво под 50 проценти и над 50 проценти; температурите се класифицирани како под 20 степени, помеѓу 20 и 40 степени и над 40 степени.

Покрај тоа, мерката на индикаторот има потреба од сигурни податоци. Податоците се дискретен факт, суров елемент или резултат од набљудување, стекнување или мерење, изведени со природен или вештачки инструмент. Податоците се објективни и не мора да функционираат за да се оцени или да се процени некој објект, односно неопходно е да се обезбеди единица формат стандард за мерење. Процесот што трансформира бројни податоци во акциски индикатори се нарекува процена на индикаторот.³¹⁵

Како заклучок, процената на отпорност врз основа на индикатори за критична инфраструктура е пристап што вклучува три фактора:

1. отпорност на критична инфраструктура,
 2. употреблив индикатор,
 3. потребни податоци и две фази (види: Слика број 12):
- ✓ процена на отпорност: процес во кој се добиваат вредностите на отпорност по употребливи индикатори и
 - ✓ процена на индикаторите: процес во кој се добиваат вредностите на индикаторите со веродостојни податоци.

314 Yang, Z., at all. (2022). Resilience Indicator of Urban Transport Infrastructure. A Review on Current Approaches. Infrastructures 7, достапно на: <https://doi.org/10.3390/infrastructures7030033>.

315 CORDIS-Smart Resilience Indicators for Smart Critical Infrastructures. (2018). Resilience indicators for SCIs based on big and open data, достапно на: <https://cordis.europa.eu/project/id/700621/results>

**Слика бр.12. Фактори и фази на процена на отпорност
базирана на индикатори**



7. ЕВРОПСКАТА УНИЈА И ОТПОРНОСТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Критичната инфраструктура опфаќа суштински објекти и системи што го поткрепуваат функционирањето на модерните држави, општества и секаков вид бизнис. Вклучува субјекти од сектори како: енергетика, транспорт, вода, здравство, телекомуникации и други. Прекините на критичната инфраструктура може да имаат сериозно влијание врз националната безбедност, јавната безбедност и економската активност. Во последниве години, сè повеќе се препознава потребата од зајакнување на заштитата на критичната инфраструктура од широк опсег на закани, вклучувајќи терористички напади, природни катастрофи и сајбер-напади. Како одговор на овие закани, Европската Унија (ЕУ) неодамна усвои неколку нови правни инструменти за подобрување на отпорноста и заштитата на критичната инфраструктура. Најзначајни меѓу нив се Директивата (ЕУ) 2022/2557 на Европскиот парламент и на Советот од 14 декември 2022 година за отпорност на критичните субјекти и укинување на Директивата на Советот 2008/114/ЕС (во натамошниот текст: CER Директива) и Директивата (ЕУ) 2022/2555 на Европскиот парламент и на Советот од 14 декември 2022 година за мерки за високо заедничко ниво на сајбер-безбедност низ Унијата, изменување и дополнување на Регулативата (ЕУ) бр. 910/2014 и на Директивата (ЕУ) 2018/1972 и укинување на Директивата (ЕУ) 2016/1148 (во натамошниот текст: NIS2 Директива).³¹⁶ „Иако ди-

³¹⁶ Robert Mikac. (2024). Protection of the EU's Critical Infrastructure: Evaluation of new legal instruments // Critical Infrastructure Protection &

рективите CER и NIS 2 се наменети за земјите членки на ЕУ, тие треба да бидат отворени за земјите кандидати што добиваат статус на набљудувач во Групите за отпорност на критични ентитети и EU-CyCLONE“. Препораките за координиран пристап на ниво на Унијата за зајакнување на отпорноста на критичната инфраструктура (2022) опфаќаат три приоритетни области: подготвеност, одговор и меѓународна соработка и предлагаат позначајна улога на Комисијата во справувањето со заканите и зајакнувањето на интеракцијата меѓу земјите членки и трети земји, особено за инфраструктурата со прекугранична важност.³¹⁷

Директивата на Советот 2008/114/ЕЗ предвидува постапка за назначување на европската критична инфраструктура во енергетскиот и во транспортниот сектор, чие прекинување или уништување би имало значително прекугранично влијание врз најмалку две земји членки. Таа директива се фокусира исклучиво на заштитата на таквата инфраструктура. Сепак, евалуацијата на Директивата 2008/114/ЕЗ спроведена во 2019 година покажа дека, поради сè повеќе меѓусебно поврзаната и прекуграничната природа на операциите со користење критична инфраструктура, заштитните мерки што се однесуваат само на поединечни средства се недоволни за да се спречат сите прекини. Затоа неопходно е да се пренасочи пристапот кон осигурување дека ризиците се подобро земени предвид, дека улогата и должностите на критичните субјекти како даватели на услуги суштински за функционирањето на внатрешниот пазар се подобро дефинирани и кохерентни и дека се усвоени правилата на Унијата да се зајакне отпорноста на критичните субјекти. Критичните субјекти треба да бидат во позиција да ја зајакнат нивната способност за спречување, заштита, реагирање, отпор, ублажување, апсорпција, приспособување и

Resilience News, Winter 2023/2024. London: The International Association of Critical Infrastructure Protection Professionals.

³¹⁷ Vasko Popovski at all. (2023). Crisis prevention and critical infrastructure in Western Balkans, Visegrad Fund, достапно на: <https://idscs.org.mk/en/2023/05/02/crisis-prevention-and-critical-infrastructure-in-western-balkans/>

закрепнување од инциденти што имаат потенцијал да го нарушат обезбедувањето на основните услуги.³¹⁸

7.1. Предизвици за примена на Директивата за отпорност на критичните ентитети

Постојат неколку идентификувани предизвици поврзани со Директивата за отпорност на критичните ентитети.

Првиот предизвик е комплексноста на системите на критична инфраструктура и меѓузависноста меѓу нив, што го отежнува предвидувањето на нивното однесување и последователно процената на ризикот и ранливоста.³¹⁹ Овој предизвик беше и една од причините за замена на директивата ЕЦИ (ECI) со Директивата ЦЕР (CER) бидејќи евалуацијата на ЕЦИ (ECI) покажа дека таа не се однесува соодветно со меѓузависности на критичната инфраструктура.³²⁰ На пример, информациско-комуникациските технологии и вселенските сектори стануваат сè поважни, придонесувајќи за зголемување на меѓузависноста меѓу критичната инфраструктура.

Втор предизвик е институционалната фрагментација и поделбата на одговорноста, поттикнати од либерализација,

318 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

319 Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, стр. 53–66. Scopus, достапно на: <https://doi.org/10.1016/j.ijcip.2014.12.002>

320 European Commission. (2020). *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Final report*. Publications Office, достапно на: <https://data.europa.eu/doi/10.2837/864404>

приватизација, дерегулација³²¹ и аутсорсинг.³²² На пример, зголемениот број актери доведе до зголемени тешкотии во систематското администрирање на собрани и достапни податоци релевантни за разбирање на сложените системи и меѓузависности.³²³ Исто така, воведе конкуренција помеѓу операторите на критична инфраструктура, што поттикнува фокусирање на стекнување пазарни удели наместо да се обезбедат сигурни услуги.³²⁴

Трет предизвик се грижите за безбедноста на информациите и доверливоста, потенцијално создавајќи неподготвеност за споделување информации помеѓу операторите на критична инфраструктура и помеѓу операторите на КИ и јавните авторитети.³²⁵ Овој предизвик, исто така, беше зголемен со институционална фрагментација, бидејќи повеќе актери треба да соработуваат и да споделуваат информации за ефикасно управување со нивната отпорност. *Сајбер-отпорноста* обезбедува доверливост, интегритет и достапност преку идентификација, заштита и воспоставување претходна состојба од сајбер-инциденти. Јавниот и приватниот сектор мора да имаат навремени и точни информации и предлози за подобрување на сајбер-безбедноста и да бидат во можност меѓусебно да соработуваат во случај на сајбер-инциденти.

321 De Bruijne, M., & Van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management*, 15(1), стр. 18–29, достапно на: <https://doi.org/10.1111/j.1468-5973.2007.00501.x>

322 Префрлување на помалку важни функции од една фирма или организација на надворешни специјализирани компании со цел да се намалат трошоците.

323 OECD. (2011). *Future Global Shocks*. Organisation for Economic Co-operation and Development, достапно на: <http://www.oecd-ilibrary.org/content/book/9789264114586-en>

324 Cedergren, A., Lidell, K., & Lidell, K. (2019). Critical infrastructures and the tragedy of the commons dilemma: Implications from institutional restructuring on reliability and safety. *Journal of Contingencies and Crisis Management*, 27(4), стр. 282–292, достапно на: <https://doi.org/10.1111/1468-5973.12262>

325 Brem, S. (2015). Critical Infrastructure Protection from a National Perspective. *European Journal of Risk Regulation*, 6(2), стр. 191–199, достапно на: <https://doi.org/10.1017/S1867299X00004499>

7.2. Мерки за отпорност на критичните ентитети

Земјите членки обезбедуваат дека критичните ентитети преземаат соодветни и пропорционални технички, безбедносни и организациски мерки за да се обезбеди нивната отпорност, врз основа на релевантните информации обезбедени од земјите членки за процената на ризикот на земјата членка и за резултатите од процена на критичниот ризик на субјектот, вклучувајќи мерки неопходни за:

(а) спречување инциденти, соодветно имајќи ги предвид мерките за намалување на ризикот од катастрофи и климатска адаптација;

(б) да обезбедат соодветна физичка заштита на нивните простории и критична инфраструктура, соодветно имајќи ги предвид, на пример, бариерите, алатките и рутините за следење на периметарот, опремата за откривање и контролите за пристап;

(в) да одговори, да се спротивстави и да ги ублажи последиците од инцидентите, соодветно имајќи го предвид спроведувањето на процедурите и протоколите за управување со ризик и кризи и рутините за предупредување;

(г) закрепнување од инциденти, соодветно земајќи ги предвид мерките за континуитет на деловното работење и идентификацијата на алтернативни синџири на снабдување, со цел да се продолжи со обезбедувањето на основната услуга;

(д) да обезбеди соодветно управување со безбедноста на вработените, соодветно земајќи ги предвид мерките како што се утврдување категории на персонал кои вршат критични функции, воспоставување права за пристап до просториите, критична инфраструктура и чувствителни информации, воспоставување процедури за проверка и назначување на категории на лица од кои се бара да се подложат на такви проверки и утврдување на соодветни барања за обука и квалификации;

ѓ) да се подигне свеста за мерките наведени во точките (а) до (д) кај релевантниот персонал, соодветно имајќи ги предвид курсевите за обука, информативните материјали и вежбите.³²⁶

³²⁶ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Имајќи го предвид наведеното, се поставува прашањето за иднината на отпорноста се позиционира во посеопфатно разбирање на ризикот и ранливоста. Приспособените мерки за отпорност, дизајнирани според специфичните потреби на различни демографски и социоекономски групи, можат да ја подобрат ефективноста. Овој пристап на „микронизација“, каде секое домаќинство и поединец имаат улога во планирањето на отпорноста, ветува силна и инклузивна подготвеност за идни кризи. Централно место за ова е потребата за академски кадар и професионалци да се вклучат во учење меѓу домени. Со разбирање на меѓусебната поврзаност на домени како сајбер-безбедност, јавно здравје и заштита на инфраструктурата, тие може да развијат холистички стратегии за отпорност.

Промовирањето на партиципативното владеење е исто така клучно. Вклучувањето на заедницата во напорите за градење отпорност гарантира дека мерките за отпорност не се планираат само на национално ниво, туку се вкоренети во структурите на заедницата. Ова вклучува иволвирање на локалните засегнати страни во процесите на донесување одлуки и обезбедување мерки да бидат инклузивни и правични. Користењето на пристапи водени од податоци, како што е имплементирање на контролни табли за отпорност, може да ја подобри транспарентноста и одговорноста. Овие алатки го следат напредокот и помагаат да се идентификуваат областите на кои им треба подобрување, промовирајќи донесување одлуки водени од податоци. И на крај, во свет на нови закани, континуираното учење и адаптација се од суштинско значење. Да се остане информиран за новите и еволуирачки закани што се развиваат помага да се одржат ефективни стратегии за отпорност, обезбедувајќи подготвеност и подготвеност за идни кризи.³²⁷

327 Rade Rajkovchevski (2024). EU vs NATO: Comparing Resilience in Civil Preparedness with Rade Rajkovchevski, Crisis Lab, достапно на: <https://www.crisislab.io/blog/eu-vs-nato-comparing-resilience-in-civil-preparedness-with-rade-rajkovchevski>

8. АКТЕРИ НА ПРИМАРНА ЗАКАНА НАСОЧЕНА КОН КРИТИЧНАТА ИНФРАСТРУКТУРА

Разбирањето на примарните актери на закана насочени кон критичната инфраструктура е од клучно значење за развој на ефективни одбранбени стратегии. Овие актери вклучуваат странски ентитети и национални држави, недржавни актери и терористи, криминални групи и инсајдери.

Странски субјекти и нации-држави. Странските ентитети и националните држави се впуштаат во сајбер-шпионажа и војување, настојувајќи да стекнат стратешки, политички или воени предности. Тие спроведуваат активности што се движат од собирање разузнавачки информации до нарушување на критичните служби, со цел да ја поткопаат безбедноста или економската стабилност на нацијата.

Недржавни актери и терористи. Недржавните актери и терористите се мотивирани од идеолошки цели и имаат за цел да ја уништат или да ја онеспособат инфраструктурата за да предизвикаат закани за националната безбедност, масовни жртви или да предизвикаат економски и социјални потреси. Нивните постапки се дизајнирани да влеат страв, несигурност и хаос.

Криминални групи. Криминалните групи се впуштаат во сајбер-криминал, како што се фишинг, напади на шпионски/малициозен софтвер, кражба на идентитет и онлајн-измама, првенствено заради парична добивка. Тие ги искористуваат пропустите во системите на критична инфраструктура за да украдат податоци, да ги попречат операциите или да изнудат пари од владини и приватни субјекти.

Инсајдери. Упатените, без разлика дали се незадоволни вработени или ненамерни актери, претставуваат значителен ризик поради нивниот директен пристап до чувствителни системи и информации. Упатените може да предизвикаат намерна штета или да станат безбедносни ризици поради небрежност или несоодветна обука за сајбер-безбедност.³²⁸

328 Jonathon Gordon. (2024). Targeting critical infrastructure: recent incidents analyzed, Industrial Cyber, достапно на: <https://industrialcyber.co/threats-attacks/targeting-critical-infrastructure-recent-incidents-analyzed>

8.1. Општ профил на ризици и закани во регионот на Западен Балкан

Регионот на Западен Балкан има комплексен регионален профил на ризик со речиси сите природни и човечки опасности, влијанија од климатските промени и висока деградација и загадување на животната средина, заедно со наследството од минатите конфликти и меѓуетнички тензии, како и нови безбедносни ризици и закани. „И покрај завршувањето на пандемијата, Западниот Балкан сега се соочува со нов сет предизвици, надополнети со војната во Украина, вклучувајќи го и зголемување на цените на енергијата и на храната, високата инфлација и забавување на трговијата и инвестициите.“³²⁹

Природни Опасности	Човечки и технолошки опасности	Безбедносни ризиви и закани
• Геофизички (земјотрес, лизгање на земјиштето, масовни движења) • Хидрометеоролошки (поројни поплави, лавини, суша, студени периоди и топлотни бранови, силни конвективни и зимски бури, шумски пожари, пораст на нивото на морето) • Биолошки (епидемии, епифитии, епизоотии) • Космички феномени (сончеви блесоци, геомагнетни бури, метеорити, астероиди)	• Индустриски несреќи/загадување • Транспортни несреќи • Големи прекини на струја • Деградација и загадување на животната средина • Зрачење • Дефекти на брани • Експлозии во фабрика • Хемиски протекувања	• Непријателски влади • Тероризам • Пролиферација • Сајбер-криминал • Климатски промени • Транснационален криминал • Граѓански војни и војни • Недоверливи инвестиции • Густина на население • Напади во синцирот на снабдување

Табела бр. 3. Ризици и закани врз критичните инфраструктурни системи во регионот на Западен Балкан³³⁰

³²⁹ The World Bank. (2022). Western Balkans Face New Economic Headwinds Despite Strong Post-Pandemic Recovery (Press-release), достапно на: <https://tinyurl.com/32e5hy5e>

³³⁰ Vasko Popovski. (2022). Guidance notes on building critical

Од доменот на природните опасности, поплавите се најчести со најголем интензитет и магнитуда, шумските пожари се зголемуваат во зачестеноста и последиците по природата и биолошката разновидност, другите настани поврзани со временските услови се во пораст со поголеми магнитуди, додека земјотресите имаат потенцијално најголемо влијание во услови за загуба на животи и долгорочни штети и загуби.

Големината на овие катастрофи врз системи за критична инфраструктура во погодените земји од Западна Балкан може да се идентификува од спроведените процени на потребите по катастрофата:

- Поплави во Босна и Херцеговина во мај 2014 година. Од вкупно ревидираните влијанија на поплавите беа проценети штети од 2,4 милијарди американски долари, 30 проценти или 706,15 милиони американски долари штети и загуби на инфраструктурните системи на погодената земја, вклучувајќи ги објектите, средствата и обезбедувањето услуги.
- Србија – поплави во мај 2014 година. Придонесот на инфраструктурните штети и загуби во вкупните проценети влијанија од поплавите (1,8 милијарди американски долари) е уште поголем, односно 47 проценти или 854,22 милиони американски долари.
- Земјотрес во Албанија во ноември 2019 година. Штетите и загубите на инфраструктурниот сектор беа 14 проценти од вкупната цена на катастрофи од 1,19 милијарди американски долари.
- Северна Македонија 2016 – скопски поплави. Односот на штетите и загубите беше 51:49 проценти или влијанието врз инфраструктурниот сектор беше ревидиран како 18,7 милиони американски долари, додека вкупната цена изнесуваше 36,37 милиони американски долари.

Овој тренд се очекува дополнително да расте со оглед на очекуваното влијание на климатските промени што „ќе ги влошат екстремните временски настани во повеќето области на регионот

на Западен Балкан, особено екстремните настани поврзани со суша и топлина³³¹ што може да има зголемено влијание врз отпорноста на критичната инфраструктура.

Постојат примери на нови ризици и закани за отпорноста на критичната инфраструктура во регионот што бараа зголемена заштита и очекување од страна на владините власти и сопствениците и операторите од јавниот и приватниот домен. На пример, континуираната мигрантска и бегалска криза резултираше со тоа што повеќето од 1,4 милиони мигранти и бегалци што стигнаа до ЕУ транзитираа кон Западнобалканската рута,³³² што значително ги притискаше ограничените ресурси на агенциите за безбедност и управување со вонредни состојби и влијаеше врз локалната комунална и транспортна инфраструктура. Понатаму, „пандемијата КОВИД-19 го нагласи отсуството на соодветна рамка за пандемиски ризик, експертиза и поврзана инфраструктура“³³³ и значително го притисна функционирањето на потсистемот на здравствената инфраструктура, ги пренасочи средствата од проекти кон одговорот на пандемиски кризи и преголем притисок лошата дигитална инфраструктура во шесте економии.

Идните ризици и закани за безбедноста на критичната инфраструктура во регионот на Западен Балкан вклучуваат неколку настани со засилена фреквенција и продлабочени влијанија, т.е. серија сајбер-напади врз сајтовите и порталите на албанските владини и финансиски институции во текот на летото и есента 2022, масивни сајбер-напади на црногорските онлајн владини платформи за информирање ја ставија на висок ризик основната инфраструктура, вклучително банкарството, системите за вода и електрична енергија, во август 2022 година или серија слични

331 UNEP. (2022). Regional Strategy For Climate-resilient Road Infrastructure. ADC/UNEP, достапно на: <https://tinyurl.com/ys3j98er>

332 Nermin Oruc, Saima Raza, Danica Santic. (2020). Analytical Report: The Western Balkan Migration Route (2015-2019). Prague Process Secretariat, достапно на: <https://tinyurl.com/u4hbx9fz>

333 Vasko Popovski. (2020). Assessment Study of the Role of NDMAs in COVID 19 Crisis Response and Impact of Covid on NDMAs Operations. UNDP/UNDRR, достапно на: <https://tinyurl.com/3u3e5uey>

настани во нашата држава, на пр. DDoS напади на страницата на Државната изборна комисија за време на изборите во јули 2020 година, закани преку е-пошта за поставени уреди за бомбардирање во 876 образовни и 42 други институции во периодот октомври 2022 – март 2023 година и напади со откупни софтвери на владини институции, на пр. Фондот за здравствено осигурување во февруари 2023 година.

Со оглед на актуелниот геополитички и безбедносен контекст во поширокиот регион, фактот што дел од земјите од регионот се земји членки на НАТО, односно Албанија, Северна Македонија и Црна Гора, како и континуираното зголемување на сајбер-нападите, неопходно е да вклучат овие ризици и закани во политиките и нормативните рамки, процените и плановите за ризик и опасност и да дизајнира и применува соодветни акции и мерки за градење отпорност.

9. ПРЕДИЗВИЦИ ЗА ДОНЕСУВАЊЕ ОДЛУКИ ВО ЗАШТИТА НА КРИТИЧНА ИНФРАСТРУКТУРА

9.1. Концептуализација на перцепцијата на ризикот и хеуристиката за донесување одлуки и предрасуди

Асоцијацијата за анализа на ризик ја дефинира перцепцијата на ризикот како субјективно расудување или процена на ризикот на една личност.³³⁴ Отстапувањето помеѓу реалниот ризик и начинот на кој се перцепира е предизвикано од низа афективни, когнитивни, контекстуални и индивидуални фактори³³⁵. Три од овие четири фактора произлегуваат од квалитетите на поединецот.

334 Aven, T., at all (2018). SRA glossary. Retrieved December 15, 2021, достапно на: <https://www.sra.org/risk-analysis-introduction/risk-analysis-glossary/>

335 Aven, T., at all. (2018a). Risk Analysis: Fundamental Principles. Retrieved December 15, 2021, достапно на: <https://www.sra.org/wp-content/uploads/2020/04/SRA-Fundamental-Principles-R2.pdf>

Афективните фактори вклучуваат емоции и чувства на личноста за која станува збор, додека когнитивните фактори може да вклучуваат медиумско покривање и врамување информации за ризик. Индивидуалните фактори се однесуваат на претходното искуство на поединецот, возраста и особините на личноста, додека контекстуалните фактори се однесуваат на начинот на кој информациите се врамени и начинот на кој се пристапува до алтернативните извори на информации. Се сугерираше дека перцепцијата на ризикот се наоѓа во поединците понекогаш како чувство, а во други случаи како вреднување на ризикот што е резултат на намерна анализа. Тврдењето е дека на нив треба да се гледа како на две страни на иста монета, без оглед на разликата што ја претставуваат. Иста личност е способна за сè, освен за рационални одлуки и пресуди под влијание на нивните сопствени предрасуди. Раните истражувања за перцепцијата на ризикот покажаа дека подлабокиот показател за ризикот за секоја дадена опасност е степенот до кој тој предизвикува чувства на страв и дека перцепирираниот ризик и корист се обратно поврзани, опишан како бавен и брз режим, последователно се покажа дека е неопходен за рационално одлучување.³³⁶ Се вели дека овие одлуки се под влијание на хеуристиката.

Хеуристиката може да се дефинира како кратенка до сложеноста на задачите во расудувањето, а пристрасноста како просторот помеѓу нормативното и хеуристичкото однесување.³³⁷ Тие се неоптимални, несовршени и ирационални пристапи кон решавање на проблемите што, сепак, можат да го забрзаат процесот на изнаоѓање задоволително решение. Хеуристиката е поврзана со когнитивните предрасуди, додека се предлагаат предвидувања на однесување пред настанот што бара формално моделирање на процесот на одлучување.³³⁸ Сепак, иако хеуристиките не се

336 Slovic, P. (2020). Risk perception and risk analysis in a hyperpartisan and virtuously violent world. *Risk analysis*, 40(S1), 2231–2239, достапно на: <https://doi.org/10.1111/risa.13606>

337 Kahneman, D., & Tversky, A. (1982). The psychology of preferences. *Scientific American*, 246(1), 160–173, достапно на: <https://doi.org/10.1038/scientificamerican0182-160>

338 Gigerenzer, G., & Todd, P. M. (1999). Simple heuristics that make us smart. Oxford University Press.

секогаш точни ниту водени од логиката, тие често се доволни за да задоволат потреба и често изгледаат како да функционираат. Всушност, се покажа дека барем за некои деловни ситуации, хеуристичкото одлучување може да биде ефективно ако некои информации намерно се игнорираат со помалку докажување дека се повеќе несигурни кога знаењето има предност пред изобилството на информации.³³⁹

Фокусирајќи се на имплементацијата на процена на ризикот во контекстот на процесот на заштита на критична инфраструктура, товарот е често на професионалната процена на ризик, чијшто камен-темелник на процесот на процена на ризик е распространет на сите нивоа на активната заштита на критична инфраструктура³⁴⁰ и чие расудување може да биде доведено во заблуда поради способноста на хеуристиката да го „подмачкува разумот“³⁴¹. Се тврди дека професионалецот мора да донесува одлуки за време на процесот на заштита на критична инфраструктура во недостиг на алатки и процеси што може да го идентификуваат и да го решат обемот на системските врски низ националните граници и во други сектори.³⁴² Следната потсекција ја испитува употребата на хеуристика за донесување одлуки во контекст на процесот на заштита на критична инфраструктура.

339 Mousavi, S., & Gigerenzer, G. (2014). Risk, uncertainty, and heuristics. *Journal of Business Research*, 67(8), стр. 1671–1678, достапно на: <https://doi.org/10.1016/j.jbusres.2014.02.013>

340 Poljanšek, K., at all. (2019). Recommendations for national risk assessment for disaster risk management in EU. Publications Office of the European Union, Luxembourg, достапно на: <https://doi.org/10.2760/147842JRC114650>

341 Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, 177(3), стр. 1333–1352, достапно на: <https://doi.org/10.1016/j.ejor.2005.04.006>

342 Pidgeon, N., & O’Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science*, 34(1–3), стр. 15–30, достапно на: [https://doi.org/10.1016/S0925-7535\(00\)00004-7](https://doi.org/10.1016/S0925-7535(00)00004-7)

9.2. Хеуристика за донесување одлуки и предрасуди во заштита на критичната инфраструктура

Како и во случајот со концептот на транснационализам, овој преглед на литературата обезбедува само ограничен број директни референци поврзани со ефектот на хеуристиката за донесување одлуки за процена на ризик и пристрасност во специфичниот контекст на процесот на заштита на критична инфраструктура. Истражувачката работа за хеуристиката и предрасудите за донесување одлуки што не се специфични за заштита на критична инфраструктура е подоминантна, иако со поголем фокус на перцепцијата на ризикот наместо процена на ризикот. Сепак, имајќи предвид дека методологијата за процена на ризик „златен стандард“, употребена за време на заштита на критична инфраструктура е процесот на управување со ризик ISO31,000:2018, збирот на хеуристики за донесување одлуки што се пријавени во литературата што треба да се користи за време на вториот процес се (во принцип) применливи и за процесот на заштита на критична инфраструктура. Краток опис на овие хеуристики и предрасуди, како и нивното потенцијално влијание врз процесот на процена на ризикот во контекст на заштита на критична инфраструктура, е даден во следните параграфи:

- **Хеуристика на афектот.** Хеуристиката на афект се дефинира како состојба на чувство како среќа или тага, но исто така и како добро или лошо, доделена на стимул што го доживуваат луѓето.³⁴³ Се смета дека е истакната хеуристичка поврзаност со ризикот. Постојат научни докази што го покажуваат директното влијание на хеуристиката на афектот врз перцепцијата на ризикот³⁴⁴ и неговото влијание врз

343 Slovic, P. (2000). The Perception of Risk, достапно на: www.routledge.com

344 Van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, 90, 101651, достапно на: <https://doi.org/10.1016/j.cose.2019.101651>

афективните информации за пресудите за перципираниот ризик. Што е уште поважно (за обемот на овој труд) во академската литература конкретно е аргументирано дека афектот (како и хеуристиката на достапноста за која се дискутира подоцна) може директно да влијае на процесот на заштита на критична инфраструктура со тоа што е извор на таканаречените „слепи точки“, што може да предизвика катастрофа низ критично-инфраструктурните системи.³⁴⁵ Интересно е што хеуристиката на афект може да има ефект и на можни дискусии на ниво на тим на нивото на ризик, што претставува типичен случај за големи проекти. Овој ефект ќе биде подетално дискутиран во следните потсекции.

- **Хеуристика за достапност.** Поединците ја користат хеуристиката на достапноста, ментална кратенка што ги заснова одлуките на непосредни примери што ќе дојдат на ум, за да ја проценат фреквенцијата на настанот или веројатноста за неговата појава со „леснотијата со која ни доаѓаат на ум релевантните примери или асоцијации“.³⁴⁶ Хеуристиката за достапност може да има значаен ефект врз перцепцијата на практикантот на ризик за веројатноста за настан. Како таков, може да влијае на активностите на процена на ризик воопшто, и на активностите на процена на ризик во контекст на процесот на заштита на критична инфраструктура, каде што најверојатно ќе се појави елементот за донесување одлуки во тимот.³⁴⁷ Хеуристиката за

345 Blackwell, J., at all. (2009). An ontology-based approach to blind spot revelation in critical infrastructure protection planning. In Setola, R., Geretshuber, S. (Eds.), Critical information infrastructure security: Third international workshop, CRITIS 2008, Rome, Italy, October 13-15 2008 (стр. 352– 359). Springer, Berlin, Heidelberg, достапно на: https://doi.org/10.1007/978-3-642-03552-4_34

346 Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, 5(2), 207–232, достапно на: [https://doi.org/10.1016/0010-0285\(73\)90033-9](https://doi.org/10.1016/0010-0285(73)90033-9)

347 Blackwell, J., at all (2009). An ontology-based approach to blind spot revelation in critical infrastructure protection planning. In Setola, R.,

достапност е потребна за ефективно да ги објасни разликите во перцепцијата на ризикот меѓу групите, културите, па дури и нациите. Ова откритие има дополнителна важност за заштита на критична инфраструктура со оглед на нејзината транснационална природа.³⁴⁸

- **Способност за когнитивна рефлексija.** Когнитивната рефлексija се однесува на способноста или наклонетоста да се одрази на прашање и да се спротивстави на автоматскиот одговор.³⁴⁹ Како таква, когнитивната рефлексija може да има потенцијален ефект врз целината на процесот на проценка на ризик во контекст на заштита на критична инфраструктура, од идентификација на закана до формулација на стратегии за ублажување.³⁵⁰ Дополнително, силата на инверзната корелација е поврзана со индивидуалните когнитивни способности, со способност за когнитивна рефлексija на преден план.³⁵¹ Меѓутоа, нема директни референци во академската литература во однос на импликациите на способноста за когнитивна рефлексija за процена на ризик во контекст на заштита на критична инфраструктура.

Geretshuber, S. (Eds.), Critical information infrastructure security: Third international workshop, CRITIS 2008, Rome, Italy, October 13-15 2008 (стр. 352– 359). Springer, Berlin, Heidelberg, достапно на: https://doi.org/10.1007/978-3-642-03552-4_34

348 Sunstein, C. R. (2005). Precautions against what? the availability heuristic and cross-cultural risk perception. SSRN Electronic Journal, 57, 75, достапно на: <https://doi.org/10.2139/ssrn.578303>

349 Toplak, M. E., West, R. F., & Stanovich, K. E. (2011). The cognitive reflection test as a predictor of performance on heuristics-and-biases tasks. *Memory & Cognition*, 39(7), стр. 1275–1289, достапно на: <https://doi.org/10.3758/s13421-011-0104-1>

350 Berger, T. B. (2015). Risk assessment competencies of risk management professionals (in Germany). SSRN Electronic Journal. SSRN 2815654, достапно на: <https://doi.org/10.2139/ssrn.2815654>

351 Skagerlund, K., Forsblad, M., Slovic, P., & Västfjäll, D. (2020). The affect heuristic and risk perception–stability across elicitation methods and individual cognitive abilities. *Frontiers in Psychology*, 11, 970, достапно на: <https://doi.org/10.3389/fpsyg.2020.00970>

- **Крос-културни разлики и културна пристрасност.**

Иако овие концепти не се хеуристика сами по себе, нивната транснационална природа може да воведо предрасуди што се протегаат надвор од границите на една нација. Особено разликите во преференциите меѓу нациите се поврзани со националните културни разлики во соодветната перцепција на ризикот на нивните народи, наместо со нивните ставови кон перцепцијата на ризикот. Студиите покажаа дека покрај меѓукултурните разлики помеѓу професионалните групи во една земја, постојат и значителни меѓунационални разлики во тоа како се перципира ризикот.³⁵² Дополнително, познато е дека широк спектар на основни психолошки процеси се под влијание на културата, вклучително и веројатноста за фундаментална грешка при припишувањето и размислување за веројатноста. Оттука очигледно е дека со мноштвото национални чинители во секоја од аспектите на заштита на критична инфраструктура, одржувањето на конзистентност во процените на ризик, како и униформирана перцепција на ризик низ регионите и државите, претставува сериозен предизвик. И покрај ова, ваквите предизвици не се разгледани/испитувани во литературата за процена на ризик во контекст на заштита на критична инфраструктура.

Сумирајќи, иако постои значителна литература за ефектот на хеуристиката за донесување одлуки и предрасудите во генеричкиот процес на процена на ризик, нивната импликација не е соодветно испитана во специфичниот контекст на заштита на критична инфраструктура.

352 Rohrmann, B. (2000). Cross-cultural studies on the perception and evaluation of hazards. In: Renn, O., Rohrmann, B. (Eds.), Cross-Cultural Risk Perception. Technology, Risk, and Society (pp. 103–143). Springer, Boston, MA, достапно на: https://doi.org/10.1007/978-1-4757-4891-8_3.

10. АНАЛИЗА ЗА ПЕРСПЕКТИВНОСТА НА ПРИВАТНАТА БЕЗБЕДНОСНА ИНДУСТРИЈА ВО КОНТЕКСТ НА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

10.1. Предизвици за приватната безбедносна професија

Приватната безбедност придонесува за заштита на критичната инфраструктура преку:

- ❖ **Физичка безбедност.** Приватни безбедносни фирми што се специјализирани за обезбедување физички средства, како што се згради, објекти и периметри. Тие користат различни мерки како контрола на пристап, надзор, патроли и безбедносни контролни пунктови за да ги заштитат критичните инфраструктурни инсталации од неовластен пристап, вандализам, саботажа и кражба.
- ❖ **Сајбер-безбедност.** Во денешната дигитална ера, заштитата на критичната инфраструктура вклучува и заштита од сајбер-закани. Приватните фирми за сајбер-безбедност обезбедуваат експертиза за идентификување на ранливости, спроведување заштитни мерки, следење на мрежи за сомнителни активности и навремено реагирање на сајбер-инциденти. Тие помагаат да се спречат нарушувања на основните услуги предизвикани од сајбер-напади.
- ❖ **Проценка и управување со ризик.** Приватните безбедносни фирми спроведуваат сеопфатни процени на ризик за да ги идентификуваат потенцијалните закани и ранливости во системите на критична инфраструктура. Со анализа на фактори како што се физичките ранливости, слабостите на сајбер-безбедноста и оперативните ризици, тие развиваат стратегии за ефективно ублажување на овие ризици.
- ❖ **Одговор во итни случаи и управување со кризи.** Приватниот безбедносен персонал често е обучен да реагира на итни случаи брзо и ефективно. Во случај на природни катастрофи, терористички напади или други кризи што

влијаат на критичната инфраструктура, тие играат клучна улога во координирањето на процедурите за евакуација, обезбедувањето прва помош и поврзувањето со службите за итни случаи за да се ублажи ударот и да се обнови нормалното работење.

- ❖ **Консалтинг и обука за безбедност.** Приватните безбедносни консултанти нудат специјализирани знаења и насоки на операторите на критичната инфраструктура за најдобрите безбедносни практики, усогласеноста со регулативата и заканите што се појавуваат. Тие дизајнираат приспособени безбедносни решенија приспособени на уникатните потреби и ризици на секој инфраструктурен сектор. Дополнително, тие обезбедуваат програми за обука за подобрување на подготвеноста и способностите за одговор на персоналот во инфраструктурата.
- ❖ **Јавно-приватно партнерство.** Соработката помеѓу субјектите од јавниот и приватниот сектор е од суштинско значење за ефикасна заштита на критичната инфраструктура. Приватните безбедносни компании често работат во партнерство со владини агенции, индустриски здруженија и други засегнати страни за споделување разузнавачки информации, ресурси и експертиза. Овие партнерства го зајакнуваат целокупното безбедносно држење и еластичноста на системите за критична инфраструктура.
- ❖ **Интеграција на иновации и технологија.** Приватните безбедносни фирми постојано инвестираат во најсовремени технологии и иновации за да ја подобрат безбедноста на критичната инфраструктура. Ова вклучува распоредување напредни системи за надзор, алатки за биометриска автентикација, сензори за откривање на упад и софтвер за предвидлива анализа за проактивно откривање и спречување потенцијални закани.

Заштитата на критичната инфраструктура се соочува со голем број предизвици:

- **Комплексност и вмрежување.** Критичните инфраструктури често се многу сложени и меѓусебно поврзани. Неуспехот во еден сектор може брзо да има влијание врз

другите сектори. Оваа меѓусебна поврзаност бара сеопфатна и координирана стратегија за заштита.

- **Сајбер закани.** Со зголемувањето на дигитализацијата, критичните инфраструктури сè повеќе се цел на сајбер напади. Заштитата од такви закани бара специјализирани безбедносни мерки и континуиран мониторинг.
- **Физички закани.** Покрај сајбер-заканите, постојат и физички закани како природни катастрофи, тероризам и саботажа. Заштитата од овие закани бара силни физички безбедносни мерки.
- **Регулаторни барања.** Различни земји и региони имаат различни регулаторни барања и стандарди за заштита на критичната инфраструктура. Усогласеноста со овие барања може да биде предизвик, особено за компаниите што работат на меѓународно ниво.
- **Недостиг на ресурси.** Заштитата на критичната инфраструктура бара значителни финансиски и човечки ресурси. Особено помалите компании и организации често се соочуваат со предизвикот да ги обезбедат потребните ресурси.

Светот на приватното обезбедување еволуираше значително, поттикнат од постојаното зголемување безбедносни закани и, од друга страна, од близината која е сè помала секој ден со внатрешните безбедносни сили.

Еволуцијата на приватниот безбедносен сектор – а со тоа и неговата способност да помогне во заштитата на светската критична инфраструктура – се карактеризира со два силни тренда.

Првиот тренд е неповратно проширување на областа на надлежност на приватните компании за обезбедување на национално ниво, со приспособена регулаторна рамка. На дневна основа, заканите по безбедноста и здравјето се зголемуваат и службите за спроведување на законот на национално и локално ниво се обврзани повторно да се фокусираат на голем број мисии. Тоа значи дека приватното обезбедување ќе станува сè поприсутно во јавниот простор, и дека одредени мисии, како на пример, евидентирање на прекршоци, кражби во продавници, насилство врз луѓето што посетуваат шопинг-центри, би можеле да им се доверат. Тоа е веќе случај за железничкиот транспорт, на ист начин како што е веќе

возможно за компаниите за обезбедување да вршат (во одредени случаи и со одредено овластување на државниот претставник) обезбедување на јавниот простор. Дури и ако е потребно време, поради институционални кочници или корпоративни реакции, трендот е потврден. Факт е дека приватните безбедносни компании (PSCs) веќе обезбедуваат заштита и безбедносните услуги до широк опсег на јавни области и згради: трговски центри, ресторани, кина, стадиони, аеродроми, возови, градски јавен превоз, плажи и планински одморалишта итн.

Вториот тренд е сè посилен технолошки микс. Додека многу се дебатираше за работниците за обезбедување во иднината како „зголемена заштита“, нема сомнеж во тоа дека тие ќе бидат многу подобро опремени. Новите технологии ќе ги олеснат нивните мисии со тоа што ќе им се овозможи подобро да ја разберат нивната околина. Тие ќе имаат пристап до информации во реално време и интеграција на податоци што ќе овозможи нивниот оперативен менаџмент да се ослободи од административни задачи, за да можат да бидат уште поприсутни на терен и поблиску до нивните клиенти.

Вештачката интелигенција во областа на однесувањето и препознавањето на лицето ќе ја надополнуваат обуката во моментов и се обезбедени на агентите, бидејќи обуката ќе биде одлучувачки фактор во способноста на припадниците на приватното обезбедување да се развиваат во заштитен свет со поефективни безбедносни технологии. Откривање „ризично или неусогласено“ однесување ќе помогне да се избегне конфликт или криминални ситуации. Откривањето на звук (вресок, плач, специфични звуци), исто така, ќе ја подобри брзината и ефикасноста на интервенциите што треба да се направат во јавните простори, како што се трговски центри.

Приватните безбедносни компании ќе мора да изградат и да понудат хибридна безбедносна услуга (човекова технологија) за нивните клиенти, водени од дигитални платформи за хипервизија, способни на управување со безбедносните операции и на обезбедување значителна додадена вредност во смисла за управување со инциденти или кризи. Со анализирање на собраните информации и инцидентите со кои се справуваат, овие алатки

обезбедуваат предвидувачки капацитет што го овозможува тоа да се предвидат времето и местото каде може да се случат можни инциденти. Услугите затоа се програмирани соодветно, а безбедносните тимови се распоредени преку управување со човечки ресурси што е можно попрецизно.

Имајќи ја предвид наведената динамика и трендови, ќе мора во иднина да се пристапи кон холистички поглед на нештата. Холистичкиот пристап овозможува да се комбинира know-how во човековата безбедност со способност за интегрирање на иновативни технологии да се задоволат потребите на клиентот, вклучително димензијата на сајбер-безбедноста. Оваа еволуција ќе резултира во создавањето споделена вредност помеѓу безбедносните компании и клиентите, со нудење на клиентите поквалитетна услуга споредбена со денешната.³⁵³

Покрај овој технички развој, приватниот безбедносен сектор, исто така, поминува низ структурни промени. Концентрацијата на компаниите се зголемува, а многу од нив се движат кон интеграција на разновидна понуда. Приватните безбедносни компании мора сега да покриваат поширок спектар на вредносниот синџир, од деловна експертиза до интеграција на безбедносни системи, дополнително традиционална понуда за човечка безбедност што е сè попрофесионална и ефикасна. Така, покрај човечките вештини очекувани од клиентите, тие мора да се посветат на холистички пристап кон нивната безбедносна понуда. Тие мора да се позиционираат себеси vis-à-vis нивните клиенти на ист начин како да ги сфатат нивните ризици, за да може да ги предвидат нивните безбедносни проблеми и да најдат соодветни решенија за нив бидејќи безбедносната закана е тридимензионална и мора да се третира како таква.

353 Jean-Philippe Bérillon. (2023). Cyber-Physical Security and Critical Infrastructure, International Security Ligue, CoESS.

Глава III

ИНТЕРПРЕТАЦИЈА НА РЕЗУЛТАТИТЕ ОД ЕМПИРИСКОТО ИСТРАЖУВАЊЕ

1. МЕТОДОЛОШКА РАМКА

Приватната безбедност во македонската држава години назазад се наоѓаше во подредена улога во однос на јавната безбедност и најчесто беше маргинализирана од медиумите, а неприфатена од обичните граѓани. Меѓутоа, денес ситуацијата е многу поразлична. Тоа се должи на трансформацијата на размислувањата за местото и улогата на дејноста приватно обезбедување во остварување на безбедноста. Значи, во изминатите неколку години се конвергира негативното мислење за приватната безбедност во позитивно што е дијаметрално спротивно од претходното, а трансформацијата направи делумно да се привлече вниманието и на академската јавност и се отвори суштинска дебата за политиката на приватната безбедност.

Значи приватната безбедност во македонската држава веќе ги има трасирано главните контури во општествено-политичкиот дискурс. Сепак, најголемата дискусија не се води околу прашањето: „Дали има потреба од приватна безбедност?“, туку за прашањето: „Каква треба да биде приватна безбедност?“. Секако дека и одредени прашања го заслужуваат потребното внимание, како што се: „Каде се преклопуваат улогите на приватното обезбедување и на полицијата, а каде се разидуваат?“, особено ако се знае дека овие два сектора се доживуваат истовремено како конкуренција и секако централното прашање: „Што ги мотивира приватните компании за обезбедување – поголема безбедност или поголем профит?“, но и важните прашања за улогата на приватната безбедност во заштита на критичната инфраструктура. Одговорот на овие прашања се заснова на спроведеното истражување за оваа намена со кое се понуди интроспекција на вработените во приватното обезбедување во доменот на придонесот на дејноста приватно обезбедување во заштитата на критичната инфраструктура. На 73 испитаници им беше испратен прашалник со четиринаесет структурирани прашања преку чии одговори се утврдува корелацијата на возрасната, половата и образовната структура на овој репрезентативен примерок и нивните

ставови за степенот на заокруженост на законската рамка на дејноста приватно обезбедување, нивото на оспособеноста и овластувањата на работниците за обезбедување, соработката со државните безбедносни институции со акцент на полицијата, како и значењето на придржувањето и исполнувањето на етичките и професионалните стандарди во вршењето на дејноста. Понатаму, се испитува каузалноста за објективната потреба од воспоставување законска рамка за заштита на критичната инфраструктура, неопходноста од соработка помеѓу приватната безбедност и полицијата во овој домен и капацитетите на приватната безбедност во осигурувањето на безбедноста и заштитата на критичната инфраструктура.

2. ИНТЕРПРЕТАЦИЈА НА РЕЗУЛТАТИТЕ

Првото прашање на кое испитаниците го дадоа својот одговор во овој прашалник се однесуваше на *возрасната структура*, во која беа опфатени возрасти од 18 до 26 години, од 27 до 36 години, од 37 до 46 години и од 47 и повеќе години, а се согледа нивниот став во контекст на нивната возраст и нејзината корелација со перцепциите за одделни прашања. Еден од испитаниците е на возраст од 18 до 26 години, 19 испитаници се на возраст од 27 до 36 години, 24 испитаници спаѓаат во возрасната група од 37 до 46 години и 29 од испитаници имаат возрасна структура над 47 години.



Графикон број 1. Возрасна структура

Второто прашање ја утврдува *половата структура* на испитаниците и нивните ставови во контекст на истата проблематика, при што се забележува изразено мнозинство на припадниците на машкиот пол во сооднос 83,6 % машки наспроти 16,4% испитаници од женски пол. Овој репрезентативен примерок отстапува двојно од целокупната застапеност на жените во приватното обезбедување, која изнесува 8 % од целокупната работна сила во согласност со процентуалната состојба во 2024 година, односно во ова истражување учество зеле два пати повеќе жени од аспект на генералните пропорции.



Графикон број 2. Полова структура

Одговорите од третото прашање го откриваат степенот на нивото на образование. На испитаниците им беше понудено да го наведат *степенот на образованието* што е класификуван во согласност со националната рамка на квалификации и соодветните нивоа, при што на испитаниците им беше понудено да одговорат во рамки на опциите: *завршено средно образование 3 години (180 ЕКТС)* или *4 години (240 ЕКТС)*; *завршено високо образование I циклус студии (180/240 ЕКТС)*; *завршени II циклус стручни или академски студии (60/120 ЕКТС)*.

Најголем дел од испитаниците, процентуално 71,2 % имаат завршено средно образование или 52 од вкупниот број испитаници, 17 испитаници имаат завршено високо образование или изразено во проценти – 23,3 %, додека 5,5 % од испитаниците,

односно четири од нив имаат завршено втор циклус – магистерски студии. Степенот на образование беше земен предвид во контекст на одредување на нивото за познавање и информираноста на работниците за обезбедување за правната и нормативна уреденост на дејноста, начините на соработка со другите релевантни институции предодредени да ја одржуваат безбедноста и можноста за унапредување на дејноста како и придонесот на приватното обезбедување во заштита на критичната инфраструктура. Притоа, се утврдува дека степенот на образование кај работниците што беа дел од ова истражување не претставува значајна варијабла поради која се забележуваат значителни отстапки во ставовите на испитаниците во целост, односно нивните ставови се хармонични и не е утврдена драстична разлика во перцепциите. Специфично е и тоа што во ова истражување, сите припаднички вработени во приватното обезбедување што беа дел од овој прашалник, имаат завршено (најмалку) високо образование.



Графикон број 3. Образовна структура

На прашањето под реден број 4 (четири): *Како го оценувате придонесот на приватното обезбедување во остварување на безбедноста на државата?*, на испитаниците им беа дадени опции да одговорат со а). *имаат многу голем придонес*, б). *остваруваат голем придонес*, в). *делумно придонесуваат и опција под број г). не знам*.

На испитаниците им беше поставено прашање поврзано со безбедноста, имајќи предвид дека приватното обезбедување

игра голема улога во остварување на безбедноста, а колку е безбедноста важна и постојана тема говори Брукс кој апострофира дека безбедноста е непредвидлива и каприциозна по природа и примена, практикувана во многу домени и со хетерогени актери. Поради оваа повеќедимензионална природа, таа е непостојана и подложна на варијации низ различни просторни и временски размери. Безбедноста е заедничка јавна, приватна, корпоративна и лична средина. Безбедносниот домен опфаќа различни сегменти од широкиот спектар активности и практики, меѓу кои се меѓународната безбедност, националната безбедност, јавната безбедност, приватната безбедност и др. Таквата разновидност го отежнува ангажманот во обезбедувањето единствена интегрална дефиниција за разните сегменти, бидејќи дефиницијата зависи од референтниот објект на безбедноста и применетиот контекст.³⁵⁴

Поимот безбедност не е ниту статичен, ниту конзистентен во онтолошки и епистемолошки контекст. Дефинициите, концептот и опсегот на безбедноста остануваат постојани точки на калибрација на прогресот и на примената на активностите преземени во име на обезбедување на безбедноста, што примарно имплицираат дисциплина, контрола и ред.

Безбедноста претставува состојба на сигурност што произлегува од самата концепција за безбедност што врши идентификација на опасностите и од перцепцијата за безбедноста што е детерминирана од личните, културните и општествените фактори. Таа е фундамент на моделот на слободно општество во контекст на непреченото уживање на политичките, економските и личните слободи. Сепак, политичките, економските и личните слободи се под многустран и постојан (потенцијален) напад што се манифестира во тековните настани.³⁵⁵

354 Brooks, D., Corkill, J., Coole, M. (2016). The Australian Security Continuum: National and Corporate Security Gaps from a Surveillance Language Perspective. In: Lippert, R., Walby, K., Warren, I., Palmer, D. (eds) National Security, Surveillance and Terror. Crime Prevention and Security Management. Palgrave Macmillan, Cham.

355 Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, 23(1), стр. 5–26. <http://www.jstor.org/stable/20097464> (посетена на 11.05.2022).

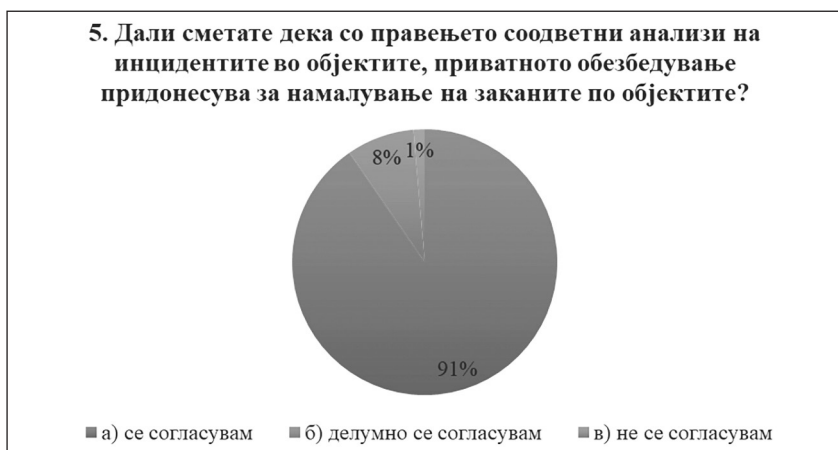
Во согласност со дадените ставови, евидентно е дека работниците за обезбедување генерално сметаат дека приватното обезбедување има значителен придонес кон остварување на безбедноста на државата како дел од целокупната или интегрална безбедност, додека една петтина (1/5) од испитаниците смета дека придонесот на приватното обезбедување во остварување на безбедноста на државата е делумен.



Графикон број 4. Придонесот на приватното обезбедување во остварување на безбедноста

Петтото прашање во прашалникот креирано за спроведување на ова истражување гласи: *Дали сметате дека со правењето соодветни анализи на инцидентите во објектите, приватното обезбедување придонесува за намалување на заканите по објектите?*“. Во однос на можните модалитети беа понудени четири можни одговори, на кои испитаниците можеа да одговорат со: *се согласувам, делумно се согласувам, не се согласувам и не знам*. Повеќе од 90 % од испитаниците сметаат дека со вршењето анализи на настанатите инциденти во објектите што се предмет на обезбедување се подобрува квалитетот на нивните услуги и се зголемува придонесот кон намалување на заканите по безбедноста. Несомнено сето ова води кон заклучок дека постои консензус за неопходноста на примена на аналитички и научни методи во перцепцијата на приватната безбедност. Кога се говори за креирањето анализи, тука се има предвид примената на апли-

кации и софтвер за мапирање, симулации и 3-Д моделирање, бази за внес на податоци за инциденти и нивно процесирање за откривање закономерности и шеми на предвидливост. Тука може да се забележи дека иако аналитичкиот аспект на управувањето со инциденти во приватното обезбедување во тековното работење се потпира на примена на напредни технолошки уреди и програми, испитаниците што спаѓаат во сите категории возрасти, 18-26, 27-36, 37-46 и над 47-годишна возраст, ја препознаваат потребата од вршење разни видови анализи на инцидентите во објектите и аналого на тоа сметаат дека приватното обезбедување ќе придонесе кон намалување на заканите по објектите.



Графикон број 5. Значењето на анализите за согледување на инциденти

На шестото прашање што беше поставено: *Дали сметате дека Законот за приватно обезбедување е солидна правна рамка што наоѓа адекватна примена во пракса?*, испитаниците што зедоа учество во пополнување на овој прашалник можеа да одговорат со: *да, во голема мера, делумно, не и со не знам* имајќи ја предвид динамиката на дејноста приватно обезбедување и предизвиците со кои се соочуваат при вршење на дејноста, а во контекст на пропорционалноста со нивните овластувања и надлежности. Тука одговорите говорат дека 71,2% од испитаниците сметаат дека

Законот за приватно обезбедување е солидна правна рамка која наоѓа адекватна примена во пракса.



Графикон број 6. Адекватна примена на законските одредби

На прашањето: *Дали сметате дека Законот за приватно обезбедување треба да претрпи одредени измени и ако сметате дека е потребно наведете во кој сегмент?*, испитаниците можеа да одговорат описно и да го искажат своето индивидуално мислење во релација со сеопфатноста на законската рамка и дали таа ги инкорпорира сите значајни сегменти што се неопходни да се заокружи процесот на легалната дезигнација на дејноста приватно обезбедување, што претставува дејност од јавен интерес.

Кај овие одговори се издвојува ставот дека е потребна поголема формална и мандаторна соработка со полицијата, дека е потребна дообјаснета пропишана постапка за употреба на оружје и примена на средства за присилба кај физичкото обезбедување при отстранување на заканите и опасностите, особено во ситуации на затекнато лице при кражба или во случаи на насилство. Понатаму, од аспект на оперативниот сегмент во работењето наведоа дека важно е да се допрецизираат овластувањата во рамки на границите за штитениот објект, од аспект на просторното важење на овластувањата дадени со законот, потоа да се иницираат измени во законот и овозможување на вработување пензиониран кадар, измени во Законот за оружје за поедноставување и убрзување на

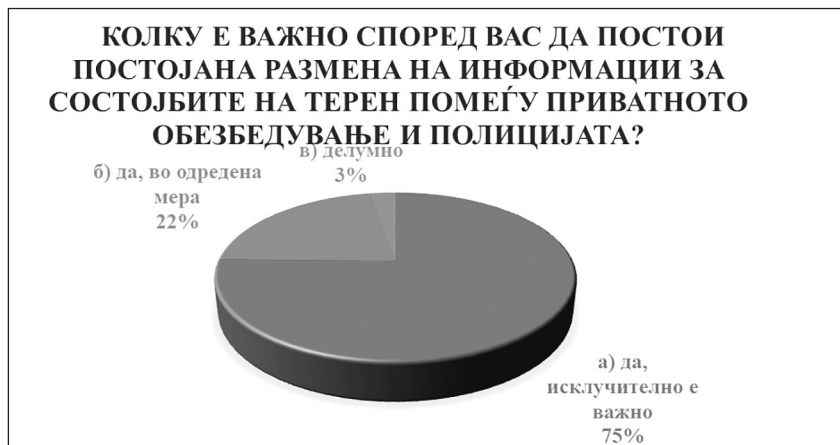
постапката за добивање дозвола за носење оружје; воведување повеќе категории и лиценци за обезбедување – транспорт на пари, мониторинг и патролно обезбедување, ВИП-обезбедување, обезбедување на јавни настани, итн.; воведување повеќе класи на агенции за обезбедување во зависност од бројот на услуги што се нудат и капацитетот (човечки и технолошки) на самата агенција; подигнување на квалитетот на обуките; како и воведување на програма за субвенционирање на лиценцирање кадар од страна на државата итн. На крајот, но не помалку значајно, легална дезигнација што ќе придонесе за поголема заштита на работниците на приватното обезбедување од аспект на работничките права, при што во оваа група одговори се забележува и ставот околу зголемување на степенот на правата, овластувањата и обврските на вработените и јасна дистинкција помеѓу видовите лиценци, т.е. степенување на лиценцата за физичко обезбедување и техничко обезбедување, како и унифицирање на обуката. Понатаму, да се направи исчекор кон добивање меѓународно признавање на добиените лиценци до мерка што е дозволена во согласност со европските закони. Исто така, се забележува и ставот околу цената на услугата за обезбедување што е квалификувана како минимална.

Во однос на значењето на соработката од аспект на размена на информациите во оперативниот домен на дејствување помеѓу секторот приватно обезбедување и полиција со цел постигнување повисоко ниво на безбедност и негово одржување, во прашалникот беше креирано прашање под реден број 8 (осум), што гласи: *Колку е важно, според Вас, да постои постојана размена на информации за состојбите на терен помеѓу приватното обезбедување и полицијата?*, при што испитанниците можеа да одберат да одговорат: под а) да, исклучително се важни, под б) да, во одредена мера, в) делумно, како и под г), не знам. Според прегледот на дадените одговори, три четвртини сметаат дека исклучително е важно да постои постојана размена на информации за состојбите на терен помеѓу приватното обезбедување и полицијата, односно 75,3 % од испитаниците сметаат дека е исклучително важно да постои постојана размена на информации за состојбите на терен помеѓу приватното обезбедување и полицијата.

Општата констатација е дека информациите се предуслов за добро работење помеѓу клучните безбедносни актери. Без

потребните сознанија, податоци, параметри, невозможно е да се донесе координирана одлука. Од друга страна, резултатот на одлучувањето – одлуката како предуслов за акција, исто така, е информацијата. Оттука, секој систем, но и човекот се бори да обезбеди точни, квалитетни, комплетни, навремени и корисни информации. Информацијата со вакви карактеристики ја намалува неизвесноста. Ако ја зголемува неизвесноста, тогаш таа е лоша, некорисна информација. Но постојат различни комбинации за карактеристиките на информациите. На пример, информациите можат да бидат точни, но некомплетни со што ќе го дезориентираат корисникот. Можат да бидат точни, но ненавремени со што нема да ја имаат очекуваната вредност за корисникот. Можат да бидат точни, но некорисни, доколку се претставени во поголем обем или пак на начин неприфатлив за корисникот итн.³⁵⁶

Општиот заклучок е дека информацијата има висока општествена употребна вредност, основен стратегиски ресурс, главен инпут на секоја човекова дејност, како и главен развоен фактор, што е поважен дури и од материјалниот фактор.³⁵⁷



Графикон број 7. Важноста од размена на информации

³⁵⁶ Поповска З., *Управување со системите*, Економски факултет, Скопје, 2006, стр. 113.

³⁵⁷ Стојановиќ П., *Теорија привредног развоја у мрежој технолошкој револуции*, Савремена Администрација, Београд, 1964, стр. 3-15.

Во оваа насока покрај размената на информациите важна е и соработката. Следното прашање имаше задача да го провери ставот во однос на соработката и гласеше: *Дали, според Ваше мислење полицијата е заинтересирана за соработка со приватното обезбедување во решавање на проблемите со криминалот?*. Одговорите главно го истакнуваат генерално афирмативниот став во однос на соработката помеѓу приватното обезбедување и полицијата во решавањето на проблемите поврзани со криминалот, каде одговорите и на машките и на женските испитаници во најголем број ја оценуваат заинтересираноста на полицијата за соработка на ниво делумно, поточно речиси половина од вкупниот број испитаници (49,3%), што остава простор за дополнително продлабочување на соработката помеѓу овие два заемно комплементарни субјекти во борбата со различните форми и облици на криминал.

Од аспект на остварување на безбедноста нема дилема дека субјектите задолжени за безбедност мора да соработуваат и заеднички да ги планираат активностите за да се обезбеди потребната благосостојбата на општеството или на поединецот. Оттука, нормалниот одговор на оваа дилема потенцира три аспирации: легитимност, професионализам и одговорност. Оттука, главните цели се насочени кон постојана легитимност, постојан професионализам и постојана одговорност. Сите три услови мора да постојат и да бидат исполнети за да говориме дека постои демократско управување. Професионалното однесување и одговорноста ја поткрепуваат легитимноста, додека одговорноста ја овозможува професионалноста, а легитимноста го овозможува потребниот степен на професионална самостојност.³⁵⁸ Одговорноста значи проактивен пристап за себе, заштита на себе од другите, одговорност кон државата, кон вредностите, кон фирмата, кон работата, кон работодавачот, кон професијата итн. Професионализмот значи и партиципативно учество и придонес, но и идеја како да се поттикне креативноста што во основа ќе значи иновативност,

³⁵⁸ Бакрески О., Контрола на безбедносниот сектор, Филозофски факултет, Скопје, 2012.

решителност, како и преземање акција за да се овозможат промените во безбедносна смисла на зборот.



Графикон број 8. Полицијата и приватното обезбедување во борба против криминалот

За да се согледа колку е важна соработката и координацијата меѓу сите чинители во безбедносниот сектор за давање соодветен одговор на современите ризици и закани по безбедноста беше поставено следното прашање: *Колку е важна соработката и координираниот напор на сите безбедносни субјекти (полиција, армија, разузнавачки служби, приватно обезбедување) во справување со потенцијалните ризици и закани?* На испитаниците им беа понудени следните можни одговори: а) многу е важна, под б) делумно е важна, в) важна е во одредена мера и г) не знам. Одговорите на ова прашање го потенцираат генералниот став на работниците за обезбедување за неопходноста од координиран ангажман на сите безбедносни субјекти што се дел од целокупниот безбедносен систем на државата во справување со потенцијалните ризици и закани, односно 85 % од вкупниот број испитаници сметаат дека соработката и координираниот напор на сите безбедносни субјекти (полиција, армија, разузнавачки служби, приватно обезбедување) во справување со потенцијалните ризици и закани е многу важна.

Во основа, потребно е да се истакне дека соодветно ниво на координација не би било постигнато доколку не му претходи оптимално ниво на соработка. Но, тоа не значи дека координацијата автоматски потекнува од доброволните напори на вработените или

безбедносните субјекти.³⁵⁹ Нема дилема дека координацијата треба да се постигне преку свесни и намерни напори на сите клучни актери, па оттука, може да се заклучи дека соработката без координација нема плод и координацијата без соработка нема корен.³⁶⁰



Графикон број 9. Соработка и координација

Имајќи ги предвид сè покомплексните задачи што се наметнуваат да ги вршат работниците за обезбедување и полицијата, логично се наметнува прашањето не дали туку: *Колку е важно приватното обезбедување и полицијата во своето работење да се базираат на строгите етички и професионални стандарди?*

Нема дилема дека работењето на принципите на строгите етички и професионални стандарди ќе придонесе и приватното обезбедување и полицијата во своето работење дека ја имаат потребната легитимирачка компетитивност.

Во основа, професионализмот дефинира три карактеристики, и тоа: експертиза, одговорност и корпоративност³⁶¹ и е

³⁵⁹ Woodward J., Industrial Organization: Theory and Practice, Second edition, Oxford University Press, 1980.

³⁶⁰ United Nations Disaster Assessment and Coordination. UNDAC Field Handbook 7th Edition, 2018. https://www.unocha.org/sites/unocha/files/1823826E_web_pages.pdf

³⁶¹ Military Professionalism in Asia: Conceptual and Empirical Perspectives. East West Center. 2001.

категоријална црта што се однесува на одредени вредности, вештини, ориентација и управување. Принципите на фер-однесување, интегритет, грижа за човековите права, одговорност и соодветна употреба на сила се основните елементи во секој концепт на демократското управување. Професионализмот не смее да се вмеша во дискриминаторно, корумпирано или насилно искористување на својата моќ. Самостојноста (ограниченоста) што ја има приватниот безбедносен сектор се базира врз довербата на општеството дека овој сектор ќе прифати дел од вредностите што ќе ја условува демократската рамнотежа на етичко и на професионално водење.³⁶² Излегувањето од преградите на професионализмот ќе резултира со грубо, корумпирано и некомпетитивно однесување, а во некои случаи може да доведе дури и до јавни скандали, што ја наметнува потребата од сериозна регулатива во овој сектор.³⁶³

Во контекст на степенот на образование и ставовите во врска со етичноста и професионалноста во дејноста приватно обезбедување и работата на полицијата, речиси сите испитаници одговорија потврдно дека е многу важно приватното обезбедување и полицијата во своето работење да се раководат според строгите етички и професионални стандарди.



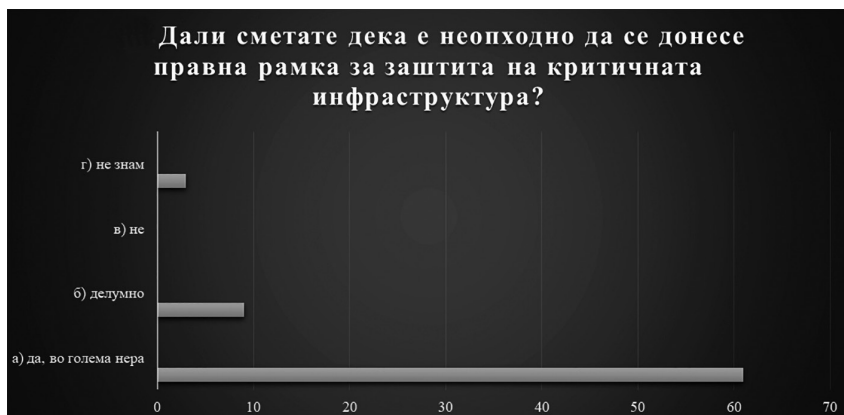
Графикон број 10. Строги етички и професионални стандарди

³⁶² Fluri P., Hadžić M., eds., 2004.

³⁶³ Born H. Caparini M. and Cole E., 2007.

За да се согледаат какви се сознанијата од неопходноста од обезбедување на потребната правна рамка за заштита на критичната инфраструктура на испитаниците им беше поставено и следното прашање, што гласи: *Дали сметате дека е неопходно да се донесе правна рамка за заштита на критичната инфраструктура?*, а коешто се надоврзува на повеќегодишните заложби и иницијативи од страна на инволвираните чинители, за донесување соодветно законско решение, испитаниците можеа да се определат за некои од понудените модалитети на одговори, и тоа: а). *Да, во голема мера*, б). *делумно*, в). *не* или пак – г). *не знам*.

Од аспект на ставовите во речиси 84 % од испитаниците имаат афирмативен став кон донесувањето закон со кој се утврдува националната критична инфраструктура и се уредуваат инструментите со кои таа се заштитува, односно во голема мера може да се констатира од изнесениот став дека е потребно да се дефинира во рамки на позитивните законски прописи.



Графикон број 11. Правна рамка за критична инфраструктура

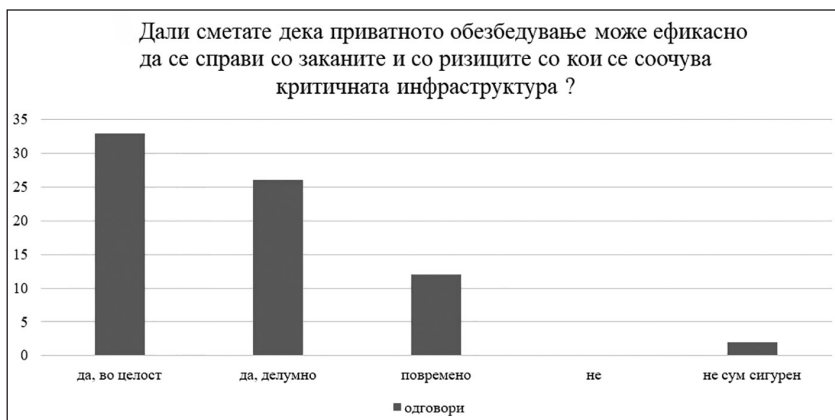
Наредното прашање беше поврзано со ефективното работење во справување со заканите по критичната инфраструктура, односно конкретното прашање беше во насока на: *Дали сметате дека приватното обезбедување може ефикасно да се справи со заканите и со ризиците со кои се соочува критичната ин-*

фраструктура? Тука податоците говорат дека една третина од испитаниците сметаат дека приватното обезбедување, со своите капацитети, овластувања и задачи во целост може да се справи со заканите и ризиците со кои се соочува критичната инфраструктура, која е составена од физички и сајбер-елементи и опфаќа мноштво од системи што се меѓусебно поврзани и заемно зависни, при што за нивната заштита е неопходно да се преземаат деликатни и комплексни мерки.

Ваквата свесност потврдена во артикулираните одговори не упатува на заклучок дека критичната инфраструктура со која се опишува фрагилниот систем на пренос и складирање на виталните ресурси за функционирање на сите општествени процеси, е мета на физички и сајбер-закани. Заканите по критичната инфраструктура се закана што зазема современ облик, но која постои и во историските сведоштва како начин на нанесување штета на одреден субјект. Во овој домен, заканите се минимизираат преку ангажман на приватното обезбедување.³⁶⁴ Потенцијалните закани по критичната инфраструктура, што директно влијаат на безбедноста, имајќи ја предвид меѓусебната поврзаност на системите на критичната инфраструктура и каскадниот ефект со кој тие се прелеваат преку националните граници и меѓу надлежностите на релевантните институции настанува во услови на недоволно прецизно утврдени актери задолжени за нејзина заштита, недостаток од размена на информации помеѓу релевантните чинители, немањето јасно поставена правна рамка, процедури и стандарди, како и отсуството на синхронизирана меѓуинституционална и меѓуагенциска координација.³⁶⁵

364 Bardjieva, L. (2017) The Role of the Private Security in the Critical Infrastructure Protection in Some of the Balkan States. Security Dialogues.

365 Slayton, R. and Clark-Ginsberg, A. (2018), Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. Regulation & Governance, стр. 115-130. <https://doi.org/10.1111/rego.12168>



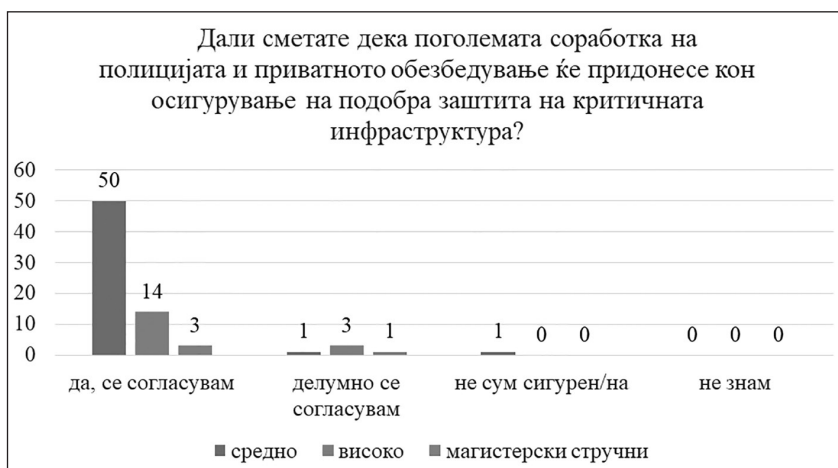
Графикон број 12. Приватното обезбедување во заштита на критичната инфраструктура

На крај, во согласност со утврдената методологија и структура на прашањата, следува четиринаесеттото и последно прашање, со кое се согледува пулсот на генералниот дискурс во која насока се движат размислувањата на испитаниците по однос на прашањето: *Дали сметате дека поголемата соработка на полицијата и приватното обезбедување ќе придонесе кон осигурување подобра заштита на критичната инфраструктура?*, каде што можните опции за одговор се: а) да, се согласувам, б) делумно се согласувам, в) не сум сигурен, г) не знам. Процентуално, речиси 92 % од испитаниците одговориле дека се согласуваат дека поголемата соработка на полицијата и приватното обезбедување ќе придонесе кон осигурување на подобра заштита на критичната инфраструктура.

Нема дилема дека поголемата соработка ќе услови и подобра заштита на критичната инфраструктура. Затоа критичната инфраструктура е во сопственост, но и управувана, регулирана и заштитена од комплексна мешавина на јавни и приватни субјекти, при што најчесто е управувана, односно менаџирана од страна на националните, од приватните и/или локалните власти.³⁶⁶ Кога ста-

³⁶⁶ Bardzieva, L. (2017) The Role of the Private Security in the Critical

нува збор за заштитата на критичната инфраструктура, конкретно, праксата на ниво на Европската Унија покажува дека приватните безбедносни актери имаат значителен удел во обезбедувањето на националните и европските системи за критична инфраструктура, преку јавни-приватни партнерства помеѓу носителите на политички одлуки, сопствениците, односно управителите на критичната инфраструктура и крајните корисници.³⁶⁷



Графикон број 13. Приватното обезбедување и полицијата во заштита на критичната инфраструктура

Општите констатации што произлегоа од резултатите на истражувањето нè упатуваат на заклучокот дека како и секоја дејност, приватното обезбедување бара можности да го прошири својот бизнис, но за да се оценат новите бизнис- перспективи во денешното опкружување, важно е тие да ги препознаат зголемените закани и ризици што можат да ги загрижуваат неговите кли-

Infrastructure Protection in some of the Balkans States. Security Dialogues Year 8, no. 2. <https://doi.org/10.47054/SD172>

367 Kovács, T., Nyikes, Z., Fürstner, I. (2022) Security-Related Advanced Technologies in Critical Infrastructure Protection. Theoretical and Practical Approach. Springer Dordrecht. <https://doi.org/10.1007/978-94-024-2174-3>

енти.³⁶⁸ Од сите наведени податоци со кои се дефинира тековната состојба на приватната безбедност, како и идните проекции што се базираат на новите безбедносни закани, се конципираат новите безбедносни трендови што претставуваат движечка сила за процесите и динамиката на работа на приватниот безбедносен сектор. Потребата изразена со синтагмата *да се добие повеќе со помалку*, само ја нагласува потребата од анализа на наведените безбедносни трендови, како и нивно приспособување, со цел исполнување на безбедносните задачи и обврски.

Во основа, важно е да се истакне дека во согласност со сите наведени податоци од студијата, може да се изведе заклучок дека настанува спојување помеѓу концептите и акцентот е ставен на интегралниот пристап, односно основните концепти се подредени на нивна меѓусебна меѓузависност, што подразбира појава на трендот на таканаречената *безбедносна конвергенција*. Безбедносната конвергенција значи интеграција на програмите за физичка безбедност и техничка безбедност со посредство на информатичката технологија. Со други зборови, тоа во суштина претставува комуникација и соработка помеѓу клучните приватни безбедносни актери за заштита на луѓето, имотот и работењето.

Значајно е да се истакне дека паралелно со општествените, со политичките, со економските и со безбедносните трендови, неопходна е формулација на соодветни стратегии и програми за дејствување од страна на приватното обезбедување, што ќе моделира соодветен одговор на овие нови безбедносни трендови преку примена на автентични и наменски решенија, со специфичности и карактеристики на локалниот, националниот и поширокиот пазар, како и потребата и побарувачката детерминирана од крајните реципиенти (клиентите), со цел постигнување и обезбедување на оптимално ниво на безбедност на сите нивоа и во сите домени.

368 Kempa, M., Stenning, P., Wood, J. (2004) Policing Communal Spaces: A Reconfiguration of the “Mass Private Property” Hypothesis. British Journal of Criminology.

ДЕФИНИЦИСКО-ПОИМЕН РЕЧНИК

- „Критичен субјект“ значи јавен или приватен субјект што е идентификуван.
- „Отпорност“ значи способност на критичниот ентитет да спречи, да заштити, да реагира, да се спротивстави, да ублажи, да апсорбира, да приспособува и да закрепнува од инцидент.
- „Критична инфраструктура“ значи средство, објект, опрема, мрежа или систем, или дел од средство, објект, опрема, мрежа или систем, што се неопходни за обезбедување суштинска услуга.
- „Суштинска услуга“ значи услуга што е од клучно значење за одржување на виталните општествени функции, економските активности, јавното здравје и безбедност или животната средина.
- „Инцидент“ значи настан што има потенцијал значително да го наруши, или што го нарушува обезбедувањето на суштинска услуга, вклучувајќи и кога тоа влијае на националните системи што го штитат владеењето на правото.
- „Заштита на критичната инфраструктура“ подразбира сет од мерки и активности од различна природа насочени кон одржување, унапредување и зачувување на карактерот и функционалноста на критичната инфраструктура со цел да се одвратат, да се ублажат и да се неутрализираат заканата, ризикот или ранливоста.
- „Ранливост“ е присуство на посебни карактеристики, специфики и околности на поединец, заедница, системи или објекти што ги прават подложни на негативните влијанија и оштетувачките ефекти на дадената опасност.

- „Опасност“ е природен феномен, човечка активност, техничко-технолошка хаварија или друг вид појава што може да предизвика: загуба на живот, повреди или други влијанија врз здравјето, имотна штета, загуба на средствата за егзистенција и услуги, општествено и економско нарушување, како и штета врз животната средина.
- „Несреќа“ – инцидент што е директно или индиректно предизвикана од човечки фактор, но се случува без планирање, на пример, како последица на ненамерно или погрешно човечко дејство, техничка неисправност или преоптоварување на системот (поврзано со безбедноста). Несреќата обично, иако не мора, има негативни последици, како што се: штета, повреда или загадување.
- „Напад“ – инцидент што е предизвикана од намерно дело (поврзано со безбедноста). За разлика од природен опасен настан или несреќа, нападот е планиран и извршен од одговорен антагонист (на пример, терорист, криминалец или сајбер-напаѓач) што дејствува во согласност со сопствените можности и во однос на одредена цел/ намера.
- „Ризик“ значи потенцијал за загуба или прекин предизвикан од инцидент и треба да се изрази како комбинација на големината на таквата загуба или нарушување и веројатноста за појава на инцидент.
- „Анализа на ризик“ се подразбира процес на разгледување на релевантни сценарија за закани, со цел да се процени ранливоста и потенцијалното влијание од нарушување или уништување на критичната инфраструктура.
- „Процена на ризик“ значи севкупен процес за одредување на природата и обемот на ризикот преку идентификување и анализа на потенцијалните релевантни закани, ранливости и опасности што би можеле да доведат до инцидент и преку проценка на потенцијалната загуба или нарушување на обезбедувањето суштинска услуга предизвикана со тој инцидент.

- Приватни безбедносни компании – регистрирани цивилни компании што се специјализирани во нудење договорни услуги од комерцијална природа на домашни и на странски клиенти со цел заштита на луѓето и на индустриските комплекси во рамките на донесените закони во државата во која таквите дејности се остваруваат. Пошироката дефиниција приватните безбедносни компании ги дефинира како јасно структурирана и хиерархиски точно определена регистрирана корпоративна асоцијација, што нуди услуги од безбедносна природа.
- Приватната безбедност се дефинира како профитно ориентирана индустрија што овозможува персонал, опрема и процедури за превенција на загуби предизвикани од човечка грешка, во-нредни ситуации, катастрофи или криминални акции.

БИБЛИОГРАФИЈА

1. Abrahamsen R., Leander A. (2015) *Routledge Handbook of Private Security Studies*. Routledge, Taylor & Francis Group London & New York.
2. Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state: private security in international politics*. Cambridge University Press.
3. Aitken, A. (2021). Community Perceptions of Private Security at a Mega-Event. *Security Journal*.
4. Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., & Walker, S. (2012). Building understanding of smart city initiatives. In *Electronic Government: 11th IFIP WG 8.5 International Conference, EGOV 2012, Kristiansand, Norway, September 3-6, 2012. Proceedings 11*. Springer Berlin Heidelberg.
5. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*.
6. Alexandra A., Baker D. P., Caparini M. (2009) *Private Military and Security Companies. Ethics, Policies and Civil-Military Relations*. 1st Edition. Routledge
7. Ambroso M. S. (2022) *Offshoring and Outsourcing Border Control: The EU's use of Private Military and Security Companies*. Robert Schuman Center.
8. Andersson, M. G et al. (2020). Communication inside Risk Assessment and Risk Management (COMRISK). *EFSA Supporting Publications*, 17(7).

9. Anwukah, O. J. (2022). *Legal conceptions of national security relevant to counter-terrorism and human rights law and policy*. Vandepas Publishing.
10. Argyroudis, S.A., et al. (2019). Fragility of transport assets exposed to multiple hazards: State-of-the-art review toward infrastructural resilience. *Reliability Engineering & System Safety*.
11. Ariel, B., Bland, M., & Sutherland, A. (2017). 'Lowering the threshold of effective deterrence'-Testing the effect of private security agents in public spaces on crime: A randomized controlled trial in a mass transit system. *PloS one*, 12.
12. Ashley K. (2014) *Security in a Globalized World. Understanding the Paradigm Shift of Contending Dynamics*. GRIN Verlag. Open Publishing GmbH
13. Avant, D. D., & Sigelman, L. (2006). *Globalization, private security, and democratic processes: implications for the democratic peace*. Research Group in International Security Groupe d'étude et de recherche sur la sécurité internationale.
14. Aven, T., et al (2018). *SRA glossary Risk Analysis: Fundamental Principles*.
15. Бакрески О. и Милошевска Т. (2022). Безбедноста на информациите и критичната инфраструктура, ДБКИ, Скопје.
16. Barroca, B., Serre, D. (2013). *Behind the barriers: a resilience conceptual model*. SAPI EN. S. Surveys and Perspectives Integrating Environment and Society 6.1
17. Barroca, B., Serre, D., Youssef, D. (2012). *Le concept de r'esilience 'al'epreuve du g'enie urbain*.
18. Benedict A. B. (2023) *Private Guards and National Security: Issues, Challenges and Opportunities/Prospects*. Author House, UK.
19. Berg, J. (2023). Private Security. *Obo in Criminology*. doi: 10.1093/obo/9780195396607-0329

20. Berger, T. B. (2015). Risk assessment competencies of risk management professionals (in Germany). *SSRN Electronic Journal*.
21. Bergin, A., William, D., & Dixon, C. (2018). Security Officers. In *Safety in numbers: Australia's private security guard force and counterterrorism*, Australian Strategic Policy Institute.
22. Bernard B. (2024) How Technology is Changing Private Security. *Private Security Conversations*. [article] Feb. 6th 2024.
23. Birkmann, J., et al. (2021). Regional clusters of vulnerability show the need for transboundary cooperation. *Environmental Research Letters*, 16(9).
24. Birta, L. G., & Arbez, G. (2007). *Modelling and simulation: Exploring dynamic system behaviour*. Springer.
25. Blackstone, E. A., Hakim, S., & Meehan, B. J. (2023). *Handbook on public and private security*. Springer.
26. Blackwell, J., et al. (2009). *An ontology-based approach to blind spot revelation in critical infrastructure protection planning*. In Setola, R., Geretshuber, S. (Eds.), *Critical information infrastructure security: Third international workshop, CRITIS 2008, Rome, Italy, October 13*, Springer, Berlin, Heidelberg.
27. Bloomfield, L. P. (1958). The U.N. and National Security. *Foreign Affairs*.
28. Boggero, M. (2018). *The Governance of Private Security*. Johns Hopkins University. Palgrave Macmillan.
29. Borghetti, F., Marchionni, G., Gugiatti, E., Ambrosi, C., Czerski, D., & Melzi, C. (2020). *Cross border critical infrastructure: A new approach for the protection evaluation*. Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference ESREL 2020 PSAM.

30. Born H., Caparini M., Cole E. (2007) *Regulating Private Security in Europe: Status and Prospects*. DCAF – №20.
31. Bossong, R. (2014). *The European programme for the protection of critical infrastructures–meta-governing a new security problem?* *European Security*, 23(2).
32. Brem, S. (2015). Critical Infrastructure Protection from a National Perspective. *European Journal of Risk Regulation*, 6(2).
33. Brown, G., et al. (2006). Defending critical infrastructure. *Interfaces (Providence)*..
34. Bruneau, M. et al. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake spectra* 19 (4).
35. Bureš, O. (2015). *Private security companies: transforming politics and security in the Czech Republic*. Palgrave Macmillan. <https://doi.org/10.1057/9781137477521>
36. Button, M. (2019) *Private policing*. 2d ed. London: Routledge. DOI: 10.4324/9781351240772
37. Buzatu, A. (2024) *Towards an international code of conduct for private security providers: a view from inside a multistakeholder process*. (2018). . Ubiquity Press.
38. Buzatu, A.M. and Buckland, B. (2010). *Private Military and Security Companies: Future Challenges in Security Governance*. Geneva: DCAF.
39. Candan, B. (2023). *Top 5 critical infrastructure cyberattacks*, Anapaya.
40. Cantelmi, R., Di Gravio, G., Patriarca, R., (2021). *Reviewing qualitative research approaches in the context of critical infrastructure resilience*, *Environment Systems and Decisions*. Springer US, достапно на: <https://doi.org/10.1007/s10669-020-09795-8>.

41. Cedergren, A., Lidell, K., & Lidell, K. (2019). Critical infrastructures and the tragedy of the commons dilemma: Implications from institutional restructuring on reliability and safety. *Journal of Contingencies and Crisis Management*, 27(4).
42. Chang, S. et al. (2014). Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments: Toward Disaster-Resilient Cities. *Risk Analysis*, 34(3).
43. Chapman, B., Gryz, J., Zombanakis, G. (2023). Introduction to Special Issue on Navigating NATO dynamics: Addressing various challenges in the international security environment. *Security and Defence Quarterly*, 44(4).
44. Chesterman, S., & Fisher, A. (2009). *Private security, public order: the outsourcing of public services and its limits*. Oxford University Press.
45. Christián L., Sotlar A. (2018) Private Security Regulation in Hungary and Slovenia – A Comparative Study Based on Legislation and Societal Foundations. *VARSTVOSLOVJE, Journal of Criminal Justice and Security*, year 20, no. 2.
46. Churchill, D., Janiewski, D., & Leloup, P. (eds.). (2020). *Private Security and the Modern State: Historical and Comparative Perspectives (1st ed.)*. Routledge.
47. Clark, R. (2019). *Securing eternity: ancient Egyptian tomb protection from prehistory to the pyramids*. The American University in Cairo Press.
48. Clarno A. (2017) *Neoliberal Apartheid*. The University of Chicago Press, Chicago, 2017.
49. Cockayne, J. and Mears, E.S. (2009). *Private Military and Security Companies: A Framework for Regulation*. New York: International Peace Institute.
50. Coleman, R., & McCahill, M. (2011). *Surveillance and crime*. SAGE.

51. Cook P. J. (2009) Crime Control in the City: A Research-Based Briefing on Public and Private Measures. Duke University and National Bureau of Economic Research. *Cityscape: A Journal of Policy Development and Research*, Volume 11, Number 1.
52. Cusumano E., Kinsey C. (2019) *Diplomatic Security. A Comparative Analysis*. Stanford University Press.
53. Cutter, S.L., Burton, C.G., Emrich, C.T., (2010). Disaster resilience indicators for benchmarking baseline conditions. *Journal of homeland security and emergency management* 7 (1).
54. Czop, A. (2017). Genesis, development and importance of private security companies in the provision of public safety in Poland. *Security and Defence Quarterly*, 17(4).
55. Dall'Asta G. (2024) The Impact of Private Security Companies Employed by INGOs on Humanitarian Operations. *Private Security Conversations*. IcoCA, достапно на: <https://blog.icola.ch/the-impact-of-private-security-companies-employed-by-ingos-on-humanitarian-operations/>
56. De Bruijne, M., & Van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management*, 15(1).
57. Deatherage, R. H. (2021). *Security operations: an introduction to planning and conducting private security details for high-risk areas* (Second edition). CRC Press.
58. Delgado G. V., Castro-Toledo F. J. (2020). Urban security and crime prevention in smart cities: a quantitative systematic review. *International E-Journal of Criminal Sciences*.
59. Deloitte. (2015). Smart Cities. How rapid advances in technology are reshaping our economy and society.
60. Deltares. (2023). *CIRCLE – Critical Infrastructures: Relations and Consequences for Life and Environment*, достапно

- на: <https://www.deltares.nl/en/software/circle-critical-infrastructuresrelations-and-consequences-for-life-and-environment-2/>
61. Demand for Private Security in Canada: Trends and Growth Factors. Security Guard Training Canada, достапно на: <https://www.securityguardtrainingcanada.ca/demand-for-private-security/>
 62. Doyle A., Lippert A., Lyon D. (2012) *Eyes Everywhere: The Global Growth of Camera Surveillance*. Routledge.
 63. Draper, H. (1978). *Private Police*. Brighton: Harvester.
 64. Drew P., McLaughlin R. (2020) Handbook on the Use of Force by Private Security Companies. United Nations, Vienna.
 65. Eski, Y. (2019) *Maritime security and piracy: Effects of armed guards on board*. Encyclopedia of Security and Emergency Management. Vrije Universiteit Amsterdam, Amsterdam, Netherlands.
 66. Espada, R. Jr., Apan, A., & McDougall, K. (2015). Vulnerability assessment and interdependency analysis of critical infrastructures for climate adaptation and flood mitigation. *International Journal of Disaster Resilience in the Built Environment*, 6(3).
 67. Eusgeld, I., Nan, C., & Dietz, S. (2011). “System-of-systems” approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6).
 68. Expert Group on Civilian Private Security Services Vienna, 12-14 October 2011
 69. Fairbrother, A. *et al.* (1995). Risk assessment in practice: Success and failure. *Human and Ecological Risk Assessment: An International Journal*, 1(4).
 70. Fennelly, L. J. (2004). *Handbook of loss prevention and crime prevention* (4th ed). Elsevier Butterworth Heinemann, достапно на: <http://site.ebrary.com/id/10180957>

71. Fischer, R. J., & Green. (1998). *Introduction to security* Robert J. Fischer, Gion Green (6th ed). Butterworth.
72. Forcht K., A., Kruck S., E. (2001) Physical Security Models, Philosophies and Context. *Journal of International Information Management. Volume 10, Issue 2*
73. Fritzson, Å., et al. (2007). Protecting Europe's critical infrastructures: Problems and prospects. *Journal of Contingencies and Crisis Management*, 15(1).
74. Galaby, A. A. R., & Abdrabo, A. A. (2021). *Handbook of research on creative cities and advanced models for knowledge-based urban development*. IGI Global, Engineering Science Reference.
75. George, B., Kimber, S. (2014). *The History of Private Security and Its Impact on the Modern Security Sector*. In: Gill, M. (eds) *The Handbook of Security*. Palgrave Macmillan, London.
76. George, R. Z., Rishikof, H., & Georgetown University Center for Security Studies. (2017). *The national security enterprise: navigating the labyrinth* (Center for peace and security (Washington, D.C.), Ed.; Second edition). Georgetown University Press.
77. Gerson, A., & Colletta, N. J. (n.d.). (2001) *Privatizing peace : from conflict to security*. Transnational Publishers.
78. Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection*. Part I: A state of the art. JRC Technical Notes, 1(1), 1–53
79. Gigerenzer, G., & Todd, P. M. (1999). *Simple heuristics that make us smart*. Oxford University Press.
80. Gill, J. C., & Malamud, B. D. (2014). Reviewing and visualizing the interactions of natural hazards: Interactions of Natural Hazards. *Reviews of Geophysics*, 52(4).
81. Gill, M. L. (2022). *The handbook of security* (Third edition). Palgrave Macmillan.

82. Global Market Trends. Securitas, достапно на: <https://www.securitas.com/en/about-us/global-market-trends/>
83. Goldman, J., & Maret, S. (2016). *Intelligence and information policy for national security key terms and concepts*. Rowman & Littlefield.
84. Good Progress on Tackling Hybrid Threats. *European Commission Press Release*, достапно на: [A_Europe_that_protects__good_progress_on_tackling_hybrid_threats.pdf](#).
85. Hakim, S., & Gaffney, M. A. (n.d.). *Private Guard Response to Alarm Activations*. US Department of Justice.
86. Hansen Löfstrand, C. (2021). The everyday reality of private security work in Sweden: negotiations at the front line of public order maintenance. *Policing and Society*, 34(1–2).
87. Heino, O. (2022). Intelligent terrorism as a security threat to critical infrastructure. *Security and Defence Quarterly*, 39(3).
88. Hermansson, H. (2012). *Defending the conception of “objective risk”*. *Risk Analysis: An International Journal*, 32(1).
89. Hilly, G., *et al.* (2018). Methodological Framework for Analysing Cascading Effects from Flood Events: The Case of Sukhumvit Area, Bangkok, Thailand. *Water*, 10(1), 81, достапно на: <https://doi.org/10.3390/w10010081>
90. Högselius, P., Hommels, A., Kaijser, A., & Van der Vleuten, E. (Eds). (2013). *The making of Europe’s critical infrastructure: Common connections and shared vulnerabilities*. Palgrave Macmillan, UK.
91. Hollnagel, E. (2014). *Resilience engineering and the built environment*. *Building Research & Information* 42 (2).
92. Homeland Security. (n.d.). *National infrastructure protection plan - risk management framework*, достапно на: https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf.
93. Hoppe, H. H. (2009) *The Private Production of Defense*. Ludwig von Mises Institute.

94. *Hybrid Conference: Critical Connections, Continuity and Supply – Assessing the Security of European Critical Infrastructure and Functions in a Hybrid Threat Context.*
95. Information Resources Management Association. (2018). *Censorship, surveillance, and privacy : concepts, methodologies, tools, and applications.* IGI Global.
96. Jaksa, J. (2023). *Security 101: an introduction to the private security industry* (Second edition). Carolina Academic Press.
97. Jean-Philippe Bérillon. (2023). *Cyber-Physical Security and Critical Infrastructure*, International Security League, CoESS.
98. Jha, A. K., Bloch, R., & Lamond, J. (2012). *Cities and Flooding: A Guide to Integrated Urban Flood Risk Management for the 21st Century.* The World Bank.
99. Johansson, J., et al. (2015). *Cascading Effects in Past Events – A Database Structured Around Originators and Dependencies* (Research Report Casceff Deliverable 2.3). Division of Risk Management and Societal Safety, Lund University.
100. Johansson, J., Hassel, H., & Svegrup, L. (2017). Capturing societal interdependencies from a flow perspective—Part I: Method and model. In *European Safety and Reliability Conference (ESREL 2016)*, CRC Press.
101. Jonathon G. (2024). Critical infrastructure protection in modern society, Industrial Cyber, достапно на: <https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/>
102. Jonathon G. (2024). Targeting critical infrastructure: recent incidents analyzed, *Industrial Cyber*.
103. Kaegi, M., Mock, R., & Kroger, W. (2009). Analyzing maintenance strategies by agentbased simulations: A feasibility study. *Reliability Engineering and System Safety*, достапно на: 94(9).
104. Kahneman, D., & Tversky, A. (1982). The psychology of preferences. *Scientific American*, 246(1).

105. Kateri C. (2010). *Private Security Contractors and New Wars*. Routledge: New York.
106. Katz, D. S. (2020). *Executive's guide to personal security*. Wiley & Sons Canada, Limited, John.
107. Kaunert, C., Wertman, O. (2020). The securitisation of hybrid warfare through practices within the Iran-Israel conflict - Israel's practices to securitize Hezbollah's Proxy War. *Security and Defence Quarterly*, 31(4).
108. Keir, H. (2013). *Bodyguard manual: for executive protection officers* (Edition 5)
109. Klaver, M., et al. (2008). *European risk assessment methodology for critical infrastructures*. 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), Rotterdam, Netrherlands: IEEE.
110. Kozłowski, T. P. (2024). Anti-terrorist cooperation as part of Poland's geopolitical shift. "Operation Bridge" and the rise of a strategic partnership with the United States. *Security and Defence Quarterly*.
111. Krahmann, E. (2010). *States, Citizens and the Privatisation of Security*. Cambridge: Cambridge University Press.
112. Latest News from Security Management. <https://www.asisonline.org/>
113. Lauge, A., Hernantes, J., & Sarriegi, J. M. (2015). Critical infrastructure dependencies: Aholistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, 8.
114. Lazari, A. (2014). *European critical infrastructure protection*. Springer International Publishing.
115. Lee A. (2023) *Private Security: Trends and Innovations*. AGS Inc.
116. Lee, S. Z. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology*, 14(1).

117. Lee, S.(. (2021). *Security: Private*. In: Shapiro, L.R., Maras, МН. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham.
118. Leveson, et al. (2017). *Engineering resilience into safety-critical systems*. In: Resilience engineering. CRC Press.
119. Li, H., et al. (2005). *Strategic Power Infrastructure Defense*, Proceedings of the IEEE.
120. Lindbom, H. et al. (2015). The capability concept - On how to define and describe capability in relation to risk, vulnerability and resilience. *Reliab. Eng. Syst. Saf.* 135.
121. Linnerooth-Bayer, J., & Sjostedt, G. (Eds.). (2010). *Transboundary risk management*. Routledge.
122. Lizzo S. (2024) Intelligence Redefined: The Interplay of Private Companies and National Security. *Journal of International Affairs*. Columbia University.
123. Luijff, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, 35.
124. Lyon, B. K., & Hollcroft, B. (2012). Risk Assessments. *Professional Safety*, 57(12).
125. Magunna, A. (2024). Charting waters: the private sector's evolving governance role in Southeast Asian maritime security. *Australian Journal of International Affairs*, 78(3), 306–325, достапно на: <https://doi.org/10.1080/10357718.2024.2337013>
126. Management System for Quality of Private Security Company Operations Standard (PSC.1, достапно на: <https://www.asisonline.org/publications--resources/standards--guidelines/management-system-for-quality-private-security-company-operations/>
127. Markolf, S. Et al. (2018). Interdependent infrastructure as linked social, ecological, and technological systems (SETs) to

- address lock-in and enhance resilience. *Earth's Future* 6 (12), 1638–1659
128. Martinage B. (2019) Security Guard Training Manual: 50-State. Volume 1 of The American Security Guard Series. Amazon Digital Services LLC - KDP Print US
129. Martinez, R. (2022). *Incident Response with Threat Intelligence : Practical Insights into Developing an Incident Response Capability Through Intelligence-Based Threat Hunting*. Packt Publishing.
130. Massoud, A. (2002). “Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)”. *Computer* (IEEE computer society).
131. May, P. J., & Koski, C. (2013). Addressing public risks: Extreme events and critical infrastructures. *Review of Policy Research*, 30(2).
132. McCrie, R. D. (2016). *Security operations management* (3rd ed.). Waltham: Butterworth-Hernemann.
133. Meehan, B., & Benson, B. L. (2017). Does private security affect crime?: a test using state regulations as instruments. *Applied Economics*, 49(48).
134. Meisam Gordan (2024). Protecting critical infrastructure against cascading effects: The PRECINCT approach, *Resilient Cities and Structures Volume 3, Issue 3*.
135. Mentges, A. et al. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, 96.
136. Meurant, G. (2014). *CCTV Surveillance: Video Practices and Technology*. Elsevier Science.
137. Michalski, D., Radomyski, A. (2019). Modern aspects of the development of security in air transport under the conditions of air terrorism. *Security and Defence Quarterly*, 26(4).

138. Mikac, R. (2024). *Protection of the EU's Critical Infrastructure: Evaluation of new legal instruments //* Critical Infrastructure Protection & Resilience News. London: The International Association of Critical Infrastructure Protection Professionals.
139. Min, H.-S. J., Beyeler, W., Brown, T., Son, Y. J., & Jones, A. T. (2007). Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions (Institute of Industrial Engineers)*, 39(1).
140. Miyazawa Koichi. (1995). *Crime prevention in the urban community*. Brill Nijhoff; Kluwer law and taxation publishers. <https://brill.com/view/title/10986>
141. Morabito A., Greenberg S. (2005) *Engaging the Private Sector To Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Office of Justice Programs. US Department of Justice.
142. Moteff, J., & Parfomak, P. (2004). *Critical infrastructure and key assets: Definition and identification*. Library of Congress Washington DC Congressional Research Service, достапно на: <http://www.dtic.mil/dtic/tr/fulltext/u2/a454016.pdf>
143. Mottahedi, A. et al. (2021). The resilience of critical infrastructure systems: a systematic literature review. *Energies* 14 (6).
144. Mousavi, S., & Gigerenzer, G. (2014). Risk, uncertainty, and heuristics. *Journal of Business Research*, 67(8).
145. Nalla M., Prenzler T. (2020) *Regulating the Security Industry. Global Perspectives. 1st Edition*. Routledge
146. Nalla, M. K., & Crichlow, V. J. (2017). Have the standards for private security guards become more stringent in the post-9/11 era? An assessment of security guard regulations in the U.S. from 1982 to 2010. *Security Journal*, 30(2).
147. Nan, C., Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety* 157.

148. National Academies of Sciences, Engineering, and Medicine. (1992). *Assessment of the U. S. Outer Continental Shelf Environmental Studies Program: III. Social and Economic Studies*. Washington, DC: The National Academies Press.
149. Nemeth C. (2023) *Private Security: An Introduction to Principles and Practice, Second Edition*. Routledge Taylor & Francis Group.
150. Nermin Oruc, Saima Raza, Danica Santic. (2020). Analytical Report: The Western Balkan Migration Route (2015-2019). Prague Process Secretariat.
151. OECD. (2011). *Future Global Shocks*. Organisation for Economic Co-operation and Development, достапно на: <http://www.oecd-ilibrary.org/content/book/9789264114586-en>
152. Ouyang, M., Dueñas-Osorio, L., Min, X., (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Struct. Saf.*
153. Oxford Dictionary. Private Security, достапно на: <https://dictionary.cambridge.org/dictionary/english/security>
154. Percy, S. (2006). *An Overview of the Industry and the Need for Regulation*. London: International Institute for Strategic Studies.
155. Percy, S. (2007). *Mercenaries: The History of a Norm in International Relations*. Oxford: Oxford University Press.
156. Pidgeon, N., & O’Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science*, 34(1–3).
157. Poljanšek, K., et al. (2019). *Recommendations for national risk assessment for disaster risk management in EU*. Publications Office of the European Union, Luxembourg, достапно на: <https://doi.org/10.2760/147842JRC11465>
158. Poorang, P., Eric R.P. Farr, Emmanuel Aboagye-Nimo, Janet Osei-Berchie Crime prevention in urban spaces through

- environmental design: A critical UK perspective, *Cities*, Volume 95.
159. Popovski, V. (2020). *Assessment Study of the Role of NDMAs in COVID 19 Crisis Response and Impact of Covid on NDMAs Operations*. UNDP/UNDRR.
 160. Popovski, V. (2022). *Guidance notes on building critical infrastructure resilience in Europe and Central Asia*. UNDP, достапно на: <https://tinyurl.com/3hm772n4>
 161. Popovski, V., et al. (2023). *Crisis prevention and critical infrastructure in Western Balkans*, Visegrad Fund, достапно на: <https://idscs.org.mk/en/2023/05/02/crisis-prevention-and-critical-infrastructure-in-western-balkans/>
 162. Pöyhönen, J. ; Nuojua, V. ; Lehto, M. & Rajamäki, J. (2019) Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. *Information & Security: An International Journal* 43:2.
 163. Prenzler, T., Sarre, R. (2023). *Public Space Crime Prevention Partnerships: Reviewing the Evidence*. In: Blackstone, E., Hakim, S., Meehan, B.J. (eds) *Handbook on Public and Private Security. Competitive Government: Public Private Partnerships*. Springer, Cham.
 164. Purpura, P. P., & Elsevier. (2013). *Security and loss prevention: an introduction* (Sixth edition). Elsevier
 165. Pursiainen, C., & Kytomaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1).
 166. Pursiainen, C., & Rød, B. (2021). National disaster risk assessments in Europe. How comparable are they and why? *Risk, Hazards & Crisis in Public Policy*, 12(2).
 167. Rajkovchevski, R. (2024). *EU vs NATO: Comparing Resilience in Civil Preparedness*, Crisis Lab, достапно на: <https://www.crisislab.io/blog/eu-vs-nato-comparing-resilience-in-civil-preparedness-with-rade-rajkovchevski>

168. Reid, S. G. (2000). Acceptable risk criteria. Progress in *Structural Engineering and Materials*, 2(2).
169. *Restitution in Theory and Practice* in Volume 12, Number 1 (1996) of the Journal of Libertarian Studies
170. Ribeiro, S.L., Bezerra, E.K., Nakamura, E.T., "Critical Infrastructure in Brazil", *1st IEEE International Workshop on Critical Infrastructure Protection*, 3-4th Nov 2005, Darmstadt, Nov 2005.
171. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6).
172. Roberson, C., & Birzer, M. L. (2010). *Introduction to private security : theory meets practice*. Prentice Hall.
173. Robert, B., H' emond, Y., (2012). Organizational resilience: A multidisciplinary sociotechnical challenge. *Resilience and urban risk management* 119–125
174. Rohrmann, B. (2000). *Cross-cultural studies on the perception and evaluation of hazards*. In: Renn, O., Rohrmann, B. (Eds.), *Cross-Cultural Risk Perception. Technology, Risk, and Society* (pp. 103–143). Springer, Boston, MA.
175. Ruddell, R., Thomas, M. O., & Patten, R. (2011). Examining the Roles of the Police and Private Security Officers in Urban Social Control. *International Journal of Police Science & Management*, 13(1), 54-69. <https://doi.org/10.1350/ijps.2011.13.1.210>
176. Sachs, M. (2022). *Reflections on executive order 13010*, достапно на: <https://mccrary.auburn.edu/work/insights/reflections-on-executive-order-13010>
177. Sage P. A. (1995). *Systems Engineering for Risk Management*, Norwel MA.
178. Sage-Passant, L. (2023). *The security intelligence services of the private sector*. Loughborough University. Thesis. <https://doi.org/10.26174/thesis.lboro.24050421.v1>

179. Schäferhoff, M., Campe, S., & Kaan, C. (2009). Transnational public-private partnerships in international relations: Making sense of concepts, research frameworks, and results. *International Studies Review*, 11(3).
180. Schildknecht, J., Dickey, R., Fink, M. D., & Ferris, L. (2018). *Operational law in international straits and current maritime security challenges*. Springer.
181. Schiller E., Aidoo A., Fuhrer J., Stahl J., Ziörjen M., Stiller B. (2022) Landscape of IoT security, *Computer Science Review*, Volume 44, 2022
182. Schneider, G. (2009). *Beyond the bodyguard: proven tactics and dynamic strategies for protective practices success*. Universal-Publishers.
183. Schreier, F. and Caparini, M. (2004). *Privatising Security*. Geneva: DCAF.
184. *Security operations: an introduction to planning and conducting private security details for high-risk areas* (Second). (2021). . CRC Press. July 12, 2024
185. Sena, L., Woldemichael, K. (2006). "Disaster Prevention and Preparedness", Lectures for Health Science Students, Jimma University.
186. Sennewald, C. A., & Christman, J. H. (2014). *Retail Crime, Security, and Loss Prevention: an Encyclopedic Reference*. Elsevier Science, достапно на: <http://qut.ebilib.com.au/patron/FullRecord.aspx?p=534927>
187. Serre, D., Heinzlef, C., (2018). Assessing and mapping urban resilience to floods with respect to cascading effects through critical infrastructure networks. *Int. J. Disaster Risk Reduct.* 30, 235–243, достапно на: <https://doi.org/10.1016/j.ijdr.2018.02.018>.
188. Setola, R., & Theocharidou, M. (2016). Modelling Dependencies Between Critical Infrastructures. In *Managing the Complexity of Critical Infrastructures*. Springer, Cham.

189. Shearing, C.D. and Johnston, L. (2013). *Governing Security: Explorations of Policing and Justice*. London: Routledge.
190. Siljander, R. P. (2008). *Introduction to Business and Industrial Security and Loss Control: a Primer for Business, Private Security, and Law Enforcement* (2nd ed). Charles C Thomas Publisher, LTD.
191. Skagerlund, K., Forsblad, M., Slovic, P., & Västfjäll, D. (2020). The affect heuristic and risk perception–stability across elicitation methods and individual cognitive abilities. *Frontiers in Psychology*, 11.
192. Slovic, P. (2020). Risk perception and risk analysis in a hyperpartisan and virtuously violent world. *Risk analysis*, 40(S1).
193. Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, 177(3).
194. Smith, C. F., Schmallegger, F., & Siegel, L. J. (2016). *Private security today* (First edition). Pearson Education.
195. Sofaer, A. D., & Goodman, S. E. (2001). *Cyber crime and security. The transnational dimension*. In A.D. Sofaer & S. E. Goodman (Eds), *The Transnational Dimension of Cyber Crime and Terrorism*, (pp. 1–34). Hoover Institution Press.
196. *South Africa: private security industry booming*. Africa, достапно на: /news <https://www.africanews.com/2024/01/05/south-africa-private-security-industry-booming/>
197. Stoddard A., Harmer A., DiDomenico V. (2008) *The use of private security providers and services in humanitarian operations*. Humanitarian Policy Group Overseas Development Institute 111 Westminster Bridge Road London
198. Strom, K., & RTI International. (2010). *The private security industry : a review of the definitions, available data sources, and paths moving forward :literature review and secondary data analysis*. RTI International.

199. Strom, K., Berzofsky M., Shook-Sa B., Barrick K., Daye C., Horstmann N., Kinsey S. (2010) *The Private Security Industry: A Review of the Definitions, Available Data Sources, and Paths Moving Forward*. RTI International, The Bureau of Justice Statistics (BJS)
200. Sterman, J.D. (2000). *"Business dynamics: systems thinking and modeling for a complex world"*. McGraw-Hill Education.
201. Sundahl, S. (2018). *Private Patrol Operator*. Lulu Com.
202. Sunstein, C. R. (2005). Precautions against what? the availability heuristic and cross-cultural risk perception. *SSRN Electronic Journal*.
203. Svegrup, L., Johansson, J., & Hassel, H. (2019). Integration of Critical Infrastructure and Societal Consequence Models: Impact on Swedish Power System Mitigation Decisions. *Risk Analysis*, 39(9).
204. Tamaro, A., et al. (2018). Characterization of the expected seismic damage for a critical infrastructure: The case of the oil pipeline in Friuli Venezia Giulia (NE Italy). *Bulletin of Earthquake Engineering*, 16(3).
205. Tang, J. (2019). *Assessment of Resilience in Complex Urban Systems*. In: Leal, F.W. et al. (Eds.), *Industry, Innovation and Infrastructure*. Encyclopedia of the UN Sustainable Development Goals. Springer, Cham, достапно на: https://doi.org/10.1007/978-3-319-71059-4_71-1.
206. *The Physical Protection of Critical Infrastructures and Key Assets*. The White House Washington, 2003.
207. *The Role of the Organization for Security and Co-operation in Europe (OSCE) in Security Sector Governance and Reform. Status and Prospects* (2013). Final Report. Geneva Centre for the Democratic Control of the Armed Forces.
208. The World Bank. (2022). *Western Balkans Face New Economic Headwinds Despite Strong Post-Pandemic Recovery* (Press-release), достапно на: <https://tinyurl.com/32e5hy5e>

209. Theocharidou, M., & Giannopoulos, G. (2015). *Risk assessment methodologies for critical infrastructure protection. Part II: A new approach*. Scientific and Technical Research Reports, Report EUR 27332 EN.
210. Toolkit for Security Sector Reporting: Media, Journalism and Security Sector Reform. 12. Private Security Companies. DCAF, 2021.
211. Toplak, M. E., West, R. F., & Stanovich, K. E. (2011). The cognitive reflection test as a predictor of performance on heuristics-and-biases tasks. *Memory & Cognition*, 39(7).
212. Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, 5(2).
213. *U.S Department of Homeland and Security*. (2022). Critical Infrastructure Security & Resilience Research (CISRR) Fact Sheet, достапно на: <https://www.dhs.gov/science-and-technology/publication/critical-infrastructure-security-resilience-research-fact-sheet>
214. U.S.-Canada Power System Outage Task Force. (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*.
215. UN's Use of PRMSC's in Peace Keeping Operations – Is There a Legal Basis? https://iapss.org/wp-content/uploads/2014/10/140_Volume-29.pdf
216. Van Asselt, M. B. A., & Renn, O. (2011). Risk governance. *Journal of Risk Research*, 14(4).
217. Andersen, T. J., Garvey, M., & Roggi, O. (2014). *Risk, Risk Management, and Risk Governance*, Oxford University Press.
218. Van der Vleuten, E., & Disco, C. (2004). Water wizards: Reshaping wet nature and society. *History and Technology*, 20(3).
219. Van der Vleuten, E., & Lagendijk, V. (2010). Interpreting transnational infrastructure vulnerability: European blackout

- and the historical dynamics of transnational electricity governance. *Energy Policy*, 38(4).
220. Van der Vleuten, E., & Lagendijk, V. (2010b). Transnational infrastructure vulnerability: The historical shaping of the 2006 European “blackout”. *Energy Policy*, 38(4).
221. Van Schaik, P., *et al.* (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, 90, 101651, достапно на: <https://doi.org/10.1016/j.cose.2019.101651>
222. Van Steden, R. and Sarre, R. (2007) The Growth of Private Security: Trends in the European Union. *Security Journal*, 2007(20).
223. Vaughan J. E. (1996). *Risk Management*, John Wiley & Ins Inc, New York.
224. Vaux T., Seiple C., Nakano, G., Van Brabant K. (2001) *Humanitarian Action and Private Security Companies*. International Alert
225. Vertovec, S. (1999). Conceiving and researching transnationalism. *Ethnic and Racial Studies*, 22(2).
226. Wakefield A. (2002) *The Public Surveillance Functions of Private Security*. Surveillance and Society.
227. Wakefield A. (2003) *Selling Security. The Private Policing of Public Space*. Routledge Taylor & Francis Group, London & New York.
228. Walby, K. and Joshua, C. (2021), “Community crime prevention and crime watch groups as online private policing”, *Safer Communities*, Vol. 20 No. 4, pp. 237-250. <https://doi.org/10.1108/SC-05-2021-0016>
229. Warren K., Thurlby R. (2012). “Understanding and Managing the Threat of Disruptive Events to the Critical National Infrastructure”, *Proceedings of the 30th International Conference of the System Dynamics Society*.
230. Webster, C. W. R. (2012). *Video surveillance : practices and policies in Europe*. IOS Press. <http://site.ebrary.com/id/10641757>

-
231. Welsh, B. C., Farrington, D. P., & Gowar, B. R. (2015). Benefit-cost analysis of crime prevention programs. *Crime and justice*, 44(1).
232. White, A. (2023) Critical workers? Private security, public perceptions and the Covid-19 pandemic. *Secur J* 36, 317–332, достапно на: <https://doi.org/10.1057/s41284-022-00339-0>
233. White, N. D., & Henderson, C. (2013). *Research handbook on international conflict and security law: jus ad bellum, jus in bello and jus post bellum*. Edward Elgar Pub. Ltd.
234. Williams B. (2022) *Private Security: An Effective Method to Prevent Being a Crime Victim*. Mises Institute. Austrian Economics, Freedom and Peace.
235. Williams, D. (2018) *The Role of Private Security in Counter Terrorism*. Security Solutions, достапно на: <https://www.securitysolutionsmedia.com/2018/12/10/role-private-security-counter-terrorism/> [27.07.2024]
236. Williams, K. (. L. I. C. (2017). *Criminology*. Oxford University Press.
237. Wiśniewski, R. (2018). Notion of strategic national security management. *Security and Defence Quarterly*, 20(3).
238. Wright R. (2024) *Surge in maritime violence boosts demand for private security forces*. [article] April 21st 2024 <https://www.ft.com/content/5175a8b4-41cc-4b60-913f-dc6f2f68307d>
239. Yang, Z. *et al.* (2022). Resilience Indicator of Urban Transport Infrastructure. A Review on Current Approaches. *Infrastructures* 7, достапно на: <https://doi.org/10.3390/infrastructures7030033>.
240. Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, 39(10), 6100–6119, достапно на: <https://doi.org/10.1016/j.enpol.2011.07.010>
241. Zanella, A., Bui, N., Castellani, A.P., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 1, 22–32.

242. Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 152.
243. Бакрески О., Ѓуровски М., Барџиева М., Ј. (2021) *Јавна и приватна безбедност – координација и соработка*. Комора на РСМ за приватно обезбедување.
244. Бакрески О., Триван Д. и Митевски С., (2012). *Корпоративски безбедносен систем*, Комора на Република Македонија за обезбедување на лица и имот, Скопје.

ИНТЕРНЕТ ИЗВОРИ

1. America's Cyber Defense Agency (2024). National Coordinator for critical infrastructure security and resilience, достапно на: <https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience>
2. Analysis of top 11 cyber attacks on critical infrastructure, 2021, достапно на: <https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/>
3. Armed Forces (DCAF) Policy Paper – №20, достапно на: https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf
4. ASIS International 2023 Annual Report, достапно на: <https://www.asisonline.org/>
5. AXIS Communications. Improving security and business performance. For a smarter, safer world, достапно на: <https://www.axis.com/about-axis>
6. Bangkok Regional Hub United Nations <https://hrdd-assessment.org/public-or-private-security-forces-are-not-bound-by-rules-of-engagement-or-standard-operating-procedures/>

7. Border Management. OSCE, достапно на: <https://www.osce.org/border-management>
8. Bretschneider, Wolfgang; Freytag, Andreas; Rieckmann, Johannes; Stuchtey, Tim (2022) State or private security supply? An analysis from the institutional economics perspective. Jena Economic Research Papers, No. 2022-009, Friedrich Schiller University Jena, Faculty of Economics and Business Administration, Jena
9. Cambridge on-line Dictionary. (2021). Transnational, достапно на: <https://dictionary.cambridge.org/dictionary/english/transnational>
10. CIPedia. (2020), достапно на: [https://websites.fraunhofer.de/CIPedia/index.php/Critical _ Infrastructure](https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure).
11. Commitments, Policies and Standards. Health, Security, Safety, the Environment (HSSE) and Social Performance (SP), достапно на: <https://www.shell.com/sustainability/our-approach/commitments-policies-and-standards.html>
12. Contemporary Threats to National and International Security, and Appropriate Security Measures. Slovenija in NATO, достапно на: <http://nato.gov.si/eng/topic/threats-to-security/>
13. CORDIS. (2011). European Risk Assessment and Contingency Planning Methodologies for Interconnected energy networks (EURACOM), достапно на: [https:// cordis.europa.eu/article/id/89833-increasing-the-securityof-europes-energy-supply](https://cordis.europa.eu/article/id/89833-increasing-the-securityof-europes-energy-supply)
14. CORDIS-IMPROVER Project. (2016). Report on Current Approaches for Defining, Evaluating and Implementing Resilience Concepts in Critical Infrastructure, достапно на: [https://cordis.europa. eu/project/id/653390/results](https://cordis.europa.eu/project/id/653390/results).
15. CORDIS-Smart Resilience Indicators for Smart Critical Infrastructures. (2018). Resilience indicators for SCIs based on big and open data. <https://cordis.europa.eu/project/id/700621/results>. Eurostat. (2014). Getting messages across using indicators - A

16. Crime, Justice and the Law. Security Industry Authority,
достапно на: <https://www.gov.uk/browse/justice>
17. Critical Infrastructure Protection Process. (2021). Homeland Security, ndFigure 2. ISO 31,000 risk management process, Pursiainen and Rød 368 M. PAPAMICHAEL ET AL.
18. Customary IHL. Rule 108. Mercenaries. International Committee of the Red Cross, Geneva, достапно на: <https://ihl-databases.icrc.org/en/customary-ihl/v1>
19. ENISA. (2021). European Union Agency for Cybersecurity, достапно на: <https://www.enisa.europa.eu/>
20. Eser A. (2024) Global Private Security Industry Statistics: \$257 Billion Market Projection. WORLDMETRICS.ORG REPORT 2024, достапно на: <https://worldmetrics.org/private-security-industry-statistics/>
21. EUR-Lex. (2010), достапно на: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum%3A33259>, 2010.
22. European Commission. (2016)), достапно на: <https://erncip-project.jrc.ec.europa.eu/events/vitex-2016-was-first-eu-wide-exercisefocussed-effects-large-scale-failure-critical>
23. European Commission. (2020). Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Final report. Publications Office, достапно на: <https://data.europa.eu/doi/10.2837/864404>
24. European Commission. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L333, 164–197.
25. European Commission. (2022). Opening remarks by commissioner Johansson at the press conference on EU critical infrastructure resilience, достапно на: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_6265

26. European Council. (2008). Directive 2008/114 - Identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
27. Eurostat (2014). Getting messages across using indicators - A handbook based on experiences from assessing Sustainable Development Indicators, доступно на: <https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-gq-12-001>
28. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. (2022). United Nations Development Programme, United Nations Plaza New York, 10017, USA, доступно на: file:///C:/Users/User/Downloads/UNDP_Guidance%20notes_v4.pdf
29. Handbook Based on Experiences from Assessing Sustainable Development Indicators, доступно на: <https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-gq-12-001>, 2014
30. Information Sharing. A Vital Resource. Cyber Security and Infrastructure Security Agency CISA, доступно на: <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/information-sharing-vital-resource>
31. International Code of Conduct for Private Security Service Providers, Swiss Confederation, November 10, 2010; доступно на: https://www.icoca.ch/sites/default/files/resources/ICoC_English.pdf
32. International Security Ligue. Critical Infrastructure), доступно на: <https://www.international-security-ligue.org/>
33. Interpreting Heat Signatures. Firefighter Nation, доступно на: <https://www.firefighternation.com/training/interpreting-heat-signatures/#gref>
34. IRGC. (2006). White paper on risk governance: Towards an integrative approach. Geneva: International Risk Governance Council.

35. IRGC. (2018). Guidelines for the Governance of Systemic Risks. Geneva: International Risk Governance Council.
36. https://international-review.icrc.org/articles/commentary-part-i-montreux-document-pertinent-international-legal-obligations-and-good?utm_term=&utm_campaign=gu_DSA_GSN_EN_traffic_Alle+Seiten_AOK_2023&utm_source=adwords&utm_medium=ppc&hsa_acc
37. <http://www.voa.mod.gov.rs/documents/national-security-strategy-of-the-republic-of-serbia.pdf>
38. NATO: The Revolution of Military Affairs – IWS. [online], достапно на: www.iwar.org.uk/rma/resources/NATO.
39. NATO-Private Sector Dialogues focus on NATO 2030 initiative, достапно на: https://www.nato.int/cps/en/natohq/news_184601.htm
40. PMSC's and the UN. Global Policy Forum, достапно на: <https://www.globalpolicy.org/pmscs/50225-pmscs-a-the-un.html>
41. Private Military and Security Companies Newsletter Latest Issue: June 2024. RAND National Security Research Division.
42. Private Sector Partners. Interpol, достапно на: <https://www.interpol.int/en/Our-partners/Private-sector-partners>
43. Private Security | Definition. Criminal Justice Glossary. International University for Applied Science, 2023.
44. Private Security Industry Act 2001, достапно на: <https://www.legislation.gov.uk/ukpga/2001/12/contents>
45. Private Security Market Research 2032. Allied Market Research, достапно на: <https://www.alliedmarketresearch.com/private-security-market-A06346>
46. Private Security Today. (n.d.). Pearson Higher Education US. достапно на: <https://app.kortext.com/borrow/1855587>
47. Public or private security forces are not bound by rules of engagement or standard operating procedures. UNDP Business and Human Rights in Asia

48. Public-private partnerships INTERPOL, достапно на: <https://www.interpol.int/en/Crimes/Cybercrime/Public-private-partnerships>
49. Report of the Task Force on Private Security. National Advisory Committee on Criminal Justice Standards and Goals. Washington 1976, достапно на: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/private-security-report-task-force-private-security>
50. Report on the role of private military and security companies in immigration and border management and the impact on the protection of the rights of all migrants. Working Group on the use of mercenaries. 09 July 2020, достапно на: <https://www.ohchr.org/en/calls-for-input/report-role-private-military-and-security-companies-immigration-and-border>
51. Report Summary. Security 2025. A Roadmap for the Future. Australian Security Industry Association Limited, достапно на: https://asial.com.au/common/Uploaded%20files/ASIAL_Public/Security%202025%20Summary.pdf
52. Republic of Slovenia Private Security, достапно на: <https://www.gov.si/en/topics/zasebno-varovanje/>
53. European Commission - Directorate-General for Humanitarian Aid and Civil Protection (DG ECH), достапно на: https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/prevention-and-preparedness-projects-civil-protection/overview-past-track-i-and-track-ii-projects/resilience-critical-infrastructure-protection-europe-recipe_en
54. Resolution 18/2 Civilian private security services: their role, oversight and contribution to crime prevention and community safety. The Commission on Crime Prevention and Criminal Justice. United Nations Office on Drugs and Crime, достапно на: https://www.unodc.org/documents/justice-and-prison-reform/Expert-group-meeting-Bangkok/Resolution_18_2.pdf
55. Security for smart and safe cities, including for public spaces. CORDIS - EU research results. European Commission,

- достапно на: https://cordis.europa.eu/programme/id/H2020_SU-INFRA02-2019
56. Security Industry Authority annual report and accounts 2022 to 2023, достапно на: https://assets.publishing.service.gov.uk/media/64c3bcc57aea5b00126a8e28/sia_annual_report_22-23.pdf
 57. Security Industry Authority, достапно на: <https://www.gov.uk/government/organisations/security-industry-authority/about>
 58. SIA Security industry; authorization to issue regulations, достапно на: <https://dejure.org/gesetze/GewO/34a.html>
 59. SITA Border Control, достапно на: <https://www.sita.aero/>
 60. Smart Cities and the Role of Defense [online] достапно на: <https://www.defenceturkey.com/tr/icerik/smart-cities-and-the-role-of-defense-2475>
 61. Smith, R. (2013) Supply and Demand: the Paradox of Private Security Companies in Libya. Open Democracy, достапно на: <https://www.opendemocracy.net/en/supply-and-demand-paradox-of-private-security-companies-in-libya/>
 62. The Business of War – Growing risks from Private Military Companies. Council of the European Union. General Secretariat. 31 August 2023
 63. The establishment of the Metropolitan Police. 2024 BBC, достапно на: <https://www.bbc.co.uk/bitesize/guides/z9f4srd/revision/4>
 64. The Montreux Document on Private Military and Security Companies, достапно на: <https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies>
 65. The Role of Private Security in Today's Society. Security Guarding 12 February 2024, достапно на: <https://theconstellation-group.com/role-of-private-security/>
 66. U rad puštena 41 nova lokacija sustava za rano otkrivanje požara [article] Zaštita 17.08.2024, достапно на: <https://zastita.info/>

- hr/novosti/u-cakovcu-postavljaju-kamere-za-nadzor-ilegalnog-odlaganja-otpada,35803.html
67. United Nations Office for the Coordination of Humanitarian Affairs (OCHA), достапно на: <https://www.unocha.org/>
68. US Congress. (2021). Public law 107-56 uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, достапно на: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>
69. US Election Assistance Commission. (2017). History of critical Infrastructure designation, достапно на: <https://www.eac.gov/ci-scoop-history-of-criticalinfrastructure-designation>
70. Westminster Security, достапно на: <https://www.westminstersecurity.co.uk/>
71. Бела книга за приватното обезбедување. Комора на РСМ за приватно обезбедување. Скопје, 2019, достапно на: <https://obezbeduvanje.org.mk/>
72. Божаниќ Д. (2011) Комплексноста на енергетската зависност – главната детерминанта за енергетската безбедност на Србија. Стратегии за регионална енергетска безбедност. Политичка мисла. Година 9, број 36, декември Скопје 2011, достапно на: https://www.kas.de/c/document_library/get_file?uuid=61754713-688c-8c49-612d-416fe75a2943&groupId=252038
73. Водич за вршење видео надзор. “Поддршка во спроведувањето на модернизираниот правна рамка за заштита на личните податоци“, финансиран од Европската Унија, достапно на: <chrome-extension://efaidnbmnnnibpcapjpcglclefindmkaj/https://azlp.mk/wp-content/uploads/2024/01/%D0%92%D0%BE%D0%B4%D0%B8%D1%87-%D0%B7%D0%B0-%D0%B2%D1%80%D1%88%D0%B5%D1%9A%D0%B5-%D0%BD%D0%B0-%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE%D0%BD%D0%B0%D0%B4%D0%B7%D0%BE%D1%80-3.pdf>

74. Електронски систем за јавни набавки. Огласи за воспоставување јавно приватно партнерство како концесија за јавни работи и јавни услуги, достапно на: <https://e-nabavki.gov.mk/PublicAccess/home.aspx#/concession-announcements>
75. Јавно приватни партнерства во Република Северна Македонија. Основен извештај за тековната рамка за ЈПП. The World Bank. IBRD IDA, достапно на: [https://economy.gov.mk/Upload/Editor_Upload/JPP/fatmire/PPP%20Diagnosti%20report%20ofinal%20MK\(1\).pdf](https://economy.gov.mk/Upload/Editor_Upload/JPP/fatmire/PPP%20Diagnosti%20report%20ofinal%20MK(1).pdf)
76. Кои се најголемите производители на камери за надзор во 2024 година? 17 јули 2024 [online], достапно на: <https://www.icseecam.com/mk/who-are-the-largest-surveillance-camera-manufacturers-in-2024/>
77. Комора на Република Северна Македонија за приватно обезбедување, достапно на: <https://obezbeduvanje.org.mk/licenca/>
78. МДН Обезбедување, достапно на: <https://mdn.com.mk/uslugi/>
79. МИНИСТЕРСТВО ЗА ВНАТРЕШНИ РАБОТИ. Скопје, декември 2020 година), достапно на: <https://mvr.gov.mk/>
80. ОСА обезбедување, достапно на: <https://osa.com.mk/?services=fizicko-obezbeduvanje>
81. Приватна и јавна безбедност, преку заедничко делување против секаков вид на криминал. 26/10/2017, достапно на: <https://tv21.tv/mk/privatna-i-javna-bezbednost-preku-zae/>
82. Тендери, неважечки пасоши и фиктивни фактури. Радио Слободна Европа јануари 19, 2024, достапно на: <https://www.slobodnaevropa.mk/a/tenderi-nevazhechki-pasoshi-i-fiktivni-fakturi/32781024.html>

ЗАКОНИ, ПОДЗАКОНСКИ АКТИ И ДРУГИ ПРАВНИ ПРОПИСИ

1. Directive (EU) 2022/2557 of European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
2. ISO (2021), ISO 22300:2021-Security and resilience-Vocabulary, достапно на: <https://www.iso.org/fr/standard/77008.html>.
3. Law on Private Security ("The Official Gazette of RS", No. 104/2013)
4. UNEP. (2022). Regional Strategy For Climate-resilient Road Infrastructure. ADC/UNEP, достапно на: <https://tinyurl.com/ys3j98er>
5. United Nations General Assembly. 72nd Plenary Meeting. A/RES/44/34. December 4th 1989.
6. United Nations. (2020). UN Common Guidance On Helping Build Resilient Societies 48.
7. Закон за внатрешни работи. Министерство за внатрешни работи. Република Северна Македонија. Скопје, април, 2022.
8. Закон за концесии и јавно приватно партнерство („Службен весник на Република Македонија“ бр. 6/12, 144/14, 33/15, 104/15 и 215/15 и „Службен весник на Република Северна Македонија“ бр.153/19, 261/19, 89/22 и 65/23).
9. Закон за приватно обезбедување (неофицијален пречистен текст). Министерство за внатрешни работи на Република Македонија. („Службен весник на Република Македонија“

бр. 166/12), Закон за изменување и дополнување на Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 164/13), Закон за изменување и дополнување на Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 148/15), Закон за изменување и дополнување на Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 193/15) и Законот за изменување и дополнување на Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 55/16), достапно на: <https://mvt.gov.mk/zakon/3> (посетена на 26.03.2019)

10. Институт за стандардизација на Република Северна Македонија, достапно на: <https://isrsm.gov.mk/mk/project/show/iso:proj:88403>
11. Предлог-закон за критична инфраструктура, Скопје 2022 година, достапно на: <https://mod.gov.mk/storage/2022/12/predlog-Zakon-za-krivicna-infrastruktura.pdf>
12. Примена на Законот за приватно обезбедување и неговото влијание во Р. Македонија, достапно на: <https://obezbeduvanje.org.mk/wp-content/uploads/2020/12/Zakon-za-privatno-obezbeduvanje-precisten-tekst-dek-2013.pdf>

