РЕПУБЛИКА С. МАКЕДОНИЈА
УНИВЕРЗИТЕТ "СВ.КИРИЛ И МЕТОДИЈ" СКОПЈЕ
ФИЛОЗОФСКИ ФАКУЛТЕТ
ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР
студиска програма: Корпоративна безбедност и безбедносен менаџмент
насока-Безбедносни менаџмент

Магистерски труд

МЕСТОТО И УЛОГАТА НА ПРИВАТНАТА БЕЗБЕДНОСТ ВО ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Изработил:
Марио Милески
Бр. Инд. 5113/18

Ментор
Проф.д-р Оливер Бакрески

Декември, 2020
Скопје

СОДРЖИНА

ГЛАВА IV

ЗАКАНИ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

ГЛАВА V

ПРИВАТНИОТ БЕЗБЕДНОСЕН СЕКТОР И ЈАВНАТА БЕЗБЕДНОСТ ВО ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО РС МАКЕДОНИЈА

ГЛАВА VI

ПРИВАТНАТА БЕЗБЕДНОСТ ВО ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА-РЕЗУЛТАТИ ОД СПРОВЕДЕНО ИСТРАЖУВАЊЕ

ГЛАВА I
МЕТОДОЛОШКА РАМКА

1.Вовед

Критичната инфраструктура е конструкт од системи, мрежи и објекти кои се толку витални, што нивната континуирана оперативност е неопходна за осигурување на безбедноста на нацијата, за нејзината економија, како и за јавното здравје и безбедност. Критичната инфраструктура може да се каже дека е слична во сите држави поради нејзината функција на обезбедување на базичните потреби за функционирање, но категоризацијата и одредувањето на објектите варира во зависност од тоа какви приоритети и потреби има самата држава.[1]

Во основа, критичната инфраструктура како витална, комплексна и меѓусебно структурно поврзана целина е од исклучителна важност и значење за непреченото функционирање на државата. Таа е јасна дијалектика и синергија што ги поврзува индустрискиот сектор, комуникациските системи, енергетскиот сектор и другите сектори, системи и мрежи што се од големо значење за државата бидејќи со неа се обезбедува потребната стабилност. Оттука нарушувањето или прекинот на работата на одредени сектори/системи може да доведе до сериозни последици што може да имаат и ослабувачки ефект на безбедноста на државата, на националната економија, на економскиот развој и просперитет, на стабилниот енергетски сектор, односно нарушувањето или прекинот на работата на само еден од наведените сектори може да доведе до сериозни последици врз другите критични сектори.[2]

Организирање на соодветна заштита на критична инфраструктура во денешни услови претставува предуслов односно претпоставка за заштита на други пошироки општествени вредности, не само на национално туку и на регионално и глобално ниво. Во овој контекст заштитата на критичната инфраструкутра, како воопштен збир на вредности и добра кои се од суштествено значење за економијата, државата и општеството и чие нарушување во функционирањето или уништувањето може да создаде долгорочни штетни

[1] Critical Infrastructure. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx, посетена на 12/12/2019.
[2] Бакрески О., Милошевска Т., Алчески Ѓ., *Заштита на критична инфраструктура*, Комора на РМ за приватно обезбедување, Скопје, 2017.

последици по основните вредности на општеството претставува императив за националните интереси.

Оттука е од суштинско значење да се истакне меѓусебната хетерогена поврзаност и зависност поради регионалната или глобалната природа и значење на безбедноста на критичната инфраструкутра. Имено, било каков напад, инцидент илии загрозување на општествено витален објект со сигурност ќе резултира со прекугранични домино ефекти. Како соодветен пример може да се истакне прекинот на висок напон на електрична мрежа во Германија во 2006година која предизвика масовен прекин на електрична енергија во Франција и Италија но истовремено и во делови на Шпанија, Португалија, Холандија,Белгија и Австрија проширувајќи се до Мароко, при што беа погодени повеќе од 10 милиони потрошувачи на енергија. Но ова е само еден пример зошто е значајно да се разбере макро сцената и генералната состојба пред се во европски рамки. Денес Европската Унија е соочено со бројни предизвици вооподнос на заштита на политиката на критичната инфраструктура. Во изминатите 10тина години европската комисија има усвоено неколку иницијативи, директиви и повеќе комуникации во правец на подобрување на безбедноста на критичната инфраструкутра, па така во 2004та година Европскиот совет иницира изработка на глобална стратегија за заштита на критична инфраструктура, како резултат на што на 29.10.2014 година Европската комисија усвојува документ така наречен Комуникација на заштита на критична инфраструктура во борба портив тероризмот, која опфаќа пред се инциденти на критична инфраструкутра предизвикани од терористички напади. Во декември 2006та година е предложена Европска порграма за заштита на критична инфраструкутра (EPCIP) која опфаќа т.н All Hazards approach. Со која се истакнува дека при заштита на критична инфраструктура треба да се имаат во предввид закани од секаков вид загрозување (човечки, технолошкии природни загрозувања) но сепак , заканата од тероризам го задржува својот приоритет. Во декември 2008 година е донесена Директива на ЕУ за идентификација и означување на европска критична инфраструкутра и проценка на потребата за унапредување на нејзина заштита(Directive 2008/114/EC). Оваа директива има за цел да воспостави и

одпочне постака за идентификација на определување на европска критична инфраструктура и заеднички пристап за проценка на потребите за подобрување на нејзина заштита.

Истражувањето кое е предвидено за потребите на магистерскиот труд има за цел да расветли одредени аспекти на заштита на критичната инфраструктура, а особено централното прашање се однесува на Приватниот безбедносен сектор и неговата улога во заштита на критичната инфраструктура. Имајќи предвид фактот дека критичната инфраструктура е под парманентна закана, тоа придонесува за јакнење на свеста на секој поединец, организација или други субјекти е да преземат одговорност за заштита на критичната инфраструктура, а секако значајна улога му припаѓа на приватната безбедност. Поради тоа, во овој домен кога станува збор за местото и улогата на приватната безбедност во општата безбедност треба да се потенцира дека карактеристична област на дејствување на приватната безбедност е токму дејствувањето во областа на обезбедување на лица и имот, фирми и компании и сл.[3] Исто така, денес приватната безбедност е одговорна не само за заштита на многу од институциите на нацијата и на системите на критична инфраструктура, туку е насочена и кон заштита на интелектуалната сопственост и чувствителните корпоративни информации.[4] Оттука нема дилема дека се забележува голема тенденција во однос на зголемување на дејноста на приватната безбедност.

Оттука, теоретската елаборација на магистерскиот труд треба да даде одговори и на следните прашања:

- Што е критична инфраструктура? Нормалниот одоговор вклучува објекти и услуги кои се витални за базичните операции на одредено општество. Секторите кои се сметаат за критична инфраструктура варираат во секоја држава, но најчесто ги опфаќаат: енергетскиот сектор, секторот за

[3] Тимова, Т., *Приватната безбедносна индустрија во Европската Унија со посебен осврт на СР Германија*, Универзитет „Св. Кирил и Методиј“, Филозофски Факултет – Скопје, Скопје, 2015, стр. 31.

[4] Kevin Strom, PhD; Marcus Berzofsky, MS; Bonnie Shook-Sa, MAS; Kelle Barrick, PhD; Crystal Daye, MPA; Nicole Horstmann, BS;Susan Kinsey, BS., The Private Security Industry: A Review of the Definitions, Available Data Sources and Paths Moving Forward, Department of Justice, December 2010, стр. 1-1.

управување со води, прехранбен сектор, транспортен сектор, телекомуникациите, здравството, банкарството и финансиите итн.[5]

- Каков пристап гради државата во заштита на критичната инфраструктура;
- Дали има правна основа за заштита на критичната инфраструктура;
- Каква е улогата на безбедносните актери во кои преовладува безбедносната компонента како природен елемент на безбедносната структура;
- Каква е улогата на приватната безбедност во заштита на критичната инфраструктура,
- Дали приватниот безбедносен сектор има капацитети да одговори на променливата природа на ризици и закани со кои се соочува критичната инфраструктура;
- Каква е соработката на безбедносните субјекти во заштита инфраструктурните објекти,
- Како може населението да се подготви за крах или дефект на критичната инфраструктура?

2. Предмет на истражувањето

Основен предмет на ова истражување е фокусиран на местото и улогата на приватниот безбедносен сектор во обезбедување и заштита на критична ифраструктура. Со цел прецизно да се одреди предметот на истражување во овој труд ќе се направи подетално истражување за функционирањето на приватниот безбедносен сектор во заштита на критична инфраструктура.

Заштитата на критичната инфраструкутра е круцијална и многу значајна тема речиси подеднакво за сите компоненти за безбедносниот сектор и секако главен предизвик на секоја држава и во секое општество. Концептот критична инфраструктура претставува феномен кој стана особено актуелен во изминатите

[5] Critical National Infrastructure. CPNI. https://www.cpni.gov.uk/critical-national-infrastructure-0 посетена на 15/12/2019.

години како централна тема за анализа и дискусија и во академската и експертската заедница. Неодминливо е да се споменат стравичните напади од 13 ноември во Париз, драматичните епизоди од 11 септември во Њу Јорк, 4 експлодирани бомби во возовите во Мадрид, координираните самоубиствени напади на 3 станици на подземната железница и еден автобус во Лондон во 2005 и други вакви немили настани кој ја повлекуваат потребата за сеопфатана национална но и интернационална кординирана политика за заштита на критичната инфраструкутра. Неоспорно е дека безбедноста на критичната инфраструкутра е витална за националните индустријализирани економии, а тука спаѓаат субјектите односно системите во секторите, енергетика (гас, нафта, струја), снабдување со вода, телекомуникации финансискиот сервис, транспортот,здравството итн.

Организирање на соодветна заштита на критична инфраструктура во денешни услови претставува предуслов односно претпоставка за заштита на други поширок општествени вредности, не само на национално туку и на регионално и глобално ниво. Во овој контекст заштитата на критичната инфраструкутра, како воопштен збир на вредности и добра кои се од суштествено значење за економијата, државата и општеството и чие нарушување во функционирањето или уништувањето може да создаде долгорочни штетни последици по основните вредности на општеството претставува императив за националните интереси.

Директивата е ограничувачка односно се применува само за енергетскиот сектор и секторот за транспорт исто времено предвидува сопствениците и операторите на критична инфрастрктура да подготват безбедносни планови и да определат лиценцирани офицери за безбедност. Понатаму во 2012 година, Европската конфедерација за приватно обезведување CoESS како матична организација и ги штити интересите на сите вршители на дејност приватно обезбедување на ниво на ЕУ, изготвува така наречена бела книга, насловена како Заштита и обезбедување на критична инфраструкутра (CoESS –White Paper, Critical infrastructure security and protection – The public private opportunity).

Иако документот е наменет пред се за стимулирање на дебата за оваа витална тема, која што последователно ќе доведе до координирани активности помеѓу јавниот и приватниот безбедносен сектор во правец на подобрување на заштита на критична инфраструктура, истиот првенствено разликува два основни термини:

1. Обезбедување –како превземање меркии активности во правец на редуцирање на можности, од криминални и терористички акции и нивно влијание,

2. „Еластичност“, „Подготвеност“ или „Способност” да се издржат или да се опораваат од намерни или природни загрозувања над објектите кои спаѓаат во критична инфраструкутра.

Истовремено, недвосмислено се укажува на потребата и важноста од јасно препозанвање од страна на државата дека обезбедување на критична инфраструктура е комплексна проблематика, која опфаќа приватни, јавни и во некои случаи и така наречени хибридни субјекти поради што од суштинско значење е експлицитна поделба на улогите и одговорносите. И што е најважно се истакнува потребата за воведување на стандарди за порценка на ризик кои може да се изработат врз основа на добри практики а заради примена на соодветно ниво на безбедност во секоја критична инфраструктура.

Во Јуни 2012 година, Еврпоската комисија излегува со работен документ за ревизија на европската програма за зашита на критична инфраструктура кој што утврдува План за подобрување на заштита на критична инфраструкутра за сите членки на ЕУ и во сите релевантни сектори на економска активност. Оваа програма произлегува како резултат на редовна размена на информации помеѓу сите членки на ЕУ и во оваа фаза не ограничува само на закана од тероризам туку вклучува и криминални активносити, природни катастрофи и други закани односно во оваа фаза тенденцијата е да се утврдат сите видови на опасности во сите сектори. Дополнително во август 2013 година Европската комисија формулира документ со нов пристап кон порграмата за заштита на критична инфраструкутра со тенденција таа да биде уште побезбедна, Документот во оваа фаза се базира на практични примени на активности од типот на превенција, подготвеност и реакција.

Дополнително се акцентира и детално се обработува меѓусебаната поврзаност на критична инфраструкутра со матичната индустрија и секако со државните институции .

Истовремено се истакнуваат последиците кои поради напад, инцидент или загрозување може да настанат кај поширок спектар на субјекти во различни инфраструктури а со оглед на прекуграничната димензија, се истакнува можноста таквите последици да се рефлектираат далеку пошироко. И не помалку значајно во делот на заштита на критичната инфраструктура во Европа е развиениот портал на Европската комисија – информативна мрежа која предупредува критична инфраструкутра (CIWIN) и преку која се обезбедува систем на размена на идеи, студии и добри практики за заштита на критична инфраструктура на ниво на ЕУ.

Сите овие активности, креирани поректи имаат за цел подготовка и зголемување на ниво на превенција, управување со кризии, заштита на граѓаните и критичните точки од терористички и други закани. Сепак клучната цел е да се обезбеди стручно знаење и научна основа за подобро разбирање и меѓузависностите на сите нивоа при обезбедување на критична инфраструкутра. Од друга страна Европската комисија сеуште е во постапка за изработка на координирана политика на земјите членки на ЕУ во однос на проблематиката за обезбедување на критичната инфраструктура и сеуште се истакнува значителниот недостаток на соработка помеѓу националните влади и институциите на ЕУ, во постапување на координирана итна реакција на потенцијалните закани. Со други зборови при услови на зголемен степен на ризик сеуште недостасува соодветен одговор од институциите на ЕУ, со цел да се подобри ефикасноста на системот на спречување од заштита на природни или вештачки катастрофи. И сеуште се чуствува нагласената проблематика пред се поради фактот што земјите членки на ЕУ секоја поединечно се на различно ниво на зрелост во однос на ефективната политика за обезбедување на критична инфрастркутра. Па оттука и потешкотијата за остварување на севкупен концепт на операции на ниво на ЕУ. Сепак недвосмислена е заложбата да се дејствува во насока на поддршка на земјите членки на национално, регионално и локално ниво, во превенирање на ризикот и

подготовка на кадрите за цивилна заштита во случај на природни или вештачки катастрофи во унијата. Промоција на брза и ефикасна оперативна соработка во рамките на унијата, меѓународните служби за цивилна заштита и следење на практиктие и технологиите да се одговори на постојаното менување на природата на заканите и промените на животна средина со цел да се обезбеди максимална заштита на критична инфраструктура на ЕУ.

Намалување на ранливоста на критичната инфраструктура и зголемувањето на отпорноста или издржливоста при инциденти од различен карактер е приоритет кој може да се обезбеди преку организирање на заштита на соодветни нивоа и максимално ограничување на штетните ефекти и последици од повреди на граѓаните и општеството.

Во правец на исполнување на горенаведените цели и ефикасна заштита на критична инфраструктура неспорна е потребата од креирање на политики за обезбедување на критична инфрастркутура кои ќе опфатат една глобална визија за безбедноста, стратегија и цврста политичка определба за постигнување на зададените цели, а аргументите кои треба да придонесат за развој и утврдување на правилни политики за обезбедување на критична инфраструктура се:

- дефинирање на стандарди, темелна проценка на ризик, идентификација на клучни субјекти итн.
- едукација и тренинг со двоен таргет, да се надоплнат недостатоците кај веќе инвловираните во процесот на заштита на критична инфрастркутра и да се подигне свеста за значењето на безбедноста на критичната инфраструктура.
- иницирање и промоција на истражувања и развој за континуиран напредок од технички аспект во однос на нови иновативни решенија.
- и конечно размена на информации заради максимална подготвеност за итна реакција, координација, подобрување на капацитетите итн.

Сублимирано националната критична инфраструкутра во Европска Унија покажува дека европската индикатива листа на сектори на критична инфраструкутра утврдена во 2005та година, дадена во Green Paper за европска програма за заштита на критична инфрасткрутра се содржи од 37 подсектори во

САД истата опфаќа 16 сектори, во Германија 9, во Велика Британија и во Хрватска по 10 сектори.

Меѓутоа она што е сигнификантно е фактот дека приватното обезбедување токму преку критичната инфраструкутра е инволвирано во обезбедување на влади и владини објекти, одбранбено – индустриски бази, телекомуникации, транспорт, банкарство, енергетика, брани и водоснабудвање, здравство, земјоделие, медиуми и други сфери на живеење и работа.

Критичната инфраструкутра во Република Северна Македонија е област која што сеуште не е законски регулирана, но сепак постојат одредени подзаконски акти коишто ја нагласуваат ваквата идентификација и ја препознаваат оваа област или заштита на критична инфраструкутра. Овде треба да се нагласи проблематиакта на задолжително обезбедување која е препознаена во глава 4, член 25 во првиот закон за обезбедување на имот донесен во 1999 година (Службен весник на РМ бр.80/99,66/07,51/11). Имено во овој член е децидно пропишано дека „Владата определува кој правни лица се должни да имаат обезбедување на лица и имот за свои потреби, ако вршењето на нивната дејност е поврзана со ракување на радиоактивни материи или другии опасни материи за луѓето и околината; со предмети и објекти од историско и културно значење; како и во други случаи кога тоа е во интерес на обезбедност односно одбраната“. Секако дека и законското решение од 2012 година со донесување со законот за приватно обезбедување содржински ги следи овие суштински определби па содржинкси издвојува глава 5 за уредување на задолжително приватно обезбедување. Дополнително прави и интервенција со определување дека приватното обезбедување може да се организира за сопствени потреби или остава можност да се склучи договор за услуги.

Од се претходно кажано јасно е дека приватната безбедност денеска е присутна во голем дел од животот и бизнисот во сите држави во светот вклучувајќи ја и нашата држава. Постојат бројни примери кои потврдуваат дека приватната безбедност како дејност со себе носи широк дијазапон и опсег на активнсоти во општественото живеење и тоа како дејност ја прави комплексна и разновидна.

Во Република Северна Македонија во системот на националната безбедност улогата на приватното обезбедување најнепосредно се препозанва токму преку обезбедување на критичната инфраструктура. Тематиката за обезбедување и заштита на критична инфраструктура во Република Северна Македонија се третира преку определени истражувања, пишана стручна литература, прирачници итн. во обид да се задоволи минимум безбедноста и да се нагласи примарно безбедносната компонента. Истовремено се прави и обид да се направи потребен баланс за воспоставување на адекватен амбиент за сите субјекти во процесот, и јавниот и приватниот безбедносен сектор со што ќе се обезбедат предуслови за квалитетен напредок и кохерентност на сите сегменти инволвирани во заштитата на критичната инфраструкутра притоа истите да не бидат зансовани сегментарно парцијални решенија туку да се засноваат на специфични знаења и континуирана инвестиција со цел воспоставвување превентивни механизми кои заеднички ќе дејствуваат. И конечно за да може сето тоа да се оствари недвосмислено се препозанва потребата од воспоставување на ефикасна стратегија за заштита на критична инфраструкутра и воспоставување на соодветна регулатива.

Предметното одредување на овој магистерски труд подразбира и дефинирање на појмовно-категоријален апарат. Во ова истражувањето ќе преовладуваат следните поими: безбедност, безбедносен сектор, приватна безбедност, концепт на критична инфраструктура, инфраструктура, критична инфраструктура, безбедност на критична инфраструктура.

Безбедноста се дефинира како „правно уредување и обезбедување на општествените односи и унапредување на состојбата во државата, што овозможува ефективна заштитеност на државата и на граѓаните кои во неа живеат од сите (надворешни и внатрешни) противправни акти (активности) со кои се загрозува уставниот поредок, суверенитетот, независноста и територијалниот интегритет на државата, работата на државните органи, извршување на стопанските и општествените дејности и остварување на слободата, правата и должностите на човекот и граѓанинот.“[6]

[6] Miletiћ S., *Policijsko pravo*, Policijska akademija, Beograd, 1997.

Безбедносниот сектор ги опфаќа сите оние државни институции, кои имаат формален мандат да ја осигураат безбедноста на државата и нејзините граѓани против актите на насилство и принуда, како што се: вооружените сили, полицијата, жандармеријата и паравоените сили, разузнавачките и тајните служби, граничните и царинските служби, како и судските и казнените институции.[7]

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.[8]

Концептот критична инфраструктура стана актуелен за државите со високоразвиена технологија во транспортот, енергетиката, телекомуникациите, медицината и др., кои успеа да развијат мултидисциплинарен и интегрален метод на организациско и технолошко ниво што ќе управува со овој витален систем.[9]

Инфраструктурата претставува основна физичка и организациска структура што му е потребна на едно општество, животна средина, организација или институција непречено да функционира во сопствени рамки.[10]

Критичната инфраструктура претставува значаен сегмент во заштитата на основните столбови на човековото дејствување и живот. Критичната инфраструктура претставува средство или систем, кој суштински придонесува за одржување на виталните општествени функции.[11]

---

[7] Бакрески О.,Контрола на безбедносниот сектор, Филозофски факултет, Скопје, 2008

[8] http://www.cops.usdoj.gov/Default.asp?Item=2034

[9] Homeland Security. Critical Infrastructure Security: http://www.dhs.gov/topic/critical-infrastructure-security, посетена на 4/11/2015.

[10] Moteff J., Parfomak P., *Critical Infrastructure and Key Assets: Definition and Identification, Congresional Research Service* - The Library of Congress, 2004, стр. 5.

[11] Kravcov, A., *et al*. Durability of Critical Infrastructure, Monitoring and Testing: Proceedings of the ICDCF 2016. Springer Nature Singapore, 2017, преземена од: https://books.google.mk/books?id=1f6qDQAAQBAJ&pg=PA249&dq=critical+infrastructure, посетена на 13/12/2019.

3. *Цели на истражувањето*

Врз основа на сложеноста на истражувачкиот проект која се темели на претпоставките како да се обезбеди ефикасна заштита на критичната инфраструктура мора да се води сметка и за детална процена на факторите кои ја условуваат соодветната заштита од приватното обезбедување и што доведува до до загрозување на критичната инфраструктура.

Оттука, **научната цел** на истражувањето ќе биде да се согледа каква е улогата на приватното обезбедување во заштита на критичната инфраструктура.

Со оглед на општата цел, **посебни цели** на истражувањето ќе бидат насочени кон:

- *да се согледа какво е местото и улогата на приватното обезбедување во поширокиот општествен контекст,*
- *да се согледа како се идентификува критичната инфраструктура во македонската држава,*
- *да се види каков е пристапот на државата во заштита на критичната инфраструктура,*
- *да се согледа каква е улогата на приватното обезбедување во заштита на критичната инфраструктура,*
- *да се види дали соодветната регулатива за приватно обезбедување ја нуди потребната рамка за превенција и заштита е доволна основа за заштита на критичната инфраструктура,*
- *да се согледа дали приватното обезбедување може да одгвоори адекватно на промените, состојбите и на се поголемата изложеност на објектите од критичната инфраструктура на ризици,*
- *да согледа дали има конзинстентност во надлежностите на одделните органи и тела кои се надлежни за обезбедување на потребната заштита;*
- *да се види дали постои координираност меѓу полицијата и приватното обезбедување во заштита на критичната инфраструктура во сфери каде имаат заеднички придонес;*

- *да се согледа нивото и степенот на загрозенот на критичната инфраструктура,.*
- *да се види каква е моменталната заштита на критичната инфраструктура во Р.Македонија.*
- *врз основа на добиените сознанија треба да се одреди местото и улогата на приватниот безбедносен сектор и на другите безбедносни актери во рамките на еден практичен модел на ефикасна заштита на критичната инфраструктура.*

4.Хипотетичка рамка

Врз основа на општиот пристап на проблемот на истражување и врз основа на поставените цели на истражување ќе ја поставиме следнава **општа или генерална хипотеза**: Заштитата на критичната инфраструктура е условена од постоење на мултиваријантен пристап кој треба да го обедини целокупниот потенцијал за да се обезбеди акдекватна заштита, а приватното обезбедување ја има приоритетната задача заедно со операторите во приватна сопственост да обезбеди непречено работење и функционирање на критичните инфраструктури.

Покрај општата хипотеза ги поставуваме и следните **посебни хипотези**:

- Приватниот безбедносен сектор има капацитети да одговори на променливата природа на ризици и закани со кои се соочува критичната инфраструктура, но сето тоа е условено од постоењето на адекватна законска рамка за заштита на критичната инфраструктура.
- Ефикасноста и функционалноста на приватниот безбедносен сектор ќе биде подобра доколку надлежностите кои треба да се пропишат во новата рамка за заштита на критичната инфраструктура се изведени од еден во друг пропис, односно се конзистентни еден со друг пропис.
- Правилно спроведени пропишани норми пропишани во соодветните акти, влијаат на ефикасност на безбедносниот сектор и придонесуваат на соодветна заштита на критичната инфраструктура;

- Улогата на приватните безбедносни актери во заштита на критичната инфраструктура зависи во голема мера од променетата природа на заканите.
- Соработката на приватното обезбедување со полицијата и со операторите на критичната инфраструктура е важна претпостака за рационално и ефикасно решавање на проблемите во заштита на критичната инфраструктура;
- Примена на соодветен модел за заштита на критичната инфраструктура во голема мера ќе ја обезбеди адекватна заштита на инфраструктурата.

5.Методи на истражувањето

Со ова истражување ќе се направи обид да се утврди местото и улогата на приватниот безбедносен сектор во заштита на критична инфраструктурана национално и меѓународно ниво.

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

1. ***експликативен карактер -*** теориско истражување ќе се заснива на согледување на причинско-последичните односи кои ги детерминираат меѓузависностите и односите меѓу приватните безбедносни актери и нивната ефикасност во заштита на критичната инфраструктура.
2. ***дескриптивен карактер -*** целта е да направи поширока елаборација на сотојбите во сферата на заштитата на критичната инфраструктура и соодветна експликација на состојбите во сферата на приватното обезбедување.
3. ***структурален карактер –*** подразбира да се согледаат појавите и законитостите преку меѓусебно влијание кое ја детерминира структуралната позиција на субјектите.

За ова истражување ќе бидат применети повеќе методи на истражување и тоа: анализа на содржина, компаративен метод, историски метод, метод на иднукција и дедукција.

Анализа на содржината ќе најде соодветна примена во анализа и синтеза на бројни извори на литература (домашни и странски), анализа на законски документи и акти за регулирање во национални и во светски рамки. Анализата на релевантите извори треба да ја даде целосната слика за состојбите и за добивање соодветни заклучоци кои ќе помогнат во подобро разбирање на оваа област.

Компаративен метод ќе најде широка примена особено во компарирање на податоци и информации од релевантната литаратура за да се споредат состојбите во нашата држава со други држави.

Историски метод ќе се користи за да се направи историска ретроспектива на поставеноста и развојот на приватната безбедност од минатото па до сега. Целта на овој метод е да овозможи користење на искуствата од минатото во сегашноста и подобрување на состојбите.

Методот на индукција и дедукција ќе се применува за донесување на конкретни заклучоци за тоа кој приспап и модел е најоодветен за конкретна примена.

Во рамките на истражувањето покрај методите ќе бидат применети и одредени инструменти. Ова истражување ќе се примени претходно изготвен прашалник со претходно изготвени 9 прашања кои ќе бидат дистрибуирани до извршителите на дејност приватно обезбедување на РСМ. Прашалникот ќе биде изработен со онлајн алатката SurveyMonkey.

ГЛАВА II
ПРИВАТНА БЕЗБЕДНОСТ

1.Општо за приватна безбедност

Постојат различни теоретски размислувања што укажуваат на растечката доминација на приватната безбедност. Почетоците на приватната безбедност датираат уште од праисторијата, од самиот развој на човекот, од тој миг кога група луѓе се заштитувале себеси и своите фамилии од напади на диви sверови и диверзантски непријатели. Исто како и развојот на човештвото во сиот свет, така и приватната безбедност ја добила својата форма и облик во локалната област. Во одреден број земји таа се состоела од група поединци, на приватни лица, на истражители со единствена цел заштита на себе и на другите. По извесен период, приватната безбедност зазема големи размери, со што ја начнува потребата од единствено означување на своите припадници, преку групна униформа, платен работен труд и организирана поставеност. Токму овие елементи укажуваат на тоа дека приватната безбедност е многу стар поим, што со текот на времето еволуира во најзначајна гранка на безбедноста. Се издвојува како посебен ентитет, со посебна и сериозна организациона стуктура, со врвни нивоа на раководење и умешност во извршување на конкретни и сложени проблематики.[12]

Приватното обезбедување и приватната безбедност кажано на класичен егзактен начин може да се разбере преку следниот пример. Ако слетате на Хитроу (Heathrow) аеродромот во Велика Британија, вработени лица од приватна компанија за обезбедување се овластени со законот да го отворат вашиот багаж и да ве претресат. Доколку допловите до одредени британски пристаништа, можеби ќе видите дека ги обезбедуваат приватни компании. Преживувајќи го тоа, ако патот ве води со воз до Лондон, ќе бидете надгледувани од Британската транспортна полиција која е еден вид хибридно тело што не е ниту јавно ниту приватно. Кога ќе излезете на улиците и дали барем единствено тогаш влегувате под јурисдикцијата на она што мислите дека е вистинската полиција. Потоа, ако влезете во некоја канцеларија или фабрика, или ако можеби пазарувате во некој трговски центар, ќе видите дека јавниот ред е заштитен не од полицијата туку од

[12] Dempsey Johan S., Introduction to Private Security (second edition), USA, 2011, стр.2, преземено од Бакрески, О. и др. Безбедноста низ призмата на приватната безбедност, Комора на Република Македонија за приватно обезбедување, Скопје, 2018, стр. 153-154.

вработени од приватна фирма кои се платени од (и се одговорни пред) дуќанџиите или менаџерите. Како што можеби ќе изгледа изненадувачки, ако маршрутата ве донесе до, да речеме, станица за нуклеарна енергија, воен гарнизон или пак владина канцеларија, тие исто така ќе бидат чувани од приватни фирми за обезбедување. На крај, ако го прекршите законот и се најдете во рацете на случаен обичен полицаец, кога ќе влезете во полициската станица, ќе откриете дека првата личност што ќе ја сретнете на бирото најверојатно нема да личи на полициски офицер туку на цивил. Самата станица ќе биде чувана, најверојатно, од приватна компанија, како што е и случајот со многу судови и некои затвори.[13]

2.*Дефинирање на приватната безбедност*

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, зборот приватна безбедност е употребуван во широк контекст и токму оваа поширока употреба создава потешкотии околу обидите за негово дефинирање.[14]

Анализирајќи ја достапната литература во оваа сфера, се наидува на заклучок дека не постои консензус за тоа што претставува приватна безбедност и има различни дефиниции кои биле користени во претходни истражувања. Разликите во дефинирањето имаат тенденција да се позиционираат и да го

[13] Policing for Profit: Welcome to the New World of Private Security, *The Economist* (April 19, 1997), стр. 20–24, во Dempsey S.John, *Introduction to Private Security*, Wadsworth, Cengage Learning, 2011, стр. 31-32, преземено од Бакрески О., и др., Приватна безбедност-теорија и концепт, Комора на РМ за приватно обезбедување, Скопје, 2015 стр. 49.

[14] Бакрески О., Даничиќ М., Кешетовиќ Ж., и Митевски С., Приватна безбедност-теорија и концепт, Комора на РМ за приватно обезбедување, Скопје, 2015 стр. 58-59.

насочуваат својот фокус на работните задачи, влијанието на профитот и клиентот, вклучително и крајниот резултат, како што се производство, дистрибуцијата и инсталацијата на опрема и технологија, итн.[15]

Според дефиницијата на американското министерство за правда, приватната безбедност ги вклучува оние самостојно вработени и приватно финансирани деловни субјекти и организации кои обезбедуваат услуги поврзани со безбедноста на одредена клиентела за одреден надомест, самостојно или за поединец или субјект што ги најмува или вработува, со цел да ги штитат своите лица, приватен имот или интереси од разни опасности.

Уште во 70-те години на XX век, Извештајот на корпорацијата RAND ја дефинираше приватната безбедност во една широка рамка како сите видови приватни организации и поединци кои обезбедуваат секаков вид на услуги поврзани со безбедноста, вклучувајќи истрага, стража, патрола, откривање измами, тревога и вооружен пренос.[16]

Понатаму, приватната безбедност е дефинирана како оние поединци, организации и услуги различни од јавните агенции за спроведување на законот, кои се занимаваат првенствено со спречување на криминал, загуба или штета за одредени поединци, организации или установи.[17]

Приватните безбедносни компании се присутни во животот на секој граѓанин: тие спроведуваат контроли на аеродромите и концертните сали, ја обезбедуваат критичната инфраструктура, ги чуваат трговските центри и приватниот имот. Приватната безбедност, исто така наречена и приватна полиција, приватна армија, итн., е дефинирана како оние лица кои се вработени или спонзорирани од трговско претпријатие на основа на договор или на база на директно доделен договор, користејќи јавни или приватни фондови, за

[15] Klopfer, F., van Amstel, N. (2015) A Force for Good? Mapping the Private Security Landscape in South East Europe. Geneva Centre for the Democratic Control of Armed Forces. https://www.researchgate.net/publication/282657912_A_Force_for_Good_Mapping_the_private_security_landscape_in_Southeast_Europe/citations (посетена на 11.11.2020)
[16] Wildhorn, S. (1971) Issues in Private Security. RAND Corporation. https://www.rand.org/pubs/papers/P5422.html (посетена на 09.11.2020)
[17] Cunningham *et al.*, (1990) The Private Security Industry: A Review of the Definitions, Available Data Sources, and Paths Moving Forward. U.S. Department of Justice Report, 2010. https://www.ncjrs.gov/pdffiles1/bjs/grants/232781.pdf (посетена на 12.1.2020)

извршување задачи каде што главната компонента е обезбедување или регулаторна функција.[18]

Според најновите дефиниции за приватна безбедност, таа е определена и значи професионализам и повеќе од што било друго, го означува најсуштинскиот елемент, што се однесува на безбедносната култура.[19]

За Џонстон, приватната безбедност се однесува на заштита на физичката сопственост, на средствата и на поединците од кражба или од насилство. Во нивните анализи оваа заштита подразбира примена на физичко/механички уреди, електрични/електронски уреди и екипажни услуги.[20]

Во констатацијата на Драјпер стои дека приватната безбедност се фокусира на надзори на врата, безбедносни консултантски услуги и производство, дистрибуција и инсталирање безбедносна опрема.[21]

Приватната безбедност најлесно може да се објасни како делегиран орган во безбедносниот сектор, кој инаку претставува ексклузивен домен и монопол на политичките структури на државата или државната заедница и како таква е во рацете на поединец или поединци, во согласност со законските решенија и овластувања што ги дава државата, односно според Гил и Харт, приватниот безбедносен сектор е еден од најголемите трговски друштва и зафаќа широко подрачје на комерцијалната дејност. Во тие рамки тој вклучува производство и монтажа на безбедносна опрема, надзор, патролни и транспортни услуги на пари, како и разни видови консултантскиуслуги врзани за заштитата и ризикот.[22]

Батон и Џорџ сметаат дека дел од функциите може да бидат идентификувани врз основа на поврзување на приватните безбедносни услуги и производи.

---

[18] Kakalik, S., J., Wildhorn, S. (1971) The Private Police Industry: Its Nature and Extent. RAND Corporation Report. https://www.rand.org/pubs/reports/R0870.html (посетена на 10.11.2020)
[19] CoESS Position Paper on the Evaluation of Council Directive 2008/114. Commission Staff Working Document, 2019, стр. 308.
[20] Johnston, L. (1999) Private Policing in Context, *Britain`s Security Industry*, London, Jordan and Sons.
[21] Draper H., *Private Police*, Sussex: Harvester Press, 1978.
[22] Gill M., Hart J. (2003) Način poboljšanja korporacijske zaštite korištenjem privatnih istražitelja, prijevod u: Izbor članaka iz stranih časopisa, Ministarstvo unutarnjih poslova RH, broj 1-2.

Тие вклучуваат превенција од криминалот, одржување на редот, превенција од загуба и заштита – иако овие не се чести или есклузивни за сите приватно-безбедносни производи и услуги.[23]

Почетната точка за анализа е обемот во кој една или повеќе од овие функции го карактеризира производот или услугата, односно колку повеќе функции го карактеризираат – толку појасно може да биде виден како дел од приватната безбедносна индустрија или колку повеќе овие функции карактеризираат производ или услуга – толку посилно е тврдењето дека се дел од приватната безбедност.[24]

Според Бакрески, приватната безбедност е насочена кон остварувањето на поставените цели и задачи кои во голема мера се детерминирани од повеќе фактори, и тоа: од ресурсите со кои располага овој сектор, од оспособеноста на персоналот, од нивото на техничка и материјална опременост, од пристапот во вршење на предвидените задачи, од големината на агенцијата за обезбедување, од мотивираноста на вработените, од политичкиот и безбедносниот амбиент во државата, од законските рамки со кои се регулира оваа материја, од услугите кои што ги нудат пред физичките и правните лица, од прифатеноста, односно неприфатеноста на корисниците на услуги, од перцепцијата што ја создаваат граѓаните за самите агенции, од одговорноста на тие што го вршат обезбедувањето, од соработката и комуникацијата што треба да се остварува со полицијата, од карактерот и барањата што клиентите ги упатуваат до агенциите за обезбедување итн. [25]

Од изнесените дефиниции и пристапи може да се заклучи дека приватната безбедност не се поврзува само со неможноста на слабите држави ефикасно да го пополнат безбедносниот вакум. Туку, таа е етаблиран сегмент и во развиените држави каде се повеќе е застапен приватниот персонал за безбедност.

[23] George, B., Button, M. (2000) Private Security Vol. 1. Palgrave Macmillan, New York. https://www.palgrave.com/gp/book/9781899287703 (посетена на 22.11.2020)
[24] Button M., (2002) *Private Policing*, Routledge, London & New York p. 10.
[25] Бакрески О., Безбедносни системи, Филозофски факултет, Скопје, 2018, стр.440-501.

3. Хронолошка генеза на приватната безбедност

Од самиот почеток на историјата на земјата, луѓето настојувале да се заштитат од опасностите и заканите. Безбедноста и сигурноста се сметаат за основни потреби, кои се рангирани веднаш по физиолошките потреби, како што е истакнато од Абрахам Маслов во неговата хиерархија на потреби.[26]

Подоцна, низ историскиот развој, преку низа еволутивни фази на општествено организирање, се создаваат градовите, а заедниците се заштитуваат со физички бариери или со организирање заштита на луѓето, најнапред приватно, а потоа и јавно. Во интерес на историските и социо-економските факти, приватната безбедност отсекогаш играла важна улога во заштитата на граѓаните и деловните субјекти од криминал. Всушност, разбирањето на јавната безбедност како државен монопол е прилично скорешен и имено датира од XIX-от век. Но оттогаш, приватната безбедност станува (повторно) важен чинител во заштитата на средствата, луѓето и инфраструктурата. Во поново време, отпечатокот на приватната безбедност се проширува бидејќи има доделени нови мисии од или во партнерство со јавните агенции за спроведување на законот.[27]

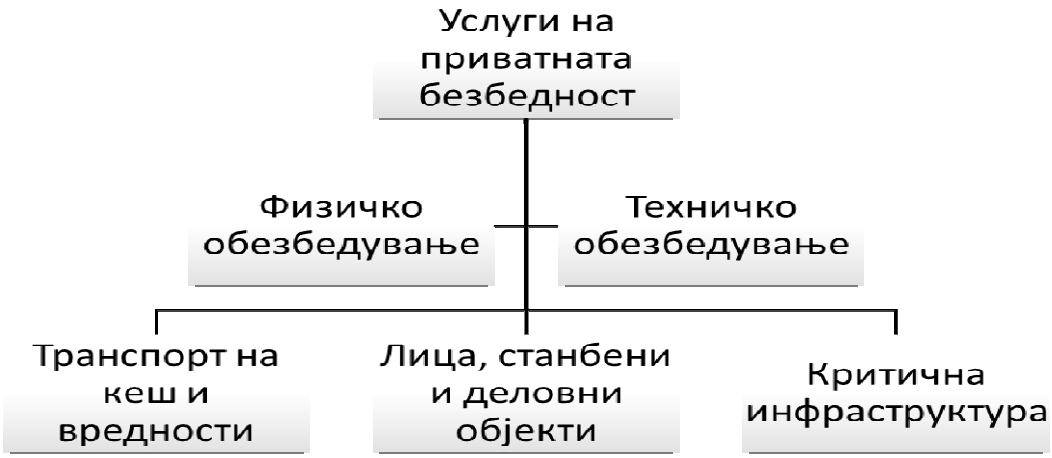
Во денешно време, човештвото сè повеќе ја бара најдобрата комбинација на луѓе и технологии за заштита на средствата, инфраструктурата и што е уште поважно, луѓето, без разлика дали тие се дома, на работа или на јавни простори.[28] Така што, следната граница за приватна безбедност без сомнение ќе има врска со вештачката интелигенција, мета податоците и предвидливата заштита, интернет на нештата и други појави што сè уште не се воведени, а ќе станат дел од концептот за *зголемена безбедност*.[29]

---

[26] Selva, J. (2020) Abraham Maslow, His Theory and Contribution to Psychology. Positive Psichology. https://positivepsychology.com/abraham-maslow/ (посетена на 06.11.2020)
[27] Nalla, M., Prenzler, T. (2020) Regulating the Security Industry: Global Perspectives. Routledge. https://www.routledge.com/Regulating-the-Security-Industry-Global-Perspectives/Nalla-Prenzler/p/book/9780367588694 (посетена на 04.11.2020)
[28] State Regulation Conerning Civilian Private Security Services and Their Contribution to Crime Prevention and Community Safety. Criminal Justice Handbook Series. United Nations Office on Drugs and Crime. New York, 2014. https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Ebook0.pdf (посетена на 04.11.2020)
[29] Private Security Joint Declaration: Ensuring Business Continuity and Protection of Workers in the Covid-19 Panemic. Uni Europa Global Union. Friday, May 8, 2020. https://www.uni-

4.Видови услуги од приватната безбедност

Приватното обезбедување и безбедносните услуги вклучуваат физичко и техничко обезбедување на лица, имот и деловни активности во рутински активности и во услови на ризични ситуации или на критични инсталации. Приватните безбедносни агенции во исто време може да вршат обука и издаваат лиценци за работа во т.н. подсектор приватна безбедност, но исто така обезбедуваат заштитна опрема и уреди. Радиусот на нивниот ангажман е потесен од надлежноста на приватните компании за воено управување, консултации и обезбедување на воени услуги.[30]



Графикон 1: Структура на индустрија на приватни безбедносни услуги. Извор: http://ficci.in/spdocument/20329/Private-security-services-industry-Securing-future-growth1.pdf

europa.org/2020/05/private-secruity-joint-declaration-ensuring-business-continuity-and-protection-of-workers-in-the-covid-19-pandemic/ (посетена на 05.11.2020)

[30] Blunt, C. (2017) Post-Brexit EU-UK Cooperation on Foreign and Security Policy. House of Commons Foreign Affairs Committee. https://www.blunt4reigate.com/sites/www.blunt4reigate.com/files/2017-04/Post-Brexit%20EU-UK%20cooperation%20on%20foreign%20%26%20security%20policy%20April%202017.pdf (посетена на 05.11.2020)

Детективската истражна активност како елемент на приватните безбедносни услуги вклучува услуги кои традиционално се под јурисдикција на јавните полициски служби, како што се потрага по исчезнати лица, наоѓање изгубени или украдени предмети, собирање информации и известувања, безбедносни (обично теренски) проверки на лица, расчистување на кривични дела за кои има постапка за кривично гонење по приватни тужби и по службена должност, но и некои многу чувствителни и често нелегални активности како што се тајно следење, надзор и евидентирање на лица, добавување информации за деловни активности на други луѓе, официјални лица и економски тајни и сл.[31]

Сите истражувачки активности, генерално, можат да се класифицираат во доменот на семејно и наследно право, каде спаѓаат воспоставување вонбрачни односи, потрага по исчезнат член на семејство, придружба и следење на деца, воспоставување контакт помеѓу родители и деца во услови на судска забрана, истражни служби во парница, собирање докази за потребите на одбраната на обвинетиот, истражување на дисциплина при работа, истражување на оправданост на барања за отштета, утврдување на стварната имотна состојба на лица и сл. Овластувањата кои им се доделени на приватните детективи, во земјите каде што е законски регулирано, се порестриктивни во однос на овластувањата на полицијата.[32]

Ако се погледне практиката и искуството во повеќето земји на Европската унија, како и во другите поразвиени земји, може да се забележи растечки тренд на обемот на услуги обезбедени од приватни детективи, телохранители (службеници за безбедност) и приватни компании за безбедност.[33]

---

[31] Differences Between Private Investigators and Security Guards. National Investigative Training Academy Incorporated. https://investigativeacademy.com/differences-private-investigators-security-guards/ (посетена на 02.11.2020)

[32] Inspection Related to Private Security and Detective Affairs. Republic of Croatia Ministry of Interior. https://mup.gov.hr/aliens-281621/inspection-affairs/inspection-related-to-private-security-and-detective-affairs/281631 (посетена на 07.11.2020)

[33] Resolution On Private Security Companies. (2016/2238(INI)) European Parliament. https://www.europarl.europa.eu/doceo/document/A-8-2017-0191_EN.html

Денес, индустријата за приватната безбедност се антиципира дека ќе достигне робустен раст. Клучните двигатели кои го придвижуваат овој тренд се постојаното чувство за безбедносна закана, како и повеќе услуги за повеќе корисници.[34]

Доменот на приватните безбедносни услуги опфаќа 18 основни елементи (ASIS, 2009) како: физичко обезбедување, безбедност на персонал, безбедност на информациони системи, истраги, спречување на загуба, управување со ризик, правни аспекти, итно планирање и вонредни состојби, противпожарна заштита, управување со кризи, управување со катастрофи, контратероризам, контраразузнавање, извршна заштита, заштита од насилство на работното место, превенција од криминал, спречување на криминал преку дизајн на животната средина и безбедносна архитектура и инженеринг.

Во изминатите три децении, приватните безбеднсони компании бележат подем, нудејќи чуварски и безбедносни услуги од полициски тип и постепено станаа побројни од националните полициски сили. Во контекст на значителната трансформација на безбедносниот и воениот сектор во 90-тите години на минатиот век, се доаѓа до заклучок дека стана приватизиран и деловно ориентиран. Тоа ја претставува еволуцијата на приватните актери во војувањето и трговијата со безбедносни услуги.[35]

[34] An Inside Look at the Future of Private Security. https://pulitzercenter.org/reporting/industry-inequality-why-world-obsessed-private-security (посетена на 07.11.2020)
[35] Krahmann, E. (2020) Private Security and Military Actors. Oxford Research Encyclopedias. https://doi.org/10.1093/acrefore/9780190846626.013.279 (посетена на 06.11.2020)

Обезбедување на лица	Активности за превентивна и репресивна заштита на телесна неповредливост на лица
Обезбедување на имот	Активности за физичка заштита против неовластен упад на имот, вклучително и режим за адмисија
Обезбедување настани	Активности насочени кон обезбедување непречено и непрекинато одржување на масовни настани и краткорочни активности
Обезбедување карго и вредни пратки	Активности за заштита на пари, благородни метали, уметнички дела и други вредни предмети, чиј пренос е неопходно да биде спроведен со вооружена придружба, со посебно опремени возила за транспорт, стабилни врски и други технички и помошни заштитни уреди
Обезбедување технички безбедносни системи	Активности за надзор и контрола на обезбедувани објекти и локации преку употреба на технички уреди и системи и реакција на здобиените резултати

Табела 1: Видови приватни безбедносни активности. https://www.securityguardtrainingcentral.com/

5. Влијание на приватната безбедност во поширокиот општествено-безбедносен контекст

Индустријата за приватна безбедност го предизвикува и го поларизира мислењето за нејзината улога и влијание. Според одредени стојалишта, едноставно е неприфатливо да се предаде одговорноста за јавната безбедност на трговски субјекти управувани чисто од мотивација во потрага по профит. За други пак, приватните компании за безбедност го нудат многу потребниот комплемент или дури и алтернатива на службите за државна безбедност.[36]

Според одредени традиционални класификации, системот на национална безбедност се состои од пет сектори: војска, полиција (јавна и тајна полиција), судство, надворешна политика и економски сектор, што од аспект на модерната држава, е потесна дефиниција.

Во традиционално организираните национални системи, безбедноста е јасно дихотомизирана. Од една страна е секторот за воена безбедност, што го

[36] McFate, S. (2019) Mercenaries and War: Understanding Private Armies Today. National Defense University Press, Washington DC. https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/mercenaries-and-war.pdf (посетена на 08.11.2020)

сочинуваат армијата, воената полиција, воените безбедносни служби, цивилната одбрана и заштита, воениот суд и воениот систем на социјално и здравствено осигурување; и од друга страна, цивилниот безбедносен сектор, кој се состои од субјектите полиција, разузнавачки служби, судство, тела за извршување на кривични санкции, инспекции и царини.

Компонентите на современите системи за национална безбедност можат да бидат поделени на цивилен и воен сектор за безбедност. Во исто време, соодветна е поделба на државни и недржавни безбедносни сектори, како поширока дефиниција коампоненти на системот за национална безбедност. Терминот не-државен безбедносен сектор се однесува на систем од непрофитни и профитни субјекти основан од недржавни актери кои им нудат на засегнатите страни одредени безбедносни услуги што е познат како приватен безбедносен сектор.[37]

Графикон 2: Димензии на приватната безбедност. Извор: https://www.alliedmarketresearch.com/private-security-market-A06346

Современиот концепт на национална безбедност е синтеза од безбедноста на граѓаните и безбедноста на државата, како и придонесот на државата во меѓународната и глобалната безбедност. Тој подразбира оптимална заштита на

[37] Lippert, R, Walby, K, Steckle, R (2013) Multiplicities of corporate security: Identifying emerging types, trends and issues. Security Journal 26(3): 206–221. https://journals.sagepub.com/doi/10.1177/1362480614527303 (посетена на 09.11.2020)

националните и државни вредности и интереси што се постигнуваат, одржуваат и унапредуваат во функција на безбедноста на граѓаните, системот на национална безбедност и наднационалните безбедносни механизми, како и отсуство на (индивидуален, групен и колективен) страв од нивно загрозување, и колективно чувство на спокојство, сигурност и контрола над развојот на идни феномени и настани од значење за животот на општеството и државата.[38]

Оваа структура е во голема мера претставена во модерните безбедносни системи, но со делумно укинување на грубите поделби на поединечните надлежности на воениот и цивилниот безбедносен сектор (на пр. во борба против тероризмот, организираниот криминал, техничките и технолошките опасности, природните катастрофи и сл.).[39]

Заштитата која што претходно беше исклучиво обезбедена од државата станува заменета со приватни компании и агенции за услуги и производи за физичко и техничко обезбедување. Паралелно со реалното проширување на спектарот на заканите по безбедноста се создаде простор за таканаречениот недржавен безбедносен сектор. Овој безбедносен сектор често се нарекува приватен сектор за безбедност. Овој назив е со нагласен контраст во однос на јавната безбедност, што традиционално и примарно ѝ припаѓа на полицијата и другите традиционални безбедносни служби.[40]

Ретроспективно, фокусот на приватната безбедност во источноевропските држави од страна на фирми кои се развиле и имаат седиште во тие држави е друга карактеристика што ја разликува оваа дејност од голем дел од постоечката студија во оваа област. Имено, многу од најпознатите истражувања се однесуваат на анализирање на обезбедување безбедност од страна на фирми кои имаат

[38] Dupont, B. (2014). Private security regimes: Conceptualizing the forces that shape the private delivery of security. *Theoretical Criminology*, *18*(3), 263–281. https://doi.org/10.1177/1362480614527303 (посетена на 08.11.2020)
[39] White, A (2011) The new political economy of private security. Theoretical Criminology 16(1): 85–101. https://journals.sagepub.com/doi/10.1177/1362480611410903 (посетена на 08.11.2020)
[40] Cook, P, MacDonald, J (2011) Public safety through private action: An economic assessment of BIDS. The Economic Journal 121(552): 445–462. https://scholar.google.com/scholar_lookup?hl=en&volume=121&publication_year=2011&pages=445-462&issue=552&author=P+Cook&author=J+MacDonald&title=Public+safety+through+private+action%3A+An+economic+assessment+of+BIDS (посетена на 09.11.2020)

седиште на Запад, но спроведуваат огромно мнозинство од нивните безбедносни активности во странство, на места како Ирак, Авганистан и Аденскиот Залив.[41]

Генерално, првично се испостави дека многу од домашно ориентираните фирми во Источна Европа воспоставиле значителни коруптивни односи со локалните полициски сили и каде, во одредени случаи, полициските службеници тврдеа дека не се во можност да обезбедат соодветна безбедност за нивните општества и потоа ги охрабруваа поединците и деловните субјекти да купат дополнителна безбедност од приватни организации кои се поседувани или ги вработуваат истите овие службеници, или нивни блиски соработници.[42]

Анализирајќи го процесот на приватизација на безбедноста што следеше по колапсот на комунизмот во повеќе источноевропски држави (Босна и Херцеговина, Бугарија, Романија или Србија), може да се открие дека овој процес, во комбинација со глобалните нормативни промени кои промовираат поголемо прифаќање на приватизираната безбедност, произведуваа комплицирани хибридни мрежи на обезбедувачи на јавни и приватни безбедносни услуги.[43]

Овие хибридни мрежи не само што ги надминуваа конвенционалните граници што ги одделуваат јавната и приватната и домашната и меѓународната сфера, тие исто така дејствуваа и како нормативни претприемачи, кои преку своето перформативно однесување ги редефинираа нормите што ја регулираа безбедноста во посткомунистичка Источна Европа.

Приватните понудувачи на безбедност во овие држави соработуваа со нивните влади, паралелно на тој начин предизвикувајќи ги традиционалните правила за обезбедување на безбедноста. Приватизацијата на безбедноста во овој регион, која следуваше по крајот на комунизмот во раните 90-ти години, претставуваше одраз на глобалниот тренд во кој безбедносните улоги што традиционално спаѓаа исклучиво во рамките на државата, постепено беа

---

[41] How Mercenaries are Resphaping the Battlefield. https://www.aljazeera.com/program/counting-the-cost/2019/11/24/how-mercenaries-are-reshaping-the-battlefield/ (посетена на 11.11.2020)
[42] Fitzsimmons, S. (2018) Review – Security Enterprenuers: Performing Protection in Post-Cold War Europe. Oxford University Press. https://www.e-ir.info/2018/12/12/review-security-entrepreneurs-performing-protection-in-post-cold-war-europe/ (посетена на 10.11.2020)
[43] Private Security Companies in the Western Balkans (2014-2017). Kosovar Center for Security Studies. http://www.qkss.org/en/Programet/Private-security-companies-in-the-Western-Balkans--385 (посетена на 07.11.2020)

ангажирани на приватни актери. Во раните години, индустријата првично не беше регулирана и прикажуваше проблеми забележани во другите економски сектори кои произлегоа од централно водената социјалистичка командна економија.[44]

Некои сегменти од индустријата во подем беа силно поврзани со организирани криминални елементи, како и во одредени ситуации со екстремна националистичка политика. Во текот на последната деценија, секторот започна да се професионализира, бидејќи владите на регионот направија законодавни напори да воведат контроли.[45]

6. Дејноста приватно обезбедување низ економска призма

Во последните години, безбедносните предизвици се префрлуваат од маргините на приоритети, кон области на влијание на развојната агенда. Безбедноста сега е препознаена како суштинско значење за егзистенцијата на граѓаните и пристапот до услугите и бесплатно остварување на граѓански, политички, социјални и економски права. Безбедноста, исто така, има директно влијание врз растот на инвестициите, социјалниот и човечкиот капитал, јавните институции и дистрибуцијата на ресурси.[46]

Приходите според услуга опфаќаат:

⇒ чување (вклучува патролирање, следење на опремата за надзор и надгледување на стационарни локации)

⇒ безбедносен мониторинг (вклучува планирање на безбедносни системи, извршување одржување и прегледување, реагирање на настани и обезбедување поддршка по настанот).[47]

---

[44] Security and Defense. Southeastern Europe Security Center. https://sesecuritycenter.org/ (посетена на 09.11.2020)

[45] Zakon o Privatnom Obezbedzenju. http://www.parlament.gov.rs/upload/archive/files/lat/pdf/predlozi_zakona/1866-13Lat.pdf (посетена на 09.11.2020)

[46] Silveti, O., Garcia, S. (2020) Industry Revenue of Private Security Activities in France from 2012-2024. Statista Business Services. https://www.statista.com/forecasts/899695/private-security-activities-revenue-in-france (посетена на 07.11.2020)

[47] Harborne, B., Dorotinsky, W., Bisca, M., P. (2017) Securing Development. Public Finance and the Security Sector. World Bank Group. https://peacekeeping.un.org/sites/default/files/securing_development-public_finance_and_the_security_sector.pdf (посетена на 06.11.2020)

Пазарите вклучуваат нерезиденцијален, владин, институционален и резиденцијален сегмент:

⇒ нерезиденцијален:

⇒ комерцијални (трговски канцеларии и деловни згради)

⇒ индустриски (производствени капацитети и магацини)

⇒ владин:

⇒ судски згради, амбасади, затвори, воени бази, споменици, затвори, комунални претпријатија, други владини згради

⇒ институционален: (вклучува центри за третман на лекови, болници, домови за стари лица, психијатриски установи и центри за рехабилитација, како и основни и средни училишта, високообразовни установи и кампуси како што се колеџи и универзитети, дневни центри, центри за туторство, институции за доделување на степен како што се сертификати, деловни или трговски програми)

⇒ други нерезиденцијални (вклучува театри, концертни сали, конгресни центри, спортски арени, стадиони и други јавни места; постројки за приватни комунални услуги; непрофитни агенции; аеродроми и поморски пристаништа, автобуски терминали, железнички станици и други превозни објекти)

⇒ резиденцијални / станбени (вклучува едносемејни домови, повеќесемејни домови и комплекс домувања).[48]

Приватниот безбедносен пазар по региони, сегментиран за потребите на регионална анализа ги опфаќа**:**

⇒ Северна Америка (САД, Канада и Мексико, итн.)

⇒ Европа (Германија, Франција, Велика Британија, Русија, ЈИЕ и Италија)

⇒ Азија-Пацифик (Кина, Јапонија, Кореја, Индија и Југоисточна Азија)

⇒ Јужна Америка (Бразил, Аргентина, Колумбија итн.)

⇒ Среден исток и Африка (Саудиска Арабија, ОАЕ, Египет, Нигерија и Јужна Африка).[49]

[48] Private Security Services. 17th Edition. https://www.freedoniagroup.com/industry-study/private-security-services-3764.htm (посетена на 14.11.2020)

Во основа, небезбедноста и несигурноста ја ослабуваат инвестициската клима со тоа што стимулациите за инвестиции стануваат покуси, уништувајќи ги материјалните средства и човечкиот капитал. даноци - т.е. дополнителните трошоци поврзани со негативните екстерни влијанија како резултат на нестабилност - и на неорганизирани пазари. Насилството и несигурноста му штети на човечкиот и социјалниот капитал современиот свет парадоксално се карактеризира како несигурен свет и некои од најистакнатите прашања од јавната политика на современото време се однесуваат на тоа како може да се зајакне нивото на безбедност. Честопати овие прашања можат дополнително да се поделат на она што е најприфатливи или ефективни средства за решавање на несигурноста.[50]

[49] Global Private Security Service Market 2019 by Companies, Regions, Types and Application Forecasts to 2024. https://www.absolutereports.com/global-private-security-service-market-14407086 (посетена на 06.11.2020)

[50] ASIS International (2013) The United States Security Industry. Alexandria, VA: ASIS International. https://scholar.google.com/scholar_lookup?hl=en&publication_year=2013&author=ASIS+International&title=The+United+States+Security+Industry (посетена на 07.11.2020)

ГЛАВА III
КРИТИЧНА ИНФРАСТРУКТУРА

1. Општо за критична инфраструктура

Поимот „инфраструктура“ за првпат е воведен во XIX век од швајцарскиот воен теоретичар Антоан-Хенри Жомини, кој го истакнува стратегиското и оперативно значење за раководењето на воените дејства. Значи, до средината на XX век терминот „инфраструктура“ е воен термин со кој се означува територијалната организација на системот за одржување и функционирање на армијата. Подоцна терминот „инфраструктура“ почнува да се користи во економската теорија и во теоријата на управувањето[51], а постепено овој термин навлегува во терминологијата на економијата, информатиката, како и во анализите за безбедноста. Со тоа постепено објектите на критичната инфраструктура претставуваат „крвоток“ за непречено функционирање на базичните елементи на општествата, така што нивната заштита претставува приоритет за секое општество.

Поимот критична инфраструктура е клучен за правилно разбирање на заштитата на критичната инфраструктура. Придавката критичен доаѓа од старогрчкиот јазик, а во современиот македонски јазик е преземена од англискиот јазик. Од повеќето значења на придавката критичен, за поимот критична инфраструктура од значење се две. Првото значење на критичен означува нешто што е суштинско, неопходно, животно важно (витално), а второто значење се однесува на нешто решавачко, судбинско, пресвртно или преломно. И двете значења може да се разгледуваат одвоено, но и заедно, надополнувачки, па така, критичната инфраструктура поимно би можеле да ја определиме како инфраструктура што е суштествено, животно неопходна и нарушувањето на нејзиното нормално функционирање може да доведе до загрозување на најзначајните вредности и добра врз коишто почива економијата, државата, општеството, благосостојбата и воспоставениот начин на живот. Оттука, јасно е дека всушност, заштитата на критичната инфраструктура е предуслов, претпоставка за заштитата на други пошироки општествени вредности, а самата

[51] Idzorek, T., *Infrastructure and Strategic Asset Allocation: Is Infrastructure an Asset Class*?, Boston a Morningstar Company, 2009, стр. 17, преземено од Бакрески О., и др., Заштита на критична инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 25-40.

критична инфраструктура може да се смета за инструментална, средствена вредност. Тоа подразбира дека критичната инфраструктура би можеле да ја дефинираме како вредност или збир вредности и добра што се од суштествено значење за економијата, државата и општеството, најчесто идентификувани како сложени материјални и нематеријални системи, чие нарушување во функционирањето или уништување би можело да создаде долгорочни штетни последици врз основните вредности на економијата, државата и општеството во целина. [52]

Значи критичната инфраструктура како поим означува елемент, систем или дел од систем, лоциран во одредена држава, чии основни функции и значење се поддршка на виталните општествени функции, здравјето, безбедноста, економската и социјалната благосостојба, а чие нарушување или деструкција би имало огромни последици во самата држава, заради неможноста да се одржат тие функции. Со оглед на фактот дека инфраструктурните мрежи се меѓусебно зависни, заемно влијаат една на друга и имаат комплексни врски, нарушувањето на нивното функционирање може да доведе до огромни материјални и човечки загуби во општествата, дури и да доведе до крах на системите. [53]

Во основа, терминот критична инфраструктура е во широка употреба во владини, раководни и академски терминологии и литература, но во голема мера е дефиниран со илустрација и категоризација наместо според збир на карактеристики, што може да се изолира со цел анализа и предвидување.[54]

Друга широка илустрација вклучува: електрична енергија, воздушен транспорт, копнен сообраќај, (патишта и масовен транзит), финансиски инструменти и корпоративно управување и регулирање (лесен кредит, глобално банкарство, права на сопственост, интернет, како и шпедиција, глобални

[52] Definition of Critical. Merriam-Webster. http://www.merriam-webster.com/dictionary/critical преземено од Правна рамка за обезбедување на критичната инфраструктура – со осврт на обезбедувањето на критичната инфраструктура во Република Македонија, Комора на РМ за приватно обезбедување, Скопје, 2016, стр. 10.
[53] Бакрески О., Милошевска Т., Алчески Ѓ., Заштита на критична инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 25-40.
[54] Interagency Security Committee 2019 Annual Report. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency CISA https://www.cisa.gov/sites/default/files/publications/ISC_2019_Annual_Report_508.pdf (посетена на 16.11.2020)

осигурителни пазари, системи за дневна грижа и универзитети (Шварц, 2003).[55] Според Белата куќа, илустрацијата за критичната инфраструктура ги опфаќа секторите земјоделство и храна, водостопанство, јавно здравје, одговор при итни случаи, одбранбена индустриска база, сектор телекомуникации, енергетски сектор, транспортна мрежа, банкарски систем и финансии, хемиска индустрија и опасни материјали, пошти и испорака.[56]

Листата назначени индустрии и сектори кои спаѓаат во критичната инфраструктура, се шири со текот на времето и развојот на технологијата. Како што се зголемува заканата од кибернетички напади паралелно со заканите од тероризам, кои продолжуваат да се појавуваат, нападите врз критичната инфраструктура се високо на списокот за загриженост помеѓу креаторите на политики и носителите на одлуки и претставуваат императив за потребата од заштитни мерки.[57]

2. Дефинирање на заштитата на критичната инфраструктура

Во согласност со зголеменото значење и важност на системите на критичната инфраструктура во однос на посредната и непосредната поврзаност на зачувување на нивната безбедност во контекст на целокупните напори за одржување на националната и меѓународната безбедност, артикулирани се неколку дефиниции за критичната инфраструктура.[58]

Развојот на критичната инфраструктура во сите домени на човечката активност е во тесна корелација со развојот на општествата. Поимот безбедност на критична инфраструктура може да се дефинира на повеќе начини. На пример, Светската здравствена организација помот безбедност го дефинира како слобода

[55] Ministry of Infrastructure of Ukraine. Branches. https://mtu.gov.ua/en/ (посетена на 05.11.2020)
[56] Proclamation on Critical Infrastructure Security and Resilience Month, 2020. Infrastructure and Technology. October 30 2020. The White House Proclamation. https://www.whitehouse.gov/presidential-actions/proclamation-critical-infrastructure-security-resilience-month-2020/ (посетена на 04.11.2020)
[57] Van der Merwe, S., Biggs, R., & Preiser, R. (2018). A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems. *Ecology and Society, 23*(2). doi:10.2307/26799110 (посетена на 11.11.2020)
[58] Federal Ministry of the Interior, Building and Community. Critical Infrastructure Protection. [article] https://www.bmi.bund.de/EN/topics/civil-protection/critical-infrastructure-protection/critical-infrastructure-protection-node.html (посетена на 09.11.2020)

од неприфатлив ризик од штета или несреќа. Понатаму, безбедноста, пак на критичната инфрастрктура е дефинирана како отсуство на несреќи, повреди и жртви кои директно влијаат на преживувањето и опстојувањето на комплексните инфраструктурни системи.[59]

Во овој контекст, при дефинирање на поимот заштита и безбедност на системите на критична инфраструктура, терминот несреќа опфаќа широк спектар несакани колизии и судари, односно настани кои главно не може да се предвидат и се случуваат ненамерно, но и несреќи кои биле предизвикани со интенција.[60]

Системите на критична инфраструктура се дефинираат како рамките на меѓусебно зависни мрежи и системи кои се состојат од идентификувани индустрии, институции (вклучувајќи луѓе и процедури), и дистрибутивни способности кои обезбедуваат сигурен проток на производи и услуги од суштинско значење за одбраната и економската безбедност на нацијата, на непречено функционирање на владата на сите нивоа, и на општеството како целина.[61]

Иако терминот критична инфраструктура не се користел низ минатото, историските записи опишуваат системи од витално значење за функционирањето на една нација, и таквите системи секогаш постоеле. Заштитата и насочувањето на овие системи често е гледано од гледна точка на националната безбедност и како тие влијаат на способноста на националната држава да функционира. Критична инфраструктура, без разлика дали под тоа име или некое друго, пред сè сепак, им служела на цивилите.[62]

---

[59] Viira, T. (2018) Lessons Learned: Critical Information Infrastructure Protection: How to protect critical information infrastructure. IT Governance Publishing. DOI: 10.2307/j.ctt1xhr7hq

[60] Madej, M., Pajak, M. (2019): Road Transport of Dangerous goods in Poland. Risk Analysis. Safety and Security in Traffic. Promet – Traffic & Transportation, Vol. 31, 2019, No. 5 https://traffic.fpz.hr/index.php/PROMTT/article/view/3106 (посетена на 12.11.2020)

[61] Raiden, A B & Aboagye-Nimo, E (Eds.) Proceedings of the 31st Annual Association of Researchers in Construction Management Conference, ARCOM 2015. Association of Researchers in Construction Management, United Kingdom, pp. 135-144.

[62] Lopez, J., Setola, R. (2012) Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defense. January 2012. Springer-Verlag. https://dl.acm.org/doi/book/10.5555/2231096 (посетена на 02.11.2020)

3. Појава и развој на критичната инфраструктура

Критична инфраструктура датира уште од стар Рим и античка Грција. Римската империја е позната во историјата за нејзините патни системи, продавници за храна и аквадукти. Аквадуктите на Рим биле критични за античката римска цивилизација и нејзината еволуција од регионална моќ во огромна империја. Овие системи биле сметани за неопходни и како такви биле заштитени и скриени од надворешни закани. Аквадуктите биле изградени за да му служат на цивилното население, но тие исто така биле и воена предност но и ранливост како цел на напаѓачки сили. Кога Римското царство започнало со изградба на аквадуктите над земјата, целта на инфраструктурата била да се претвори од скриен наменски систем, во видлив симбол на величина преку употреба на технологијата. Честопати противничката сила ја напаѓала критичната инфраструктура за да ги ослабне не само воените сили, туку и општата популација. На пример, опсадата на Хелеспонт, изворот на увоз на жито за Атина во античка Грција, резултирал со гладување на градот и последователен пораз на Атина кај Егоспотами.[63] Снабдувањето со храна и вода не биле единствените рани форми на насочена критична инфраструктура. Транспортната мрежа и средствата за превоз исто така имале витално значење за функционирање на општествата и поради тоа биле честопати мета на непријателите. За време на Втората светска војна, сојузничките сили го бомбардирале железничкиот систем на Германија, што ја запрело испораката на стоки и ја довело германската економија на работ на колапс.[64] Нападите врз виталните системи одат и подалеку од влијанието врз владата на една нација или воени операции и често имаат разорни ефекти врз цивилните популации. Кога станува збор за заштитата на критичната инфраструктура, постојат разни видови соработка кои поврзуваат повеќе области на работење, така што во обезбедувањето на критичните

[63] Дарданел, поранешен Хелеспонт, турски Чанакале Богази, теснец во северозападна Турција. Hellespont. https://www.britannica.com/place/Dardanelles (посетена на 02.11.2020)
[64] Bombing, States and Peoples in Western Europe 1940-1945. Centre for the Study of War, State and Society. University of Exeter. https://humanities.exeter.ac.uk/history/research/centres/warstateandsociety/projects/bombing/germany/ (посетена на 04.11.2020)

инфраструктурни системи се вклучени компании кои за примарна дејност имаат инженерски услуги, како во доменот на видео и радарски сензори за набљудување на транспорт, набљудување на сообраќај, контрола и безбедност на граници, заштита на имот, индустриски постројки, безбедносни решенија, итн.[65]

4. Критичната инфраструктура – меѓузависност на системите

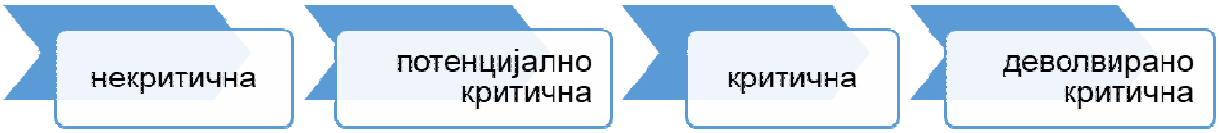
Кога одделни критични инфраструктурни системи се постројуваат заедно, критичните елементи на секој од нив индивидуално, стануваат критични елементи на сите, поради веројатноста крахирањето во еден дел од поединечниот систем да биде екстернализиран кон другите. Меѓузависноста помеѓу системите и елементите на системите исто така ја зголемува ранливоста преку екстернализација на критичноста. Критичната екстернализација е всушност точката каде ризикот од затајување од еден елемент на системот негативно влијае на другите елементи од тој систем.[66] Веројатноста за откажување на системот претставува комбинација на помали дефекти низ системот што каскадираат во поголем системски неуспех за чие ублажување напорите стануваат сложени и тешки, што аналогно се зголемува со бројот или диференцијацијата на типот на критичност на компонентите на системите.

Меѓузависните системи на критична инфраструктура подлежат на егзогени фактори; оние предизвикани од било што надвор од системот и од неговиот амбиентален пејзаж, како што се пазари, регулативи, конкуренција, перцепција на јавноста и природни катастрофи, а кои се поставени пред нив како резултат на промени во нивната околина. Така што, битно е да се истакне дека два потенцијални начини на пресретнување на поставените предизвици преку егзогени фактори: редукција на вишок и нови технологии, може да додадат на ранливоста.

---

[65] CoESS Critical Infrastructure Private Guarding Company Requirements Check List.
[66] Linkov, I., Wenning, R., J., Kiker, G., A. (2007) Managing Critical Infrastructure Risks: Decision Tools and Applications for Port Security. NATO science for peace and security series. Series C, Environmental security, 2007.
https://campbell.summon.serialssolutions.com/search?s.q=critical+infrastructure+and+private+security&spellcheck=true#!/search?ho=t&l=en&q=critical%20infrastructure%20and%20private%20security
(посетена на 11.11.2020)

Отстранување на вишок во критичните инфраструктурни системи има тенденција да не го решава проблемот на меѓузависноста, делумно затоа што отстранувањето на вишок додава сложеност на системот, а приватните корпорации кои обезбедуваат многу критично инфраструктурни услуги немаат мотивација да плаќаат за системи на технолошки вишок. Потпирањето на новопојавените критични технологии и услуги претставува посебен проблем затоа што, како што се набрзина пуштени на пазарот за да служат за одредена и многу потребна цел, можеби не се целосно тестирани во однос на дизајнот или перформансите. Овие технологии создадоа огромен збир придобивки поради ефикасноста и намалените ранливости на различни начини, станувајќи сè повеќе критични.



Графикон 3: Спектар на критичност. Извор: Journal of Contingencies and Crisis Management Volume 15 Number 1 March 2007

Спектарот на критичност (графикон 3) илустрира како одредна технологија влегува на пазарот обично категоризирана во „некритична фаза“ и станува сè покритична како што станува важен дел од инфраструктурата.[67]

Кога одреден елемент е критичен, системите што се потпираат на него и нивната функција зависи од него, тие би пропадне во услови на затајување или крах; оттука, електричните мрежи се критични заради сите критични системи кои се потпираат на нивната функционалност.

[67] Vaughan, G. (2018) Critical Infrastructure Public-Private Partnerships. Volume 14, Issue 1. Campbell University. http://bx7pv2zc6r.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=Critical+Infrastructure+Public-Private+Partnerships&rft.jtitle=Security+Challenges&rft.au=Vaughan+Grant&rft.date=2018-01-01&rft.pub=The+Kokoda+Foundation&rft.issn=1833-1459&rft.volume=14&rft.issue=1&rft.spage=40&rft.epage=52&rft.externalDocID=26488490&paramdict=en-US (посетена на 13.11.2020)

Одредени технологии, од друга страна, деволуираат од категорија на критичност бидејќи новите технологии ги заменуваат или потребата од нив избледува; на пример, бензинскиот автомобилски мотор може да се смета дека е во рана фаза на деволуција на критичност како што хибридните технологии почнуваат да го заземаат своето место.

Многу организации имаат развиено системи за да се компензираат разновидните ранливости што тие ги имаат создадено, но остануваат неподготвени за ранливоста на поновите системи што ги заменуваат, што евентуално резултира со намалување на сигурноста. Карактеризацијата на критичност заснована на последици го проширува спектарот на критичност за да се обезбеди груба рамка за оние кои се потпираат на новите технологии за да ги предвидат ранливостите што ги создаваат. Имајќи на ум дека бројот на технологии и услуги што претставуваат поддршка на критичната инфраструктура, и кои се дел од самите критични инфраструктурни системи, е прилично мал, мнозинството од нив не е, и веројатно нема никогаш да премине во критичност.[68] Ова овозможува пристап базиран на ризик или хазард кон управувањето со ранливоста. Еден од методите за управување со ранливост заснован на проценка на хазард бара идентификување на сите опасности создадени од самата технологија која се аплицира, вклучувајќи и споредби за различни нивоа на сигурност. Ова повлекува разбирање на точките на интерактивност помеѓу технологијата или услугата и систем што ќе го поддржува. Откако точките на интеракција ќе бидат добро перцепирани, организацијата може подобро да управува со своите ранливости. Критичноста се зголемува кога неуспехот на една технологија или услуга ќе резултира со губење на човечки живот или деградација на животната средина.[69]

[68] Simpkins B.K. (2019) Critical Infrastructure: Critical Manufacturing Sector. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_61-1 (посетена на 10.11.2020)

[69] S. V. N., Bhushan N. (2020) Critical Infrastructure: Defense Industrial Base Sector. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_123-1 (посетена на 09.11.2020)

5. Услуги за потребите на критичната инфраструктура

Креирањето листа на критични инфраструктурни услуги е важно и суштинско прашање. Сепак, самото креирање листа или список не е доволно за планирање на активностите што следуваат. Исто толку е важно и да се опишат критичните инфраструктурни услуги. Како и врз основа на што може да се каже дека функционира критичната инфраструктурна услуга? Како да се идентификува што е специфична критична услуга и што ја карактеризира? Ако не се дефинира како изгледа функционална услуга, тогаш е невозможно објективно да се процени дали функционира или не, или пак дали услугата функционира по потреба?[70]

Откако ќе се утврди листата на критични инфраструктурни услуги, откако сите ќе бидат опишани и ќе бидат утврдени нивните нивоа на услуги, следниот чекор е да се идентификуваат давателите на услуги.[71]

Даватели на услуги во доменот на критична инфраструктура не се само организации од јавниот сектор. Во многу земји, основните елементи на критичната инфраструктура се во сопственост или се управувани од приватни компании.[72]

Во зависност од услугата, пазарот, регулативата и многу други фактори, услугата може да ја обезбедат еден или повеќе даватели на услуги. Некои земји може да имаат само еден давател на одредена услуга ако давателот на услуги е монопол.

При конципирањето на целокупната стратегија за заштита на критичната ифраструктура, со цел создавање сеопфатен преглед на суштината на самиот процес, посебен акцент се става на опишаните принципи и препораки кои се

[70] Critical Infrastructure – Cooperation with the Private Sector. Rządowe Centrum Bezpieczeństva. http://rcb.gov.pl/en/critical-infrastructure-cooperation-with-the-private-sector/ (посетена на 09.11.2020)
[71] Jensen, C., R. (2020) Security Workers Classified as Essential Critical Infrastructure Workers. Security Today. Mar 24, 2020 [article] https://securitytoday.com/articles/2020/03/24/security-workers-classified-as-essential-critical-infrastructure-workers.aspx (посетена на 09.11.2020)
[72] Critical Infrastructure Protection. Governor's Office of Emergency Services. https://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/critical-infrastructure-protection (посетена на 09.11.2020)

валидни и во организации кои не се даватели на услуги во критичната инфраструктура.[73]

Тие акцентирани предиспозиции би требало да ги опфаќаат следните наведени точки:

- Анализа и идентификација на меѓузависностите на услугите,
- Визуелизација на податоците за критичната инфраструктура,
- Воспоставување стабилни односи и одржување,
- Дефинирање на давателите на услуги за заштита на критична инфраструктура,
- Дефинирање на критични инфраструктурни услуги,
- Идентификација и анализа на интерконекциите и зависностите на информациските системи,
- Идентификација на важните информациони системи и проценка на нивната важност,
- Идентификација на заканите и слабостите,
- Идентификација на критични активности, ресурси и одговорни лица потребни за да се обезбеди услугата на заштита на критична инфраструктура,
- Обезбедување услуги за заштита на критичната инфраструктура со намалена функционалност и / или во намален обем,
- Обука на вработените,
- Опис на критичната инфраструктурна услуга и утврдено ниво на услугата
- Подготвеност да се обезбедат услуги за заштита на критични инфраструктурни системи, со намалување на зависноста од ИТ системите, доколку е можно,
- Подготовка на планови за континуитет на бизнисот и закрепнување од катастрофи и нивно тестирање во разумни интервали,

[73] United States: The National Strategy for Homeland Security – Protecting Critical Infrastructures and Key Assets. https://www.resdal.org/Archivo/usa-home-prote.htm (посетена на 08.11.2020)

- Правење подобрувања доколку системот за заштита на критичната инфраструктура не функционира како што е планирано или не го дава посакуваниот исход,
- Приоритизација на активностите,
- Процена на безбедносното ниво на информационите системи и надворешна експертска проценка во разумни интервали,
- Процена на влијанието од потенцијално нарушување на услугите,
- Процена на ризиците поврзани со системот за услуги и информации,
- Следење на прописите за подобрување на еластичноста на критичните инфраструктурни услуги,
- Создавање функционална организација за заштита на критичната инфраструктура,
- Споделување информации,
- Спроведување на потребните безбедносни мерки.[74]

За да се обезбеди сигурност на услугите на критична инфраструктура, потребно е да се знае како се обезбедува услугата. Каков вид деловни процеси мора да работат за да може давателот на услуги да ја обезбеди услугата, а потрошувачот да ја консумира? Обезбедувањето критични инфраструктурни услуги честопати зависи од разни под-услуги без кои услугата не може да се обезбеди.[75]

Во зависност од организацијата и услугата, ваквите услуги може да се обезбедат:

1. Внатрешно: еден оддел обезбедува услуга на друг оддел.
2. Надворешно: пренесување услуги од надворешни даватели на услуги преку аутсорсинг.[76]

---

[74] Critical Infrastructure Book. Professional Security Magazine [online] 05th January 2018. https://www.professionalsecurity.co.uk/news/commercial-security/critical-infrastructure-book/ (посетена на 08.11.2020)

[75] Alexandru, A., Vevera, V., Ciuperca, E. (2019): National Security and Critical Infrastructure Protection. International conference KNOWLEDGE-BASED ORGANIZATION 25(1) DOI: 10.2478/kbo-2019-0001 (посетена на 08.11.2020)

[76] Viira, T. (2018). Critical Activities and Required Resources. In *Lessons Learned: Critical Information Infrastructure Protection: How to protect critical information infrastructure* (pp. 21-23). Ely, Cambridgeshire,

Заштитата на инфраструктурните системи и градежните проекти е клучна компонента за целокупниот успех на проектите и компаниите и клучна за развој на одржување на инфраструктурата и економијата на земјата.[77]

Персоналот за безбедност кои нуди услуги заштита на критичната инфраструктура, во таа насока ги извршува следните активности:

- физичка заштита на лице место,
- точки за проверка на возила,
- заштита на влезови/излези и перимерни патроли
- следење опасности и небезбедни услови за заштита на вработените и опремата, со цел да се намали ризикот од доцнење во работењето, кражба на опрема и вандализам.[78]

За исполнување на различните барања на проектите и развојот на инфраструктурните компании се изготвува план за безбедност, што треба да е исто толку темелен како и деловниот план на самите компании.[79]

Со редовните патроли, заштитата на средствата и набљудувањето на теренот се обезбедува секоја нова развојна активност или проект, со цел постигнување клучни перформанси и зацртани цели, како и избегнување на инциденти за да се намалат ризиците, влијанијата и евентуалната загуба на средства.[80]

Покрај заштитата на клучните средства и инфраструктурата, услугите на приватната безбедност вклучуваат активности во веќе погодени зони, преку поинаков вид услуги обезбедени од тимови за одговор при катастрофи, кои вклучуваат:

- Обнова и транспорт на средства
- Спасување на вработени или клиенти заглавени на локации со оштетена инфраструктура

United Kingdom: IT Governance Publishing. Retrieved November 7, 2020, from http://www.jstor.org/stable/j.ctt1xhr7hq.9 (посетена на 09.11.2020)

[77] Cummings, S. (2017). *A new history of management*. Cambridge, UK: Cambridge University Press.

[78] Martin, G. (Ed.). (2014). *Handbook of security* (2nd ed.). London: Palgrave Macmillan.

[79] Papa, M., Shenoi, M. (2008) Critical Infrastructure Protection. IFIP Advances in Information and Communication Technology. https://www.springer.com/gp/book/9780387885223 (посетена на 09.11.2020)

[80] Sullivant, J. (2016). *Building a corporate culture of security*. Waltham: Butterworth-Heinemann.

- Заштита на мобилните средства, како што се камиони за напојување и конвои за снабдување, кои транзитираат низ погодени области
- Обезбедување итни комуникации, храна, гориво, превоз и медицинска помош.[81]

[81] Global Customized Private Security & Investigative Solutions. Critical Infrastructure Security. Lasorsa & Associates. https://www.lasorsa.com/wp-content/uploads/2019/08/LA-Critical-Infrastructure-Brochure.pdf (посетена на 12.11.2020)

ГЛАВА IV

ЗАКАНИ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

1. Закани по критичната инфраструктура

Критичната инфраструктура е под закана од два фактора. Првиот е природниот фактор и тука спаѓаат опасностите од земјотреси, пожари, поплави, епидемии и сл., и вториот фактор што се однесува на намерното предизвикување штети (кражби, вандализам, тероризам итн).[82] Значи, што се однесува до заканите за критичната инфраструктура, тие може да бидат вештачки, како резултат на тероризам или други криминални активности, но може да бидат и природни, предизвикани од временските услови, како што се бури, вулкански ерупции, поплави или други еколошки катастрофи. Исто така, критичната инфраструктура може да биде загрозена и од болести, пандемии и да влијае врз голем број критичен персонал.[83] Од друга страна, заштитата на критичната инфраструктура е сегмент од политиката за национална безбедност и предуслов за непречено и сигурно функционирање на општествениот живот на државите, но и меѓународната заедница. Поради димензијата на ранливоста на критичната инфраструктура, нејзината меѓузависност и поврзаност која ги надминува националните територијални граници и правни рамки, меѓународната заедница реализира повеќе документи кои претставуваат рамка за координирано дејствување во правец на заштитата на критична инфраструктура, првенствено од терористички напади и несреќи предизвикани од природата, но и други видови хибридни и асиметрични закани кои се резултат на современото живеење.[84]

Постојат голем број на причини поради кои инфраструктурата треба дабиде добро заштитена и обезбедена. Критичната инфраструктура претставува огромен, глобален сектор и не е можно да се обезбеди нејзина целосна заштита во секое време и на сите места. Оттука, веројатно е дека некои терористички напади врз критичната инфраструктура ќе успеат. Терористите имаат цел да шират страв,

---

[82] Flammini, F., *Critical Infrastructure Security: Assessment, Prevention, Detection, Response,* 2012, стр.9.
[83] Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.
[84] Митевска.М.,Милевски Т.,Микац Р., Критична инфраструктура:концепт и безбедносни предизвици, Скопје 2019, стр.28, преземено од Марковски С., Потреба од заштита на критичната инфраструктура-со осврт на обезбедување на сообраќајната инфраструктура во Република Македонија, магистерски труд, стр. 57-59.

вознемиреност и паника, создавајќи перцепција дека секој граѓанин и главен јазол во инфраструктурата на земјата се подложни на напад. Не така одамна бевме сведоци на авионските киднапирања и самоубиствени напади извршени во САД од страна на мрежата „Ал Каеда“, при што загинаа 2.507 цивили, 343 пожарникари, 72 службеници за спроведување на законот, 55 воени лица и 19 сторители. Четири домашни комерцијални авиони биле киднапирани истовремено додека летале во Североисточниот дел на Соединетите држави; два авиона удрија директно во кулите близначки на Светскиот трговски центар во Њујорк, третиот авион удри во Пентагон веднаш пред Вашингтон, додека четвртиот авион се урна на поле во Шанксвил, Пенсилванија.[85]

2. Потреба од заштита на критичната инфраструктура

На самиот почеток на XXI век, предизвиците поставени со градење и одржување на критичната инфраструктура се искачија високо на агендите за креирање политики низ западниот свет. Оттука, егзистенцијално е важно да се препознаат ризиците што можат да го загрозат интегритетот на критичните инфраструктурни системи. Кога се размислува за безбедноста на системот или мрежата, скоро секогаш веднаш се помислува на хакерски или терористички закани, но има и други закани што исто така треба да бидат земени во предвид, како што се откажување на опремата, човечка грешка и природни причини (времето, на пример). Во контекст на ова тврдење, е податокот дека Интерпол забележа раст од 200%, на бројот на профили на странски терористички борци, помеѓу јануари 2017 година и април 2018 година.[86]

Прашањето за критична заштита на инфраструктурата се појавува и како една од примарните грижи за националните влади, управителите на инфраструктурата и локалните власти. Европската унија, преку својата Европска

[85] September 11 Attacks. Updated September 11, 2020. https://www.history.com/topics/21st-century/9-11-attacks преземено од Марковски С., Потреба од заштита на критичната инфраструктура-со осврт на обезбедување на сообраќајната инфраструктура во Република Македонија, магистерски труд, стр. 57-59.
[86] Identyfing Terrorist Suspects. Interpol. https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects (посетена на 18.11.2020)

програма за заштита на критична инфраструктура (EPCIP), ја објави важноста на заштитата на критичната инфраструктура за сите свои земји-членки.[87] При избор на решенија што откриваат и идентификуваат безбедносни ризици и аномалии во очекуваното однесување, важно е да се факторизираат што е можно повеќе од овие ризици.[88]

Критичната инфраструктура игра активна и динамична улога во поддршката на непречена прогресија и асимилација на современото општество. Перформансите, безбедноста, сигурноста, континуираното работење, одржување и заштитата на критичната инфраструктура се меѓу националните приоритети за земјите низ целиот свет.

Критичните сектори на инфраструктурата се состојат од средства, мрежи и системи, без разлика дали се физички или виртуелни. Физичката заштита на критичната инфраструктура може да спречи извршување терористички напади со големо влијание и да ги избегне каскадните ефекти што често се поврзани со такви напади.

Стремежот за хипер-ефикасност и приватизацијата на многу капацитети на критична инфраструктура ја намалија еластичноста на многу од овие системи, со што се придонесе за поголем степен на ранливост и зголемување на критичноста. Еден од соодветните методи за одговор на тие видови ранливост е да се создаде системска еластичност, но се покажало како инсуфициентно затоа што пазарите имаат тенденција да не го продуцираат ова решение самите. Извршните директори на корпорациите сметаат дека да се трошат повеќе на претпазливост отколку што е неопходно, со што се нарушува нивната доверителска должност кон нивните акционери.[89]

---

[87] European Program for Critical Infrastructure Protection. https://ec.europa.eu/home-affairs/e-library/glossary/european-programme-critical_en (посетена на 11.11.2020)

[88] Hurst W., Merabti M., Fergus P. (2014) A Survey of Critical Infrastructure Security. In: Butts J., Shenoi S. (eds) Critical Infrastructure Protection VIII. ICCIP 2014. IFIP Advances in Information and Communication Technology, vol 441. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45355-1_9 (посетена на 10.11.2020)

[89] "Critical Infrastructure Protection Market - Growth, Trends, and Forecasts (2020 - 2025)" - https://www.reportlinker.com/p05815019/?utm_source=GNW https://www.globenewswire.com/news-release/2020/07/23/2066822/0/en/Critical-Infrastructure-Protection-Market-Growth-Trends-and-Forecasts-2020-2025.html (посетена на 10.11.2020)

Според „Kaspersky“ и „Symantec“, нападите врз системите за индустриска контрола се зголемуваат. Земјите во развој се нападнати првенствено, но овој тренд не е занемарлив ниту во високо развиените земји како земјите од Западна Европа и Северна Америка. Повеќето напади се преку интернет, отстранливи дискови или е-пошта. Понатаму, помеѓу 1%-4% од системите на информациска критична инфраструктура се нападнати од малициозен софтвер со криптовалути секој месец.[90]

Пазарот за заштита на безбедноста на инфраструктурата е високо конкурентен, како резултат на присуството на многу мали и големи играчи на пазарот што работат со своите деловни активности на домашните и меѓународните пазари. Со надоаѓањето на нападите на инфраструктурата, многу продавачи реагираат на зголемената закана нудејќи критични решенија за безбедност на мрежите и системите на критичната инфраструктура и информациите кои се пренесуваат за нејзино функционирање. Овие понуди треба да доведат до нови услуги, технологии и партнерства со водечките суштински оператори на инфраструктура.[91]

3. Преку заштита на критичната инфраструктура до зачувување на националната безбедност

Заедно со проширувањето на значењето на концептот на национална безбедност со вклучување на други сфери освен воените по нејзино значење, вниманието на експертите беше природно насочено кон оние субјекти кои придонесуваат за благосостојбата на граѓаните и за нивните основни потреби. Институциите одговорни за храна, вода, енергија и транспорт станаа видливи, но исто така беа запознати и со нивната ранливост и тешкотијата да се заштитат од ширење на асиметрични закани. Овој вид закани беше, пак, нова причина за трансформација на традиционалната безбедносна парадигма дека постоењето на

[90] Information Security. Symantec Product Categoroies. https://securitycloud.symantec.com/cc/#/landing (посетена на 12.11.2020)
[91] Mohammadi, A. (2018) Critical Infrastructure Management: Ports. CTRF 53rd Annual Conference, Ottawa. https://www.researchgate.net/publication/325347526_Critical_Infrastructure_Management_Ports (посетена на 13.11.2020)

моќни воени сили повеќе не претставува гаранција за социјалниот мир денес. Во исто време, движењето на ризиците, капиталот, интерконекцијата на транспортните објекти, дистрибуцијата на ресурсите, нафтата, природниот гас или мрежата за електрична енергија, епидемиолошките траектории на различни пандемии ги преминаа границите на една држава.

Заштитата на најкритичните услуги во земјата не е лесна задача. Потребна е постојана соработка и координација помеѓу клучните агенции и оддели и континуирана примена на подобрени технологии и процеси за рационална заштита на критичната инфраструктура.[92]

На почетокот, заштитата од еколошки закани беше главниот фокус на заштитата на критичната инфраструктура. Сепак, појавата на сајбер напади го смени фокусот - инфраструктурите се соочуваат со друга опасност што има опасни по живот последици и ризик од значителни економски загуби. Се предвидува дека со текот на времето, светот ќе се дели на силни, средни и слаби сајбер сили, при што првите ќе ги принудуваат другите и ќе доминираат во правилата на игра. Понатаму, се прогнозира дека демократските граѓански општества не се гарантира дека ќе се робустни.[93]

Јасно е дека конвенционалните безбедносни техники се борат да бидат во чекор со обемот на иновативни и нови напади. Потребни се свежи и прилагодливи решенија за безбедност во инфраструктурата. Заштитата и безбедноста на критичната инфраструктура бараат експресно откривање на нови закани.[94]

---

[92] IACP and COPS. (2004). *National policy summit: Building private security/public policing partnerships to prevent and respond to public disorder*. Alexandria: International Association of Chiefs of Police. https://link.springer.com/referenceworkentry/10.1007/978-3-319-69891-5_42-1#howtocite (посетена на 14.11.2020)

[93] Lee S.. (2019) Security: Private. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_242-1

[94] Ball, D., & Ball - King, L. (2013). Safety management and public spaces: Restoring balance. *Risk Analysis, 33*(5) https://scholar.google.com/scholar_lookup?title=Safety%20management%20and%20public%20spaces%3A%20Restoring%20balance&author=D.%20Ball&author=L.%20Ball%20-%20King&journal=Risk%20Analysis&volume=33&issue=5&pages=763-771&publication_year=2013 (посетена на 15.11.2020)

Разбирањето од каде (ќе) потекнуваат најголемите закани е императив кога се утврдува што треба да се заштити и зошто. Според одредени тези, се тврди дека нападите врз критичната инфраструктура како да се смета дека се поврзани повеќе со тероризмот и војната отколку со која било друга област. Но, не треба да се занемарат и природните процеси кои постојано носат промени на земјата. Поплави и цунами, земјотреси и вулкани, урагани и торнада, метеори и соларни одблесоци и други природни настани влијаат на теренот секојдневно.[95]

Појдовните точки кои се сметаат за иницијални каписли за секуритзација на прашањата поврзани со заштитата на критичната инфраструктура и го одбележаа почетокот на новиот милениум, како што беа нападите на 11 септември на Светскиот трговски центар и Пентагон и нападите врз системот на подземна железница во Лондон во Велика Британија, беа насочени кон аспектите на она што се нарекува критичната инфраструктура. Сепак, постојат дилеми околу прашањето дали е префорсиран тероризмот (првенствено од превентивни и преемптивни побуди) и се занемарува опасноста од заканите кои демнат од мајката природа?[96]

Аналогно на тоа, и двете области бараат соодветен одговор за заштитата на критичната инфраструктура. Прашањето е на кои области треба да им посвети повеќе време, напор и финансии: човечки предизвикани закани како што се тероризам, граѓанска војна, мотивирани групи и слично, или природни закани како што се земјотрес, поплави, пожари, циклон, суша итн?

Одговорот можеби не е едноставен како што може да се претпостави, но сепак, сигурно е дека сите такви инциденти мора да се земат предвид за да се обезбеди холистички и координиран пристап кон заштитата на критичната инфраструктура. Важноста на заштитата на критичната инфраструктура ги надминува традиционалните режими за безбедност и сигурност, и затоа е евидентна промена во традиционалното размислување со цел вклучување на

[95] Triantafyllou S. (2020) Protection and Security in Public Spaces. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_225-1 (посетена на 15.11.2020)

[96] Holmes, F. (2014) The importance of Critical Infrastructure Protection. Australian Security Magazine. https://australiansecuritymagazine.com.au/the-importance-of-critical-infrastructure-protection/ (посетена на 02.11.2020)

избалансиран и координиран пристап, кој не се фокусира само на заштитата на самите средства, туку и како може да се управува со заканите, да се одговори на нив и нужно да се опорави од вакви инциденти. Овие активности и задачи се однесуваат на намерни активности што се преземаат пред инцидентот за развој на оперативни способности за да се олесни ефективен одговор. Според објективните и реални прогнози, масивни закани за критичната инфраструктура ќе го преземат водството во глобален контекст, но сепак, останува да се стори што е можно повеќе за да се минимизира ефектот, преку интензивирање на подготовките што е можно повеќе.[97]

Како резултат на тоа, деловниот континуитет на критичната инфраструктура гледа не само на справување со инцидентите, туку и на ефектот што може да го има секое нарушување или загуба. Со заштитата на критичната инфраструктура се обезбедува идентификација и консензус за критичноста на средството и ланците на снабдување како целина, наместо да се насочува фокусот само на тоа како да се справи со инцидентот изолирано.[98]

Постојат многу предизвици поврзани со заштитата на системите и средствата на критичната инфраструктура и често може да вклучуваат ограничена безбедносна свест, недостаток на прифаќање или разбирање на безбедносните барања, или дури и кога перспективата на една личност може погрешно да процени дека безбедноста воопшто не е потребна. Имајќи предвид дека на глобално ниво голема пропорција од критичната инфраструктура е оперирана од приватни компании или е во приватна сопственост, претставува реален предизвик кога се одредува кој ќе штити, плаќа и одговара за инциденти околу критичната инфраструктура.[99]

---

[97] European Conference of Ministers of Transport (ECMT). (2003). *Vandalism, terrorism and security in urban public passenger transport.* Economic Research Centre. Paris, France (ECMT Publications are distributed by: OECD Publications Service, 2, rue André Pascal, 75775 PARIS CEDEX 16, France.) https://www.itf-oecd.org/sites/default/files/docs/03rt123e.pdf. (посетена на 16.11.2020)

[98] Norman, T., L. (2016) Risk Analysis and Security Countermeasures Selection. Second Edition. CRC Press, Taylor & Francis Group, Boca Raton, Fl. https://scholar.google.com/scholar?cluster=10101363799213031995&hl=en&as_sdt=2005&sciodt=0,5 (посетена на 16.11.2020)

[99] Gritzalis, D., Theoharidou, M., Stergioupoulos, G. (2019) Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies. Springer International Publishing. DOI:10.1007/978-3-030-00024-0 (посетена на 12.11.2020)

Со цел проектирање на прифатлива идна општествена благосостојба во сеуште еволуирачкиот и нетранспарентен сајбер свет, на носителите на одлуки им треба системски пристап заснован врз логиката на комплексни социотехничко-економски системи за да создадат системска еластичност и капацитети за резилиентност при нарушување преку споделување (меѓу сојузниците/секторите) безбедносни архитектури од суштинско значење со цел постигнување робусна состојба на еластичност на системите на критична инфраструктура.[100]

4. Резилиентност и еластичност на системите на критична инфраструктура

Фокусот на заштита на критичната инфраструктура не застанува на границите на одделните национални држави бидејќи сè погласно се упатуваат повици за меѓународни напори за заштита на националните критични инфраструктури. Понатаму, она што е заштитено не е секогаш самата инфраструктура, туку услугите што ги обезбедува.[101] Затоа заштитата на критичната инфраструктура вклучува низа стратегии со цел да се заштити не само физичката инфраструктура, туку и сите средства што се сметаат за критични во смисла дека не се може без нив, или во најмала рака, нарушувањето на нивните услуги би го отежнало животот или би влијаело на националната безбедност. Голем број од овие стратегии вклучуваат заштитна безбедност, спречување криминал, деловен континуитет и управување со ризици и управување со итни случаи. Одреден систем може да се смета за критичен кога услугите што ги обезбедува се од витално значење за една држава или за нацијата како целина.[102]

---

[100] Dombrowski, P., Demchak, C., C. (2015) Thinking Systematically About Security and Resilience in an Era of Cybered Conflict. Cybersecurity Policies and Strategies for Cyberwarfare Prevention. DOI: 10.4018/978-1-4666-8456-0.ch014 (посетена на 15.11.2020)

[101] O. Reg. 210/11: GENERAL. Ministry of Infrastructure, Ontario. https://www.ontario.ca/page/ministry-infrastructure (посетена на 15.11.2020)

[102] Advisory Memorandum on Ensuring Essential Critical Infrastructure Workers Ability to Work During the Covid-19 Response. US Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/Version_4.0_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers_FINAL%20AUG%2018v3.pdf (посетена на 15.11.2020)

Без јасно дефинирани граници за тоа што претставува критична инфраструктура на глобално ниво, сепак, меѓународните напори за заштита на критичната инфраструктура ќе бидат непотребно оптоварувачки и прекумерни. Пред да се пристапи кон меѓународни напори за заштита на критичната инфраструктура, глобалната заедница мора да се собере да дефинира кои критични инфраструктури вредат за ова дополнително ниво на заштита.[103]

Зајакнувањето на еластичноста на системите на критична инфраструктура бара од нивните сопственици / оператори да се утврди способноста на системот да издржи специфични закани и да се врати во нормална оперативност набргу по деградација. Така, методологијата на еластичност бара сеопфатно разгледување на сите делови на критичните инфраструктурни системи - од закани до последици. Притоа, методологијата треба да генерира репродуктивни резултати што можат да го поддржат донесувањето одлуки во управувањето со ризици, одговор на катастрофи и деловен континуитет.[104]

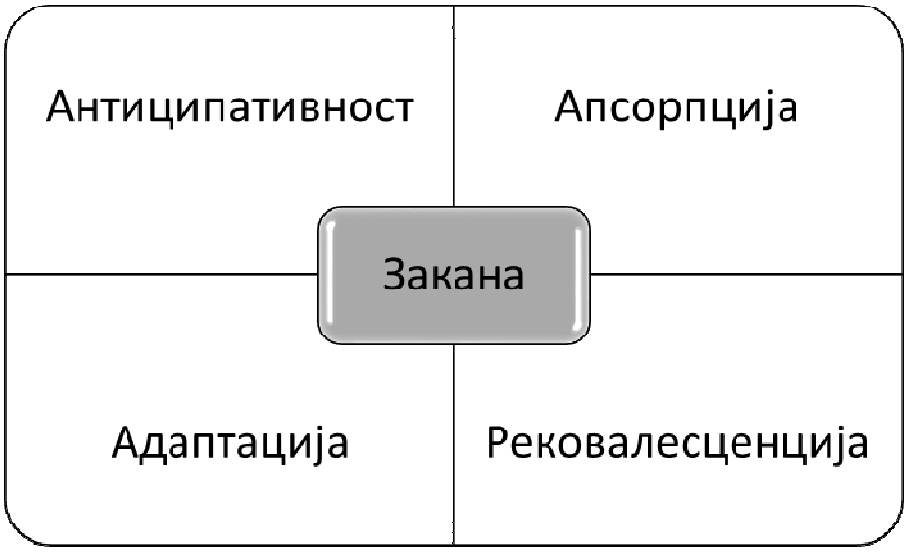
Развивањето сеопфатна методологија која користи униформирани и конзистентни податоци за развој на индекс на отпорност врз основа на собраните податоци придонесува кон креирање на план за проценка на загрозеност и ризик на критична инфраструктура. Програмата според која се пресметува индексот на отпорност е изведена од три категории: стабилност, снаодливост и закрепнување. Индексот на отпорност се движи од 0 (мала еластичност) до 100 (висока еластичност). Висок индекс на отпорност не значи дека одреден настан нема да влијае на објектот и нема да предизвика сериозни последици. Спротивно на тоа, нискиот индекс на отпорност не значи дека одреден непредвиден настан автоматски ќе доведе до неуспех на критичната инфраструктура и до сериозни последици. Наместо тоа, индексот на отпорност го споредува нивото на еластичност на критичните инфраструктури и води приоритет на ограничените ресурси за подобрување на еластичноста. Индексот на отпорност исто така

[103] Newbill, C. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies, 26*(2), 761-780. Retrieved November 4, 2020, from https://www.jstor.org/stable/10.2979/indjglolegstu.26.2.0761 (посетена на 08.11.2020)

[104] Constructing a Resileince Index for the Enhanced Critical Infrastructure Protection Program. Decision and Information Sciences Division, Agronne National Laboratory. US Department of Energy, 2010. https://publications.anl.gov/anlpubs/2010/09/67823.pdf (посетена на 12.11.2020)

обезбедува вредни информации за сопствениците / операторите во однос на капацитетите и за начините на кои може да се зголеми еластичноста.[105]

Апликациите и примената на проценатa на еластичност, или исто така наречена отпорност и резилиентност, продолжуваат да се развиваат и подобруваат и се антиципираат дополнителни пристапи кои се очекува да созрејат.[106] Исто така, индексот на отпорност може да биде комбиниран со други индекси како што се индексот на ранливост, индексот на заштитни мерки и индекс на критичност, во насока на поддршка на целокупното носење одлуки при проценка на ризици, заштита, деловен континуитет и управување со итни случаи.



Графикон 4: Четири димензии на отпорност. Извор: https://publications.anl.gov/anlpubs/2010/09/67823.pdf

Сеопфатните мулти-секторски јавни политики за поддршка на отпорноста или заштитата на критичните инфраструктури започнаа да се појавуваат во 2000-та година, при што 34 земји на OECD, кои одговорија на Анкетата за управување со критични ризици, 90% посочија дека назначиле специфични сектори за

[105] Jaafar, M., N. (2012) Identifying the Criteria for Critical Infrastructure Selection. International Real Estate Conference Kuala Lumpur, Malaysia, 9-10 June, 2012
[106] Coleman, L. (2017), The Power of Resilience Yossi, Sheffi The MIT Press, Cambridge MA, 2015, 14 pp. . J Contingencies and Crisis Management, 25: 114-115. https://doi.org/10.1111/1468-5973.12167 (посетена на 10.11.2020)

инфраструктура како критични (OECD, 2018).[107] Многу од овие земји дефинираа критични инфраструктурни сектори, воспоставија попис на средства преку процес на проценка на критичност и ризик и поставија национални програми за зајакнување на нивната отпорност на шокови. Ваквите програми обично се изградени врз механизам за управување што овозможува споделување на информации помеѓу владините и критичните оператори на инфраструктурата и вклучува комбинација на алатки за политика, почнувајќи од регулатива до стимулативни механизми за поддршка на спроведувањето на целите на критична отпорност на инфраструктурата.[108]

Анализата на критичноста треба да вклучува проценка на влијанијата на критичкото нарушување на инфраструктурата врз низа претходно утврдени критериуми. Неколку пристапи се користат во земјите на OECD. На пример, во Швајцарија се прави прва диференцијација помеѓу различните сектори и под-сектори со три категории критичност (многу висока критичност, висока критичност, нормална критичност).[109] Во Холандија, економските, физичките и социјалните критериуми овозможуваат да се дефинираат различните критични инфраструктурни процеси, но потоа се прави разлика помеѓу категоријата А каде нарушувањата можат да имаат големи влијанија и каскадни ефекти и категоријата Б каде влијанијата можат да бидат помали, со цел да се рефлектираат различноста во рамките на критичната инфраструктура и да се утврдат приоритетите. Во однос на критериумите, Европската комисија дефинира минимален сет за проценка на критичната инфраструктура, вклучително и влијанија врз јавноста, економски влијанија, влијанија врз животната средина,

[107] OECD (2019), *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://doi.org/10.1787/02f0e5a0-en. (посетена на 10.11.2020)
[108] State of play in the governance of critical infrastructure resilience. OECD Library. https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en (посетена на 14.11.2020)
[109] Pescaroli, G. and Kelman, I. (2017), How Critical Infrastructure Orients International Relief in Cascading Disasters. Journal of Contingencies Crisis Management, 25: 56-67. https://doi.org/10.1111/1468-5973.12118 (посетена на 16.11.2020)

меѓузависност, политички влијанија и психолошки влијанија (Европска Комисија, 2020).[110]

Критичните инфраструктурни организации мора да користат робустна рамка што може да ја предвиди и ублажи катастрофата низ целата нивна критична инфраструктурна средина. Заштитата на критична инфраструктура им помага на организациите да се подготват и да одговорат на сериозни инциденти кои се во склоп на критични инфраструктурни средини; и да се заштитат од постојано растечкиот број закани, имајќи во предвид дека во современи услови меѓународниот систем сега зависи од инфраструктурата на сајбер просторот, кој претставува глобален супстрат од масивни, сложени, несигурно дизајнирани мрежи кои обезбедуваат системски предности на масите предатори и непријатели.[111] Државите денес се соочуваат со невиден спектар на сајбер конфликт меѓу мирот и војната со растечки егзистенцијални импликации врз системите на критична инфраструктура. Парцијалните обиди за одбранбени механизми и јурисдикции создаваат растечки сајбер-вестфалистички свет и често делумни, некоординирани или нејасни стратегии.

5. Анализа на ризик на критична инфраструктура

Анализата на ризикот е релативно млада наука која е широко применета од организациите на јавниот сектор за да се подобри донесувањето одлуки. Во последниве години беше усвоен од сè поголем број организации во приватниот сектор.[112] Анализата на ризик е наменета за организации кои донесуваат одлука

[110] European Critical Infrastructure. European Commission. https://ec.europa.eu/home-affairs/what-is-new/work-in-progress/initiatives/european-critical-infrastructure-eci_en (посетена на 16.11.2020)
[111] National Security: Breakthrough in Research and Practice: Information Management Association USA. IGI Global. 2019 https://books.google.mk/books?id=hzyEDwAAQBAJ&pg=PA619&lpg=PA619&dq=Demchak+infrastructure+elements&source=bl&ots=xL67SVUFrx&sig=ACfU3U1MBZZhAN672JrUfe7iv1DMqkw88A&hl=en&sa=X&ved=2ahUKEwjDrNeM8OrsAhUH9aQKHU0uCO4Q6AEwDXoECAEQAg#v=onepage&q=Demchak%20infrastructure%20elements&f=false (посетена на 06.11.2020)
[112] Phillps, B. (2020) Three Steps to Avoid Security Theater. Security Management. Publication of ASIS International. [article] https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2020/three-steps-to-avoid-security-theater/?_t_tags=language%3aen%2csiteid%3ab1140b07-9e31-4808-809a-878911c7f3f1&_t_hit.id=ASIS_Models_Pages_SMArticleDetailPage/_3bc8b41c-957e-4fe5-9377-e212b0dcd900_en&_t_hit.pos=3 (посетена на 06.11.2020)

под несигурност. Јазикот на анализа на ризик е нерасчистен и сè уште се развива.[113] Бројот на квалитативни, полуквантитативни и квантитативни методи достапни за проценка на ризик расте со сè поголема стапка. Во употреба се неколку десетици различни програми, апликации и алатки за идентификување на опасност, проценка на последици, проценка на веројатност, карактеризација на ризик, карактеризација на несигурност, опции за управување со ризик и други, што го олеснува прилагодувањето на алатката до задачата.[114] Меѓу нив се вклучуваат:

- Баезијска статистика и Баезијски мрежи (Bayesian),[115]
- анализа на рибон (машна) транскрипција,
- анализа на причини, влијанија, последици,
- анализа на трошоци и придобивки,
- техники на Делфи,
- проценка на еколошки ризик,
- дијаграми на настани,
- мапи со докази,
- извлекување експертиза,
- режим на неуспех и анализа на ефекти,
- дијаграми на грешки,
- криви на кршливост,
- FN криви,[116]
- генерички процеси,
- HACCP,
- квантитативна процена на ризик HAZOP,
- топлинска мапа,

[113] CIP Security Within a Converged Plantwide Ethernet Architecture. White Paper May 2020. https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/CIP_Security/WP/CPwE-5-1-CIPSec-WP/CPwE-5-1-CIPSec-WP.html (посетена на 05.11.2020)
[114] Nadai, L. Padanyi, J. (2018) Critical Infrastructure Protection Research: Results of the First Critical Infrastructure Protection Research in Hungary. Springer International Publishing. https://books.google.mk/books/about/Critical_Infrastructure_Protection_Resea.html?id=216HtQEACAAJ&redir_esc=y (посетена на 05.11.2020)
[115] Bayesian Network. Introduction to Algorithms for Data Mining and Machine Learning. 2019. https://www.sciencedirect.com/topics/mathematics/bayesian-network (посетена на 05.11.2020)
[116] Duzgun, S. (2019) F-N Curves, Social Aspects and Risk Acceptability. Middle East Technical University, Ankara.

- LOPA, анализа на Markov,
- процес на Монте Карло, MCDA,
- квалитативни модели за проценка на ризик,
- полуквантитативна проценка на ризик,
- анализа на чувствителност,
- ефикасност на контрола на ризикот, индекси на ризик, матрица на ризик, наратив на ризик,
- проценка на безбедноста,
- анализа на сценарио, планирање сценарио, SWIFT,
- извлекување на субјективна веројатност и
- проценка на ранливост.[117]

Безбедносната архитектура CIP се заснова на логичка сегментација според зоните ISA / IEC 62443-3-2 и моделот на мрежи. Безбедносните својства на CIP имплементирани во рамките на моделот Zone and Conduits овозможуваат IACS мрежите да се движат кон безбедносен модел со нулта доверба со поместување на периметарот подалеку од работ на мрежата и кон вистинските податоци.[118] Безбедносен модел со нулта доверба се заснова на безбедноста „никогаш не верувај и секогаш проверувај“. Зоните создаваат помали домени на доверба за да помогнат во заштитата на мрежата IACS од познатите и непознатите ризици во мрежата. IACS уредите се идентификуваат и групираат во зони според заедничката функционалност и безбедносни потреби и барања. Ова може да биде комбинација на CIP Security способни IACS уреди, како и уреди што не се класифицирани во оваа категорија.[119]

Уредите го контролираат пристапот до и од различни зони. Секоја комуникација EtherNet / IP помеѓу зоните мора да биде преку дефиниран канал. Уредите може да се дефинираат со користење на следниве својства:

---

[117] Yoe, C. (2019) Principles of Risk Analysis: Decision Making Under Uncertanity. https://www.routledge.com/Principles-of-Risk-Analysis-Decision-Making-Under-Uncertainty/Yoe/p/book/9781138478206 (посетена на 08.11.2020)

[118]Security for industrial automation and control systems - Part 3-2: Security Risk Assessment for System Design https://webstore.iec.ch/publication/30727 (посетена на 22.11.2020)

[119] Integrated Administration and Control System. European Commisssion. https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/financing-cap/financial-assurance/managing-payments_en (посетена на 15.11.2020)

комуникациските технологии што се користат, протоколот што го транспортира и безбедносните својства што треба да ги обезбеди на поврзаните зони.

Способноста за проактивно контролирање на интеракциите помеѓу уредите IACS и управувањето со тековите на внатрешни и надворешни податоци ќе помогнат да се намалат безбедносните ризици по системите на критична инфраструктура.[120]

[120] IACS – Classification International Association of Classification Societies. https://www.iso.org/organization/9196.html (посетена на 15.11.2020)

ГЛАВА IV

ПРИВАТНИОТ БЕЗБЕДНОСЕН СЕКТОР И ЈАВНАТА БЕЗБЕДНОСТ ВО ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ВО РС МАКЕДОНИЈА

1. Односот на приватната и јавната безбедност во заштитата на критичната инфраструктура

Постои широко признаен консензус дека големината на приватната безбедносна индустрија е зголемена буквално во секоја земја во светот, честопати затемнувајќи ги конвенционалните полициски сили во бројот на персоналот и трошоците. Давателите на безбедност се разликуваат од службениците за спроведување на законот на многу начини, но сепак природата на нивните активности за намалување на криминалот ги доведува во чест контакт со граѓаните, привлекувајќи се на најистакнатите прашања за обука, професионалност и отчетност.[121]

За разлика од полициските службеници, чии стандарди за обука и лиценцирање се добро утврдени, прописите за давателите на безбедност честопати се минималистички или целосно отсутни. Во таа насока, потребно е обединувачко истражување на регулаторните режими и стратегии од целиот свет, опфаќајќи го и големиот приватен сектор за безбедност и проширувањето на областа на не-полициска заштитна улога во зачувување на оптимално ниво на безбедност на критичната инфраструктура, покрај онаа на јавниот сектор.[122] Таквото истражување и анализа ја испитува природата и степенот на лиценцирање и следење и минималните стандарди наметнати на индустријата од страна на владите низ целиот свет во однос на заштитата на критичната инфраструктура.[123]

---

[121] Sveinsdottir, T. *et al*. (2016) Taxonomy of Security Products, Systems and Services. CRISP. Evaluation and Certification Schemes for Security Products. https://www.trilateralresearch.com/wp-content/uploads/2018/09/CRISP-D1.2-Taxonomy-of-Security-Products-Systems-Services_REVISED.pdf (посетена на 05.11.2020)

[122] McCrie, R. (2006). A history of security. In M. Gill (Ed.), *Handbook of security*. London: Palgrave Macmillan.

[123] Ocena Stanja Privatnih Bezbednosnih Kompanija. Kosovar Center for Security Studies, 2009. http://qkss.org/web/images/content/Ocena%20stanja%20privatnih%20bezbednosnih%20kompanija.pdf (посетена на 16.11.2020)

Графикон 5: Потенцијални домени на соработка. Извор: https://www.pwc.com/gx/en/industries/government-public-services/public-sector-research-centre/achieving-safety-security.html

При конципирањето на целокупната стратегија за заштита на критичната ифраструктура, со цел создавање сеопфатен преглед на суштината на самиот процес, посебен акцент се става на опишаните принципи и препораки кои се валидни и во фирми кои не се даватели на услуги во критичната инфраструктура.[124] Тие акцентирани предиспозиции би требало да ги опфаќаат следните наведени точки: дефинирање на критични инфраструктурни услуги, опис на критичната инфраструктурна услуга и утврдено ниво на услугата, дефинирање на давателите на услуги за заштита на критична инфраструктура, идентификување на критични активности, ресурси и одговорни лица потребни за да се обезбеди услугата на заштита на критична инфраструктура, анализа и идентификација на меѓузависностите на услугите, визуелизација на податоците за критичната инфраструктура, идентификација на важните информациони системи

[124] Hemme, C. (2015) Critical Infrastructure Protection: Maintenance is National Security. Journal of Strategic Security. Volume 8, No. 5. DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1471 (посетена на 16.11.2020)

и проценка на нивната важност,[125] идентификација и анализа на интерконекциите и зависностите на информациските системи, приоритизација на активностите, идентификација на заканите и слабостите, процена на влијанието од потенцијално нарушување на услугите, процена на ризиците поврзани со системот за услуги и информации, спроведување на потребните безбедносни мерки, создавање функционална организација за заштита на критичната инфраструктура, следење на прописите за подобрување на еластичноста на критичните инфраструктурни услуги, процена на безбедносното ниво на информационите системи и надворешна експертска проценка во разумни интервали, подготовка на планови за континуитет на бизнисот и закрепнување од катастрофи и нивно тестирање во разумни интервали, воспоставување стабилни односи и одржување, споделување информации, обука на вработените, правење подобрувања доколку системот за заштита на критичната инфраструктура не функционира како што е планирано или не го дава посакуваниот исход, подготвеност да се обезбедат услуги за заштита на критични инфраструктурни системи, со намалување на зависноста од ИТ системите, доколку е можно, обезбедување услуги за заштита на критичната инфраструктура со намалена функционалност и / или во намален обем.[126]

2. Јавни – приватни партнерства во заштита на критичната инфраструктура

Постигнувањето ефективни јавни-приватни партнерства е долг и макотрпен процес, кој вклучува отстранување на многу пречки и проблеми и воспоставување на поинаква перспектива кон самите безбедносни проблеми што постојат во релевантните министерства работи и приватното обезбедување.[127]

---

[125] Critical Infrastructure Sector Partnerships. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/critical-infrastructure-sector-partnerships (посетена на 02.11.2020)
[126] Critical Infrastructure Book. Professional Security Magazine [online] 05th January 2018. https://www.professionalsecurity.co.uk/news/commercial-security/critical-infrastructure-book/ (посетена на 02.11.2020)
[127] S. V. N., Bhushan N. (2020) Critical Infrastructure: Defense Industrial Base Sector. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_123-1 (посетена на 04.11.2020)

Решавањето на основните тешкотии во овие два безбедносни сегменти создава добра основа за успех на проектите за јавните-приватни партнерства. Секако, тоа не претпоставува дека е потребно претходно решавање на сите или повеќето проблеми со цел да се започне со јавни-приватни партнерства. Активната контрола која ќе има објективен увид во состојбата на самите организации и нивното функционирање, ќе влијае на покачувањето на нивото на услугата во секоја смисла.[128]

Во однос на носењето одлука за иницирање јавни-приватни партнерства во областа на заштитата на критичната инфраструктура, потребно е суштински да се постават неколку клучни прашања, кои ја потврдуваат или одрекуваат оваа соработка. На пример: како се формираат, организираат и одржуваат ефективните партнерства? На кој начин е најдобро да се споделат одговорностите во партнерствата од страна на раководството? Како партнерите и потенцијалните партнери можат да се осврнат на довербата и правните проблеми кои се предизвик за размена на витални информации? Кои фактори даваат најголем придонес за успех во партнерството? Кои се најважните лекции што треба да се земат во предвид од партнерствата? Дополнително, останува ли потреба повеќе да се направи во правец на постојано подобрување на комуникацијата, професионалноста, и финалните резултати?.[129]

За да се справат со новонастанатите ризици, многу субјекти брзаат да донесат безбедносни решенија за да ги одржат своите бизниси оперативни и усогласени со ново воспоставените здравствени и безбедносни стандарди. И покрај тоа што е охрабрувачки да се види бизнисот како повеќе инвестира во програми за физичка безбедност, не сите мерки за ублажување на ризикот се изедначени Кога менаџерите воведуваат контрамерки без претходно разбирање и решавање на специфичното управување на ризикот на компанијата, тие придонесуваат за „безбедносен театар“ - концепт што се однесува на безбедносни

[128] Litavski, J. (2012) Izazovi Privatnog Sektora Bezbednosti u Novom Veku. Tromesecnik Centra za Evroatlantske Studije. Novi vek, broj 2. https://www.ceas-serbia.org/images/tromesecnik/Novi-vek-broj-2-Jan-Litavski.pdf (посетена на 01.11.2020)
[129] Trends and Practices in Law Enforcement and Private Security Collaborations. Operation Partnership US Department of Justice, 2009. http://www.justiceacademy.org/iShare/Library-COPS/cops-p169-pub.pdf (посетена на 15.11.2020)

мерки што ги прават луѓето да се чувствуваат побезбедни без да направат ништо за да ја подобрат нивната безбедност.[130]

Тешкотиите што може да се сретнат при реализацијата на јавните-приватни партнерства може да имаат квалитативен и квантитативен карактер. Квалитативните потешкотии произлегуваат од фактот дека државата со своите безбедносни служби прави монолит, каде што нема доволно критична маса дел од одговорностите глатко да се пренесат на приватните компании, освен ако претходно не се трансформирале. Квантитативната содржина на потешкотиите кои произлегуваат од јавните-приватни партнерства извираат од фактот дека во одредени случаи, приватните компании немаат доволно експертиза да се справат со широкиот спектар на безбедносни услуги. [131]

Овие два фактори на потешкотии имаат свои внатрешни и надворешни карактеристики, кои ги обележуваат и ја одредуваат нивната релација. Оттука, при решавање на проблеми и трасирање на вистинскиот пат за реализација на јавни-приватни партнерства, потребно е да се започне од точно и јасно дефинирани цели. Во таа насока, со цел да се запази временската рамка на реализација и симултаноста со потребите, проектите треба да се воведат во фази, пред сè во оние области каде што се најлесни за спроведување, а потоа, по воспоставувањето редослед во обата сектори и во другите области на безбедноста. [132]

Заштитата на критичната инфраструктура е една од најоптималните области за воспоставување партнерства помеѓу јавниот и приватниот сектор, со оглед на нивниот многу чест јавен/национален или локален карактер, што може да се преведе од јавна сопственост или јавно управување, или пак, јавни цели.[133]

Во таа насока, неприфатливо е да се прави разлика помеѓу јавниот и приватниот безбедносен сектор затоа што приватниот безбедносен сектор често

---

[130] Alizadeh, H., Sharifi, A. (2020) Assessing Resilience of Urban Critical Infrastructure Networks: A Case Study of Ahvaz, Iran. *Sustainability* 2020, *12*(9), 3691; https://doi.org/10.3390/su12093691
[131] Critical infrastructure Protection. Science Direct. https://www.sciencedirect.com/topics/computer-science/critical-infrastructure-protection (посетена на 15.11.2020)
[132] Указ за прогласување на Законот за енергетика. https://www.erc.org.mk/odluki/Zakon%20za%20energetika%20MK.pdf (посетена на 03.11.2020)
[133] Baggett, R. K., & Simpkins, B. K. (2018). *Homeland security and critical infrastructure protection* (2nd ed.). Santa Barbara, CA: Praeger Security International.

има углед со комерцијален епитет, бидејќи неговите услуги се наплаќаат. Но, од друга страна, услугите на безбедносните служби во јавниот сектор исто така се наплаќаат и според повеќето проценки, се поскапи од оние на приватните сектор. Сепак, тој трошок е помалку видлив за јавните безбедносни услуги, бидејќи тие трошоци поминуваат низ државниот буџет.

Како релевантен пример во тој контекст, во Европската унија има трендови во врска со прераспределбата на одговорностите на јавниот сектор во корист на приватниот безбедносен сектор, што несомнено ги претставува насоките за понатамошен развој на приватниот безбедносен сектор. Факт е дека во секоја европска земја постојано расте присуството на приватни компании за безбедност во јавните служби за заштита. [134]

Анализите и студиите на случај презентираат и недвосмислено укажуваат дека добро дефинирани, ефикасно управувани и добро контролирани партнерства помеѓу јавните и приватните субјекти без никакво сомневање придонесува за зголемување на безбедноста на критичната инфраструктура. Искуството за јавно приватно партнерство во областа на безбедноста во земјите на ЕУ, поради зголемување на ефикасноста, овие партнерства ги заснова на следните принципи: отворен дијалог помеѓу надлежните јавни институции и приватни даватели на безбедност, јасни упатства за улогата на секој партнер индивидуално, јасна правна и договорна рамка за соработка, режим на комуникација за размена на релевантни информации и редовен процес на неопходни корекции и подобрувања кога се потребни.[135]

[134] Mihaljević, B. (2018) Protection of Critical National Infrastrucutre: Challenges for the Private Security Sector. Ann. Disaster Risk Sci. 2018, 1, 47-56

[135] Mulowayi, E., et al.: (2017) The Influence of Critical Infrastructure Interdependencies on Post-Disaster Reconstruction: Elements of Infrastructure Interdependency that Impede the Post-Disaster Recovery Effort. http://www.arcom.ac.uk/-docs/proceedings/5c0fdbc531a915738ce7dcc9bfa2ade9.pdf (посетена на 06.11.2020)

3. Потреба од координација и соработка во заштита на критичната инфраструктура во македонската држава

Координацијата произлегува од потребата за соработка меѓу релевантните субјекти и таа е задолжена да ги поврзе одделните елементи што имаат префикс на заштитна компонента. Оттука проучувањето на внатрешниот механизам на приватниот безбедносен сектор првенствено треба да се заснова на негово целосно разбирање и разграничување за да се избегне каква било импровизација и парцијализам, особено ако знаеме дека високиот степен на соработка е од голема корист за работата на секторите којашто не е едноставна и којашто е непредвидлива.[136]

Денес се смета дека одредена состојба може да се проблематизира поради лошите процени на состојбата, вклучувајќи ја и самата координација, но и од недостаток на навремени информации што укажуваат на постоење опасност, како и од неподготвеноста субјектите да се справат со безбедносните предизвици. Следствено на тоа, практичен момент за подготовките за справување со потенцијалната опасност е носење одлука на вистински начин и во вистинско време, како и постоење на потребната координација на релевантните субјекти, која не секогаш е навремена. Тоа значи дека не е сеедно кога ќе биде донесена одлуката, затоа што избрзана или задоцнета одлука може да биде опасна и пресудна во заштита на критичната инфраструктура. Оттука не е сеедно како се гледа на конкретните закани по критичната инфраструктура и како и на кој начин се реагира на нив.[137]

За да може да се понуди кохерентно објаснување што ќе биде приспособено за изучување на сложените структурни, институционални, социјални и други проблеми што го оптоваруваат работењето на критичните инфраструктурни објекти, нашето стојалиште е дека најдобрата основа за анализа

[136] Бакрески О., Милошевска Т., и Алчевски Ѓ., Заштита на критична инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 192.
[137] Исто., стр. 192.

е да се согледа каква е координацијата и соработката на релевантните субјекти во обезбедување на потребното ниво на заштита на овие сектори. [138]

Македонската држава треба да преземе чекори за кохерентна имплементација на мерки за подобрување на заштитата на критичната инфраструктура и дефинирањето на обврските и должностите на сите субјекти во земјата засегнати со оваа проблематика. Спроведувањето на мерките е директно поврзано со имањето, односно немањето на соодветна процена која треба да укаже или да претпостави на одредена закана. Проценатa на ризици врз самите критични инфраструктури претставува процес во кој се анализираат собраните безбедносни информации со определување на приоритети по однос на критериумите, евалуацијата и веројатноста.

Што се однесува до заканите и ризиците врз критичната инфраструктура нема дилема дека централната улога му припаѓа на приватното обезбедување во нашата држава. Оттука потребно е преземање соодветни чекори во однос на превенција, подготвеност и одговор на заканите врз критична инфраструктура ќе се обезбеди адекватна заштита и врвните приоритети во заштита на критичната инфраструктура.

Во координацијата во безбедноста за заштита на критичната инфраструктура, во нашата држава треба да претходат фази на подготовка, планирање и усвојување и адаптација на подзаконски акти од различни закони, меѓу кои: законот за енергетика, законот за заштита и спасување, законот за приватно обезбедување, законот за одбрана, закон за безбедност на мрежи и информациски системи, понатаму Националната стратегија за сајбер-безбедност, Стратегијата за одбрана и други.[139] Исто така, кога ќе се воспостави систем со јасни контури, фактори и резултати од работата, се олеснува имплементацијата на јавните-приватни партнерства согласно променетите и прилагодени елементи на јавни-приватни партнерства во оваа област.

---

[138] Исто., стр. 192-193.

[139] Стратешки документи. Министерство за одбрана на Република Северна Македонија. http://www.mod.gov.mk/?page_id=39286&lang=mk

Поголем ефект во оваа насока ќе се постигне ако сегашните власти прават процес на пренасочување, реорганизација и едукација. Утврдувањето пропусти и проблеми се налага да биде транспарентно и овие детекции би требало да бидат коригирани тековно.

4.Предности на соработка

Приватниот безбедносен сектор заедно со полицијата во македонската држава се предодредени да соработуваат најнапред заради комплементарноста на функциите што ги и извршуваат и заради обезбедување на повисоко ниво на безбедност за граѓаните и за државата. Начинот на соработката треба во голема мера да обезбеди поголема заштита на државниот имот како и на приватниот имот, но секако во фокусот се граѓаните кои имаат потреба за соодветно ниво на заштита. Значи, нема дилема дека соработката е клучна во креирањето партнерство и таа всушност е своевидна предност во заедничкото дејствување.

Постојат бројни предности од соработката на приватната безбедност во македонската држава и јавната безбедност, а како особени важни можат да се наведат следните: соработка во заеднички активности за спречување на криминалот, давање поголема безбедност во урбаните средини, спречување криминал; заеднички ангажман во насока на заедничко патролирање, споделување информации; давање на заедничко користење на ресурси кои им припаѓаат на двата субјекта итн.

Бројни примери говорат дека има недостаток од соработка што треба да биде суштинска алка и темел на јавно-приватното партнерство. Значи, и покрај сличните интереси за спречување криминал, полицијата и приватното обезбедување меѓусебно ретко соработуваат. Бројни истражувања потврдуваат дека соработката е недоволна а сепак е круцијална во справување со криминал и опасноста од терористички напади, други природни катастрофи и општествени безредија, односно се има впечаток дека се изоставува приватниот безбедносен сектор.

Секако важен елемент на соработка треба да биде заштитата на критичната инфраструктура во македонската држава. Соработката и координацијата треба да се издигнат на повисоко ниво со посебно вклучување на претставници од критичните инфраструктури во сите тела што ја третираат безбедноста на државата. Потребни се што повеќе експертски дебати, обуки, вежби со цел да се зголеми комуникацијата помеѓу клучните ресори, а сето тоа да биде поткрепено со правна рамка.

ГЛАВА V

ПРИВАТНАТА БЕЗБЕДНОСТ ВО ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА-РЕЗУЛТАТИ ОД СПРОВЕДЕНО ИСТРАЖУВАЊЕ

1. Примерок на истражување

За потребите на магистерскиот труд со наслов “Местото и улогата на приватната безбедност во заштита на критичната инфраструкутра” беше направено истражување (анкета). Анкетата беше анонимна и се спроведуваше писмено преку анонимни прашалници и преку интернет алатката SurveyMonkey. За реализација на истражувањето беа дистрибуирани вкупно 207 анкетни прашалници.

Основната идеја на истражувањето беше да се согледа мислењето на испитаниците за улогата на приватните агенции за обезбедување во заштита на критичната инфраструктура. Прашањето е исклучително сензитивно и оттука, примарната задача на ова истражување беше да се согледаат состојбите но и да се скенираат мислењата и првичните сознанија за оваа проблематика што е солидна основа за мерење на ставовите и согледување на основната перцепција на лицата кои непосреднои се ангажираат во заштита на критичната инфраструктура. Ова истражување внесе и нова димензија затоа што беа анализирани прашања кои се својствени во заштитата и се примарна задача на вработените во приватниот безбедносен сектор. Анализирањето на резултатите ни овозможи да ја согледаме реалната слика за местото и улогата на приватното обезбедување во заштита на критичната инфраструктура и особено внимание се посвети на економските оператори кои се задолжени со управување на критичните инфраструктурни објекти.

Клучната цел беше да се изнајдат можни решенија кои ќе овозможат подобра заштита, ефикасно спроведување на соодветните стратегии за заштита и аналогно на тоа утврдување на реалната позиција на приватниот безбедносен сектор во јавната и во стопанската сфера. За остварување на поставените цели беше конструиран содветен прашалник во кој најнапред од испитаниците се бара да дадат основни податоци за: полот, возраста, образованието, за потоа да следат прашања со кои треба да се утврдат ставовите за приватната безбедност, соработката со јавната безбедност во заштита на критичната инфраструктура. Понатаму, од значење беше да се утврди улогата на приватните агенции за

обезбедување на критичната инфраструктура, а испитаниците имаа можност да ги изнесат своите мислења и за самите оператори и што преземаат како мерки, планови за заштита на критичните објекти.

2.Резултати од спроведеното истражување

Во продолжение следи соодветната интерпратација на резултатите од истражувањето.

Најнапред, (види Табела 1) дадени се прашања за да се стекне претстава за категоријата на испитаници кои се групирани според пол, образование и возраст. Поголем број од испитаниците во броен соодност се претставници на машкиот пол, а значаен број испитаници се на зрела возраст (со животно искуство), и имаат испитаниците со средно образование кое е достојно за професијата приватно обезбедување. Мора да се нагласи дека одреден процент на испитаници имаат високо образование, а дел се со заврсени магистерски и докторски студии.

Табела 1: ПРИМЕРОК

Пол		
%		
	Маж	59.9
	Жена	40.1
	Без одговор	-
Возраст		
%		
	18-30	37.96
	31-45	41,75
	Над 45	20,39
	Без одговор	0

Образование		
%		
	Основно	0,49
	Средно	41,35
	Вишо и Високо	40,38
	магистратура/докторат	17,79
	без одговор	0

По општите прашања кои се однесуваа на полот, возраста и образованието, во продолжение даден е целосен преглед на суштинските прашања кои беа и главни варијабли во истражувањето. Првиот сет на прашања се однесува на безбедносните ризици и закани со кои е соочена критичната инфраструктура. Нема дилема дека критичната инфраструктура е под постојана опасност од широк спектар безбедносни ризици и закани.[140] Ризиците се особено тешки за идентификување и справување. Тоа наметнува потреба системите на критична инфраструктура да се чуваат заштитени од закани и да бидат безбедни од секаква компромитација и деструктивно поткопување. Дополнително, важно е системите на критичната инфраструктура да бидат заштитени поради растечката и еволуирачка малигност. Значајно е да се има сознанија за потенцијалните безбедносни закани и како тие ефективно да се изменаџираат, со употреба на ефективни техники и методи за заштита. Соодветната подготвеност и оправување наметнува потреба од зајакнување и инвестирање во отпорност за минимизација на подсистемските ранливости за да се ограничи појавата, интензитетот и ширењето на дефектите/ краховите и импактот на системите на критична инфраструктура и следствено, на општеството. Во овој контекст, отпорноста или резилиентноста е фундаментална во ситуации на генерална криза и во дискурсот на управување со катастрофи и претставува фокус на оспежните напори за отпор, апсорпција, адаптација и оправување од ефекти на

[140] Gregg, S., H.: Defining and Distinguishing Secular and Religious Terrorism. Perspectives on Terrorism. Vol 8, No. 2 2014. [article] http://www.terrorismanalysts.com/pt/index.php/pot/article/view/336/html, посетена на 22/12/2019.

безбедносни закани. Тука се истакнува иницијативата за превенција, ублажување и подготвеност на активности априори, односно пред криза, одговор за време на криза, како и опоравување по криза. Каскадите на интегралните зависности и дефектите/краховите треба да се земаат предвид при анализата и дизајнот за резилиентност, и тие треба да го истакнат целиот циклус на безбедносната криза во критичната инфраструктура.[141]

Кога станува збор за критичната инфраструктура во македонската држава, неминовно се наметнува прашањето за ризиците со кои е соочена истата. За да се согледа перцепцијата за изложеноста на безбедносни ризици на испитаниците им беше поставено прашањето „Дали сметате дека критичната инфраструктура е изложена на безбедносни ризици. Интересно е да се напомне дека најголем број од испитаниците (60,87%) сметаат дека е изложена, а делумно или 34,30% се на мислење дека делумно е изложена, додека мал процент смета дека не постои опасност. Од изнесеното произлегува дека детектирана е важноста на критичната инфраструктура и реално е да се биде загрижен за изложеноста на потенцијална опасност.

Графикон 1. Изложеност на критичната инфраструктура на безбедносни ризици

[141] Исто., дел 2.

Заканите кои се насочени кон критичната инфраструктура имаат за цел да го нарушат нормалното функционирање на системите и да создадат тотална конфузија чија цел е да дестабилизираат одредени сегменти или цели системи за да го доведат во прашање целокупниот опстанок. Речиси и да нема сектор кој не може да биде цел на напад и се смета дека бројните закани можат да бидат од различна природа и преку постигнување на целите повеќекратно можат да направат штета на системот на критична инфраструктура.

Постојат голем број на закани кои можат да нанесат сериозни последици за критичната инфраструктура. Во литературата тие се рангираат според димензијата на ранливоста на критичната инфраструктура. Овие закани првенствено се однесуваат на терористички напади, разни форми и облизци на организиран криминал, но и на други несреќи предизвикани од антропогени фактори, вандализам, кражби, како и хибридни и асиметрични закани кои се резултат на современиот развој.

Следствено на тоа, во овој контекст е неопходно да се идентификуваат заканите и ризиците по системите на критична инфраструктура и нивната меѓусебна зависност. Одредени закани и ризици се поврзани со географскиот регион или пак може да се однесуваат на целата држава, па дури може да имаат и глобално значење. Тие се следните:

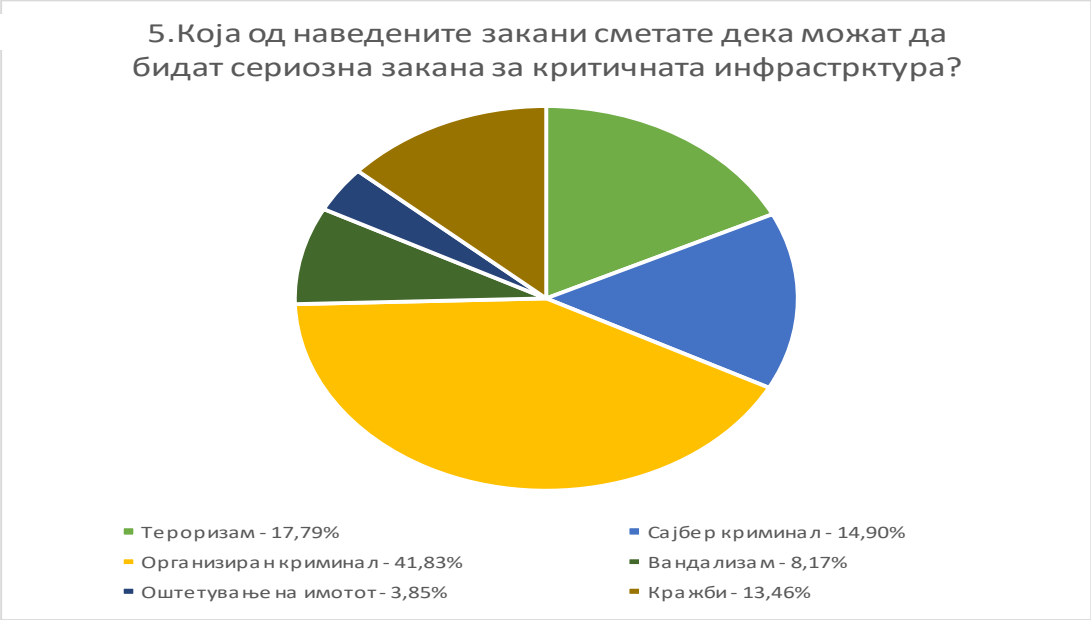
- климатски и атмосферски влијанија (екстремни температури, суша, шумски пожари);
- хидролошки несреќи (поплави);
- метеоролошки појави (тропски циклони, силни конвективни бури, екстремни зимски бури);
- геофизички настани (земјотреси, цунамија, вулкански ерупции);
- пандемии (глобални епидемии на одредени болести);
- вселенски временски настани (геомагнетни бури);
- технолошки и индустриски акциденти (структурни дефекти, индустриски пожари, ослободување на хазардни супстанци, хемиски излевања);
- непланирани прекини (дотраена инфраструктура, дефект на опрема, големи прекини на снабдување со електрична енергија);

- криминални инциденти и терористички напади (вандализам, кражба, оштетување на имот, инциденти со огнено оружје – активни стрелачи, кинетички напади);
- сајбер инциденти (напад со одбивање на пристап, малициозен софтвер, фишинг)
- напад врз ланецот за набавка (експлоатација на ранливостите за предизвикување на системски и/или мрежен дефект);
- операции со странско мешање (ширење дезинформации и поткопување на демократски процеси);
- несигурни инвестиции (потенцијално да им се даде на странски инвеститори непотребно влијание врз националната критична инфраструктура).[142]

Со цел да се согледа со што е соочена критичната инфраструктура во македонската држава од аспект на заканите, на испитаниците им беше поставено прашање според кое можат да ги посоцат заканите по веројатност кои се најголеми. Така, најголем број од оговорите се групирани на заканата организиран кримина или изразено во проценти 41,83% додека 17,79 % сметаат дека тероризмот е сериозна закана за критичната инфраструктура, а 14,90% од вкупниот број испитаници семтаат дека сајбер криминалот е реална закана. Следуваат кражбите со 13,46%, па вандализмот со 8,17 %, 3,85 % оштетување на имотот итн. Од изнесените ставови следува дека критичната инфраструктура е ранлива и реално изложена и на внатрешни и на надворешни извори на загрозување.

[142] CISA. Critical Infrastructure Sectors. https://cset.inl.gov/Lists/Critical_Infrastructure_Sectors/DispForm.aspx?ID=1&Source= посетена на 16/12/2019.

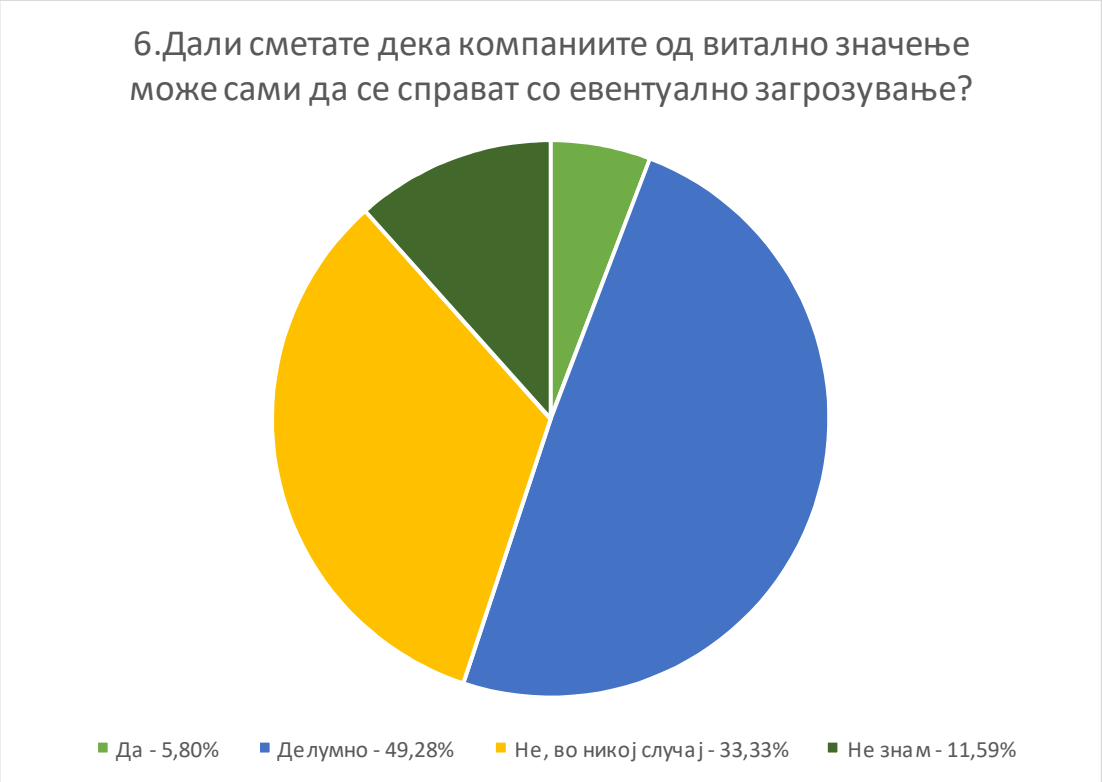
Графикон 2. Закани по критичната инфраструктура



Важна претпоставка за непречено функционирање на субјектите кои се од витално значење е дали можат самостојно да се справат со потенцијалните закани. Во контекст на справување со определени облици на загрозување првиот чекор што треба да го направат компаниите е да воспостават безбедносни цели. Вториот чекор се однесува на идентификацијата на ресурси, системи, мрежи и функции. Понатаму е важно да се обезбедат потребните информации врз кои ќе се направи потребната процена на ризиците која треба да овозможи овозможува рационални и целосни резултати со употреба на квантитативни, систематски и ригорозни процеси. Во фазата на приоритизација на активностите, потребна е соработка со безбедносните актери за целосна синхронизација на активностите. Во фазата на имплементација на заштитните програми, треба да се користи искуството и од други компании, но ефективноста зависи од воспоставениот систем кој треба да биде подготвен да превенира и секако и да обезбеди интегриран пристап за оптимизација на отпорноста и заштита на критичната инфраструктура.

За да се согледа фазната поставеност на компаниите во македонкста држава и особено дали се подготвени компаниите за да се справат со евентуална загрозување на испитаниците им беше поставено прашањето „Дали сметате дека компаниите од витално значење може сами да се справат со евентуално загрозување“?. Од изнесените одговори може да се констатира дека има голема резервираност дека компаниите можат самостојно да се спротистават на одредена закана или приближно 50% сметаат дека можат нецелосно да одговорат на овој предизвик. Малиот процент од 5,8% кои се изјасниле потврдно говори дека компаниите се предодредени да соработуваат со други субјекти во заштита на своите капацитети. Од анализата произлегува дека мора да постои заеднички пристап и напор на сите субјекти од повеќе дејности за да се обезбеди синхронизиран одговор во насока на справување со потенцијалните закани.

Графиокон бр. 3. Комнаниите и подготовките за евентуална закана

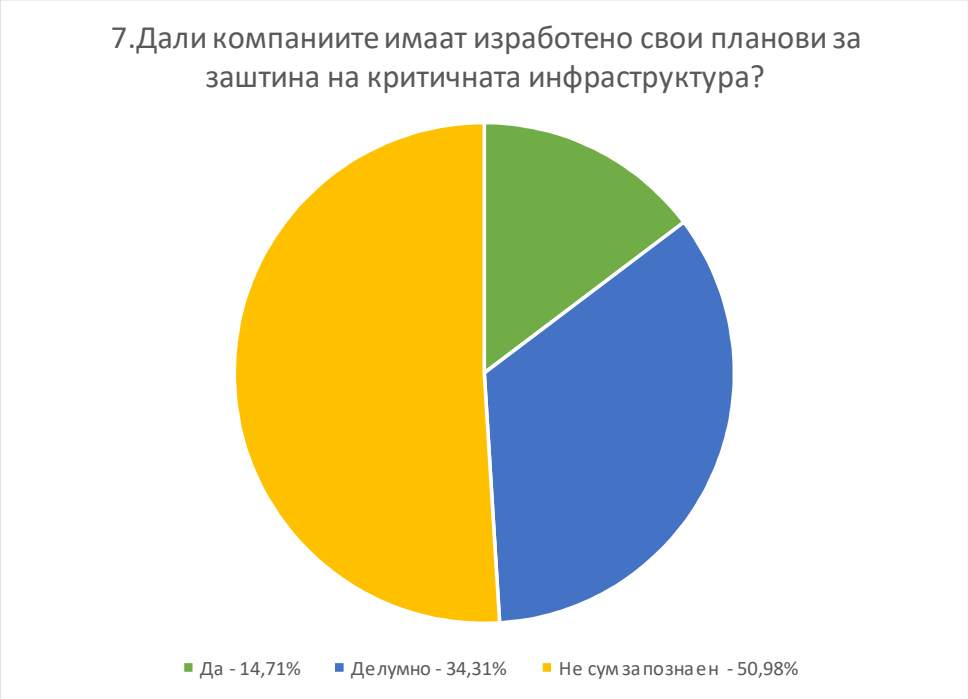


Изработката на плановите претставува административно-техничко обликување на планската одлука и нејзино претставување низ еден или повеќе плански документи. Во плановите се внесуваат сите елементи на одлуката, како што се: целите, задачите, силите, средствата, просторот, роковите и слично. Со планот мора да се предвиди и можноста за промена на планските задачи, доколку дојде до важни промени на околностите во кои институцијата ја извршува својата дејност. Затоа процесот на планирање не завршува со донесување на планскиот документ, туку планирањето се врши континуирано. Со планот се одредуваат и неопходните материјални средства и кадрите за остварување на предвидената цел. Ако постои големо несогласување меѓу средствата и кадрите со коишто располага организацијата и оние коишто се неопходни за остварување на предвидената цел, со планот се предвидува начинот на кој ќе може да се дојде до кадрите и средствата што недостасуваат, за да се оствари целта.[143]

За да се согледа како плановите на компаниите влијаат во заштита на критичната инфрастуктура на испитаниците им беше поставено следното прашање „Дали компаниите имаат изработењо свои планови за заштита на критичната инфраструктура“. Нема дилема дека соодветните планови ја даваат детелната шема за заштита на критичната инфраструктура. И покрај значењето мора да се нагласи дека загрижува познавањето, односно непознавањето на важноста на плановите кое е видливо во изјаснувањето на 58,98% од испотаниците. Интересно е само мал процент од 14,71% што сметаат дека планопвите се рационална претпоставка за остварување на поставените цели за заштита на критичната инфраструктура.

[143] Dragišić Z., *Bezbednosni menadžment,* Službeni glasnik i Fakultet bezbednosti, Beograd, 2007, str. 82

Графикон бр. 4 Планови за заштита на критичната инфраструктура



Приватната безбедност денес опфаќаат широк спектар на активности, односно компаниите за приватно обезбедување нудат различни видови услуги на објектите од витално значење. Основното ниво на услуга вклучува безбедност на објектите, услуги на надзор, истражни услуги, сеопфатна процена на ризик и услуги за намалување на ризикот итн. Тоа значи дека улогата на приватното обезбедување во заштита на критичната инфраструктура е голем и се фокусира на обезбедување на највисокиот ранг на услуги кои во одредени држави вклучуваат и заштита на нуклеарни централи, брзо распоредување тимови за одговор при катастрофи и прекуморски воени мисии. Ова говори дека овој сектор има голема улога во заштитата и дека во целина достигнал зрелост во однос на обемот и разновидноста на услугите што ги нуди на пазарот.

За да се согледа каква е улогата на приватната безбедност во заштита на критичната инфраструктура во Македонија, на испитаниците им беше поставено идентично прашање. Интересно е да се потенцира дека големата улога веќе ја препознаваат голем број од испитаниците, односно на модалитетот многу голема и голема се изјасниле 18,27% и 42,31% или заедно над 60%. Ова говори дека

испитаниците се свесни за придонесот на приватната безбедност во заштита на критичката инфраструктура, во споредба со 28,37% од вкупниот број на испитаници кои сметаат дека приватната безбедност има мала незначителна улога што говори за непознавање на овој сегмент кој е клучен и суштински во заштита на критичната инфраструктура.

Графикон бр. 5 Улогата на приватната безбедност во заштита на критичната инфраструктура

За да се согледа дали се прават неопходните анализи во самите агенции од аспект на барањата и потребите на услуги, квалитетот на услугите, капацитетите итн.,, на испитаниците им беше поставено следното прашање: „Дали сметате дека компаниите кои вршат дејност приватно обезбедување во вид на давање услуги имаат капацитет да се справат со потенцијалните закани кои се насочени кон критичната инфраструктура“?. Интересно е да се констатира дека 22,33% од вкупниот број испитаници сметаат дека во нивните агенции за обезбедување имаат доволен капацитет за справување со потенцијалните закани, додека повеќе

од половина испитани испитаници или 50,49% сметаат дека ако се анализира квалитетот на услогите што ги нудат и дека тие секогаш се адекватни на потребите на клиентите, но посочија дека не се убедени целосно дека агенциите имаат капацитет за справување со сложени безбедносни закани, а 24,27% не се воопшто сигурни во можноста на агенциите. Од ова произлегува заклучокот дека постои секогаш можноста за надоградување и усовршување на бараната потреба на услуга што треба да биде и примарна грижа на самата агенција и примарна цел во нејзиното работење.

Графикон број 6. Приватното обезбедување и неговите капацитети во заштита на критичната инфраструктура

Во рамките на државата се вклучени бројни правни сбјекти кои остваруваат определена дејност. Секако за државата се важни сите субјекти но посебно место им припаѓа на компаниите кои се од витално значење за државата. За нивното работење секако дека треба да ја имаат потребната поддршка од државата, но исто така важно е да се напомене дека во одредени сфери заради комплементарноста, во други елементи заради комплексноста и важноста и компаниите сами межу себе се предодредени да соработуваат. Соработката е важна и повеќе од потребна особено кога треба да се постапува во сложени околности кои излегуваат и надвор од моќта на одреден субјект во постапувањето.

Менаџерите ја остваруваат соработката на два начина: прво, тие добро го потпомагаат координирањето преку адекватна организациона структура и избирање способни и извежбани поединци, понатаму преку објаснување на интегралните планови и програми кои подредените ќе ги извршуваат, како и воспоставување средства за определување дали плановите и програмите се извршени адекватно. Второ, тие треба да се убедени дека нивните подредени ги разбираат принципите на координирање и важноста на дејствување во согласност со нив.[144]

За да се согледа колку е важна соработката помеѓу економските оператори и приватното обезбедување на испитаниците им беше поставено прашање во исти контекст. Потребата за соработка ја препознаваат речиси 45% од вкупниот број испитаници, додека околу 23% сметаат дека е делумно важна. Ова само по себе говори дека најголем број испитаници ја воочиле важност за соработка и дека таа треба да се постави како доминантна организациона цел.

[144] Petit T., *Fundamentals of Management Coordination*, New York, 1975, стр. 52.

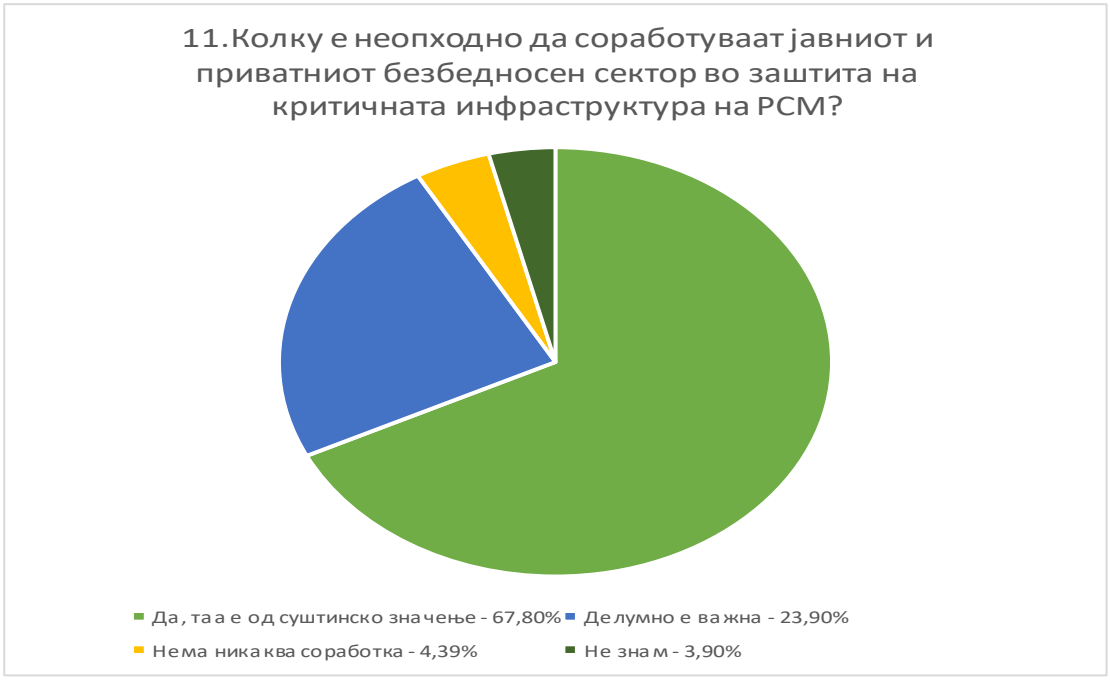
Графикон бр.7. Економските оператори и приватниот безбедносен сектор

Посебно важна варијабла и прашање, често истакнувана во анализите е прашањето „Колку е неопходно да соработуваат јавниот и приватниот безбедносен сектор во заштита на критичната инфраструктура?“. Во одредени држави ова прашање е регулирано со соодветни законски решенија, во коишто прецизно е регулирана работата и овластувањата на носителите на приватниот безбедносен сектор од каде произлегуваат и односите со државните органи што активно учествуваат во остварувањето на активностите од системот на обезбедување, меѓу кои е и полицијата. Во либералните држави практично полицијата не е во можност да ја гарантира безбедноста на секоја личност или да заштити сечиј имот. Секако полицијата има моќ, но нема монопол и апсолутни гаранции во однос на безбедноста.[145]

[145] Olschok H.,*Private Security in Germany and the Cooperation with the Police*, 2012, стр. 12.

Податоците од нашето истражување покажаа дека со огромно мнозинство дури 67,80 од испитаници се изјасниле дека соработката е од суштинско значење, додека 23,90% сметаат дека е делумно важна соработката, а 4,39% сметаат дека постои слаба соработка и координација меѓу агенциите за обезбедување и полицијата, што укажува на фактот дека оваа состојба може да доведе до редица негативни ефекти во процесот на планирање и остварување на активностите поврзани со безбедноста на земјата. Мал број испитаници претставници на агенциите за обезбедување сметаат дека постои одредена соработка.

Графикон бр.8. Јавна и приватна безбедност-соработка



Безбедност на виталните објекти е од примарно значење. Во рамките на остварување на безбедноста своја улога има и приватното обезбедување. Овие констатации се потврдени и во ставовите на испитаниците кои во најголем број сметаат 60,49 % дека со ангажирање и со проактивен однос ќе се зголеми повеќекратно безбедноста на објектите кои се од витално значење за државата, додека само незначителни 6,83 % не се убедени во тоа. Од ова произлегува дека сите напори треба да се насочени кон обуката и оспособувањето на работниците

за обезбедување за да можат адекватно да одговорат на реалната потреба на компаниите од витално значење.

Графикон бр. 9. Безбедноста на објектите од витално значење

ЗАКЛУЧОЦИ

1. Безбедноста како посакувана состојба претставува консолидација на аспектот на заштита на јавно добро, а во ситуација со изразени и нагласени безбедносни закани е дополнително збогатен со современиот тренд на приватизација на безбедноста во осигурување на безбедноста претставува процес на конспиративност, поврзување и трансформација.

2. Приватната безбедност е следствен елемент на промената на односот територија – овластувања – права. Таа е предмет на регулација и е резултат на нараснатата потреба за зголемена безбедност во ситуација кога има ерозија на употребата на моќ од страна на државата или се губи постепено монополот на принуда кој беше во ексклузивно права на државата единствено таа во минатото да спроведува конкретни овластувања во осигурување на безбедноста.

3. По истакнатата улога која ја добива приватната безбедност во сите општествени сфери е резултат на објективната реалност и претставува дел од вкупните напори да се оствари повисоко ниво на безбедност во ситуација кога јавната безбедност не може да биде сеприсутен феномен за да одговори на сите барања на физичките и правните лица и секако во интензивирање на безбедносните активности низ општествените сегменти бара поголема будност од сите безбедносни актери вклучувајќи ја и приватното обезбедување. Овие процеси во одредена мера се поттикнати од самата држава, кои се одговор на зголемената побарувачка, која пак произлегува од концептот на комодификација и постојаното чувство на изложеност на ризик.

4. Зголемената потреба од приватната безбедност значи и рационална претпоставка за фундаменталните политички цели кои се засноваат на идејата за осигурување на безбедноста како едно суштинско јавно добро кое има висока употребна вредност.

5. Во ситуација на зголемени безбедносни закани тоа е јасен показател за давање на заеднички одговор на сите безбедносни актери што од друга страна значи и давање на интегриран безбедносен одговор и намалувањето на диспаритетот јавна безбедност-приватни безбедносни агенции во осигурувањето

на мирот и поредокот, контрола на криминалот и владеење на правото, како и одржување на внатрешната безбедност.

6. Анализата супстанционално потврди дека границите меѓу економијата и безбедноста се многу тесни. Главната цел на изведувачите е да ја исполнат мисијата дадена од клиентот кој склучил договор со нив. Приватните компании за обезбедување се фокусираат на комплексната динамика на осигурување на капиталот што се генерални барања на клиентот. Значи, приватниот безбедносен сектор, и вработените се водени од идејата за потребата да задоволат клиент во замена за финансиска награда.

7. Вкупното работење во приватниот безбедносен сектор мора да се базира на етичноста, почитувањето на човековите права итн. Оттука напорите се насочени кон зајакнување на активностите преку спроведување на воспитни мерки, како и механизми за следење и отчетност за да се намалат кршењата на човековите права и обезбедуваат подобра човечка безбедност.

8. Анализата потврди дека концептот на приватната безбедност во заштита на критичната инфраструктура има огромно влијание затоа што тој е најнепосредно и најекспониран во заштитата на критичните објекти кои се од витално значење односно вклучува широка платформа за реализација и конкретизација на одредени задачи за подобрување и заштита на виталните инфраструктурни објекти.

9. Се потврди хипотезата дека критичната инфраструктура во нашата држава е релативно нова област која се уште е недоразвиена од аспект на поимање, етаблирање, поставување на соодветна рамка за идентификување и немање на јасна регулатива со која ќе се утврди местото и улогата во општествената стварност.

10. Истражувањето супстанционално потврди дека концептот на критичната инфраструктура е исклучително сериозно и сеопфатно прашање кое бара темелна анализа за да се даде одговорот на основното прашање „Која критична инфраструктура е услов за ефикасно функционирање на државата“?. Дополнително прашањето е уште поспецифично ако се знае дека треба да се

унифицира имплементацијата на секторскиот и на потсекторскиот пристап кој е важен катализитор во вкупбите односи и работењето.

11. Анализиата поптврди дека во целокупниот концепт на критичната инфраструктура свое место и улога имаат сите активни чинители од економските оператори, до министерствата, агенциите и дирекциите што функционираат во рамките на државата; понатаму локалните власти; безбедносниот сектор и во негови рамки приватното обезбедување, како и поширокатa јавност.

12. Критична инфраструктура како што потврди и самото истражување се соочува со бројни предизивици кои во денешни околности може слободно да се каже дека растат експоненцијално. Тоа е резултат на променетата природа на околностите кои се и јасен сигнал за поголема безбедност и аналогно на тоа за зголемено барање на безбедност која е исправена со сериозни закани, кои ја намалуваат отпорноста на системите на критичната инфраструктура.

13. Современите закани и ризици по критичната инфраструктура ги стават на тест системите дали можат да одговорат на современите предизвици и поттикнуваат нови пристапи кои се во функција на остварување на повисоко нмиво на заштита, а истовремено ги намалуваат и ги ограничуваат ризиците што доведува до нивна редукција. Ова бара постојана предвидливост и развиивање на систем кој треба да ги сведе на миниумум заканите што претставува скапа работа. Затоа особено е важна соработката на сите инфраструктурни оператори заедно со безбедносните актери за да се намалат несаканите последици предизвикани од штетни појави.

14. Инфраструктурата како осетлива и суштински важна артерија во општеството бара постоење на кохерентен пристап и постоење на соодветни анализи, процени итн., кои ќе ги идентификувваат заканите и кои ќе значат дејствување на превентивен план за да се намали веројатноста за појава. Оваа манифесност е секако важен елемент на горесинтетизираната анализа.

15. Анализата ја потврди каузалноста на мерките и активностите што се применуваат во заштита на критичната инфраструктура наспроти плановите кои ги имаат компаниите кои се всушност и логичен след на постапки како треба да се постапува во исклучителни ситуации.

16. Заштитата на критичната инфраструктура е предуслов за опстанок на самата држава и затоа има инструментална и средствена вредност. Тоа подразбира дека критичната инфраструктура е и суштински важна и значајна за непречено фунционирање на економијата и на општеството во целост, а нејзиното нарушување ќе предизвика сериозни последици на економијата и на државата што значи дека ќе се наруши непреченото функционирање на базичните елементи на општеството.

17. Истражувањето потврди дека заканите врз критичната инфраструктура како современиот тероризам, кражби, вандализми итн., се извесни и во ситуација на перманентна изложеност на вакви безбедносни закани треба да се напрви систем кој сам по себе треба да одговори во ситуацијата или да нагласи подготвеност и одговор на потенцијалните закани врз критична инфраструктур.

18. Анализата супстенционално потврди дека недостасува во македонската држава соодветна стратегија за интегриран пристап во заштитата и дефинирањето на обврските и должностите на сите субјекти во земјата кои се инволвирани во овој процес. Ваквата проактивна заложба треба да овозможи брза реакција, но и спроведувањето на мерките за заштита на виталните објекти.

ЛИТЕРАТУРА

1. Andrew Alexandra, Baker D. P, and Caparini M.: Private Military and Security Companies: Ethics, Policies and Civil-Military Relations, 2008.
2. Abazović D. M., Državna bezbjednost-Uvod i temeljni pojmovi, Fakultet krimminalističkih nauka, Sarajevo, 2002.
3. Ahić J., Sistemi privatne sigurnosti, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo, 2009.
4. Andersen, L., R. The HIPPO in the room: The pragmatic push-back from the UN peace bureaucracy against the militarization of UN peacekeeping, *International Affairs*, Volume 94, Issue 2, March 2018.
5. Auerswald, E., P., Branscomb, M., L., LaPorte, T. (2006) Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability. Cambridge University Press
6. Austin, R., DiSera, D., Brooks, T. (2016). GIS for Critical Infrastructure Protection. Boca Raton: CRC Press,
7. Avant, D, Haufler, V (2012) Transnational organizations and security. Global Crime 13(4).
8. Бакрески О., Милошевска Т., Алчески Ѓ., Заштита на критична инфраструктура, Скопје, 2017
9. Бакрески О., Триван Д. и Митевски С., *Корпорациски безбедносен систем*, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012.
10. Бакрески О., Даничиќ М, Кешетовиќ Ж. и Митевски С., *Приватна безбедност – теорија и концепт*, Комора на Република Македонија за приватно обезбедување, Скопје, 2015.
11. Бакрески О., Ахиќ Ј. и Наѓ И., Приватен безбедносен сектор во Југоисточна Европа, Комора на РСМ за приватно обезбедување, Скопје, 2019.
12. Бакрески О. Славески С. и Гацоски Ж., *Безбедноста низ призмата на приватната безбедност*, Комора на РМ за приватно обезбедување, Скопје, 2018.
13. Бакрески О., Безбедносни системи, Филозофски факултет, Скопје, 2018.
14. Baggett, R. K., & Simpkins, B. K. (2018). *Homeland security and critical infrastructure protection* (2nd ed.). Santa Barbara, CA: Praeger Security International.
15. Bailes, J., K. A. & Frommelt, I. (2004) Business and Security. Public-private Sector Relationships in a New Security Environment. Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/files/books/SIPRI04BaiFro/SIPRI04BaiFro.pdf
16. Baljak, M. The Role of Private Security Agency in the 21st Century. DOI: 10.7251/DEFEN1501002Bhttps://pdfs.semanticscholar.org/a281/43f22ce9a40028eed8a78febe684163600f2.pdf
17. Baljak, M. Uloga Privatnih Bezbednosnih Agencija u 21 Veku. Defendologija GODINA XVIII, BROJ 36, 2015. DOI: 10.7251/DEFSR1501002B
18. Ball, D., & Ball - King, L. (2013). Safety management and public spaces: Restoring balance. *Risk Analysis, 33*(5)
19. Bayley, D, Shearing, C (2001) The New Structure of Policing: Description, Conceptualization and Research Agenda. Washington, DC: National Institute of Justice. https://journals.sagepub.com/doi/10.1177/1362480614527303
20. Bhushan N. (2020) Critical Infrastructure: Defense Industrial Base Sector. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_123-1

21. Bhushan N. (2020) Critical Infrastructure: Defense Industrial Base Sector. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham.https://doi.org/10.1007/978-3-319-69891-5_123-1
22. Button, M., Stiernstedt, P. (2018) Comparing private security regulation in the European Union. Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK https://core.ac.uk/download/pdf/44341285.pdf
23. Button, M., Stiernstedt, P. (2020) The Evolution of Security Industry Regulation in the European Union. [chapter] Researchgate. DOI: 10.4324/9781351010375-6
24. Calazans, E. (2016) The Implications Under International Law of Doing Business in War. Cambridge Scholars Publishing. https://www.cambridgescholars.com/download/sample/63234
25. Cameron, L. (2006) Private Military Companies, Their Status Under International Humanitarian Law and its Impact on Their Regulation. International Review of the Red Cross. Volume 88, Number 863. https://www.icrc.org/en/doc/assets/files/other/irrc_863_cameron.pdf
26. Cassidy K. (2019) Corporate Security (Structure, Roles, Duties). In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_19-1
27. Charles, C., A. (2020) Security Guards: Authority and Power. Encyclopedia of Security and Emergency Management. DOI: 10.1023/A:1008701310152
28. Coleman, L. (2017), The Power of Resilience Yossi, Sheffi The MIT Press, Cambridge MA, 2015, 14 pp. . J Contingencies and Crisis Management, 25: 114-115. https://doi.org/10.1111/1468-5973.12167
29. Cook, P, MacDonald, J (2011) Public safety through private action: An economic assessment of BIDS. The Economic Journal 121(552)
30. De Vard, J. (1999) The Private Security Industry in International Perspective. European Journal on Criminal Policy and Research 7(2)
31. Dekker, A., H., Colbert, B. (2004) Scale-Free Networks and Robustness of Critical Infrastructure Network. chool of Information Technology, Deakin University.
32. Dekker, H., A. (2005) Simulating Network Robustness for Critical Infrastructure Networks. Defence Science and Technology Organisation Department of Defence, Canberra ACT 2600.
33. Demchak, C., C. (2012) Resilience and Cyber Space: Recongizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI).journal of Comparative Policy Analysis: Research and Practice> Volume 14 2012 Issue 3. https://doi.org/10.1080/13876988.2012.687619
34. Dombrowski, P., Demchak, C., C. (2015) Thinking Systematically About Security and Resilience in an Era of Cybered Conflict. Cybersecurity Policies and Strategies for Cyberwarfare Prevention. DOI: 10.4018/978-1-4666-8456-0.ch014
35. Dupont, B. (2014). Private security regimes: Conceptualizing the forces that shape the private delivery of security. *Theoretical Criminology*, *18*(3), 263–281. https://doi.org/10.1177/1362480614527303
36. Duzgun, S. (2019) F-N Curves, Social Aspects and Risk Acceptability. Middle East Technical University, Ankara.
37. Egan, J., M. (2007) Anticipating Future Vulnerability: Defining Characteristics of Increasingly Crtitical Infrastructure-Like Systems. Journal of Contingencies and Crisis Management. Volume 15 Number 1. March 2007.
38. Fekete, A., Fiedrich, F. (2018) Urban Disaster Resilience and Security: Addressing Risks in Societies. The Urban Book

39. Fiott, D. (2020) European Union Institute for Security Studies. The CSDP in 2020. The EU's Legacy and Ambition in Security and Defense.
40. Hemme, C. (2015) Critical Infrastructure Protection: Maintenance is National Security. Journal of Strategic Security. Volume 8, No. 5. DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1471
41. Holmes, F. (2014) The importance of Critical Infrastructure Protection. Australian Security Magazine.
42. Holmquist, C. (2005) Private Security Companies: The Case for Regulation. SIPRI Policy Paper no. 9
43. Hurst W., Merabti M., Fergus P. (2014) A Survey of Critical Infrastructure Security. In: Butts J., Shenoi S. (eds) Critical Infrastructure Protection VIII. ICCIP 2014. IFIP Advances in Information and Communication Technology, vol 441. Springer, Berlin, Heidelberg.
44. Isles, A. (2018) Government and the Private Sector Share Responsibility for Secure Infrastructure. Security Infowatch. [article] sep 20th 2018
45. J. R. Laracy and N. G. Leveson, "Apply STAMP to Critical Infrastructure Protection," *2007 IEEE Conference on Technologies for Homeland Security*, Woburn, MA, 2007, pp. 215-220, doi: 10.1109/THS.2007.370048.
46. Jaafar, M., N. (2012) Identifying the Criteria for Critical Infrastructure Selection. International Real Estate Conference Kuala Lumpur, Malaysia, 9-10 June, 2012
47. Jensen, C., R. (2020) Security Workers Classified as Essential Critical Infrastructure Workers. Security Today. Mar 24, 2020 [article]
48. Klopfer, F., van Amstel, N. (2016) Private Security in Practice: Case Studies from South East Europe. DCAF, Geneva.
49. Le Coze, J.-C. (2015), Was Charles Perrow Right for the Wrong Reasons?. J Contingencies & Crisis Man, 23: 275-286. doi:10.1111/1468-5973.12090
50. Lee S.. (2019) Security: Private. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_242-1
51. Lewis, T. (2014). *Critical infrastructure protection in homeland security: Defending a networked nation* (2nd ed.). Hoboken, NJ: Wiley.
52. Linkov, I., Wenning, R., J., Kiker, G., A. (2007) Managing Critical Infrastructure Risks: Decision Tools and Applications for Port Security. NATO science for peace and security series. Series C, Environmental security, 2007.
53. Lippert, R, Walby, K, Steckle, R (2013) Multiplicities of corporate security: Identifying emerging types, trends and issues. Security Journal 26(3)
54. Litavski, J. (2012) Izazovi Privatnog Sektora Bezbednosti u Novom Veku. Tromesecnik Centra za Evroatlantske Studije. Novi vek, broj 2.
55. Lopez, J., Setola, R. (2012) Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defense. January 2012. Springer-Verlag.
56. Louise K. Comfort (2012) Designing Disaster Resilience and Public Policy: Comparative Perspectives, Part II, Journal of Comparative Policy Analysis: Research and Practice, 14:3, 199-201, DOI: 10.1080/13876988.2012.696440
57. Luiijf, E., Klaver, M. (2019) Resilience Approach to Critical Information Infrastructures. Springer International Publishing.
58. Lum, C., Kennedy, L. W., & Sherley, A. (2006). Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research. *Journal of Experimental Criminology, 2*(4).
59. Madej, M., Pajak, M. (2019): Road Transport of Dangerous goods in Poland. Risk Analysis. Safety and Security in Traffic. Promet – Traffic & Transportation, Vol. 31, 2019, No. 5

60. Maggio, E. (2009) Private Security in the 21st Century: Concepts and Applications. NYIT Center for Security Disaster and Response. Jones and Bartlett Publishers.
61. McCrie, R. (2006). A history of security. In M. Gill (Ed.), *Handbook of security*. London: Palgrave Macmillan.
62. McFate, S. (2019) Mercenaries and War: Understanding Private Armies Today. National Defense University Press, Washington DC. https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/mercenaries-and-war.pdf
63. Mihaljević, B. (2018) Protection of Critical National Infrastrucutre: Challenges for the Private Security Sector. Ann. Disaster Risk Sci. 2018, 1, 47-56
64. Moteff, J.D., & Parfomak, P.W. (2004). Critical Infrastructure and Key Assets: Definition and Identification.
65. Mulowayi, E., et al.: (2017) The Influence of Critical Infrastructure Interdependencies on Post-Disaster Reconstruction: Elements of Infrastructure Interdependency that Impede the Post-Disaster Recovery Effort. http://www.arcom.ac.uk/-docs/proceedings/5c0fdbc531a915738ce7dcc9bfa2ade9.pdf
66. Nadai, L. Padanyi, J. (2018) Critical Infrastructure Protection Research: Results of the First Critical Infrastructure Protection Research in Hungary. Springer International Publishing.
67. Nemeth, C. (2012) Private Security and the Law. Fourth Edition. Elsevie
68. Newbill, C. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies, 26*(2), 761-780. Retrieved November 4, 2020, from https://www.jstor.org/stable/10.2979/indjglolegstu.26.2.0761
69. Norman, T., L. (2016) Risk Analysis and Security Countermeasures Selection. Second Edition. CRC Press, Taylor & Francis Group, Boca Raton, Fl. https://scholar.google.com/scholar?cluster=10101363799213031995&hl=en&as_sdt=2005&sciodt=0,5
70. Page, M. Rynn, S., Taylor, Z., Wood, D. (2005) SALW and Private Security Companies in South Eastern Europe: A Cause or Effect of Insecurity? Safeworld.
71. Rød, B., Lange, D., Theocharidou, M., Pursiainen, C. (2020) From Risk Management to Resilience Management in Critical Infrastructure. ASCE Library. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795 2020/11/19
72. Selva, J. (2020) Abraham Maslow, His Theory and Contribution to Psychology. Positive Psichology. https://positivepsychology.com/abraham-maslow/
73. Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-69891-5_123-1.
74. Shearing, C., D., Stenning, C. P.(1981) Modern Private Security: Its Growth and Implications. Crime & Justice Vol. 3. The University of Chicago Press. https://www.jstor.org/stable/1147380
75. Silveti, O., Garcia, S. (2020) Industry Revenue of Private Security Activities in France from 2012-2024. Statista Business Services.
76. Simpkins B.K. (2019) Critical Infrastructure: Critical Manufacturing Sector. In: Shapiro L., Maras MH. (eds) Encyclopedia of Security and Emergency Management. Springer, Cham.https://doi.org/10.1007/978-3-319-69891-5_61-1
77. Singer, P., W., Friedman, A. (2014) Cyber Security and Cyber War: What Everyone Needs to Know. Oxford University Press. https://www.cybersecurityandwar.com/
78. Stajic, Lj. (2019) Pravni okvir private bezbednosti u svetlu savremenog shvatanja pojma bezbednosti
79. Sullivant, J. (2016). *Building a corporate culture of security*. Waltham: Butterworth-Heinemann.

80. Sveinsdottir, T. *et al*. (2016) Taxonomy of Security Products, Systems and Services. CRISP. Evaluation and Certification Schemes for Security Products.
81. Van Buuren, J. (2009) D.3.3. 'A report on the ethical issues raised by the increasing role of private security professionals in security analysis and provision' Department of Governance Studies. VU University Amsterdam.
82. Van der Merwe, S., Biggs, R., & Preiser, R. (2018). A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems. *Ecology and Society, 23*(2). doi:10.2307/26799110
83. Vaughan, G. (2018) Critical Infrastructure Public-Private Partnerships. Volume 14, Issue 1. Campbell University.
84. Viira, T. (2018) Lessons Learned: Critical Information Infrastructure Protection: How to protect critical information infrastructure. IT Governance Publishing. DOI: 10.2307/j.ctt1xhr7hq
85. Viira, T. (2018). Critical Activities and Required Resources. In *Lessons Learned: Critical Information Infrastructure Protection: How to protect critical information infrastructure* (pp. 21-23). Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Retrieved November 7, 2020.
86. Vukadinovic, R. (1999) Challenges to Security in Southeast Europe. South-East Europe Studies. Politicka misao Vol. XXXVI No. 5 pp.3-14
87. Weick, E., K. Enacted Sensemaking in Crisis Situations. University of Michigan, USA. Journal of Management Studies. 25:4 July 1988.

Законски акти и други документи:

88. A Framework for Establishing Critical Infrastrucutre Resilience Goals. Final Report and Recommendations by the Council. National Infrastructure Advisory Council.
89. Staff Working Document (2019) 308
90. CoESS Welcomes Update of the EU Security Union Strategy.
91. Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program. Agronne National Laboratory.
92. Council Directive3 2008/114/ EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection of 2008.
93. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are on the Way, but Challenges Remain. Government Accountability Office, 2007.
94. Federal Act on Private Security Services Provided Abroad. Federal Department on Foreign Affairs. Schweizerische Eidgenossenschaft.
95. Federal Ministry of the Interior, Building and Community. Critical Infrastructure Protection. [article]
96. Green Paper on a European programme for critical infrastructure protection/* COM/2005/0576 final
97. Guidelines on the Use of Armed Security Services from Private Security Companies Annex A - Statement of Works. United Nations Security Management System, United Nations Department for Safety and Security. 08.11.2012.
98. IACP and COPS. (2004). *National policy summit: Building private security/public policing partnerships to prevent and respond to public disorder*. Alexandria: International Association of Chiefs of Police.
99. International Convention Against the Recruitment, Use, Financing and Training of Mercenaries. New York, December 4, 1989. United Nations Treaty Collection.

100. NATO Energy Security Centre of Excellence. Recommendations on the Importance of Critical Energy Infrastructure (CEI) Stakeholder Engagement, Coordination and Understanding of Reponsibilities in Order to Improve Security. Vilnus, 2018.https://enseccoe.org/data/public/uploads/2018/04/d1_2018.04.23-recommendations-on-the-importance-of-critical-energy.pdf
101. OECD (2019), *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://doi.org/10.1787/02f0e5a0-en.
102. Proclamation on Critical Infrastructure Security and Resilience Month, 2020. Infrastructure and Technology. October 30 2020. The White House Proclamation. https://www.whitehouse.gov/presidential-actions/proclamation-critical-infrastructure-security-resilience-month-2020/
103. Resolution On Private Security Companies.European Parliament. https://www.europarl.europa.eu/doceo/document/A-8-2017-0191_EN.html
104. Sixt European Union Security Summit White Paper. The Security Continuum in the New Normal. Rome, 10 October 2019. https://www.coess.org/newsroom.php?news=CoESS-speaks-at-EU-High-level-Counter-UAS-Conference
105. United Nations Security Management System. Security Policy Manual. United Nations Department of Safety and Security. https://www.un.org/undss/sites/www.un.org.undss/files/docs/security_policy_manual_spm_e-book_as_of_29_nov_2017_0.pdf
106. United States: The National Strategy for Homeland Security – Protecting Critical Infrastructures and Key Assets. https://www.resdal.org/Archivo/usa-home-prote.htm

Интернет извори и публикации

107. Bayesian Network. Introduction to Algorithms for Data Mining and Machine Learning. 2019. https://www.sciencedirect.com/topics/mathematics/bayesian-network
108. Beyond Covid-19: Private Security Services Call for a Political Action. https://www.coess.org/newsroom.php?news=Beyond-COVID-19-Private-Security-Services-call-for-Political-Action
109. Bombing, States and Peoples in Western Europe 1940-1945. Centre for the Study of War, State and Society. University of Exeter.https://humanities.exeter.ac.uk/history/research/centres/warstateandsociety/projects/bombing/germany/
110. Brexit: Common Security and Defence Policy missions and operations. Chapter 4: Third Country Participation in CSDP Missions and Operations. https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/132/13207.htm
111. Capital Intensive Definition. Wall Street Mojo. https://www.wallstreetmojo.com/capital-intensive/
112. Critical Infrastructure – Cooperation with the Private Sector. Rządowe Centrum Bezpieczeństva. http://rcb.gov.pl/en/critical-infrastructure-cooperation-with-the-private-sector/
113. Critical Infrastructure Book. Professional Security Magazine [online] 05th January 2018. https://www.professionalsecurity.co.uk/news/commercial-security/critical-infrastructure-book/

114. Critical Infrastructure Book. Professional Security Magazine [online] 05th January 2018.https://www.professionalsecurity.co.uk/news/commercial-security/critical-infrastructure-book/
115. Critical Infrastructure Protection Market - Growth, Trends, and Forecasts (2020 - 2025)- https://www.reportlinker.com/p05815019/?utm_source=GNW https://www.globenewswire.com/news-release/2020/07/23/2066822/0/en/Critical-Infrastructure-Protection-Market-Growth-Trends-and-Forecasts-2020-2025.html
116. Critical Infrastructure Protection. Governor's Office of Emergency Services.https://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/critical-infrastructure-protection
117. Critical infrastructure Protection. Science Direct. https://www.sciencedirect.com/topics/computer-science/critical-infrastructure-protection
118. Critical Infrastructure Protection: Home. Campbell University.https://guides.lib.campbell.edu/HSEC340
119. Differences Between Private Investigators and Security Guards. National Investigative Training Academy Incorporated. https://investigativeacademy.com/differences-private-investigators-security-guards/
120. From Risk Management to Resilience Management in Critical Infrastrucutre. https://ascelibrary.org/doi/10.1061/%28ASCE%29ME.1943-5479.0000795
121. Global Customized Private Security & Investigative Solutions. Critical Infrastructure Security. Lasorsa & Associates. https://www.lasorsa.com/wp-content/uploads/2019/08/LA-Critical-Infrastructure-Brochure.pdf
122. Global Private Security Service Market 2019 by Companies, Regions, Types and Application Forecasts to 2024. https://www.absolutereports.com/global-private-security-service-market-14407086
123. Hellespont. https://www.britannica.com/place/Dardanelles
124. Holmes, F. (2014) The Importance of Critical Infrastructure Protection. Australian Security Magazine. Asia Pacific Security, Australian Security, Frontline Security. https://australiansecuritymagazine.com.au/the-importance-of-critical-infrastructure-protection/
125. How Mercenaries are Resphaping the Battlefield. https://www.aljazeera.com/program/counting-the-cost/2019/11/24/how-mercenaries-are-reshaping-the-battlefield/
126. Information Security. Symantec Product Categoroies. https://securitycloud.symantec.com/cc/#/landing
127. Inspection Related to Private Security and Detective Affairs. Republic of Croatia Ministry of Interior. https://mup.gov.hr/aliens-281621/inspection-affairs/inspection-related-to-private-security-and-detective-affairs/281631
128. Interagency Security Committee 2019 Annual Report. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency CISA https://www.cisa.gov/sites/default/files/publications/ISC_2019_Annual_Report_508.pdf
129. Is Private Security an Essential Service? New Zealand Security Magazine, march 24, 2020. [article] https://defsec.net.nz/2020/03/24/covid-19-alert-levels/
130. Market Scope and Structure Analysis. Allied Market Research. https://www.alliedmarketresearch.com/private-security-market-A06346
131. National Security: Breakthrough in Research and Practice: Information Management Association USA. IGI Global. 2019 O. Reg. 210/11: GENERAL. Ministry of Infrastructure, Ontario. https://www.ontario.ca/page/ministry-infrastructure
132. Ocena Stanja Privatnih Bezbednosnih Kompanija. Kosovar Center for Security Studies, 2009. http://qkss.org/web/images/content/Ocena%20stanja%20privatnih%20bezbednosnih%20kompanija.pdf
133. Private Security Companies (PSCs). Small Arms Survey. [article]http://www.smallarmssurvey.org/armed-actors/private-security-companies.html
134. Private Security Companies in the Western Balkans (2014-2017). Kosovar Center for Security Studies. http://www.qkss.org/en/Programet/Private-security-companies-in-the-Western-Balkans--385

135. Private Security Industry Outlook. https://blog.signal88.com/franchising/private-security-industry-outlook
136. Private Security Joint Declaration: Ensuring Business Continuity and Protection of Workers in the Covid-19 Panemic. Uni Europa Global Union. Friday, May 8, 2020. https://www.uni-europa.org/2020/05/private-secruity-joint-declaration-ensuring-business-continuity-and-protection-of-workers-in-the-covid-19-pandemic/
137. Private Security Services. 17th Edition. https://www.freedoniagroup.com/industry-study/private-security-services-3764.htm
138. Privatna bezbednost. Beogradski Centar za Bezbednosnu Politiku.https://bezbednost.org/teme/bezbednosna-politika-srbije/privatna-bezbednost/
139. Report of the Liberia National Dialogue on Security Sector Reform 2005. The International Policy Institute. King's College London. Monrovia, Liberia. https://issat.dcaf.ch/Learn/Resource-Library2/Policy-and-Research-Papers/Report-of-the-Liberia-National-Dialogue-on-Security-Sector-Reform
140. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. US Department of Energy. https://publications.anl.gov/anlpubs/2013/07/76797.pdf
141. Russia, Wagner Group Continue Military Involvment in Syria. July 24, 2020. Defense News. https://www.defense.gov/Explore/News/Article/Article/2287821/russia-wagner-group-continue-military-involvement-in-libya/
142. Russian Oil Deals in Syria Linked to "Putun's Chef" – Novaya Gazeta. The Moscow Times. Jan 20, 2020. [article] https://www.themoscowtimes.com/2020/01/20/russian-oil-deals-in-syria-linked-to-putins-chef-novaya-gazeta-a68964
143. Secure the Route to Future Proof, Robust Solutions for New and Upgraded Assets. Royal Haskoning DHV https://www.royalhaskoningdhv.com/en-gb/capital-intensive-industry
144. Security and Defense. Southeastern Europe Security Center. https://sesecuritycenter.org/
145. Security Management. https://www.asisonline.org/security-management-magazine/monthly-issues/archive/2020/october/