Оливер БАКРЕСКИ
Тања МИЛОШЕВСКА

БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И КРИТИЧНАТА ИНФРАСТРУКТУРА

БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И КРИТИЧНАТА ИНФРАСТРУКТУРА Оливер Бакрески, Тања Милошевска

9 786086 671501

Оливер БАКРЕСКИ
Тања МИЛОШЕВСКА

БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И КРИТИЧНАТА ИНФРАСТРУКТУРА

Оливер БАКРЕСКИ
Тања МИЛОШЕВСКА

БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И КРИТИЧНАТА ИНФРАСТРУКТУРА

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

БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И КРИТИЧНАТА ИНФРАСТРУКТУРА

Рецензенти

Проф. д-р Митко БОГДАНОСКИ
Воена академија „Генерал Михаило Апостолски“− Скопје

Проф. д-р Денис ЧАЛЕТА
Институт за корпоративни безбедносни студии − Љубљана

Издавач
Дирекција за безбедност на класифицирани информации

Графички уредник
Билјана Иванова

Лектор
д-р Жанет Ристоска

Печати
СТУДЕНТСКИ СЕРВИС ДОО Скопје

Тираж: 300

CIP - Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски”, Скопје

007:004.056.5(497.7)
343.9:004.7
004.773.7.056.53

БАКРЕСКИ, Оливер
Безбедноста на информациите и критичната инфраструктура / Оливер Бакрески, Тања Милошевска. - Скопје : Дирекција за безбедност на класифицирани информации, 2021. - 214 стр. : илустр. ; 21 см

Фусноти кон текстот. - Библиографија: стр. 195-214

ISBN 978-608-66715-0-1

1. Милошевска, Тања [автор]
а) Критична инфраструктура -- Безбедносни системи -- Заштита -- Македонија
б) Информации -- Сајбер напади -- Безбедносни системи -- Заштита -- Македонија в) Компјутерски криминал -- Безбедносни системи

COBISS.MK-ID 54112773

СОДРЖИНА

ПРЕДГОВОР

Прашањата коишто се поврзуваат со безбедноста, информациите, критичната инфраструктура итн., како и начините на нивна заштита се постојано отворени прашања за кои се бараат нови одговори, а колку безбедноста на информациите и критичната инфраструктура се значајна и сложена тема најдобро говори податокот дека ова прашање ги заинтересирало повеќе истражувачи. Приодот кон безбедноста на информациите предупредува на нешто што е премногу важно и сè останато е неважно, што секако не е оправдано. Сепак, повеќедимензионалноста и сложеноста на проблемот поврзан со информациите може да се симплифицира со симболиката дека тие се како „неодреден симбол" кој може, но и не мора да има некое значење, но се неопходно важна тема.

Значи, анализирањето на сегментот на прашања поврзани со информациите и безбедноста е комплексна и тешка работа бидејќи тие се одликуваат со голема сложеност, специфичност, меѓузависност и противречност. Поради тоа, проучувањето на овој сегмент треба да се заснова на нивно целосно разбирање и темелно согледување на состојбите во коишто се развиваат и во коишто функционираат, за да не се соочиме со каква било импровизација и парцијализам.

Оттука, денес основното прашање не е: „Дали има потреба од информации?", туку прашањето: „Какви информации се потребни?", и уште поважно е прашањето „Како да се обезбедат информациите, односно како да се заштитат како ресурс важен за критичната инфраструктура"?. Ова е особено важно ако се земе предвид фактот дека новите безбедносни закани кои се појавуваат во различни сложени околности и под одредени специфични услови имплицираат потреба за информации и приспособувања на новата безбедносна средина.

Во основа, безбедноста на информациите е условена од две конституирачки и профилирачки компоненти: прво, резимирачка енумеративна ретроспективна реконструкција на концептот на безбедноста за да се согледаат концептуализациските стипулации на идиомот безбедност, и второ, што е особено важно за нас, дека истражувањето за безбедноста на информациите мора да биде системски засновано на поимната конфигурација на референтната категорија информација.

Сложеноста, променливоста и меѓусебната условеност на безбедноста и на информациите е доволна причина што на едно место се анализирани овие два сегмента. Анализата ќе биде поткрепена со многу прашања, и аналогно на тоа, многу одговори поврзани со безбедноста, со информациите, со нивната заштита, со нивниот придонес во функционирањето на безбедносниот систем, со условите во кои се остварува националната безбедност, итн. Со ваквиот пристап се изразува нашата определба овие проблемски аспекти да се доближат до вработените во безбедносните институции, и особено до вработените во Дирекцијата за безбедност на класифицирани информации, но книгата со начинот на кој ја идентификува суштината на самиот истражувачки проблем ќе ја направи привлечна и за сите оние кои директно или индиректно се занимаваат со прашањата на безбедноста.

Пред да се соочи книгата со јавноста, им должиме голема благодарност на рецензентите проф. д-р Митко Богданоски и проф. д-р Денис Чалета, кои со своите сугестии придонесоа за квалитетот на книгата. Им изразуваме благодарност на сите оние кои имаа значаен придонес во создавањето и публикувањето на ова дело. Особена благодарност упатуваме на Дирекцијата за безбедност на класифицирани информации, којашто ја поддржа оваа публикација и овозможи да биде достапна до читателите.

Авторите

ВОВЕД

Проучувањето на основните концептуални репери во интерпретативната безбедносна парадигма ги конкретизира и ги валоризира напорите преку систематска анализа да се дојде до сите аспекти на безбедноста, информациите и критичната инфраструктура со што ќе се овозможи да се создаде јасна, кохерентна и систематски комплетна слика за безбедноста на информациите и критичната инфраструктура.

Според нивото, квалитетот и дијапазонот на тематско-проблемската елаборација и експликација на третираниот проблем, оваа книга може да се разгледува низ неколку сегменти. Прво, сегментот на прашања врзан за безбедноста кој се гледа како концепт кој е поврзан за граѓаните и за државата, а не како концептот сам за себе, бидејќи безбедноста како синтетизирана и воопштена функција е насочена кон осигурување на вредностите на луѓето или социјалните групи, и особено кон природата и интензитетот на заканите кон тие вредности. Второ, студијата главно се базира на критичната инфраструктура. Критичната инфраструктура е синтетизирана и воопштена преку процесите, системите, објектите, технологиите, мрежите, средствата и услугите кои се неопходни за здравјето на граѓаните, за економската благосостојба, за безбедноста и за ефикасното функционирање на владата. Трето, како појдовни елементи се земени информациите и определени секвенци кои произведуваат специфични ефекти. Значи, третиот пристап се базира на заканите и на заштитата на критичната инфраструктура. Демонстрирањето на подробниот опис на заканите како текст и контекст, и контекстуално – текстуалната метафорика за заштита на критичната инфраструктура се презентирани на доследно ниво и квалитет. На заштита на критичната инфраструктура се гледа како на потреба да се заштитат виталните инфраструктури и дека подготвеноста, реакцијата и обновувањето по катастрофи предизвикани од определени закани се врвни приоритети. Прекините во критичната инфраструктура може да резултираат со катастрофално губење животи, да предизвикаат неповолни економски ефекти и значителна штета во однос на довербата на јавноста. Ова ни овозможи аналитичко согледување на суштинските елементи на заштитата на критичната инфраструктура, но беа опфатени и други аспекти кои се однесуваа на критичната инфраструктура,

особено разработката на индикативната листа на сектори. Четвртиот пристап се осврна на прашањето за информациите и безбедноста на информациите. Состојбите во областа на безбедноста на информациите се интерпретирани врз основа на релевантна литература. Ваквиот пристап преку внатрешната структура на книгата ја обезбеди потребната хоризонтална и вертикална симетрија и хармонија. Петтиот пристап се базира на сајбер-безбедноста. Така, се согледува општествената реалност низ призмата на сајбер-безбедноста и сајбер-заканите, се апострофираат определени специфични димензии, се респектира комплексноста на проблемите што се истражуваат и се поврзани со сајбер-безбедноста, но и се нагласуваат посебните научни аспекти.

глава I

БЕЗБЕДНОСТ

1. ОПШТО ЗА БЕЗБЕДНОСТА

Безбедноста како витална човекова потреба и клучен општествен и државен интерес се смета за сложен феномен како во поглед на правилното поимање и толкување, така и во поглед на практичното остварување.[1]

Во обичниот живот кога го употребуваме зборот безбедност, најчесто подразбираме чување, заштита на нешто, заштита на некоја вредност, (материјална или духовна) или заштита на човекот. Секако, апсолутна безбедност не постои, ниту за човекот ниту за другите вредности. Според тоа, можеме да зборуваме за можно ниво на безбедност што би овозможило „нормална“ егзистенција на луѓето и „нормална“ заштита на другите вредности.[2]

Во основа, корените на безбедноста, датираат уште пред постоењето на државата, што значи дека безбедноста постоела многу порано, дури и пред настанувањето на државата, односно за безбедноста се говори дека настанала уште кога се појавил човекот и неговите напори како да се преживее. Дури подоцна безбедноста се проширува на целата заедница, односно на државата. Значи, во почетокот со цел да се обезбеди потребното ниво на безбедност, луѓето почнале да се здружуваат во мали заедници. Многу брзо овие мали заедници со својата структура и едноставен систем на општествена контрола почнале да се менуваат, односно да еволуираат во големи групирања.[3]

---

[1] За поимот безбедност во различните јазични системи се употребуваат различни термини: англиски - security, словенечки - varnost, француски - sécurité, германски - sicherheit, шпански - seguridad, руски - безопасностъ, турски - güvenlik, украински - bezpeka, шведски - säkerhet, бугарски - sigurnost, албански - siguri, sigurim, грчки - asfalia, српски - безбедност, хрватски – sigurnost. Види: Мојаноски, Ц., За поимот наука за безбедноста, *Годишник на Факултетот за безбедност*, Скопје, 2010, стр. 12.

[2] Ивановски, З., Ангелески, М., *Безбедносни системи,* Европски универзитет, Скопје, 2005, стр. 80.

[3] Masleša R., *Teorije i sistemi sigurnosti,* „Magistrat“ Sarajevo, 2001, стр. 3.

Паралелно со еволутивниот пат и развој на безбедноста со појавата на човекот и организирајќи се преку мали заедници до системски заснована безбедност се појавуваат и првите поимања и сфаќања за безбедноста кои ги наоѓаме уште кај древните мислители на стара Кина и Грција. Платон го употребувал поимот „стабилност" на општественото уредување и улогата на законот во отстранување на општествените конфликти. Аристотел забележува дека е потребно да постои одлучна власт на мажот над жената и над децата за да биде семејството стабилно. Заедничко кај нив е што улогата на законот е во функција на спречување конфликти и гарантирање на овозможена правда (што е налик на идеалната правда), којашто е неопходна за мирни односи во општеството. Понатаму, заштитата на правата на граѓаните ја пропишува и Римското право, во коешто веќе се назираат моменти на ограничување на моќта на владетелот.[4] Од периодот на владеење на римскиот император Август (I век пред нашата ера), како и во текот на средниот век, поимот безбедност е употребуван во политичка смисла и е доведен во корелација со поимите мир (лат. pax Romana, pax christiana), слобода (лат. libertas) и постојаност, односно постојаност на власта (лат. securitas Augusti). Во римската митологија олицетворение на безбедноста било женското божество Securitas. Распадот на Римската Империја довел до феудализација на политичкиот живот и до децентрализација на моќта во Европа. Во духовен поглед, највисоката власт ја поседувала црквата, а од политички аспект, таа настојувала да го постигне тоа преку Светото Римско Царство. Покрај конфликтот со папството, царството морало да се справи со бројните и сè помоќните кралеви и нивните вазали. Подоцна, реформацијата ја довела во прашање врховната духовна власт на црквата, што ја интензивирално безбедносната дилема на сите нивоа, од поединецот, па сè до папството. Од XVI век, поимот безбедност се поврзува со јавната безбедност (лат. securitas publica), која се однесувала на заштита на поданиците во мир, како и поддршка на поданиците на владетелот во време на војна. Верските граѓански војни кои беснееле во Европа во првата половина од XVII век, ја поттикнале идејата за тоа дека за безбедноста на поединецот може да се грижи само суверена држава.[5] Од Вестфалскиот мир, склучен во 1648 година па наваму, су-

[4] Luard, E.*, Basic texts in International Relations*, St. Martin's Press, New York, 1993, стр. 5-26.

[5] Јовановска И., Местото и улогата на недржавните актери во спроведување контрола на безбедносниот сектор на Република Македонија (магистерски труд одбранет на Филозофски факултет), 2019, стр. 9-30.

верените држави стануваат најмоќните актери во меѓународниот систем, кои се единствени кои поседуваат монопол над легитимната примена на физичка сила и кои не признаваат никаков повисок политички авторитет. Безбедноста, така станала примарна функција на суверените државни власти. Меѓутоа, зборот безбедност, во XVII век и понатаму се однесувал, пред сè, на поединците. На тој начин, безбедноста ја сфаќал и Томас Хобс во делото „Левијатан" кое за прв пат било објавено во 1651 година. Според Хобс, како и кај други мислители од тој период, ултимативниот референтен објект на безбедноста е поединецот, бидејќи во природната состојба поединците живеат во постојана војна на сите против сите и не се во можност да ја обезбедат својата лична безбедност, тие склучуваат општествен договор и основаат државна власт. Во следниот период, поимот безбедност сè повеќе се поврзува со поимот за суверена државна власт, за нејзината внатрешна и надворешна заштита, пред сè, со помош на полицијата и војската, но и на другите политички установи.[6]

Во овој контекст се размислувањата и на англискиот филозоф, Џон Лок (John Locke, 1632-1704 година) кој заклучува дека луѓето создаваат држава со цел да им се обезбеди безбедност, односно да си ја сочуваат својата сопственост (животот, личната слобода и добрата). За разлика од Томас Хобс, Џон Лок не кажува директно дека луѓето ја жртвуваат својата неограничена слобода заради безбедност, туку констатира дека слободата на поединецот е ограничена со еднаквите слободи и права на другите поединци.[7]

Ваквите фундаментални размислувања се солидна основа и добра платформа со која започнува историјатот за теориското втемелување на безбедноста како функција на државата. Всушност, преку овој пристап безбедноста и државата станале главен интерес на државната власт којашто на безбедноста гледа како на централно поставено прашање важно за остварување на целите на државата.

Со развојот на национализмот и националните држави во XVIII и XIX век, безбедноста на државите станува безбедност на националните држави. Заклучно со Првата светска војна, воспоставувањето на држа-

[6] Barry Buzan, Ole Waever and Jaap de Wilde, (1998), *Security: A New Framework for Analysis,* Lynne Rienner Publishers, London, стр. 125, преземено од Јовановска И., Местото и улогата на недржавните актери во спроведување контрола на безбедносниот сектор на Република Македонија (магистерски труд одбранет на Филозофски факултет), 2019, стр. 9-30.

[7] Јованов, Д. Ј., Џон Лок и право на отпор, во *Зборник радова Правног факултета у Новом Саду*, Правни факултет у Новом Саду, Нови Сад, 2015, стр. 1389-1401; Lok, Dž., *Dve rasprave o vladi*, Knjiga 2, Beograd, 1978, стр. 71-74.

вите како централни референтни објекти на идентитетот и носители на безбедноста било комплетно. По завршувањето на Првата светска војна, со основањето на Лигата на народите, направени се првите сериозни обиди идејата за колективна безбедност да се спроведе и во пракса, а доаѓа и до развивање на посебна научна дисциплина која ги изучува меѓународните односи. Во текот на меѓувоениот период, зборот безбедност за прв пат влегува во меѓународно-политичкиот речник. Уште во првата реченица на Пактот на Лигата на народите стои, односно пишува дека „високите страни потписнички, со цел за промовирање на меѓународната соработка и обезбедување на мирот и безбедноста во светот", ја прифаќаат обврската да не посегнуваат по војна, односно по оружје, туку да соработуваат и да го почитуваат меѓународното право. Синтагмата „меѓународен мир и безбедност" ја користеле тогашните *status quo* држави, пред сè Франција и Велика Британија, за да ги претставаат своите интереси како интереси на целото општество. Затоа, како што одлично забележува авторот Оле Вавер, воопшто и не зачудува дека првата критика на концептот за безбедноста ја напишал токму еден Германец, во текот на триесеттите години од XX век. Сепак, меѓународната безбедност како еден од многуте аспекти на меѓународните односи, доаѓа во прв план по завршувањето на Втората светска војна.[8]

Денес безбедноста е многу комплексен и изразито сложен општествен феномен и генерално треба да се разбере дека безбедноста сама по себе не создава ништо, но од друга страна таа го овозможува опстанокот и развојот на општеството и во однос на државата и во однос на поединецот, таа е и биолошки и е рационално фундирана за да го обезбеди потребното ниво на безбедност за државата, за нацијата, за граѓаните итн. Во однос на државата, безбедноста ги синтетизира државните функции врз основа на искажани потреби на граѓаните. Значи, во процесот на гарантирање оптимален степен на безбедност, државата остварува одредени функции. На неа се гледа како на комплексен процес кој бара учество на бројни институции. Државата ги изведува следните работи за да гарантира висок степен на национална безбедност: прво, внатрешни политички гаранции за националната безбедност. Државата, со помош на националната дипломатија, се стреми да постигне внатрешна средина во која националната безбедност е гарантирана. Второ, безбедност. Безбедноста значи гарантирање и давање поддршка на мирот и на стабилноста, заштита на националните интереси и вред-

[8] Barry Buzan, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, London, 1998, стр. 125.

ности, поддршка на економијата итн., и трето, менаџмент и контрола на процесот на гарантирање на висок степен на национална безбедност. Ефикасно постигнување на националната безбедност е невозможно без управувачка и контролна функција.[9]

2. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ ОКОЛУ ПОИМОТ И УПОТРЕБАТА НА ТЕРМИНОТ БЕЗБЕДНОСТ

Очигледно е дека безбедноста била предмет на интерес од самото човеково постоење и значела различни нешта за луѓето во зависност од историското време и место, но нејзиното институционализирање е тесно поврзано со настанокот на државата, нејзината организација, органи и функција. Имајќи предвид дека се работи за поим, но и појава што е неизоставен дел од сите области од човековото живеење, сепак меѓу припадниците на научната мисла изразени се дилеми и потешкотии при дефинирањето на безбедноста. Значи, безбедноста е тесно поврзана со различните перцепции и варијации за нејзино дефинирање, односно различните интереси се пресудни за креирање на нејзиниот концепт. Тргнувајќи од ова, безбедноста не може да се одреди со една строга дефиниција, не само заради различните сфаќања за тоа што е безбедност, туку и поради фактот што едно општество никогаш не може да биде целосно безбедно.[10]

Во овој контекст во техничкиот жаргон на општествените науки, безбедноста често се објаснува како „суштински оспоруван концепт", односно тој е еден од оние концепти за коишто по дефиниција не може да се постигне консензус за неговото значење. На определен начин, ова е секако точно бидејќи безбедноста без сомневање значи различни нешта за различни луѓе и вака е определена на апстрактно ниво, додека на конкретно ниво безбедноста вклучува отстранување закана од негативни влијанија.[11]

---

[9] *Management of Defence*, Democratic and Civilian Control, Including Integration of Security Sector, стр. 2-3.

[10] Lindström, Susanne "The changing nature of security: The Euro-Mediterranean Partnership and non-military security", International Mediteranian Studies, workshop on 06.10.2005, European Research Institute, стр. 3.

[11] Gallie W.B., Essentially contested concepts, Proceedings of the Aristotelian Society, 56, 1956, стр. 167-191, во *Security Studies: An Introduction*, Routledge, 2008, стр. 1-12.

Во оваа насока се и размислувањата на Дејвид Болдвин, кој потенцира дека „безбедноста во концептуална смисла е толку спорна што не е (ниту приближно) можно да се изнајде начин за нејзино универзално разбирање и дефинирање,“[12] односно „поимот безбедност е еден од најчесто употребуваните, но истовремено и еден од најмалку објаснетите поими,“[13] додека за Бузан пак, терминот безбедност е во широка употреба и се смета прифатен како централен организирачки концепт и од практичарите и од академската заедница, додека во литературата на тој план е многу неизбалансирана, предизвикувајќи негово различно адресирање.[14]

Сепак, без разлика на определени потешкотии во дефиницискиот пристап ние ќе издвоиме неколку од широкиот спектар дефиниции без притоа понатаму пошироко да ги разгледуваме и да ги анализираме сите поединечно. Така, според класичниот пристап безбедноста е повеќезначна и во теоријата и во практиката и таа се користи за да се означат разновидните елементи и односи, а безбедноста во своите правни рамки е носечки темел на целокупниот човеков, општествен и државен живот. Безбедноста, притоа, не е само објективна основа за идниот темел на разни подрачја на општествениот живот, туку е и решавачка внатрешна психолошка диспозиција за здрав, хармоничен и успешен човеков и општествен развој.[15]

Во енциклопедиска смисла, под безбедност подразбираме отстранување на сите активности (чинења) и пропуштања (нечинења) што ги загрозуваат или што може да ги загрозат луѓето, редот, јавниот поредок, материјалните и духовни добра, објектите, определен простор или некоја друга вредност.[16]

Во десеттото издание на Мериам-Вебстер факултетскиот речник, безбедноста е опишана како „слобода од страв и анксиозност… нешто што заштитува… мерки преземени да спречат шпионажа или саботажа,

[12] Baldwin, D., The Concept of Security, *Review of International Studies*, Vol 23, No 1, Aberystwyth, 1997, стр. 3–26.

[13] Dimitrijević, V., *Pojam bezbednosti u međunarodnim odnosima*, Savez udruženja pravnika Jugoslavije, Beograd, 1973, стр. 17-19.

[14] Бузан Б., *Луѓе, Држави и Страв: Проблемот со националната безбедност во меѓународните односи*; Академски печат; Скопје 2010, стр. 11.

[15] Stamper, A., Versuch einer sicherheits-analytischen Bewertung der inneren Konfliktsituationen in unserer Zeit, *Kriminalistik*, 2/1981, стр. 26.

[16] Спасески, Ј., Аслимоски, П., *Безбедност, одбрана и мир*, Институт за истражување на туризмот, Факултет за туризам и угостителство, Охрид, 2001, стр. 17.

криминал, напад или бегство… организација или оддел чија задача е безбедноста". Исто така, во Вебстеровиот меѓународен речник, стои дека безбедноста е состојба на заштитеност или неизложување на опасност. Исто така, „безбедноста е отстранување на страв, загриженост итн."[17]

Според дефиницијата за безбедност изработена во рамките на ООН во 1986 година, „безбедноста е состојба во која државите сметаат дека нема опасност од воен напад, од политички принуди или од економски присили, така што можат слободно да се развиваат и да напредуваат".[18]

Според Манголд, безбедноста се изразува преку високиот степен на неприкосновено право за опстанок и за одбрана на виталните интереси на државата. Така, безбедноста се стреми кон осигурување на стабилност на државата преку насочување на своите потенцијали за справуваање со заканите.[19] Во тој контекст се и размислувањата на Фискер, кој смета дека „безбедноста е состојба во која државите сметаат дека нема опасност од загрозувања, па така тие можат слободно да се развиваат. Исто така, во понатамошната елаборација тој наведува дека безбедноста на индивидуите и на заедниците од кои се состојат државите е примарна функција и гаранција за ефикасно почитување на индивидуалните слободи, политички, социјални и економски права, како и заштита или обнова на поволната животна средина за сегашните и за идните генерации.[20]

„Безбедноста", како што ја опишуваат Роберт Фишер и Гион Грин, е стабилна, релативно предвидлива средина во која поединец или група може да ги постигне своите цели без попречување или штета, или чувство на страв од вознемирување или од повреда,[21] додека Пост вели дека безбедноста настојува да обезбеди заштита од човечки, од природни и од еколошки ризици.[22]

---

[17] *Vebster's New international dictionary,* second edition, 1934.

[18] *Conception de la sécurité*, Série d`études 14, Publication des Nations Unise, 1986, A/40/533

[19] Mangold, P., *National Security and International Relationsm*, Rotledge, London and New York, 1990, преземено од: Бакрески О., Драган Т., Митевски С., *Корпорациски бебедносен систем*, Комора на Република Македонија за обезбедување лица и имот, Скопје, 2012, стр. 23.

[20] Fischer, D., *Nonmilitary Aspects of Security: A Systems Approach*, Aldershot: United Nations Institute for Disarmament Research, 1993, стр. 10.

[21] Fischer J.R., Halibozek E. and Green G., *Introduction to Security*, Elsevier Inc., New York, 2008, стр. 20-40.

[22] Post R.S., Security Administration: An introduction. Cincinnati: Anderson, 1970, во *Principles of Security Management*, Pearson Prentice Hall, New Jersey, 2005.

За Гарвер, безбедноста (како впрочем и демократијата) е „есенцијално оспорен концепт“, кој создава неразрешливи дебати,[23] додека за Фиксер, „безбедноста имплицира дека основните човекови потреби, пред сè во делот на исхраната, образованието, домаќинството и јавното здравство, се осигурани на трајна основа, и дека е потребно да се одржува адекватна заштита од евентуални опасности за безбедноста. Начините и средствата за добивање ваков вид безбедност се дефинирани во национални, во меѓувладини, во невладини и во глобални услови.“[24]

Според Јан Лодер и Нил Вокер, безбедноста е драгоцено јавно добро, односно нужен елемент на секое „добро општество”, и дека нужна и доблесна задача на демократската држава е да го создаде и да го одржува ова јавно добро.[25]

За Асберг и Валенштајн, дефинирањето и детерминирањето на содржината на безбедноста зависи од следните елементи: а) суштински вредности, кои се однесуваат на аспектите на она што сакаме да го обезбедиме; б) заканите се тие кои ни покажуваат на какви предизвици и опасности се изложени овие вредности; и в) способностите/средствата за справување со заканите, т.е. ресурсите и актерите, кои можат да се справат со заканите, односно да ја гарантираат безбедноста.[26].

Урсик и Пагано ја дефинираат „безбедноста“ како „веќе препознатлива состојба, но нивната дефиниција има тенденција да биде нејасна и тешка за формулирање на сеопфатен и содржаен начин“.[27]

Милетиќ безбедноста ја дефинирал како „правно уредување и обезбедување на општествените односи и унапредување на состојбата во државата, што овозможува ефективна заштитеност на државата

[23] Eugene Garver, “Rhetoric and Essentially Contested Arguments”, *Philosophy and Rhetoric*, Vol.11, No.3, (Summer 1978), стр.156-172.

[24] Fischer, D., *Nonmilitary Aspects of Security: A System Approach*, Aldershot: United Nations Institute for Disarmament Research, 1993, стр. 10.

[25] Ian Loader and Neil Walker, *Civilizing Security*, Cambridge: Cambridge University Press, 2007., преземено од Ванковска Б., Меѓународна безбедност – критички пристап, Филозофски факултет, Скопје, 2001, op. cit.

[26] CJ Asberg and P Wallensteen, “New Threats and New Security: The Post-Cold War Debate Revisited”, in Peter Wallensteen (ed.), *Preventing Violent Conflicts: Past Record and Future Challenges*, Uppsala: Uppsala University, 1998, стр. 169; види: Ванковска Б. *Меѓународна безбедност – критички пристап*, Филозофски факултет, Скопје, 2001, стр.15.

[27] Ursic H.S. and Pagano L.E., Security Management systems: illinous, Charlies C.Thomas, 1974, стр. 24, во Principles *of Security Management*, Pearson Prentice Hall, New Jersey, 2005, стр. 1.

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."[28]

Вукадиновиќ пак, безбедноста ја сфаќа „не само како отсуство на страв од секаков напад, туку како категорија која не се остварува само со воена сила, односно подигнување на културното и образовното ниво, јакнење на билатералните односи особено со соседите, јакнење на националната економија, развој на демократијата и слободата, како и почитување на човековите права."[29]

Во елаборацијата на Бакрески и Милошевиќ стои дека безбедноста во објективна смисла претставува отсуство на закани за усвоените вредности, додека во субјективна смисла претставува отсуство на страв дека вредностите ќе бидат загрозени. Преку безбедноста како фундаментална потреба на современото демократско општество, можеме да го следиме и политичкото расположение и положбата на граѓаните.[30]

3. ПОТРЕБА ЗА БЕЗБЕДНОСТ

Остварувањето на безбедност е фундаментална задача на државата во новата безбедносна средина во која државните институции треба да одговорат адекватно на променетата природа на внатрешните и надворешните закани. Така, во контекст на намалената веројатност за воен конфликт помеѓу државите, општествата сè повеќе ги согледуваат организираниот криминал, трговијата со дрога, трговијата со луѓе, перењето пари и економскиот криминал, тероризмот како главни закани по нивната безбедност. Друг голем предизвик во безбедносната средина претставува и процесот на глобализација. Глобализацијата е феномен карактеризиран од неколку процеси и услови, вклучувајќи доминација на капитализмот и слободната трговија, интеграција на економските и

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

[29] Вукадиновиќ, Р., *Нови проблеми сигурности у Европи*, Међународна политика, Београд, 1991, стр. 28.

[30] Бакрески О. и Милошевиќ М., *Современи безбедносни системи – Компаративна анализа на земјите од Југоисточна Европа,* Аутопринт Т.А., Скопје, 2010, стр. 30.

на политичките системи, технолошки прогрес, глобални комуникации и отсуство на бариери за протокот на информации, ресурси, идеи и вредности. Глобализацијата го зголемува просперитетот на учесниците во процесот, но во исто време наметнува ризици и закани за државите.[31]

Значи, неизвесноста и постојаната ранливост претставуваат постојан придружник на човекот во современи услови за живеење. Како рационално суштество, човекот постојано е опкружен со техничко-технолошки и општествени состојби. Токму тоа опкружување ги создава изворите на својата ранливост во форма на процеси кои, според нивното постоење, го загрозуваат општествениот поредок, материјалните добра и еколошките системи воопшто. Ако човекот не е во состојба да се заштити, тој станува жртва дури и со најмал интензитет на ранливост. Поради сето ова, човекот се залага за подобра заштита, бидејќи ќе биде подобро и побезбедно со неа.[32]

Наједноставниот начин да се обезбеди безбедност и заштита би се свел на определбата дека во суштина апсолутната безбедност е само илузија и факт е дека не може да се постигне во ниту едно општество. Но она што е потребно е тенденцијата за воспоставување рамнотежа меѓу безбедноста, заштитата на човековите слободи и права и интересите на заедницата, а на безбедноста е потребно да се гледа како на варијабилна големина на дивергентни, конфликтни и непомирливи интереси на поединците и групите во секое општество.[33]

Во такви услови на живот на општеството постои одредена политичка и безбедносна нестабилност. Разликите кои постоеле низ историјата и сè уште постојат помеѓу државите, ја создаваат потребата од одмерување на силата на политички, воен, идеолошки и економски план, со цел да се промени рамнотежата на моќ и наметнување на соодветен систем на вредности, така што ова е време на големи политички, национални, економски, безбедносни и други процеси со различни ставови за решавање на прашања кои се од значење за судбината на човекот. Имајќи ги предвид претходно изнесените констатации, треба да биде јасно дека безбедноста и заштитата се предуслов, неопходност и цел на секое општество и заедница.[34]

---

[31] Management of Defence, Democratic and Civilian Control, Including Integration of Security Sector, стр. 1-2.

[32] Бакрески О., Ахиќ Ј., и Наќ И., *Приватен безбедносен сектор во ЈИЕ*, Комора на РМ за приватно обезбедување, Скопје, 2019, стр. 10-12.

[33] Gagjinovic, R., Klasifikacija bezbednosti, *Nauka, bezbednost, policije*, Krimminalisticko-policijska akademija, Beograd, 2007, стр. 23.

[34] Бакрески О., Ахиќ Ј., и Наќ И.*, Приватен безбедносен сектор во ЈИЕ*, Комора на РМ за приватно обезбедување, Скопје, 2019, стр. 10-12.

4. ТЕОРИСКО-КОНЦЕПЦИСКА РАМКА НА БЕЗБЕДНОСТА

Општата теориска рамка за разгледување на поимот „безбедност“ би требало да ги вклучи следните безбедносни теории: структурална теорија за безбедноста, реалистичка теорија за безбедноста, функционална и структурално-функционалистичка теорија, дијалектичка теорија на безбедноста, системска теорија на безбедноста и формална теорија на безбедноста. На овие теории, по правило, им се додаваат и: идеалистичката и либералната, односно неолибералната теорија и теоријата на меѓузависност во односите. Овие либерално-идеалистички доктрини се во тесна врска со функционализмот (и неофункционализмот), односно доктрината на меѓузависност (во безбедноста) се сведува на структурално-функционалистичко објаснување на безбедноста. Критиката на овие теории и концепции, ќе доведе до идејата за примена на релационистичката теорија во научното согледување на феноменот, појавата и поимот за безбедноста.[35]

Во продолжение, акцентот ќе биде ставен на основните карактеристики на споменатите теории за појасна класификација на методолошките правци во науката за безбедноста. Така, структуралната теорија за безбедноста е базирана на општиот структуралистички метод на општествените науки. Оваа теорија настојува да открие, да прикаже (опише) и да објасни од кои елементи и едноставни својства се конституира безбедноста. Тука се идентификуваат, лица, групи или установи кои се заштитуваат од другите субјекти (од ист или сроден тип) кои ги загрозуваат. Потоа, се објаснуваат или опишуваат елементите на методите и постапките на загрозување, па елементите на методот на заштита, како и други компоненти во рамки на елементаристичко-структуралниот приод. За разлика од споменатата теорија, реалистичката теорија, се развива наспроти идеалистичкиот институционализам, односно се заснова на објаснувања на безбедноста, особено во меѓународните односи, преку единствената сила или системски условената сила (неореализмот). Реалистичката теорија во основа останува во рамките на методолошкиот правец структурализам, со извесно отстапување во рамките на неореализмот, кој елементаристичкиот приод го комбинира и го проширува со аспектите и компонентите на општата теорија на системите.[36]

[35] https://www.researchgate.net/publication/5223115, посетена на 12/12/2018.

[36] Ејдус Ф., *Меѓународна безбедност: теории, сектори и нивои*, Службени гласник, Београд, 2012, стр. 37.

Наспроти овие групи теории, се разви функционалистичката теорија која ја дополнува идеалистичко-институционалната концепција и која настојува на експликацијата на појавата „безбедност“ да ѝ овозможи нови димензии низ квалитетно објаснување на врските, односно конгломератите на врски меѓу елементите на појавата на безбедноста. Функционализмот и неофункционализмот се засновуваат на објаснувањето на потребата за поврзаност на елементите во целина и причините за ваквата поврзаност во структурата. Либерализмот ова го дополнува со мноштво мотиви или типови потреби (цели) кои дејствува на преформулација на појавата „безбедност“, каде силата (на субјектот) повеќе не е единствена, монолитна и основна компонента на безбедноста. Функционализмот, понатаму, има екстензија во настанување и во развојот на теоријата на меѓузависноста. Овој методолошки и теоретски правец настојува да ја преформулира меѓународната безбедност низ укажување на значењето на разновидната (поливалентна) плурално мотивирана меѓународна соработка и, особено, значењето на креирање мрежа од сложени или комплексни заемни зависности помеѓу државите во меѓународните односи. Значителна, екстензија на теоријата на безбедноста наоѓаме, потоа, во дијалектичкиот концепт, каде безбедноста се формулира (со противречности на борбата на спротивности) во широкиот меѓународен поредок. Понатаму, особено важна надградба на основниот функционализам се сретнува во системската теорија за безбедноста. Таа, покрај динамичната развојност, внесува и системско, синергистички ефекти, како и други колективни ефекти или варијабли кои динамички ја обликуваат појавата на безбедноста. Овде треба да се забележи дека единствено неореализмот ги вклучил до крај ваквите динамични аспекти во формулацијата на безбедноста. Слични обиди во рамки на неолиберализмот правец досега не беа забележани во досегашниот развој на таа теориска група. Конечно, следи и формалната теорија за безбедноста. Таа се базира на екстензија на математичко-оперативните истражувања на областа безбедност. Овде особено место нашла теоријата на игрите (посебно *Зеро-Сум*) и на овие модели (повеќе или помалку на конфликтна игра), која се заснова на примена на постапките од теоријата на веројатноста. Безбедноста во многу аспекти може да се сведе на конфликтна игра која се повторува, ограничен или неограничен број пати. Мерењето на исходот од овие игри претставува важна дисциплина на теоријата на игрите во областа на безбедноста.[37]

[37] Исто., стр. 38.

Во проучувањето на безбедноста покрај теориите соодветно место им припаѓа и на концептите. Во литературата постојат различни перцепции и варијации кои се пресудни за креирање на основните концепти. Во овој контекст, се полемизира дека безбедноста генерира дебати, што всушност укажува на тоа дека концептот на безбедност не само што не губи од актуелноста, туку сè повеќе се „збогатува". Затоа сведоци сме на суштинско продлабочување и проширување на концептот за безбедност, па оттука денес различните димензии на безбедноста ја нагласуваат потребата од поголема заштита на човекот, заштита на енергенсите, суровините и критичната инфраструктура, заштита на посебноста на културата и на идентитетот, заштита на имотот, заштита на корпорациите итн. Ова доведе до тоа на безбедносната агенда да бидат прифатени нови безбедносни концепти, како „човекова безбедност", „енергетска безбедност", „социетална безбедност"[38], „приватна безбедност", „корпоративна безбедност" и др. Овие концепти јасно ја изразуваат и ја отсликуваат промената која се случи во сфаќањето на традиционалните концепти за безбедност, наспроти растечката важност на новите безбедносни концепти.

Сепак, во продолжение ќе бидат аргументирани неколку клучни концепти значајни за безбедноста на државите во современи услови и тоа: концептот на индивидуална безбедност, концептот на национална безбедност и концептот на меѓународна безбедност.

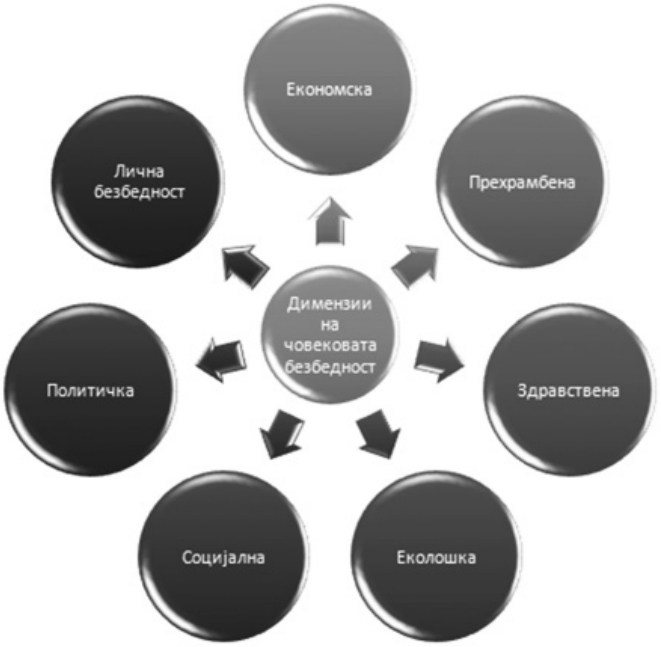
На прво место е *концептот на индивидуална безбедност*. Поради многубројните фактори кои влијаат на безбедноста на поединецот, индивидуалната безбедност е многу тешко да се дефинира. Таа во голема мера има детерминирачко значење за задоволување на нејзините севкупни потреби (личен интегритет, слобода на избор, економски статус, вработување, признавање на неотуѓиви права, образование итн.). Сите овие фактори се во непосредна корелација со функционирањето на демократската и на правната држава. Значи, научната елаборација на индивидуалната безбедност треба да се набљудува во контекст на нејзината поврзаност со националната безбедност на државата.[39]

[38] Социеталната безбедност е дефинирана како „способност да се обезбедат соодветни услови за развој на посебноста на јазикот, културата, религиозниот и национален идентитет и обичаите," во: Waver Ole, *Societal Security: The Concept*, 1993, стр. 23.

[39] Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era*, Second Edition, Lynne Riener Publishrs, Boulder, Colorado, 1991, стр. 25.

Во последната декада на минатиот век наместо за индивидуалната безбедност сè повеќе се говореше за концептот на „*човекова безбедност*“. Програмата на Обединетите нации за развој (United Nations Development Program – UNDP) во Извештајот за човековиот развој за 1993 година апелира дека „...концептот на безбедноста мора да биде сменет, така што, наместо на националната безбедност, поголем акцент ќе биде ставен на безбедноста на луѓето, и наместо на безбедноста која е остварена со вооружување, акцентот ќе биде ставен кон безбедноста која е остварена со човековиот развој, односно акцентот ќе биде ставен на безбедноста на храната, вработувањето и животната средин.[40] Вака дефинираната човекова безбедност, идентификувала седум димензии, кои се прикажани во продолжение на слика број 1.

Слика број 1: Седум димензии на човековата безбедност



Извор: Ејдус Ф. Меѓународна безбедност: теорије, сектори и нивои, Службени гласник, Београд, 2012

[40] United Nations Development Program, Human Development Report 1993, Oxford University Press, New York, 1993, стр. 251.

Врз основа на наведените седум димензии, може да се заклучи дека човековата безбедност се врзува, како за заштита на поединецот од насилство, така и за неговиот севкупен развој. Човековата безбедност, во споменатите извештаи и во другите документи кои подоцна се усвоени од страна на ООН, како референтен објект на безбедноста, го препознава човекот, односно граѓанинот како поединец. Државата се оспорува како референтен субјект на безбедноста, а не се идентификува кој има или кој би требало да има таква надлежност, притоа подразбирајќи дека таа е надлежна за заштитата на човековата безбедност. Слична воопштеност е евидентна и во поглед на субјектот на опасност.[41]

На второ место се наоѓа *концептот на национална безбедност*. Иако концептот на национална безбедност е политички многу моќен и припаѓа помеѓу централните концепти на меѓународните односи, не постои согласност за тоа што поточно, или попрецизно се подразбира под овој концепт. Голем број толкувања за националната безбедност, во објективна смисла на зборот, може да се класифицираат на различни начини. Една од класификациите може да биде на нејзините потесни и пошироки области, при што, „потесната ја сведува националната безбедност како средишна категорија на традиционално сфатениот поим за национален интерес на државата“, а пошироката класификација „воведува и некои други елементи како што се на пример, отсуството на закани; квалитет на живот заснован на политички, на економски и на социјални вредности, како и на поединци, на општествени групи и на општеството во смисла на објектот којшто треба да се штити од надворешните закани“.[42]

Во „Меѓународната енциклопедија на општествените науки“ националната безбедност е дефинирана како способност на државата (нацијата) своите внатрешни вредности да ги заштити од надворешните опасности.[43] Во политичката енциклопедија, пак, националната безбедност се дефинира во една широка правна смисла. Така, таа опфаќа мерки и активности за чување и заштита на независноста и интегритетот на една земја од загрозување на внатрешниот уставен и правен поредок. Доколку државата не го обезбеди потребното ниво на безбедност, не може да се зборува и за индивидуалните слободи во тоа

[41] Исто., стр. 251.

[42] Савиќ А., Национална безбедност, Криминалистичко-полицијска академија, Београд, 2007, стр. 19.

[43] Sills L.David, Merton K. Robert (eds), *internacional Encyclopedia of the Social Sciences*, vol.XI, MacMillan Publishing Company, New York 1968, стр. 40.

општество.[44] Интересно е да се потенцира дека А. Хеведи ја толкува националната безбедност како функција на националните држави, со помош на која, во согласност со сопствените можности сега и во иднина, а почитувајќи ги глобалните промени и развојот во светот, го штитат сопствениот идентитет, опстанокот и интересите,[45] додека за Љ.Стајиќ, националната безбедност треба да се сфати како интегрален поим во кој се обединети два нормативни поими – безбедност на државата и безбедност на општеството, при што, основниот критериум на безбедноста на државата претставува нејзиниот суверенитет, а за безбедноста на општеството претставува идентитетот.[46] Нашите размислувања упатуваат на тоа дека националната безбедност е термин со повеќекратно значење, кое денес се користи за означување на многу поширок поим од изворното значење, бидејќи под истиот се подразбира посакувана состојба на безбедност во една држава, која се постигнува преку елиминирање на внатрешните и на надворешните ризици и закани.[47]

Во обид да придонесе на суштинското одредување на националната безбедност, Б. Бузан критички ги опсервира сите постојни дефиниции на националната безбедност. Истите, тој ги смета за корисни, но не и во целост доволни за разбирање на суштината на националната безбедност. Националната безбедност, Бузан ја разгледува од три нивоа (индивидуално, државно и меѓународно) и неколку подрачја од човековото дејствување (воено, политичко, економско, социјално и еколошко подрачје). Според неговото мислење, најважно е државното ниво, бидејќи тоа ги одредува останатите две. Од подрачјата на човечкото дејствување, военото ги вклучува офанзивните и дефанзивните способности на државата, додека политичкото подразбира грижа за државата во организација на својата стабилност, концептот и идеологијата што ја легитимира власта. Економското подрачје претставува можност за пристап и користење на националното богатство, пазарот и финансиите, а социјалното ги одредува постојните услови и еволуцијата на културата, традицијата, јазикот и националниот идентитет, додека еколошкото

[44] Мала политичка енциклопедија, Савремена администрација, Београд, 1966, стр. 96.

[45] Hewedy Amin, *Militarization and Security in the Middle East*, Printer Publishers, London 1989, стр. 16.

[46] Стајиќ Љ. и Гаћиновиќ Р., *Увод у студије безбедности*, Драслар партнер, Београд, 2007, стр. 25.

[47] Бакрески О., Нови предизвици за безбедноста*, Годишник на Полициската академија*, Скопје, 2007, стр. 90.

подрачје претполага грижа за заштита на биосферата како важен систем од кој зависат сите човекови достигнувања.[48]

Во рамките на концептот на национална безбедност, особено место им припаѓа на сегментите приватна безбедност и корпоративна безбедност. *Приватната безбедност* е резултат на постојаната ерозија на државниот монопол над сите форми на организирано насилство и е предизвикана од неможноста државата на традиционален начин ефикасно да одговори на современите предизвици, ризици и закани настанати по завршувањето на Студената војна. По падот на Берлинскиот ѕид во 1989 година и колапсот на СССР, воените и безбедносни функции кои претходно се сметаа за исклучиво државни функции, сè повеќе се препишуваат и на приватниот сектор.[49] Како последица на тој процес, државите ја предаваат својата улога на единствен легитимен провајдер и гарант на безбедноста на приватните безбедносни актери.[50] На ова треба да се надополни и фактот дека по завршувањето на Студената војна се јавува процес на масовни отпуштања на персоналот во одбранбениот сектор (потребата од мал персонал и помали вооружени сили) за да се намалат државните трошоци поврзани со безбедноста.[51]

Значи, завршувањето на Студената војна е еден од настаните што се оценуваат како важни за развој на приватната безбедност. Трендот на појава и континуирано зголемување на бројот на приватни агенции за обезбедување започна поради последиците на Студената војна и веќе се шири низ сиот свет. Крајот од војната се карактеризирал со масовни намалувања на персоналот. Намалувањето на безбедносните сили ја зголемило понудата од обучена и од висококвалификувана работна сила што потоа била барана од страна на приватните компании заинтересирани за безбедносниот бизнис. Истовремено, појавата на нови војни во земјите во развој во текот на 90-тите години на минатиот век и тенденцијата за користење услуги од воено обучените лица резултирале

[48] Buzan B., *States, People and Fear: An agenda for International Security Studies in the Post-Cold War Era,* Harvesetr Wheatsheaf, London, 1991, стр. 19-20, преземено од Василевски Г., Функцијата на разузнавачко-безбедносните системи во остварувањето на националната и меѓународната безбедност, докторска дисертација одбранета на Филозофски факултет, Скопје, 2011, стр. 29-42.

[49] José L. Gómez del Prado, *The Role of Private Military and Security Companies in Modern Warfare: Impacts on Human Rights*, достапно на: http://www.globalresearch.ca/the-role-of-private-military-and-security-companies-in-modern-warfare/32307.

[50] Zorić D., *Privatna bezbednost razvijenih i zemalja u tranziciji,* Fakutet za bezbednost i zastitu, Banja Luka, стр. 23-101.

[51] Исто., стр. 23-101.

со вклучување на приватните агенции за обезбедување во безбедносниот сектор и нивно прераснување како клучен актер во него.[52]

Генерално, концептот на приватната безбедност е базиран на реалните ситуации во современите национални и меѓународни односи што се однесуваат на безбедноста и е содржан во многу аспекти на економското, на политичкото и на социјалното организирање, во зависност од конкретниот случај, што значи дека овој концепт покрива широка област во која настануваат и се случуваат сложени процеси и се вршат дадени функции во насока на создавање и одржување на безбедноста, во која се вклучени и останатите субјекти присутни на ова поле. Исто така, на овој концепт може да се гледа од две страни – со позитивното влијание што го има во општеството и во локалната заедница и со придонесот како во националните безбедносни прашања, така и во странство во мировните мисии; и од негативна страна, која се однесува на корупција, повреда на правата на приватност, шпионажа и преземање на државните овластувања.[53]

Мора да се нагласи дека секторот доживеа огромен раст во последните години, а денес се проценува дека има околу 20 милиони приватни безбедносни работници во светот, додека индустријата вреди околу 180 милијарди долари. Според Forbes, до 2020 година се очекува уште поголем пораст до 240 милијарди долари, вредност поголема од БДП на 100 држави, вклучувајќи ги и Португалија, Романија и Унгарија.[54]

Покрај приватната безбедност и *корпорациската безбедност,* без сомнение, е нов концепт кој се базира на релативизирање на монополот на сила од страна на државата, а тој се фокусира на прашањата врзани за безбедноста во компаниите. Корпорациската безбедност е приспособена да одговори на структуралните ризици во компанијата, преку примена на определени модели на симулација за спроведување на најдобрата безбедносна практика во компанијата[55] или корпоративната безбедност треба да ја обезбеди потребната избалансираност меѓу

[52] Nyamuya Maogoto, Jakson Sheehy Benedict, *Private Military Companies & International Law: Building New Leaders of Legal Accountability & Responsibility,* 2009, стр. 99-104.

[53] Бакрески О., Данчиќ М., Кешетовиќ Ж. и Митевски С., *Приватна безбедност: теорија и концепт*, Комора на Република Македонија за приватно обезбедување, Скопје, 2015, стр. 23-24.

[54] https://www.forbes.com/sites/niallmccarthy/2017/08/31/private-security-outnumbers-the-police-in-most-countries-worldwide-infographic/#219af810210f

[55] Michael Genser, *A Structural Framework for the Pricing of Corporate Securities: Economic and Empirical Issues,* Springer-Verlag New York, LLC, 2005, стр. 196-238.

нивото на безбедност во компанијата, бизнисот и конвенционалните барања на работа надополнета со мудрост, и на таков начин да нуди радикален, но инспириран предлог за успех. Во таа насока треба да биде и истражувањето на компаниите за здрав разум и логика кон подобра бизнис конзистентност.[56]

На трето место е *концептот на меѓународна безбедност*. Инаку, поимот „меѓународна безбедност" ферментира уште од завршувањето на Студената војна и е нејзин директен продукт, а наоѓа верификација во убедувањето дека безбедноста во периодот на сеопшта нуклеарна загрозеност, може да биде постигната единствено преку меѓународна соработка и минимално ниво на заедничко разбирање.[57]

Во основа, меѓународната безбедност не претставува само обичен збир на националните безбедности (безбедност на националните држави), туку подразбира и усвојување определени вредности како во меѓународните односи, така и во односите во самата држава. Исто така, меѓународната безбедност претставува збир на мерки што им го обезбедуваат опстанокот на сите држави, што претставува темелен предуслов за опстанокот и за развојот на меѓународната заедница.[58] Меѓународната безбедност би требало да значи дека сите членови на меѓународната заедница како целина се чувствуваат безбедни и дека во меѓународниот политички систем постојат такви односи, или такви механизми, кои им овозможуваат на сите држави да им се гарантира и да им се обезбеди безбедност.[59]

Меѓународната безбедност е условена од преземањето мерки од страна на нациите и на меѓународните организации за остварување на безбедноста и овозможување заеднички опстанок. Ваквите мерки, меѓу другото, вклучуваат дипломатска активност и воени акции, а со цел постигнување на договори и конвенции за решавање на одредена негативна безбедносна состојба од поширок опсег. Комплексноста од креирање меѓународна безбедносно-одбранбена политика, покрај другото, произлегува од временските, од законските, од финансиските и од системските ресурси. Тоа побарува креирање на флексибилен механизам со можност за критичко преиспитување, односно согледување на потребата од негово егзистирање или редефинирање во согласност

[56] Reid P., *How to Land a Top-Paying Corporate securities research analysts Job,* Emereo Pty Ltd, 2012, стр. 5-25.

[57] Dannreuther R., *International Security; the contemporary agenda*, Polity Press, Cambrige, 2007, стр. 1.

[58] Славески С., *Безбедносен систем*, Европски универзитет, Скопје, 2009.

[59] Vukadinović R., *Teorije o međunarodnim odnosima*, Zagreb, 1978.

со промената на околностите, а со тоа и на дефинираните безбедосни цели. Ова подразбира обликување еластични сојузи кои во согласност со заеднички верификувани глобални цели, би дејствувале во одбрана на стратегиските интереси. Од друга страна, националната безбедност дефинирана преку соодветни стратегиски документи во едно општество, треба да ја декларира определбата за почитување на основните демократски вредности и на меѓународното право. Во основа, тоа треба да значи подготвеност со своето учество во рамките на официјални меѓународни организации да се придонесува во изградба на сопствената, регионалната и меѓународната безбедност.[60]

5. ПРОМЕНИТЕ ВО СОВРЕМЕНИОТ СВЕТ КОИ ВЛИЈААТ НА БЕЗБЕДНОСНАТА СРЕДИНА

Евидентно е дека меѓународниот поредок во минатиот век имаше суштествено поинаков „квалитет" отколку денес. Нерамномерноста во развојот на одделни високоразвиени држави се манифестираше во сè попродлабочен јаз меѓу државите кои го креираат денешниот свет и може да се каже дека тоа се суштински противречности што го потресуваат современиот свет. Ако на ова се додадат и политичките судири, индустриските спорови и прашањата чие нерешавање може да биде извор на криза, како и опасноста од тероризмот и од меѓународниот организиран криминал со сигурност може да се каже дека овие нови и растечки предизвици ја исцртуваат мапата на меѓународната безбедност. Оттука, современите околности и односи не упатуваат на заклучокот дека денес се соочуваме со сложени реалности.

Првата реалност се однесува на перцепцијата за државите, односно не можеме да ги поимаме како во XX век, кога проблемот беше, во суштина поврзан со моќта и со амбицијата. Традиционалниот фокус на пропорционалноста на силите не може да се отфрли; ривалството помеѓу суперсилите и опасностите од воен конфликт нема да исчезнат. Сепак, тие се дел од заканите со кои треба да се соочиме, но не се толку значајни како порано. „Во иднина нема да има војна меѓу држави/воени сили, туку меѓу групи кои денеска ги нарекуваме терористи, герилци, бандити и кои, за да се истакнат, без сомнение ќе

[60] Василевски Г., Функцијата на разузнавачко-безбедносните системи во остварувањето на националната и меѓународната безбедност, докторска дисертација одбранета на Филозофски факултет, Скопје, 2011, стр. 29-42.

удрат по поформални титули". Вистинскиот предизвик е дека светот е навлезен во ера кога државата треба да е квалификувана. Проблемот се слабите држави што не се способни да покажат авторитет и легитимност, како и да обезбедат соодветна грижа за нивните граѓани. Државите што се неспособни да се справат со критичните зони на нивната територија стануваат засолниште за транснационалните криминални или терористички мрежи.[61]

Втората реалност се врзува за недржавните актери. Во последно време сè повеќе се препознаваат недржавни елементи кои сакаат да ја наметнат својата моќ. Значи, вниманието повеќе не е фокусирано само на државите; туку неопходно е да се обрне внимание и на широкиот спектар на недржавни актери.[62] Многу од овие актери не само што можат да мобилизираат многу средства и значајно да влијаат на политичките и на економските текови, туку исто имаат и моќ да наштетат.[63] Со тоа, клучните теми за расправа за иднината на глобалната политика се наизменичната игра помеѓу државноцентричниот свет (традиционалниот свет на високата геополитика) и повеќе-центричниот свет (свет на недржавни актери што сè повеќе се присутни во меѓународните односи).

Третата реалност подразбира соочување со ново мултиплицирање на недржавни актери што се мрежно поврзани; транснационални во обем; високофлексибилни во нивните операции; имаат способност да експлоатираат и да се вклопат во социјалните и во финансиските институции и на тој начин да бидат неоткриени; и поседуваат капацитет за регенерирање дури и кога пребродуваат значајна деградација.[64] (Зло)употребата на сајбер-просторот и придобивките на модерната технологија овозможуваат голем дострел и брза придобивка за постигнување на различни политички цели. Недржавните актери секојдневно ги користат придобивките на модерната технологија за мултиплицирање на моќта. Неретко, и самите држави дејствувајќи отворено или прикриено, го злоупотребуваат истиот простор, навлегувајќи во прокси војни, искористувајќи ги сите еле-

[61] Martin van Creveld., *The Transformation of War*, New York, NY: The Free Press, 1991.

[62] Види пошироко за суверенитетот на слободните актери кај: James Rosenau, *Turbulence in World Politics*, Princeton, NJ: Princeton University Press, 1990.

[63] Thomas C Shelling, *Arms and influence*, New Haven CT: Yale University Press, 1967.

[64] Johan Arquilla and David Ronfeldt (eds)., *Transnational Criminal Networks*, in Networks and Netwars, Santa Monica, CA: RAND, 2001, стр. 61-98.

менти на национална моќ за здобивање со определена предност или постигнување на цел која го поддржува нивниот национален интерес. Случајот *Стакснет* успеа да ја врати иранската нуклеарна програма многу наназад,[65] додека низа земји во светот ја обвинија Русија за наменски сајбер-напади,[66] особено во контекст на случувањата во Грузија[67] и Естонија. Основачот на *Телеграм* изјави дека „приватноста не е на продажба"[68] по лиферувањето на информацијата дека токму таа апликација ја користат за координација терористичките групи. Криминалните организации и терористичките мрежи треба да бидат разбрани како „организации за проучување". Треба да се препознае капацитетот на терористичките и на криминалните мрежи, да се учи, да се приспособи и да се подобри она што го прават, независно дали е тоа центрирање или експлоатирање на пазарите, е почеток на мудроста во справувањето со нив.[69]

Четвртата реалност се однесува на мултинационалните корпорации и постојаната игра со државно-центристичкиот свет. Постои мислење дека денешното корпорациско насочувано глобално деловно опкружување во голем дел е глуво на принципите на општествената праведност и солидарност, а ефектите од досегашната коорпорациска глобализација се познати и препознатливи, како меѓу богатите, така и меѓу сиромашните делови на светот, но и меѓу општествените групи и слоеви во внатрешноста на секоја национална економија. Меѓутоа, истовремено, појавата на глобалното светско управување што го спроведуваат транснационалните корпорации, коренспондира и со развојот на „глобалните цивилни општества", односно со појавата и вмрежувањето илјадници доброволни, невладини асоцијации насе-

[65] Fruhlinger, Josh, (2017), What Is Stuxnet, Who Created It And How Does It Work?. CSO Online, достапно на: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it- work.html.

[66] Berlinger, Joshua, and Nina dos Santos, (2018), "UK Blames Russian Military For 'Reckless' Cyber Attacks". CNN, достапно на: https://edition.cnn.com/2018/10/03/uk/uk-russia-cyber-attacks-intl/index.html.

[67] Danchev, Dancho,"Coordinated Russia Vs Georgia Cyber Attack In Progress | Zdnet". Zdnet, 2008.
https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.

[68] Privacy Is Not For Sale, (2018), Promises Telegram Founder Pavel Durov Adding The App Will Use Built In Systems To Bypass Russian Ban-Technology News, Firstpost. Tech2.

[69] Michael Kenney., When Criminals Outsmart the State: Understanding the Learning Capacity of Colombian Drug Trafficking Organizations, *Transnational Organized Crime* 5/1, 1999, стр. 97-119.

каде во светот како ATTAC, Amnesty International, Greenpeace и многу други. Оние што непосредно го чувствуваат економскиот, политичкиот и општествениот ефект на глобалното бизнис опкружување како и сè помоќните, покажуваат подготвеност да му се спротистават на сето тоа.[70]

*Петтата реалност се медиумите***.** Со појавата на националните радиомрежи, весниците и списанијата во XX век се создал и терминот масовни медиуми, односно медиуми за масовно комуницирање. Главна цел на масовните медиуми е да допрат до огромна маса на публика (милионска) на која, речиси истовремено, ќе можат да ѝ пренесат голем број пораки. Под поимот масовни медиуми во денешно време се подразбираат: *печатени* – книги, весници, магазини, *електронски* – радио, аудио и видео снимки, и новите *електронски медиуми* – мобилните телефони, интернетот и компјутерите.[71]

Со процесот на глобализација и проширување на медиумите и надвор од една држава, тие станаа: конгломерати, профитот вртоглаво им се зголемува, и имаат сè поголема моќ. Меѓутоа, паралелно со зголемување на публиката им се зголемува и конкуренцијата. Така се создава сè поголем притисок за профит. Во основа, медиумите ориентирани кон профит, се екстремно толерантни кон оние што се рекламираат, бидејќи тие им се еден од главните извори за средства или како што вели Овен Фис - „богатите, на пример, би можеле толку многу да доминираат на рекламниот простор во медиумите и во дерогатните јавни домени, што јавноста ќе ја чуе само нивната порака“ и гласот на помалку моќните ќе биде задушен.[72]

Покрај медиумите и невладините организации имаат своја релевантност. Терминот „невладини организации“ (НВО), започна да се користи во 1945 година поради потребата на Организацијата на обединетите нации (ООН) во нивната повелба, да направат разграничување помеѓу правата на партиципирање во меѓувладините специјализирани агенции и оние права за партиципирање во меѓународните приватни организации. Според Организацијата на обединети нации, практично сите типови на приватни тела можат да се подведат под терминот невладини

[70] Blomstrom Magnus, Hettne Bjorn, *Development Theory in Transition: The Dependency Theory and Beyond -Third World Responses*, Zed Books, London, 1998., стр. 59-62.

[71] Хаг, Р., Хароп, М., (2009), *Компаративна анализа на власта и полиииката,* Академски печат, Скопје, стр. 87.

[72] Вилкокс К. и Норандер Б., *Разбирање на јавното мислење*, Вашингтон, 2002, стр. 120.

организации. Тие само треба да се независни од владината контрола, да не ѝ бидат конкуренција на владата во смисла на политичка партија која се бори за власт, да бидат непрофитно ориентирани и да не бидат со криминални, со противправни и со илегални идеали и вредности.[73] Во повелбата на Организацијата на обединетите нации, во член 71, е наведено дека Економскиот и социјален совет треба да се консултира со НВО,[74] што укажува на фактот дека НВО се сериозен недржавен актер во меѓународната политика.[75]

Шестата реалност е организираниот криминал. Организираниот криминал, и покрај тоа што долг период бил поврзан само со одредени нации и со специфични географски подрачја, во последните децении на XX век, почнува да се третира како вистински меѓународен проблем, што го привлече вниманието на бројни меѓународни организации, на државни институции и на јавното мислење во многу земји, што резултира со многубројни иницијативи за одлучна и ефикасна борба против оваа појава. Изразот организиран криминал сè до крајот на 80-тите години од минатиот век во светот се користел како фраза со која се означува ескалација и загриженост на националните институции и поединци, во врска со експанзија на внатрешни и на меѓународни криминални пазари, со сè поголемата мобилност на носителите на криминално дејствување преку националните граници и штетата која организираниот криминал ја нанесува на легалното работење и на економските движења, како и криминалното рушење на демократските политички институции.[76] Организираниот криминалитет претставува еден вид класичен криминалитет, а крајната цел е постоење и дејствување организирани криминални групи кои се насочени кон противправно стекнување профит. Тој вид криминал е од неидеолошки карактер, поради тоа тој не смее да се поистовети со некои облици на политички криминал, како што е тероризмот.[77] Од друга страна, организираниот криминал се обидува на различни начини да се инфилтрира во политичкиот систем на државата. Тоа првенствено го

[73] An introduction to Non-Governmental Organizations (NGO) Managemanent – Compliled by Ali Mostashari – Indian Studies Group at MIT, June 2005, стр. 98.

[74] Бејлис Џ. Смит С. и Овенс П., *Глобализација на светската политика, Вовед во меѓународни односи*, Скопје, Табарнакул, 2009, стр. 92.

[75] Виоти, П. Каупи, М., *Меѓународни односи и светска политика. Безбедност, економија, иденитет,* Скопје, Академски печат, 2009, стр. 126.

[76] Paoli Letizia, Fijnaut Cyrille, „Organised Crime in Europe: General Introduction", in: Paoli Letizia, Fijnaut Cyrille (eds.), *Organised Crime in Europe: Manifestations and Policies in the European Union Beyond*, Springer, Dordrecht NL, 2003, стр. 1-2.

[77] Šukulih M., *Organizovani kriminalitet*, Dosije, Beograd, 2003, стр. 39.

прави со финансирање политички и предизборни кампањи на одредени кандидати или партии и корумпирање на гласачкото тело на изборите, по пат на корупција или застрашување на активните политички фактори во државата.[78]

Седмата реалност е тероризмот. Тероризмот како вид насилство стана еден од најзначајните предизвици за државите. Терористичките активности во XX век беа енигма и голем проблем за меѓународната безбедност, но сè уште се голем проблем и во XXI век. Во основа, тероризмот е политички мотивиран, многу деструктивен феномен и опасен вид насилство кое најинтензивно ги погаѓа цивилното население и институциите на државата. Исто така тероризмот е насилен или се заканува со насилство, насочен кон далекусежни психолошки последици надвор од непосредната жртва, а воден од некоја терористичка организација. И покрај тоа што сите во светот формално го осудуваат тероризмот, во практиката се потврдува фактот дека тероризмот, сепак, е ефикасно оружје за остварување на политички цели.[79] Значи, тероризмот станува еден од најголемите проблеми на современото општество кој како средство и метод за остварување на своите цели го наметнуваат различни групи, организации итн., при што како директна последица се јавува интересот на поединци, на сили и на структури за промена на односите во некоја заедница со примена на сила или со насилство против лицата или имотот. Современиот тероризам има некои карактеристики кои го прават различен од другите извори на загрозување, а се однесуваат на следните црти: тајност при работата, подготвеност за извршување радикални акции, добра подготвеност за извршување акции, често страдање на случајни цивилни жртви, нанесување голема материјална штета, со цел во што поголема мера да се заинтересира целокупната јавност (меѓународната и домашната) и да се оствари големо медиумско внимание.

Осмата реалност се остроумните непријатели. Терминот сајбер-безбедност алудира на примена на интегритет, сигурност, доверливост и достапност на информации. Сајбер-безбедноста развива серија на механизми, пристапи за управување со ризик, технологии, обука и најдобри практики дизајнирани да ги заштитат мрежите, уредите, програмите и податоците од напад или од неовластен пристап.[80] Значи, сајбер-безбедноста се техники и технологии што се применува-

[78] Savić A., Stajić Lj., op. cit. стр. 161.

[79] Gađinović R., *Antiterorizam,* Draslar Partner, Beograd, 2006, стр.15-27.

[80] What is Cyber Security? Cyber Security Defined, Explained and Explored. https://www.forcepoint.com/cyber-edu/cybersecurity, посетена на 11/5/2019.

ат за заштита на податоците, компјутерите, мрежите и програмите од напади и активности со цел експлоатација. Сајбер- безбедноста може дополнително да се категоризира во следните области: безбедност на информации, безбедност на апликација, мрежна безбедност и обнова на катастрофи.[81] Безбедноста на информациите ги штити информации од неовластен пристап за да се спречи кражба на идентитет и да се заштити приватноста. Во основа, организациите пренесуваат чувствителни податоци преку мрежи и други уреди во текот на целиот бизнис, а сајбер-безбедноста опишува дисциплина посветена на заштита на тие информации и системи што се користат за обработка или складирање информации. Екрипцијата е процес на кодирање на податоци што го прави неразбирлив и често се користи за време на трансферите на податоци за да се спречи кражба при транзит. Како што растат обемот и софистицираноста на сајбер-нападите, компаниите и организациите, особено оние кои се одговорни за чување информации за национална безбедност, здравствени или финансиски информации итн. Во последните години, може да се каже дека сајбер-нападите и дигиталното шпионирање се најголеми закани за националната безбедност, надминувајќи ги дури и заканите од тероризам.[82]

Деветата реалност е глобализацијата. Глобализацијата, која, покрај предностите, како распространување на либерално демократските вредности и слободниот пазар, има и темна страна. Иако законските бизниси имаат корист од можноста да ги експлоатираат глобалните пазари, најголемите корисници се транснационалните криминални мрежи, кои го користат глобалниот трговски систем за да ги вклопат нелегалните продукти во легален тек на стоката за широка потрошувачка; потоа глобалниот финансиски систем им овозможува да ги преместат и да ги скријат нивните пари, а глобалните телекомуникациски системи им користат за да ги пренесуваат директивите и пораките.[83]

[81] Cyber Security. Definition of Cyber Security. Merriam Webster. https://www.merriam-webster.com/dictionary/cybersecurity, посетена на 7/6/2019.

[82] What is Cyber Security? Definition, Best Practices & More преземена од: https://digitalguardian.com/blog/what-cyber-security, посетена на 4/5/2019.

[83] Phil Williams. *Non-State Threats and Future Wars*, in Robert J. Bunker (eds), Frank Cass & Co. Ltd, 2003, стр. vii-xiii.

глава II

КРИТИЧНА ИНФРАСТРУКТУРА – ТЕОРИЈА И КОНЦЕПТ

1. КРИТИЧНАТА ИНФРАСТРУКТУРА КАКО КОНЦЕПТ

Историските податоци говорат дека концептот „критична инфраструктура“, всушност е стар колку и човековата цивилизација. Во стар Рим, критичната инфраструктура најчесто значела патишта и аквадукти. Патиштата биле наменети за војската, што овозможувало најбрз транспорт на војници и воена опрема кон одредени привинции на Римската Империја кои биле под закана. Аквадуктите овозможувале свежа и питка вода за населението, што покрај тоа што било иновативно решение за снабдување, имало и здравствена и санитетска придобивка. Во древна Кина, критичната инфраструктура била ѕид кој обезбедувал заштита против инвазии и олеснувал економски, воен и културен развој. Во колонијална Шпанија, критичната инфраструктура подразбирала златни рудници во Јужна Америка, пристаништа и флотата која го пренесувала овој скапоцен суров материјал во земјата. Во денешни услови, секако, поимот за критичната инфраструктура е многу поширок поради технолошкиот прогрес, појавата на новите феномени, итн. Но сепак, системите на критичната инфраструктура, од аспект на нивното значење, остануваат исти.

Во прилог на генезата на развојот на концептот на критична инфраструктура, е да се наведе фактот дека генерално, подготвеноста на инспораката на добрата и услугите од критичната инфраструктура била во рацете на државата, што довело до поголем број големи компании и претпријатија во државна сопственост. Овој баланс, каде државата преовладувала во грижата за заштита на критичната инфраструктура, во современи услови е сменет.[84]

По крајот на Студената војна, голем број влади од западниот свет го редуцираа својот удел во овие капацитети. Оваа промена е на ракурс веќе неколку декади, и во овој домен спаѓаат компаниите за производство и дистрибуција на електрична енергија, електрична мрежа, телекомуникациски компании, комуникациски мрежи, национални авионски компании,

[84] Riedman, D.: The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks. Homeland Security Affairs. *The Journal of the NPS Center for Homeland Defense and Security*. June 2017. [article] https://www.hsaj.org/articles/13976, посетена на 21/12/2019.

аеродроми и писти, пристаништа, и разни видови продукти и услуги кои претходно беа ексклузивно државни, како што се поштите, изградба и одржување патишта, железници, воден сообраќај, здравствени услуги, итн. Така што, во денешни услови, инфраструктурата не треба да се поима во тесната смисла на транспортни мрежи или пак обезбедување на јавните услуги. Во современиот стил на живот, се наметнува потребата за проширување на оваа дефиниција и вклучување на широкиот спектар закани кои ги вбројуваат дигиталните мрежи, банкарскиот и финансискиот сектор, прехранбениот сектор, јавното здравство итн.[85] Може да се заклучи дека модерната критична инфраструктура претставува ефективен инструмент во рацете на противниците кои се во можност и кои посегнуваат да употребат хибридни методи.[86]

При одговор на прашањето што е критична инфраструктура и која е нејзината улога во секојдневниот живот на луѓето и функционирањето на општествените активности, доволно е само да ги погледнеме вестите во кои се известува за земјотреси, урагани, протекувања на опасни хемикалии од фабриките итн. Станува јасно дека е неопходна потребата за зајакнување на капацитетите на системите на критична инфраструктура за да се намалат ефектите и последиците од овие ризици.[87] Еден фактор кој е директно поврзан со редукција на ризиците од катастрофи е пристапноста и одржувањето на критичната инфраструктура.[88] Во тој контекст, се дава одговор на следните пет прашања:

1. Што е критична инфраструктура? Критичната инфраструктура генерално подразбира 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

[85] Hybrid Threats. European Union. Institute for Security Studies. https://www.iss.europa.eu/tags/hybrid-threats, посетена на 20/12/2019.

[86] A Europe That Protects: Good Progress on Tackling Hybrid Threats. European Commission. 29 May 2019.https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788, посетена на 20/12/2019.

[87] Taquechel, F., E. & Lewis, T., G: Right-Brained Approach to Critical Infrastructure Protection Theory in Support of Strategy and Education> Deterrence, Networks, Resilience and "Antifragility". Homeland Security Digital Library. Naval Postgraduate School (US) Center for Homeland Defense and Security. Homeland Security Affairs (October 2017), v.13, article 8. https://www.hsdl.org/?abstract&did=805457, посетена на 15/12/2019.

[88] Fay, J., J. & Patterson, D. (2018): Vulnerability Assessment. Contemporary Security Management (Fourth Edition), 2018, https://www.sciencedirect.com/topics/computer-science/critical-infrastructure-and-key-resource, посетена на 15/12/2019.

ги опфаќаат: енергетскиот сектор, секторот за управување со води, прехранбениот сектор, транспортниот сектор, телекомуникациите, здравството, банкарството, финансиите итн. Сепак, важно е да се напомене дека не постои универзално прифатена дефиниција и секоја држава ги дефинира овие сектори во согласност со своите интереси. Многу земји подготвуваат национални стратегии за заштита на нивната критична инфраструктура од природни и антропогени ризици и катастрофи. Дополнително, сајбер-безбедноста станува приоритет во заштитата на инфраструктурата од секој сектор.[89]

2. Како се разликува критичната инфраструктура низ светот? Пристапот и достапноста на критичната инфраструктура, како на пример енергетиката, е суштинска за стабилноста и развојот, но сепак, варира во секоја земја одделно. На пример, граѓанин на Германија во 2015 година, во просек бил изложен на 15-минутен недостаток на струја, додека граѓаните на Непал биле изложени на 26 целосни системски колапси и околу 91 час без дистрибуција на енергија во рамки на една недела за време на редукција на оптоварувањето во фискалната 2015/16 година. Сепак, во овој контекст, треба да се забележи дека големи прекини на снабдување на енергија понекогаш се случуваат и во земји со развиена и сигурна инфраструктурна мрежа, каде изворот на загрозување може да се наоѓа во сајбернападите. Во оваа насока, како податок е значајно да се потенцира дека руралните средини се посклони на дефицит и прекин во снабдувањето, а обновата на инфраструктурата може да трае подолго. Прекините на снабдување во градовите имаат тенденција да влијаат повеќе врз луѓето и имаат потенцијал да предизвикаат поголеми економски загуби.
3. Што претставува дефект или крах на критичната инфраструктура? Како илустративен пример може да се наведе Порторико, кога островот беше погоден од ураганот „Марија“, што предизвика речиси целиот остров да остане без електрична енергија, што наскоро предизвика и други, каскадни проблеми, како недостаток на чиста вода, разладување, како и потешкотии во обезбедување на соодветна медицинска нега итн. Кога настанува колапс на одредена критична инфраструктура, диспропорционално, последиците повеќе ги чувствуваат ранливите елементи на општествената популација. Речиси половина од жртвите во ураганот „Катрина“, на пример, биле

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

лица во поодминатa возраст, или пак неподвижни лица кои биле врзани за својот дом, каде ситуацијата се компликува дополнително, доколку тие зависат од електронски помагала и медикаменти во услови кога се затворени патиштата и кога се оштетени системите за пренос на електрична енергија. Во овој контекст, секторот за итни служби мора да води грижа за потребите на сите социетални групи.

4. Како се редуцираат катастрофите преку критичната инфраструктура? Достапноста на инфраструктурите е витална за навремено опоравување откако ќе настане катастрофа. Одржувањето или брзото обновување на патните приоди, дотокот на питка вода или здравствените услуги спасуваат животи. Дополнително, многу од несреќите се зголемуваат по својот интензитет и последиците поради слабата инфраструктура. Како пример, бројот на жртвите од земјотресот на Хаити во 2010 година беше дополнително зголемен поради слабата инфраструктура која пак беше резултат на лошите економски услови. Исто така, подготвеноста на критичната инфраструктура, како и подготвеноста на населението за долгорочни прекини во снабдувањето поради катастрофи има клучно значење.
5. Како може населението да се подготви за крах или дефект на критичната инфраструктура? Потпирањето единствено на владина поддршка во случаи на долготрајни недостатоци на водоснабдување, енергенси, или други инфраструктурни продукти и услуги може да нанесе значителна штета од повеќе аспекти. Така што, подготовките како што се резерви на храна и вода, како и резерви на медикаменти, се препорачливи дури и за земјите каде прекините во снабдувањето со овие витални продукти и услуги е исклучок. Повеќе примери од реалните случувања на катастрофални настани покажуваат дека подготвеноста на заедницата и соработката помеѓу засегнатите страни се моќни алатки што може да придонесат за намалување на ранливоста кога настанува дефект или крах на критичната инфраструктура.[90]

[90] Critical Infrastructure Resilience as a Minimum Supply Concept. United Nations University. Institute for Environment and Human Security. https://ehs.unu.edu/research/critical-infrastructures-resilience-as-a-minimum-supply-concept-kirmin.html#outline, посетена на 13/12/2019.

2. ПОИМ И ЗНАЧЕЊЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Поимот „критичен“ е клучен за правилно разбирање на терминот „критична инфраструктура“. Придавката критичен доаѓа од старогрчкиот јазик, а во современиот македонски јазик е преземена од англискиот јазик. Од повеќето значења на придавката „критичен“, својствени се две поимања, и тоа: првото значење на критичен означува нешто што е суштинско, неопходно и животно важно (витално), а второто значење се однесува на нешто решавачко, судбинско и пресвртно.[91] 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, а нарушувањето на нејзиното нормално функционирање може да доведе до загрозување на најзначајните вредности и добра врз коишто се потпираат државата, општеството, економијата, 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 критична инфраструктура може да се смета за инструментална, средствена вредност. Тоа подразбира дека критичната инфраструктура би можеле да ја одредиме поимно како вредност или збир вредности и добра што се од суштествено значење за економијата, за државата и за општеството, најчесто идентификувани како сложени материјални и нематеријални системи, чие нарушување во функционирањето или уништувањето би можело да создаде долгорочни штетни последици врз основните вредности на економијата, на државата и на општеството во целина.[92]

Значи, критичната инфраструктура претставува значаен сегмент во заштитата на основните столбови на човековото дејствување и живот. Критичната инфраструктура претставува средство или систем, кој суштински придонесува за одржување на виталните општествени функции. Оштетувањето на критичната инфраструктура, уништувањето или прекинот на функционирањето на овие системи, предизвикано од природни катастрофи, малициозно однесување, криминални активности

[91] http://www.merriam-webster.com/dictionary/critical, посетена на 20/11/2015, во Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016, стр. 9-29.

[92] Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016, стр. 9-10.

и тероризам може да предизвика значајни последици врз безбедноста на луѓето, општествата и меѓународниот поредок.[93]

Развојот на критичната инфраструктура во сите сегменти е тесно поврзан со развојот на општеството. Заради тоа, критичната инфраструктура како витална, комплексна и меѓусебно структурно поврзана целина е од исклучителна важност за 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 ослабнувачки 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.[94]

Оттука, нема дилема дека критичната инфраструктура е есенцијален, односно суштински дел на националната безбедност на секоја држава, па оттука нејзината заштита е врвна цел и приоритет на секоја земја, особено ако се знае фактот дека општествените девијации (на пример: кражби, измами, индустриски шпиунажи, саботажи, диверзии, злонамерни оштетувања и сл.), природните катастрофи, техничко-технолошките несреќи, човечките пропусти итн., сите може да предизвикаат големи човечки загуби и материјални штети. Ако на овие елементи се надоврзат и одредени специфични облици на загрозување, во чии рамки спаѓа и употребата на современите оружја и напредни технологии, вклучувајќи го и нуклеарниот материјал, хемиските и биолошките оружја и слично, сето тоа е јасен сигнал дека имаме сериозен безбедносен ризик кој надополнет со веројатноста таквото оружје да биде употребено во акти на незаконско постапување и врз критичната инфраструктура, ја наметнува потребата од создавање соодветни механизми за заштита на критичната инфраструктура.[95]

[93] 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.

[94] Бакрески О., Милошевска Т. и Алчески Ѓ., Заштита на критична инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 7-17.

[95] Исто., стр. 7-17.

Беше истакнато дека заканите по критичната инфраструктура може да бидат проценети како природни, предизвикани од човек и технолошки. Критичната инфраструктура и клучните ресурси се физички и виртуелни системи кои се неопходни за операциите во економијата и во владините институции. Заканите за критичната инфраструктура еволуираат, и најчесто, како што беше истакнато, вклучуваат пандемии, екстремни временски услови, несреќи и технички дефекти, терористички дејствија, како и сајбер-напади. Ризиците треба да бидат утврдени врз основа на овие закани, вклучувајќи ја и веројатноста за настанување и последиците од овие закани по непосредната критична инфраструктура, како и меѓу-зависните системи и објекти. Така што, критичната инфраструктура не е одделен збир на физички објекти, туку меѓусебно поврзан систем од системи, каде секој дел зависи и влијае на оперативноста на други делови во системот, исто така познат и како каскаден импакт. Дефект или крах на еден дел од системот, ќе влијае врз системот и ќе создаде каскадни ефекти низ него. На пример, рафинериите за гориво зависат од транспортните системи, како возови, бродови, цистерни, цевководи, итн., за да ги движат своите производи,[96] односно транспортните состеми зависат од производството на рафинериите за да им обезбедат гориво за да бидат во можност да се движат и да функционираат. Дополнително, компјутерските системи кои ги контролираат поголемиот дел од инфраструктурните системи зависат од електричната мрежа за да се оперативни во процесните контроли и системите за индустриска контрола кои се неопходни за функционирање на сложените процеси. Нарушувањата и прекините во кој било дел од меѓусекторскиот ланец на набавка може да има директно влијание на локалната, на регионалната и на државната економска стабилност, така што развивањето на план за заштита на критичната инфраструктура и на виталните клучни ресурси е есенцијално за избегнувањето и за ублажувањето на последиците.[97]

[96] Critical Infrastructure. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx, посетена на 14/12/2019.

[97] Critical Infrastructure and Key Resources Support Annex. CISA. Homeland Security. [online] https://www.dhs.gov/cisa/critical-infrastructure-and-key-resources-support-annex, посетена на 15/12/2019.

3. ОПРЕДЕЛУВАЊЕ НА КРИТИЧНАТА ИНФРАСТРУКТУРА

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, нејзината економија, како и 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.[98]

Сепак, треба да се нагласи дека не постои глобално прифатена дефиниција за тоа што претставува критичната инфраструктура. Различни држави и организации развија своја дефиниција за тој концепт, меѓу нив и ОБСЕ, според кој критичната инфраструктура претставува „меѓусебно поврзани информатички системи и мрежи, а прекинот или уништувањето може да предизвика сериозни последици врз здравјето, врз безбедноста, врз економската благосостојба на граѓаните, или пак врз ефикасното функционирање на владата и економијата.“[99]

За Европската Унија „критичната инфраструктура претставува имот, систем или дел од него лоциран на територијата на една земја-членка и неопходен за одржување на клучните општествени функции, здравје, безбедност, сигурност, економска или социјална заштита и чие мешање или уништување би имало значително влијание врз земјата-членка.“[100]

Во рамките на програмата за планирање на вонредни состојби на НАТО, критична инфраструктура се состои од ресурси, од капацитети, од мрежи и од услуги чие повремено онеспособување или уништување би имало сериозни последици врз здравјето, безбедноста, стабилноста, економската благосостојба или врз вообичаеното функционирање на државата. Доколку не се заштити критичната инфраструктура, би можела да страда во случај на природни и на други непогоди, вклучувајќи го и тероризмот.[101]

---

[98] Critical Infrastructure. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx, посетена на 12/12/2019.

[99] Lopez, J., Setola, R., Wolthusen, S., *Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defense, Springer*, 2012, стр. 39.

[100] Интернет извор; http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_3-2015/67-2015-3-14-Skero.pdf, стр. 2

[101] Миќовиќ М., Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуацијама, докторска дисертација, Белград, 2016, стр. 34.

Интересно е да се спомене дека Светската здравствена организација поимот безбедност го дефинира како „слобода од неприфатлив ризик од штета или несреќа, а пак, безбедноста на критичната инфраструктура е дефинирана како отсуство на несреќи, повреди и жртви.[102] Во овој контекст, терминот несреќа опфаќа широк спекар несакани колизии и судири, односно настани кои главно не може да се предвидат и се случуваат ненамерно, но и несреќи кои биле предизвикани со интенција.[103]

Во одредени држави, како на пример САД, се смета дека критичната инфраструктура е клучна за непречено функционирање на економијата и на општеството и е еден од основните ресурси терминолошки кој се однесува на широк спектар на различни средства и имот кои се неопходни за секојдневно функционирање на социјалните, економските, политичките и културните системи во САД. Секој прекин во елементите на критичната инфраструктура претставува сериозна закана за правилното функционирање на овие системи и може да доведе до оштетување на имотот, човечки жртви и да предизвика значителни економски загуби“. За разлика од САД, Австралија има поинаков пристап кој говори дека критичната инфраструктура ги претставува оние физички објекти, снабдувачки синџири, информатичка технологија и комуникациски мрежи кои, ако бидат уништени или прекинати долго време, би можеле да имаат значително влијание врз социјалната или економската благосостојба на нацијата или ќе влијае на способноста на Австралија да ја одржи националната одбрана и да ја обезбеди националната безбедност.

За Мотеф и Парфомак, „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.“ Тие исто посочуваат дека инфраструктурата е множество на меѓусебно структурно поврзани елементи што обезбедуваат поддршка за целокупното функционирање на една средина.[104] Оттука, овие автори сметаат дека критичната инфраструк-

[102] Biringer, B., et al.: Critical Infrastructure System Security and Resilience. https://books.google.mk/books?id=IMPMBQAAQBAJ&pg=PA79&dq=critical+infrastructure+definition&посетена на 11/12/2019.

[103] Madej M., Pajak M., Road Transport of Dangerous goods in Poland. Risk Analysis. *Safety and Security in Traffic. Promet – Traffic & Transportation*, Vol. 31, No. 5, 2019. https://traffic.fpz.hr/index.php/PROMTT/article/view/3106, посетена на 13/12/2019.

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

тура треба да се прошири од она што е витално за националната одбрана и економската сигурност и континуитет на власта, до она што е витално за јавното здравје и безбедност, како и она што е значајно за националниот морал.[105]

Сличен пристап во дефинирањето имаат определени согледувања кои сметаат дека критичната инфраструктура се состои од повеќе елементи и потсистеми. Помеѓу потсистемите на критичната инфраструктура постојат поврзаности со кои, во случај на нарушување на функционалноста на еден потсистем, се проширува функционирањето во поврзаните потсистеми, и на тој начин го ескалираат импактот на вонредните состојби врз општеството.

Од изнесените дефиниции пристапи може да се заклучи дека разликите во дефинирањето на критичката инфраструктура имаат негативни ефекти кои влијаат на интегритетот на системот за заштита. Разликите потекнуваат пред сè од недостаток на единствена дефиниција за критична инфраструктура, која се меша во потсектори, ефективна комуникација и размена на информации. Покрај тоа, разликите во перцепцијата за важноста на инфраструктурата се очигледни меѓу одредени засегнати страни, вклучително и разликите помеѓу бизнис-заедницата и владините институции. Претставени се две крајности: потценување на важноста на критичката инфраструктура или преценувањето на критичноста на одредени критични инфраструктурни сектори, со цел да се добие монопол во критична заштита на инфраструктурата. Затоа неопходно е да се добие теоретски и научен консензус за дефинирање на критичната инфраструктура, со примена на два главни пристапа: прво, утврдување на критичната инфраструктура според симболичката важност што таа ја има за заедницата или системот и второ, врз основа на структурната позиција што ја има во целокупната инфраструктура да се направи потребната диференцијација.[106]

[105] Исто., стр. 5.

[106] National *Critical Infrastructure and Key Resources, Cansas City Regional Tew, Interagency Analisys Center*, стр. 10.

4. ИНДИКАТИВНА ЛИСТА НА СЕКТОРИ

Општеството традиционално зависи од широк спектар услуги, кои ги обезбедува инфратруктурата. Со текот на времето, некои од овие инфраструктури или пак нивните елементи се сметало дека се витални според важноста во одредено општество, па така започнуваат да бидат сметани како критични. Дополнително, некои инфраструктури кои во минатото се сметале за витални, во современ контекст се заменуваат или прераснуваат во други сектори и елементи од системите на критичната инфраструктура.

Анализирајќи ги сите аспекти кои ги детерминираат критичните инфраструктури, а имајќи ги предвид сложеноста, динамичноста и специфичноста во третирањето на оваа област, несомнено е дека најчесто тие претставуваат физички средства, мрежи или организации, чие нарушување или оневозможување ќе предизвика сериозна, трајна штета на општествениот и на економскиот живот. Различните национални власти имаат подготвено листи на стопански гранки, односно сектори. Тие обично вклучуваат енергија, вода и храна, управување со отпад, клучни транспортни системи (аеродроми и железници), финансиски институции, здравството, државните институции за справување во вонредни ситуации и др.[107] Оттука произлегуваат и начините на нивното обезбедување и заштита. Во повеќето земји тоа претставува симбиоза на државните органи (полиција, специјализирани заштитни сервиси и повремено војската), компании за приватно обезбедување и други служби и сервиси.[108]

Во принцип, дефинирањето на рамката на критична инфраструктура во многу земји е направена врз основа на прецизна спецификација на критичните инфраструктури. За некои држави илустративно оваа листа е прикажана на Табела број 1.

[107] Critical Infrastructure Security and Protection, The Public-Private Opportunity-White Paper and Guidelines by CoESS And its Working Committee Critical Infrastructure December, 2010, стр. 5.

[108] Исто., стр. 6.

Табела број 1:
Критична инфраструктура во различни земји во светот

КАНАДА	ВЕЛИКА БРИТАНИЈА	САД	ГЕРМАНИЈА	НОРВЕШКА	ШВАЈЦАРИЈА
Енергија (објекти со електричен и нуклеарен потенцијал, природен гас, нафта, производни и транспортни системи)	Енергија	Енергија	Енергија (електрична, нафта и гас)	Енергија и објекти	Објекти и служби
Комуникации	Телекомуникации	Информации и телекомуникации	Телекомуникации и информациска инфраструктура	Снабдување со нафта и гас	Телекомуникации
Сервиси (финансии, дистрибуција на храна, јавно здравство)	Здравствени служби	Јавно здравство	Јавно здравство	Телекомуникации	Дистрибуција на информации
Транспорт (воздушен, поморски, копнен)	Финансии	Храна	Банкарство, финансирање и осигурување	Јавно здравство	Јавно здравство
Безбедност (нуклеарна безбедност, служби за спасување, итни служби)	Транспорт	Земјоделство	Транспортни системи	Банкарство и финансии	Храна
Влада (важни владини објекти, служби за информациски системи и мрежи)	Итна служба	Банкарство и финансии	Итни и спасувачки служби	Транспорт	Финансии
	Централна власт	Итни служби	Установи на јавни служби (полиција, војска, царина итн.)	Спасувачки служби	Транспорт
	Вода и одводнување	Влада		Одбрана	Цивилна одбрана
		Основна одбранбена индустрија		Полиција	Администрација
		Вода		Општествена безбедност	Воена одбрана
		Хемиска индустрија и опасни материи			Снабдување со вода

Извор: Škero M. Zastita kriticne infrastrukture, стр. 193-194.

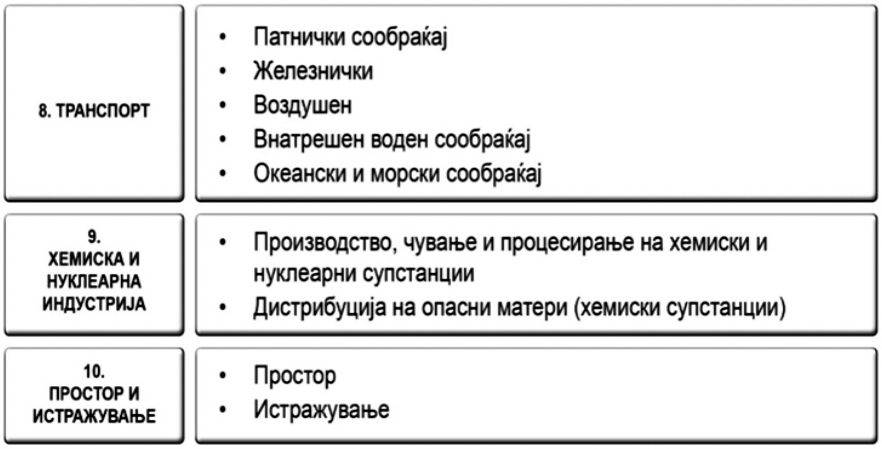
Генерално, табеларниот приказ од наведените идентификувани листи на сектори во одделните држави се во корелација со Директивата на Европската Унија за критични сектори 2008/114, која грубо ги препознава следните сектори: енергетика, информациските и комуникациските технологии, вода, храна, финансии, јавна администрација, транспорт, хемиска индустрија, истражувачки дејности,[109] со сите нивни капацитети и дејности, производи или услуги.

Идентификуваните области и објекти од витален интерес, односно критична инфраструктура, претставени од страна на Европската комисија целосно се прикажани во Табела бр.2:

Дефинирани сектори во Европската критична инфраструктура

1. ЕНЕРГИЈА	• Производство на нафта и гас, рафинирање, одржување и чување, вклучувајќи и водови • Производство на ел. енергија • Пренос на ел енергија, нафта и гас. • Дистрибуција на ел енергија, нафта и гас.
2. ИНФОРМАЦИСКИ И КОМУНИКАЦИСКИ ТЕХНОЛОГИИ	• Заштита на информациските системи и мрежи • Инструментализација, автоматизација и контролни системи. • Интернет • Обезбедување на фиксната телекомуникација • Обезбедување на мобилната телекомуникација • Радио комунукација и навигација • Сателитска комуникација • Емитување
3. ВОДА	• Обезбедување на вода за пиење • Контрола на квалитетот на водата • Контрола на количество на вода
4. ХРАНА	• Снабдување со храна, обезбедување и заштита на храната
5. ФИНАНСИИ	• Платежни сервиси и структури • Владини финансиски структури
6. ЈАВНА И ЗАКОНСКА ЗАШТИТА	• Одржување на јавен ред и мир, обезбедување и безбедност • Судска администрација
7. ЈАВНА АДМИНИСТРАЦИЈА	• Владини функции • Оружени сили • Цивилна администрација • Служби за хитни ситуации • Пошти

[109] Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005, COM, (2005), 576 final, Annex II.



Извор: Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005 COM (2005) 576 final Annex II

Во продолжение ќе се осврнеме на одредени сектори кои се често апострофирани како важни и критични во речиси сите индикативни листи, и тоа: енергетски сектор, информатички и комуникациски технологии, сообраќај и транспорт, водата како критичен ресурс, храната како критичен енергенс, хемиски сектор, финансиски и банкарски сектор, здравствен сектор.

4.1. Енергетски сектор

Секторот за енергетика се карактеризира со разновидни компоненти на инфраструктурата, за повеќеслојна оперативна средина и со комплексни структури на сопственост и регулатива. Исто така, секторот за енергетика е еден од клучните сектори врз кои се потпираат сите други критични сектори во инфраструктурата. За возврат, секторот за енергетика зависи од многу други критични сектори во инфраструктурата, како што се транспортот, информатичката технологија (ИТ), комуникациите, водата и финансиските услуги. Покрај тоа, секторот се соочува со развивачки закани и ризици, како што се настани поврзани од природна непогода, закани за компјутерската и физичка безбедност, стареење/пропаѓање на инфраструктурата и потенцијален недостиг на квалификувана работна сила.[110]

[110] Energy Sector-Specific Plan, 2015, стр. VII.

Генерално, секторот за енергетика се состои од разновидни и географски дисперзирани критични средства и системи кои честопати се меѓусебно зависни. Овој сектор на критичната инфраструктура е поделен на три меѓусебно поврзани сегменти или потсектори - електрична енергија, нафта и природен гас. За вклучување на производство, рафинирање, складирање и дистрибуција на нафта, гас и електрична енергија, освен хидроелектрични потребни се и комерцијални нуклеарни постројки и далеководи. Секторот за енергетика снабдува горива во транспортната индустрија, електрична енергија за домаќинствата и деловните субјекти и други извори на енергија што се составен дел на растот и производството низ целата нација.[111]

Во услови на либерализација на производството и дистрибуцијата на енергија, безбедноста на приватизираните енергетски производни погони не е обезбедена само преку јавниот сектор, односно исклучиво на товар на државата. Оттука произлегуваат проблемите со интерното осигурување што правните лица го имаат при производство и дистрибуција на енергијата, како и проблемот со осигурувањето на преносните делови на енергетските постројки, со што се отвораат и дополнителни проблеми во односите помеѓу јавниот и приватниот сектор. Истото важи и за управувањето со резервите со енергија и во делот на регулација на односите помеѓу објектите на критичната енергетска инфраструктура и локалните заедници. Ризикот е иманентен на начинот на кој е изградена критичната енергетска инфраструктура, а комплексноста на инфраструктурата дополнително го зголемува интензитетот на ризикот.[112]

Во основа, ризикот е дефиниран како функција на последици - човечки и економски, ранливости и закани. Различни субјекти постојано проценуваат ризици и закани во секторот за енергетика, од владини и академски институции, до трговски здруженија и индивидуални компании. Значителното внимание на медиумите, исто така, е насочено кон заканите за енергетската инфраструктура, вклучувајќи сајбер-закани и можни терористички напади. Откако ќе се идентификуваат заканите, последиците и ранливоста може да се измерат за да се утврдат трошоците за мерките за намалување на ризикот. Како и да е, видовите закани со кои се соочуваат индустриите за електрична енергија, нафта и природен гас се разликуваат во голема мера, како и значењето на „ризикот“, како што се гледа од секоја организација.[113]

[111] Исто., стр. 3.

[112] http://www.pilar.hr/kritina-infrastruktura-u-hrvatskoj#sadržaj, посетена на 23/09/2016.

[113] Energy Sector-Specific Plan, 2015, стр. 4.

4.2. Информатички и комуникациски технологии

Информатичката технологија е глобална и затоа можеме да претпоставиме дека таа, исто така, придонесе за развој на глобалната комуникација. Благодарение на информатичката технологија, количината на јавно достапни информации се шири неизмерно. Бројот на луѓе кои активно ги користат овие информации се зголемува, така што треба да се прошири просторот за развој на комуникациската култура. Поради повеќе информации за социјални настани, информатичката технологија охрабрува поширок круг луѓе да учествуваат во јавниот живот. Новите форми на двонасочна, интерактивна комуникација ја намалуваат зачудувачката функција на медиумите. Ова значи дека е зголемена можноста за јавно контролирање на информациите, но и повторно ја намалува можноста за медиумска конструкција на реалноста. Бидејќи информациите стануваат универзални, ефектите од идеологијата преку јавна комуникација се дискутабилни. Природата на компјутерските информации е јавна и не може да стане монопол на поединците. На овој начин се намалува манипулацијата со информации. Новата структура на информации и комуникации воведува нова информативна писменост што ги придвижува следните генерации на сеопфатно разбирање на природата, општеството и светот. Информативната култура, со својот нов начин на живот и нова писменост, формира нов стил на живеење.[114]

Во основа, информатичко-комуникациските технологии (ИКТ) вклучуваат напредни телекомуникациски системи, Интернет мрежи, мултимедијални услуги, медиуми и нови технологии за економија, компјутерски структури и системи, знаења, технологии за управување со системи и роботика, односно ИКТ е термин за чадор што ги опфаќа сите комуникациски уреди или апликации што вклучуваат: радио, телевизија, мобилен телефон, компјутер, мрежен софтвер и хардвер, сателитски системи итн, како и разни услуги и сродни апликации, како што се видео конференција и учење од далечина.[115]

Генерално, под информатичко-комуникациски технологии подразбираме трансфер и употреба на секаков вид информации. Информатичко-комуникациската технологија е камен-темелник на економијата и е поттикнувач на социјалните промени во XXI век. Таа влијае на секој аспект

[114] Vreg F., *Demokratsko komuniciranje*, NUB BiH, Sarajevo, 1991, стр. 328-333.

[115] http://www.inst-antonatrstenjaka.si/gerontologija/slovar/1029.html, посетена на 17/12/2019.

на животот што го знаеме денес. Без оваа технологија животот ќе биде скоро незамислив.[116]

За информатичко-комуникациските технологии често се дискутира во специфичен контекст, како што се ИКТ во образованието, во здравствената заштита, во социјалната сфера итн. Исто така, секторот за информатичка технологија е од централно значење за безбедноста, за економијата, за јавното здравство и за безбедност на нацијата. Бизнисот, стопанството, владата, академските институции и граѓаните се сè повеќе зависни од информатичката технологија. Од тие причини, безбедноста на овој сектор потребно е да се темели на заштита на информациските системи и мрежи, на инструментализација, автоматизација и контролни системи; на интернетот; на обезбедување на фиксната телекомуникација; на обезбедување на мобилната телекомуникација; на радиокомуникацијата и навигацијата; на сателитска комуникација; на емитувањето и др. Комплексноста и динамичниот развој на секторот го прави сложен од аспект на идентификување на заканите и слабостите, што бара огромна компаниска соработка и креативен начин на заштита. Иако инфраструктурата што се однесува на информатичката технологија има одредено ниво на својствена еластичност поради големите меѓузависности, сепак претставува предизвик, како и можност за координирање на активностите помеѓу јавните и приватните сектори. Фактот дека потенцијалот на терористичките организации и поединци и во иднина постојано ќе се зголемува заедно со промените во информатичко–комуникациските технологии, справувањето со ваков вид закани е многу комплицирана задача на сите критични инфраструктури, што ги обединува оваа област.[117] Исто така, глобалното вмрежување во системот на комуникациска и на информатичка технологија стана основа на организираниот криминал, додека пак, тероризмот доби уште една алатка во своите раце. Од аспект на употреба на интернетот во функција на организираниот криминал и тероризмот би ги издвоиле планирањето на противправните дејства, крадење податоци или хакирање, предизвикување насилства, регрутација и радикализација на корисниците на овие мрежи и др. Во овој контекст, нападот на информатичките системи, може да се дефинира како директна акција против мрежата или информатичкиот систем, со цел неовластено да се пресретне или да се прекине некоја

[116] Čelebić G., Dario Ilija Rendulić, ITdesk.info – načrtovanje računalniškega e-izobraževanja s prostim dostopom - Priročnik za digitalne pismenosti, Zagreb, 2012, стр. 5.

[117] https://www.dhs.gov/information-technology-sector посетена на 24/10/2015.

операција, да се преземе контрола или да се уништи, да се промени или да се корумпира податокот (со меморирање или обработка).[118]

Улогата на државата во поглед на заштита на критичната инфраструктура од областа на ИТ безбедноста е клучна, но исто така секако дека е важна и улогата на операторите, односно компаниите што стопанисуваат со овие критични инфраструктури. Оттука заштитата треба да обезбеди да не дојде до компромитирана приватност и углед, грабежи на пари од банкарските сметки на поединци и компании, хендикепиран компјутер, но исто така и личната и семејната безбедност може да бидат доведени во потешкотии.

4.3. Сообраќај и транспорт

Сообраќајната инфраструктура го претставува јадрото на стопанската инфраструктура, односно таа е основа за движење на луѓето, на предметите, на стоките и на информациите, без коишто не би можело да се замисли развојот на човештвото.[119]

Сообраќајната инфраструктура ја сочинуваат како патиштата за сите видови сообраќај, така и објектите кои се изградени на одредено место и служат за регулирање на безбедноста во сообраќајот и производство на сообраќајни услуги. Сообраќајната инфраструктура, составена од сообраќајници, морски и речни пристаништа, воздушни пристаништа, цевководи, како и постојани и стабилни уреди на патиштата, ја сочинуваат структурата на сообраќајниот систем и неговите потсистеми. Од моментот на проектирањето, конструирањето, изградбата, експлоатирањето и инвестициското и тековното одржување на сообраќајната инфраструктура, самата таа, во поголема или помала мера влијае на оптимизацијата на сообраќајниот систем, а интензитетот на нејзиното влијание во одредени сообраќајни гранки значително е променлив.[120]

Денес, како и во минатото, улогата на сообраќајот во стопанскиот развој на секоја земја е повеќекратна и многу значајна. Постои силна меѓузависност помеѓу степенот на развој на сообраќајот во една земја и развојот на стопанството во истата. Сообраќајот се јавува како резултат на одредено ниво на економски развој од една страна, а пак од

[118] Stallings William, Network and Internetwork Security – Principles and Practices, Prentice Hall, Englewood Cllifs, New Jersey 1995., стр. 29–30, преземено од *Корпорациски безбедносен систем*, Комора на РМ за приватно обезбедување, Скопје, 2012, стр. 165-243.

[119] Здравковски Б., *Сообраќајна инфраструктура*, Скопје, 2010, стр.11

[120] Исто, стр. 11.

друга страна врши влијание врз економскиот развој на секоја земја.[121] Сообраќајната инфраструктура (патишта, пруги, реки и канали) со основните инфраструктурни објекти го овозможува процесот на сообраќајните услуги, додека транспортот е самостојна дејност која се занимава со пренос на стока, луѓе и вести, од едно до друго место, со цел да ги задоволи потреби на човекот, како во сферата на материјалното производство, така и во секојдневниот живот. На денешното ниво на развој на општеството, транспортот стана важна област за која е поврзано извршувањето на многу важни економски функции. Важноста на превоз може да се види во сферата на транспортот, односно единствени пазари и вклучување на земјите во меѓународната поделба на трудот. Транспортот игра голема улога во историскиот развој на човечкото општество и почетоците на една голема социјална поделба на трудот. Со доаѓањето на паробродот, развиен е поморскиот транспорт, а во 1825 година железничкиот транспорт, со појавата на моторот со внатрешно согорување се развива патниот сообраќај, додека во 1897 година со појавата на авионот, започна и развојот на воздушниот сообраќај. Современиот транспорт е поврзан со индустриската револуција кога се јавил брз развој на производствените сили, на трговијата, а аналогно на тоа се јавил и брз развој на меѓународниот транспорт. Напредокот во транспортната технологија има силен одраз во примената на нови методи во производните процеси, нови и зајакнати социјални, политички и економски врски помеѓу земјите во географскиот простор.[122]

4.4. Водата како критичен ресурс

Водните ресурси, и опсегот на услугите што ги обезбедуваат, придонесуваат за намалување на сиромаштијата, економски раст и одржливост на животната средина или кажано на класичен јазик, од безбедност на храната и енергијата до здравје на луѓето и животната средина, водата придонесува за подобрување на социјалната благосостојба и инклузивен раст, кои влијаат на животот на милијарди луѓе,[123] и затоа тоа што е ретко е и скапо. Оттука, водата како најважен ресурс во светот нема цена.[124]

[121] Jusufranić I., *Osnove drumskog saobracaja, Tehnologija – Organizacija – Ekonomika – Logistika – Upravljanje*, Травник, 2007, стр. 17.

[122] Темјановски Р., Транспортните коридори: предизвици и ограничувања во економскиот развој стр. 2.

[123] http://www.iph.mk/svetski-den-na-vodata-2015-vodata-i-odrzliviot-razvoj/ посетена на 17/12/2019.

[124] Платон, 427-347 година п.н.е.

Значи, водата е од непроценливо значење за здравјето на луѓето. Човечкото тело може да издржи со недели без храна, но само неколку дена без вода. Затоа, водата е од суштинско значење за нашиот опстанок. Човечкото тело, во просек содржи од 50-65% вода. Бебињата имаат највисок процент на вода; новороденчиња имаат 78% вода. Секој ден, на секој човек му е потребно пристап до вода за пиење, готвење и лична хигиена. Светската здравствена организација препорачува 7,5 литри на жител дневно ќе ги исполни барањата на повеќето луѓе во повеќето услови, а поголема количина од околу 20 литри на жител дневно ќе е доволна за основните хигиенски потреби и основната хигиена на храната.[125] Според ООН, една милијарда луѓе на Земјата немаат постојан пристап до здрава вода за пиење, а 2,4 милијарди во моментов немаат пристап до вода за хигиена или канализација. Секоја година осум милиони луѓе умираат во светот, вклучувајќи и два милиони деца, од болести предизвикани од пиење неисправна вода. Недостаток на вода значи несигурност во храна, глад, сиромаштија и ширење на заразни болести, но исто така е одлична можност да се заработат пари за транснационалните компании за вода. Се проценува дека околу половина милијарда луѓе зависат од приватните корпорации за производство на вода.[126] Проценките на Светската здравствена организација говорат дека само 2,5% од слатката вода на планетата Земја се наоѓа во подземни води, а 30,8%, во езерата, во реките 0,3%, додека повеќето слатки води се заробени во глечерите (68,9%). Се проценува дека само 1% од свежата вода или 0,007% од вкупната количина на вода може да се користи за човештвото. Резервите на вода за пиење не се неисцрпен природен ресурс. Во повеќето земји во Африка и во Азија, хронични недостатоци на вода се присутни. Најголемото потенцијално зло што денес му се заканува на човештвото е загадувањето на водата, воздухот и почвата. Динамичниот развој на општеството и зголемените притисоци врз природната средина, а со тоа и на водата, стануваат едно од клучните прашања за одржлив развој, бидејќи загадувањето на подземните води, езерата, реките и морињата дополнително придонесува за намалување на постојните водоснабдувања.[127]

[125] http://www.iph.mk/svetski-den-na-vodata-2015-vodata-i-odrzliviot-razvoj/ посетена на 17/12/2019.

[126] Mikulandra A., 22. ožujka obilježavamo Svjetski dan voda, Osnovna škola Čazma, 2014.

[127] https://www.zzjzfbih.ba/svjetski-dan-voda-voda-i-energija/ посетена на 17/12/2019.

Синтагмата дека без вода нема живот е потврдена со фактот дека на целиот жив и нежив свет на нашата планета му е потребна вода. Таа е дар на природата и сите ние имаме исто право на тој подарок. Водата е општо добро што нема и не знае граници и не смее да биде во приватна сопственост или да се тргува. Но, денес, всушност, сме сведоци на тоа. Природата не ни наплаќа за водата што ни ја дава, така што продавањето на водата за профит го уништува природното право на дарот на природата и ги лишува сиромашните од дел од нивното основно човеково право.[128]

Земјоделството е едно од најголемите корисници на вода, така што потребите за наводнување се големи. Количеството вода што е потребно за земјоделско производство зависи од видот на растението, климатските услови на подрачјето каде се одгледува растението и технологијата на одгледување, но сепак потребите за вода секогаш се доста големи. Бидејќи количината на природни врнежи од дожд честопати не е доволна или врне во „погрешно време“, луѓето долго време се обидуваа да го решат проблемот со наводнување. Денес се применува површинско наводнување и современ систем на подземно наводнување, како и наводнување со вештачки дожд и наводнување капка по капка.[129] Во последните 30 години земјоделското производство се зголеми за повеќе од 100%, а 3/4 од вкупната потрошена вода се троши за земјоделско производство.[130]

Во некои делови на светот, водата е главен извор на енергија. На пример, Норвешка добива 99% од електричната енергија од хидроцентралите. Меѓу континентите во однос на хидроелектричната енергија е водечка Јужна Америка, каде повеќе од 73% електрична енергија се произведува во хидроелектрани. Поради спротивставување на еколошкиот дел од јавноста, доцни изградбата на нови хидроцентрали. Поточно, хидроцентралите одамна се сметаа за најчисти и најеколошки извор на енергија затоа што не се придружени со какви било штетни емисии или зрачење. Како и да е, во последно време станува сè повеќе очигледно дека големите вештачки езера негативно влијаат врз животната средина затоа што доаѓа до потопување на големи области на квалитетно земјоделско или шумско земјиште. Ова повторно влијае на микрокли-

[128] Beraković, M., Voda-vječna tajna prirode, Zagreb, Antibarbarus, 2015., стр. 205.

[129] Mayre, D., Voda od nastanka do upotrebe, Zagreb, Prosvjeta, 2004, стр. 126-142.

[130] Mikulandra A., 22. ožujka obilježavamo Svjetski dan voda, Osnovna škola Čazma, 2014.

мата, флората, фауната и животниот стил на луѓето. Затоа, т.н. „зелени" предлагаат еколошки мали хидроцентрали. Овие се објекти од долната граница на инсталираниот капацитет од 5 kW, до горната рана од 30 MW. Важно е тие да се градат во помали ридови и планински водотеци со минимални градежни работи, така што нивните потенцијални влијанија врз животната средина ќе се минимални.[131]

Земајќи ја предвид важноста на водената инфраструктура во сите домени на живеењето, таа со илјадници години наназад била цел на напади.[132] Оттука, заштитата на водата и на водните ресурси е исклучителна грижа на државата бидејќи снабдувањето со вода е првенствена потреба за граѓаните, но и за другите системи од критичната инфраструктура.

4.5. Храната како критичен енергенс

Во основа, храна се нарекуваат сите супстанции од растително, од животинско и од минерално потекло кои служат за извршување на одредени функции во човечкото тело, односно храната за човечкото тело има неколку карактеристики како: физиолошки градење нови клетки, обезбедување енергија, заштита на организмот (витамини и минерали), потоа таа евоцира чувство на уживање, има лековита улога, превентивна (нормален раст, развој и функционирање на организмот) и куративна.[133]

Значи, храната е супстанција која се внесува во организмот за да ги задоволи гладот и хранливите потреби (енергија, градивни и регулаторно-заштитни). Храната е исто така супстанција која со апсорпција во организмот придонесува за зачувување на хомеостазата (одржување на биолошкиот систем и неговата внатрешна средина во рамките на физиолошките процеси) и како таква значително влијае на физичката, менталната, емоционалната и духовната состојба на луѓето. Со тоа, храната е директно поврзана со исхраната, која е дефинирана како процес или група на метаболички процеси што се одвиваат во организмот од моментот кога се зема храна (јаде) до нејзиното искористување во организмот. Супстанциите коишто се внесуваат во организмот, а при тоа се искористуваат за да му обезбедат на телото потребна енергија (јагленхидрати, липиди, протеини/белковини), изведуваат сврзна (про-

[131] Исто., стр. 145-150.

[132] Dan Kroll, Aqua ut a Telum "Water as a Weapon", 2010, http://hachhst.com/technical-library

[133] http://studenti.mojsajt.rs/uploads/20177/documents/1_deoishrana.pdf/ посетена на 17/12/2019.

теини / белковини) и регулаторно-заштитна улога (минерали и витамини) се нарекуваат хранливи материи. Науката која ја проучува храната е наука за храна (engl. Food science), додека исхраната се проучува од науката за исхрана; (engl. Nutritionism). Двете науки се мултидисциплинарни, многу слични и честопати се поистоветуваат. Разликата помеѓу термините храна и исхрана е во основата на разликувањето помеѓу науката за храна и науката за исхрана. Двете, во принцип, ја третираат храната, меѓутоа, науката за исхрана повеќе го проучува односот помеѓу човекот и храната.[134]

Кога станува збор за храната основното прашање кое се наметнува е прашањето „Каква храна се внесува“. Луѓето ширум светот се разболуваат од храната што ја јадат, а повеќе од 250 познати болести се пренесуваат преку храната. Болести предизвикани од храна се болести кои се резултат на консумирање загадена храна. Храната е загадена ако се присутни патогени микроорганизми и / или нивни токсини.[135]

Значи храната претставува многу лесно подрачје за контаминација во функција на биотероризмот, за што постојат голем број сомнителни контаминации, било тоа да се од економски или од други побуди, но сепак прехранбената индустрија претставува висок ризик кога станува збор за актите на незаконско постапување.[136] Од тие причини, потребен е адекватен приод кон проценките на ризици, со цел спречување на контаминација на храната во сите облици на користење. Во тој контекст, проценката на ризик од терористички напади по пат на храна ги содржи следните компоненти: идентификација на опасноста, карактеризација на опасноста, процена на изложеност и карактеризација на ризикот. Оваа постапка е развиена во Агенцијата за храна и лекови во САД (FDA, 2003). Мерките на превенција, заедно со зголемениот надзор и средствата за адекватен одговор во случај на намерен или случаен инцидент, подоброто следење на храната и можноста од брзо повлекување, двонасочната комуникација на државните служби и прехранбената индустрија, однапред предвидените сценарија што ќе ги распределат ресурсите и поедноставување на приоритетите во случај на инциденти, како и координацијата помеѓу владата, индустријата и јавноста, треба да биде минимумот што треба да го реализира секоја влада.[137]

---

[134] Alibabić V. Mujić I., *Pravilna prehrana i zdravlje, Veleučilište, Rijeka, 2016, стр. 3.*

[135] http://www.batut.org.rs/download/aktuelno/briga/pdf, посетена на 17/12/2019.

[136] Antunovic B., Varga I, Kralik G, Baban M, Poljak V, Njari B, Pavlovic Z, Mackic S: Racunalna simulacija kao alat za procjenu rizika od teroristickih napada u lancu proizvodnje hrane – Krmiva 53, Zagreb, 2011, стр. 31-46.

[137] Исто., стр. 31-46.

Суштинските правни основи на законодавството за храна се Регулативата бр.178/2002 (ЕС) и Регулативата бр.882/2004(ЕС) кои директно се применети во сите земји-членки на ЕУ. Со Регулативата бр.178/2002 (ЕС) дадени се генералните принципи и барања на законодавството за храна на Унијата. Регулативата ги опфаќа сите фази на производство и обработка на храна во синџирот на храна врз принципот „од фарма до трпеза". *Со Регулативата бр. 882/2004(ЕС)* се дадени генералните принципи за спроведување контрола, деталите за изготвување на повеќегодишни национални контролни планови од страна на земјите членки и кореспондентни извештаи во рамките на Унијата. Проценатa на ризикот е институционално одвоена од управувањето со ризикот. Комуникацијата со ризик, третата компонента на анализата на ризикот, е поделена помеѓу проценителите и управувачите со ризик. Проценитe на ризик се објавуваат на интернет.[138]

4.6. Хемиски сектор

Хемиската индустрија потекнува од XIX век (во времето на индустриската револуција). Нејзините производи опфаќаат две главни категории – органски производи засновани на нафта и природен гас (етилен пропилен, метанол и деривати) и неоргански производи (индустриски гас, големи киселини – сулфурни, хлороводородни, азотни и соли). Производите за органска хемија претставуваат 70% од вкупното производство на хемиската индустрија. Производството на хемиската индустрија е насочено кон две големи гранки на производи – лесни и тешки хемикалии. Лесната хемија се наоѓа во составот на фармацевтската индустрија, производство на парфеми, козметика, производи за одржување, мастила, тушеви, бои, лакови, но и во составот на електронската, оптичката и агропрехранбената индустрија, производството на специјални лепила за авиони и летала, кожа и текстил. Тешката хемија, опфаќа производи од широк спектар, како што се петрохемиски или карбохемиски, засновани на јаглен. Најуспешните производи на тешката хемиска индустрија во 1998 година беа производите за дезинфекција и одржување, наменети за домаќинства или професионална употреба и растечки асортиман на производи за заштита на растенија (продажба на фитосанитарни производи, односно пораст од околу 8,5-9% на годишно ниво). Петрохемијата е најновата гранка на хемиската индустрија, која се појавува (веднаш

[138] Бакрески О. Милошевска Т. и Алчески Ѓ., *Заштита на критична инфраструктура*, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 61-62.

по завршувањето на Првата светска војна) во време кога „Стандард оил"(Standard Oil) произведува изопропанол (антифриз, растворувач), додека „Унион карбид" (Union Carbide) произведува карбид, гликол (антифриз), а „Ситис сервис" (Cities Service) го усовршува производството на метанол (растворувач) и од 1928 година, синтетизиран амонијак, пропилен, кој од 1938 година овозможи производство на полиестер, а во 1939 година револуционерна најлонска основа на полиамидна смола. Петрохемијата напредува брзо во 50-тите и 60-тите години на минатиот век. Во раните 70-ти години, три региони преовладуваа во петрохемиското производство - САД, Западна Европа (ФР Германија, Франција и особено Велика Британија) и Јапонија. Хемиската индустрија е сектор во кој научното истражување и развој се од големо значење во однос на континуираната иновација. На почетокот на 1988 година, во рамките на хемиската индустрија, беа извршени повеќе од 10% истражувања од вкупното истражување и развој. Хемиската индустрија е предмет на посебен надзор по катастрофите (Италија, 1976 година – контаминација на диоксин) и Бопал (Индија – истекување токсичен гас, убивајќи повеќе од 2.000 луѓе). Во производството во хемиската индустрија, прва е ЕУ со 32% од вкупното светско производство, пред САД (26%), Јапонија (15%) и Азија без Јапонија (12%). Размената помеѓу партнерите (ЕУ, САД, Јапонија) е балансирана. Половина од производството на петрохемиски производи доаѓа од региони надвор од САД и Западна Европа, некогаш најголемите пазари во светот. Хемиските компании од запад инвестираа во азиските земји до 1997 година. На Блискиот Исток се појавија производствени единици од областа на основната хемија, чија работа се заснова на наоѓалишта на природен гас, кои се многу поисплатливи од единиците во старите индустријализирани нации, особено за производство на она што Англичаните го нарекуваат нафта (нафтен дериват помеѓу бензин и керозин). Поради оваа причина, поранешните поголеми производители се откажуваа од дел од своето производство во областа на основната хемија и развиваат активности со поголема додадена вредност, во областа на лесната хемија и парахемијата.[139]

Останува да заклучиме дека хемискиот сектор претставува составен дел на економијата на сите современи држави. Според официјалните податоци, овој сектор на ниво на ЕУ опфаќа 60.000 компании што вработуваат околу три милиони работници. Во САД хемискиот сектор преработува суровини во повеќе од 70.000 различни производи и е главна

[139] https://borefor.wordpress.com/2011/05/24/hemijska-industrija/, посетена на 12/12/2019.

компонента на американската економија, што учествува со околу 25 проценти од бруто-домашниот производ. Исто така, 96 проценти од производите во САД во 2013 година се произведени со поврзаност на хемискиот сектор. Од тие причини овој сектор е од суштинско значење за националната и за економската сигурност на САД.[140]

4.7. Финансиски и банкарски сектор

Финансискиот сектор се состои од финансиски институции, финансиски пазар и финансиска инфраструктура. Финансискиот сектор во повеќе држави е „банкоцентричен", бидејќи доминантен дел од пазарот (над 90% од вкупната актива на финансискиот систем) го сочинуваат банки и преку нив се одвива најголем дел од финансиската интермедијација. По банките, втори и најважни се осигурителните компании, во кои доминираат компаниите за неживотно осигурување. Покрај тоа, остатокот од финансискиот сектор главно се состои од инвестициски фондови (отворени и затворени), микрокредитни финансиски институции, компании за лизинг и пензиски (приватни) фондови. Политиката за финансиски услуги треба да осигура стабилен, безбеден и ефикасен финансиски пазар и да обезбеди кохерентност и конзистентност помеѓу различни области, како што е банкарството, осигурувањето, хартиите од вредност и инвестициските фондови, инфраструктурата на финансиските пазари, финансиските услуги на мало и платните системи.[141]

Во последната деценија, финансискиот сектор, а особено неговиот банкарски сегмент, се најде во центарот на вниманието на јавноста, како резултат на бројните скандали кои резултираа во финансиски распаѓања и беа еден од главните генератори на последната глобална економска криза. Ова резултираше со усвојување на построги регулативи и доведе до зголемен надзор од страна на централните банки, што се протега надвор од контролата на банките кон ревизорските фирми.[142]

Нема дилема дека финансискиот сектор треба да биде соодветно заштитен со цел да се овозможи непречено банкарско работење, фукционирање на финансиските пазари и на регулаторните институции

[140] Chemical Sector Specific Plan An Annex to the NIPP, 2015 Homeland Security https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf, посетена на 7/07/2016.

[141] http://ec.europa.eu/finance/general-policy/index_en.htm, посетена на 23/09/2016.

[142] https://www.moore-serbia.rs/sectors/sample-sector-(7), посетена на 17/12/2019.

и складиштата за документи и финансиски средства.[143] И покрај тоа што денес голем број финансиски активности се извршуваат електронски, сепак сè уште постои и физички пренос на средства. Инфраструктурата на финансиските услуги вклучува електронски уреди како што се компјутери, уреди за складирање и телекомуникациски системи. Покрај клучните физички компоненти, овој сектор вклучува и високо специјализирани вештини за работа што се сметаат како основни елементи на критичната инфраструктура.[144]

4.8. Здравствен сектор

Здравствениот систем е еден од најсложените системи во секоја земја. Секоја држава има обврска да се грижи за здравјето на својата популација. Здравствениот систем опфаќа здравствена инфраструктура која обезбедува широк спектар на програми и услуги и обезбедува здравствена заштита на поединци, семејства и заедници. Здравствениот систем мора да обезбеди физички, географски и економски достапна и прифатлива, интегрирана и квалитетна здравствена заштита. Исто така, треба да обезбеди развој на здравствениот персонал, одржливост на финансирањето, децентрализација на управувањето и финансирање на здравствената заштита и сместувањето на граѓаните во центрите на здравствениот систем. Целта на здравствениот систем е да се зачува и подобри здравјето на луѓето преку обезбедување на здравствени услуги на населението со модерната и традиционалната медицина на ефикасен начин, кои се во исто време достапни и прифатливи за луѓето. Со оглед на нејзината важност и влијанието врз здравствената состојба на населението на секоја држава, како и од неговото големо економско влијание, државата спроведува голем број мерки во планирањето и управувањето со здравствениот систем, со цел да обезбеди стабилно финансирање и рационален и квалитетен систем на испорака на здравствена заштита, како и обезбедување основна здравствена заштита на населението во рамките на расположливите средства. Поради стареењето на популацијата и воведувањето нови и скапи технологии, во сите земји постои постојан пораст на трошоците за здравствена заштита. Современите системи за здравствена заштита најмногу се разликуваат во методите за собирање средства за здравствена заштита, како и во

[143] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the White House Washington February 2003, стр. 75.

[144] Исто., стр. 75.

начините на плаќање на давателите на здравствени услуги. Проблемите со здравствената заштита ретко можат да се решат засекогаш. Како што земјите се развиваат, нивните системи за здравствена заштита мора да излезат во пресрет на нови предизвици.[145]

Заради сета оваа сложеност и противречност, здравствениот систем на секоја земја опфаќа голем број компоненти на условени и меѓусебно поврзани целини кои се детерминирани од политичките односи, од социо-економски околности и голем број други фактори кои, директно или индиректно, влијаат врз неговиот квалитет и ефективност. Од друга страна, здравствениот систем има директно или индиректно влијание врз скоро сите компоненти на современото општество, преку квалитетот и ефикасноста на услугите што ги нуди за граѓаните и општеството како целина. Една од вообичаените карактеристики на здравствените системи во скоро сите земји во светот е зголемувањето на потребите на јавното здравство, повеќе од кога било досега, како резултат на демографската состојба, епидемиолошкиот притисок, брзиот развој на медицинската технологија за дијагностика и третман, зголемувањето на цените на лековите (и иновативните и биолошките, итн.), превенцијата и третманот растат побрзо од економската основа на општеството. Затоа, неопходно е да се воведат соодветни системи за финансирање кои ќе обезбедат долгорочен финансиски одржлив и стабилен развој на системот за здравствена заштита.[146]

Генерално, системот на јавно здравство како сегмент од критичната инфраструктура ги претставува системите, мрежите, третманот, раководењето, како и одговор на вонредни и на итни ситуации на сите нивоа. Така што, осигурувањето на резилиентен и отпорен систем на здравствена заштита што ќе биде издржлив на нарушувања и конзистентен во зачувувањето на здравјето и животите за време на вонредни и непредвидени ситуации претставува императив за безбедноста и сигурноста на државата.[147]

Во ситуација на кризни или вонредни состојби овој сектор ќе биде доминантен и ќе има значајна улога заради карактерот на состојбите и евентуалните повреди и човечките загуби. Затоа предизвиците што ги

[145] Jovanović S. Milovanović S. Mandić J. i Jovović S., Sistemi zdrastvene zastite, *Engrami*, vol. 37 januar-mart, 2015, b. 1, стр. 75.

[146] https://medicalcg.me/zdravstveni-sistem-u-crnoj-gori-realnost-i-perspektive/ посетена на 17/12/2019.

[147] Lewis, L. P., Petit, F.: Critical Infrastructure Interdependency Analysis: Operationalizing Resilience Strategies, преземена од: https://www.unisdr.org/files/66506_f415finallewisandpetitcriticalinfra.pdf, посетена на 19/11/2019.

носи овој сектор стануваат врвен приоритет на секоја современа држава и особено ако се знае фактот дека јавното здравство и медицинските установи ја носат главната улога кога се во прашање човечките животи. Кај конвенционалните терористички напади, институциите како што се полицијата, противпожарните единици и итната помош ја претставуваат првата линија на отпор, додека од аспект на биотерористичките напади, јавните здравствени установи и медицинските институции се директно на првата линија на одбраната. Во случај на добиени сознанија дека постои закана со биолошки оружја и информацијата дека смртоносните патогени супстанци може да бидат пуштени на јавно место, лекарската фела е таа што треба да ги препознае овие закани и соодветно да реагира. Во ваквите случаи соработката на владата, локалните и национални здравствени организации, јавната безбедност, разузнавачките служби е неминовна.[148] Во ситуации на предизвикување големи медицински загрозувања, односно наплив на зголемени медицински потреби предизвикани, на пример, од биолошки тероризам или друг вид пандемии, овој сектор ќе биде со примарно значење и ќе има врвна улога кога станува збор за справување со настаната ситуација.[149]

5. МЕЃУЗАВИСНОСТА НА СЕКТОРИТЕ НА КРИТИЧНА ИНФРАСТРУКТУРА

Нациите и општествата ширум светот се соочуваат со значителни предизвици во формулирањето и имплементацијата на ефективни стратегии за одговор на ризиците наметнати од многубројните природни и антропогени хазарди. Иако заштитата на животот е императив пред, за време, и по катастрофата, потенцијалното влијание од овие настани за системите, објектите и операциите на критичната инфраструктура кои ги овозможуваат основните функции на општествените институции, јавните здравствени системи, како и економските активности се исто така голема грижа. Зајакнувањето на отпорноста на критичната инфраструктура е препознаено како итна цел во рамки на националните влади и меѓународните институции и мрежи за меѓународен развој и управување со ризици и катастрофи.

[148] Милиќ Д., Биотероризам и употреба биолошког оружја, *Ревија за безбедност - стручни часопис о корупции и организованом криминалу* – Центар за безбедносне студије, Београд, број 2, 2010, стр. 113.

[149] Purpura Ph., *Security An Introduction*, CPP 2011, стр. 520.

Сепак, со цел успешна операционализација на овие цели потребно е овие стратегии да бидат базирани на информации од страна на нераскинливите системски меѓузависности што ги споделува секој сектор на критична инфраструктура со другите инфраструктурни сектори, со ланецот за набавка и управувачките структури.

Во основа, овие меѓузависности претставуваат „систем од системи" кои сеопфатно ја карактеризираат отпорноста на критичната инфраструктура. Последиците од катастрофи може да се прошират надвор од индивидуалниот систем на критична инфраструктура директно погодени од одреден настан, и да ги пренесат потенцијалните ризици во каскадни и ескалирачки дефекти/крахови кон други меѓузависни инфраструктурни системи и во други јурисдикциски граници. Од овие причини е потребно потемелно познавање на комплексните интеракции помеѓу критичната инфраструктура при подготвувањето, при одговорот и при опоравувањето од катастрофи. Анализата на меѓузависноста кај критичната инфраструктура може да служи како поддршка на националните и на локалните актери во однос на подобро информирани и холистички решенија при носењето одлуки за одговор при кризите со кои се соочуваат. На овој начин се создава комплексна мулти-системска поврзаност и интеракција наречена систем од системи (SoS). Значи, меѓузависноста на системите на критична инфраструктура може да биде дефинирана и опишана како „систем на системи" кој се состои од многубројни, хетерогени, дистрибуирани, повремено независно оперативни системи, инкорпорирани во мрежи на повеќе нивоа кои еволуираат со текот на времето.[150] Според CoC пристапот (SoS – System of Systems), како алатка за системска анализа се зема Муировата мрежа,[151] со цел да се анализира придонесот на меѓузависноста помеѓу дистрибуцијата на вода и струја, како и транспортните мрежи и нивната поврзаност со критичните фабрики.[152] Усвојувањето на пристапот „систем од системи" за исцртување на проектите за модернизација се стреми кон намалување на трошоците и ризиците кои беа наведени. Пристапот „систем од системи" вклучува

[150] Protecting Critical Infrastructure. Homeland Security. CISA. https://www.dhs.gov/cisa/protecting-critical-infrastructure, посетена на 4/12/2019.

[151] Urban Ecology Muir Web. http://www.brooklyn.cuny.edu/web/aca_centers_casegk12/MuirWebDescriptionExamples.pdf посетена на 4/12/2019.

[152] Eusgeld, Irene & Nan, Cen & Dietz, Sven. "System-of-systems" approach for interdependent critical infrastructures. Reliability Engineering & System Safety, 2011, стр. 679–686. 10.1016/j.ress.2010.12.010. https://www.researchgate.net/publication/257391861_System-of-systems_approach_for_interdependent_critical_infrastructures, посетена на 4/12/2019.

технологии дизајнирани да овозможат интеракција помеѓу системите, апликациите, сензорите и контролните уреди преку повеќе комуникациски медиуми, користејќи повеќе протоколи. Ова овозможува корелација на податоци во реално време преку повеќе домени и платформи за оптимална ситуациона анализа и добивање оперативни сознанија. Пример за таков вид пристап „систем од системи" е DERMS – дистрибуиран систем за управување со енергетски ресурси кој е платформа која им помага најмногу на операторите на дистрибутивните системи да управуваат со нивните мрежи кои главно се засноваат на дистрибуирани енергетски ресурси.[153]

Системите на критична инфраструктура се зависни и меѓузависни на повеќе начини, каде што пристапот на зависноста се однесува на едностраната врска, а меѓузависноста подразбира двонасочна интеракција. Анализата на меѓузависностите во рамки на системите на критичната инфраструктура првенствено бара еднонасочни врски (зависности) и потоа земање предвид на двонасочните односи (меѓузависностите). Овие два вида поврзаности претставуваат основа за спроведување на процена на ризици и пресметување на ефектите од меѓузависноста на системите на критична инфраструктура и нивната ранливост, отпорност и последици.

Релевантните студии од овој вид пристап се групирани според нивниот фокус на истражување. Тоа што е важно да се забележи е дека меѓузависноста помеѓу системите на критичната инфраструктура тешко може да биде идентификувана во услови на нормална оперативност, поради тоа што некои нематеријални меѓузависни односи се невидливи со употреба на стандардни пристапи за прибирање податоци, или пак, единствено се појавуваат по настанувањето на непредвидени акцидентни настани. Оттука, историските меѓузависни инциденти може да бидат употребени за да се откријат структурите на меѓузависност или врските помеѓу системите на критична инфраструктура при екстремни настани.[154] Воспоставувањето посебни датотеки и бази на податоци од инцидентните извештаи и последователното нивно анализирање може да идентификува чести и значајни шеми на дефекти.

[153] What is DERMS? Next Kraftwerke GmbH, Cologne. https://www.next-kraftwerke.com/knowledge/derms

[154] Ouyang, M.: *Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems.* School of Automation, Huazhong University of Science and Technology. July 16, 2013. https://s3.amazonaws.com/academia.edu.documents/39898015/2014_Review_on_modeling_and_simulation_of_interderpendent_critical_infrastructure_systems.pdf?response-content-disposition=inline, посетена на 4/12/2019.

Емпириският пристап е корисен за идентификација на потенцијалните значајни шеми на меѓузависност, при што во раководењето се добива подетална слика и се зголемува капацитетот за одговор во идните случаи. Сепак, овој вид на пристап има неколку слабости. Прво, поради пристрасност во известувањето, каде може да постои недостаток на известување за некои одредени зачестени дефекти/крахови кои се меѓузависни, и кои може да имаат значително влијание. Второ, експертите и истражувачите во ова поле користат различни датотеки на податоци за прибирање податоци за дефекти и крахови, без стандардизирана методологија за прибирање за меѓузависната изведба на системите на критична инфраструктура. За ова се потребни унифицирани методи за прибирање информации, вклучувајќи и прецизни дефиниции за системите на критична инфраструктура и нивната меѓузависност, така што системот за известување може да ги следи потребите за прибирање информации и да поддржува брза анализа на податоците, редуцирајќи го времето за кодирање и сортирање на содржините на извештаите од инциденти. Трето, потпирањето на емпириските пристапи на податоци од претходни извештаи за дефекти/крахови, што може да придонесе за прецизна предикција на идни слични настани, во опсегот на прибраните податоци кои веќе се заверени во датотеката, може да не прикаже точни предвидувања за идни несреќи. Овие слабости наметнуваат потреба за пристапи на моделирање и симулација за дополнителна поддршка за донесување одлуки. Според историските податоци за дефекти/крахови и експертските искуства, емпириските анализи на ризик може да бидат изведувани за да ги идентификуваат ранливостите на системите на критична инфраструктура, и да обезбедат алтернативи за минимизирање на ризикот за дисфункционалност. За прогнозирање на потенцијални идни инциденти, според податоците од претходните инциденти и катастрофи се креира дијаграм за да ги опише процесите на каскадните дефекти/крахови во рамки на системите на критична инфраструктура, по одреден специфичен иницијален настан.[155] Потоа се проценува ризикот поврзан со иницијалниот настан и се идентификува оптималната стратегија за редукција на ризикот. Исто така, со употреба на низа временски матрици, каде што секој од нејзините елементи, во одредено време (мерено од експерти со квалитативни податоци, како што се нула, низок, среден,

[155] Hokstad, P., *et al*.: Risks and Interdependencies in Critical Infrastructures – A Guideline for Analysis. DECRIS (Risk and Decision Systems for Critical Infrastructures) Norwegian Research Council, 2012. http://folk.ntnu.no/jvatn/pdf/FrontMatter.pdf, посетена на 4/12/2019.

висок) одговара на деградацијата на квалитетот на услугата на инфраструктура која настанала заради прекинување на инфраструктурата. Понатаму, се воведува метод кој се базира на импактот за да се конструира органограм временски зависен од секој инцијален настан на дефект/крах кој придонесува за релевантни информации во услови на носење вонредни одлуки. Слични вакви модели произлегуваат од студијата на Езел (Ezell), каде се анализира и менаџира ризикот од меѓу-зависни системи на критична инфраструктура, врз основа на емпириски податоци и органограмот на настани, како и анализата на специфични механизми за каскадни дефекти/крахови помеѓу хидроелектрична мрежа за производство на електрична енергија и мрежа за транспорт на електрична енергија.[156]

Анализата на ризик базирана на емпириски податоци во најголем степен зависи од емпириските податоци и експертските одлуки. Располагањето со малку податоци може да доведе до големи грешки во резултатите од анализата. Но, доколку се располага со доволен обем на податоци за функционирањето на системите на критична инфраструктура за време на непогоди и непријателски настани, грешките може да бидат редуцирани. Исто така, доколку се располага со доволно податоци и некои други методи, како што е теоријата за статистичко учење, може да бидат употребени за директно да се извлекуваат заклучоци од голем комплекс податоци и да се обезбеди значајна поддршка за управување со ризик, како во непосредна близина на екстремни настани, така и на долгорочен план.[157]

Во основа, зголемениот тренд на конвергенција и мултисистемска меѓуповрзаност во системите на критична инфраструктура доведува до појава на неколку безбедносни прашања кои претставуваат закана за нормалните економски и општествени функции.[158] Како што се воведуваат новите технологии и *интернет на нештата*, (IoT), настануваат и нови безбедносни ризици (закани, ранливости и напади), за кои се потребни специфични безбедносни решенија.

Ризиците се особено тешки за идентификување и справување, со оглед на фактот дека интернетот на нештата произлегоа од низа

[156] Global Business Expansion: Concepts, Methodologies, Tools and Applications. Information Resources Management Association, USA. IGI Global, 2018.

[157] Input-Output Analysis. Wassily W. Leontief. Encyclopedia Britannica. https://www.britannica.com/topic/input-output-analysis, посетена на 4/12/2019.

[158] The Need for an Intelligent Grid Management System of Systems. Part 2. https://www.mprest.com/blog/item/the-need-for-an-intelligent-grid-management-system-of-systems-part-2, посетена на 6/12/2019.

различни области на студии. Користа од системите на критична инфраструктура може да биде реализирана доколку функционираат соодветно и не се нарушени. 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 опоравување 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 опоравување од ефекти на 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.[159]

Од индустриска перспектива, како и во контекстот на управувањето со ризици, првиот чекор е воспоставување на безбедносни цели. Круцијалните прашања како што се загуба на живот, економски последици и импакт врз националната безбедност, треба да бидат земени предвид при формулирањето на безбедносните цели. Вториот чекор се однесува на идентификацијата на ресурси, системи, мрежи и функции и наметнува потреба за развој на инвентар и управување со залихите. Исто така, треба да содржи основни информации за средствата, системите и мрежите во државата вклучувајќи ги и материјалните добра, човечките карактеристики и системските информации. Ова претставува прва фаза за осигурување на резилиентноста. Методологијата во фазата на процена на ризиците овозможува рационални и целосни резултати со употреба на квантитативни, систематски и ригорозни процеси. Во фазата на приоритизација на активностите, потребна е соработка со

[159] Исто., дел 2.

безбедносни партнери за воспоставување приоритети за процена на ризици, со цел да се дефинира каде е неопходна редукција на ризиците, и потоа да се утврдат проактивни безбедносни мерки кои треба да се преземат. Овој чекор бара споредување на релативните нивоа на ризици и ресурси, како и алтернативи за остварување на безбедносните цели. Понатаму, заштитните мерки се аплицираат каде што е можно да се намали безбедносниот ризик, што резултира со поекономични решенија. Во фазата на имплементација на заштитните програми, заштитните мерки се насочени кон намалување на ризиците. Фазата во која се мери ефективноста е воспоставена од систем на индикатори за да се обезбедат информации за постигнувањето на конкретните безбедносни цели.[160] Со оглед на природата на динамичните и нејасни закани, постои критична потреба за интегриран пристап за оптимизација на отпорноста и заштита на критичната инфраструктура.

Зависностите и меѓузависностите на критичната инфраструктура се комплексни елементи за пресметување. Тие се карактеризираат со различни димензии, како на пример: вид, оперативна средина, спојување и однесување при одговор, вид на дефект/крах, инфраструктурни карактеристики и состојба на работа. Тие влијаат на сите компоненти на ризикот; тие може да претставуваат закана или опасност; да влијаат на еластичноста и изведбата на критичната инфраструктура и да доведат до размножување на каскадни и ескалациони дефекти/крахови. Од тие причини, од суштинско значење е да се интегрира карактеризација на зависности и меѓузависности во методологиите за процена на ризик и отпорност. За да се постигне оваа крајна цел, развојот на сеопфатна и интерактивна процена на критичната инфраструктура и нејзините зависности и меѓузависности потребно е интегрирање на повеќе области на експертиза (на пр. инженерство, општествени науки, бизнис-континуитет, управување со итни и вонредни случаи) во комбинација со пристапи од врвот кон дното и од дното кон врвот.[161] Пристапот од врвот кон долу овозможува симултана анализа на целиот систем, што овозможува носителите на одлуки да ги дефинираат мерките за отпорност кои треба

[160] Critical Infrastructure Protection. NATO Science for Peace and Security series 2019. 26 July 2019. https://www.nato.int/cps/en/natohq/topics_168104.htm? посетена на 9/12/2019.

[161] Rinaldi, M., S., *et al*.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 2001. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.2276&rep=rep1&type=pdf посетена на 4/12/2019.

да се имплементираат на системско ниво. Пристапот од долу кон врвот е посоодветен за утврдување на отпорноста на процедурите на ниво на објект. Комбинацијата на пристапите од врвот кон долу и од долу кон врвот претставува сеопфатен метод што може да се користи за поддршка на носењето на одлуки базирано на прифатените принципи за инженеринг.[162]

6. МОДЕЛИРАЊЕ НА МЕЃУЗАВИСНОСТА НА СИСТЕМИТЕ НА КРИТИЧНА ИНФРАСТРУКТУРА

Во литературата, постојат два вида теории кои се аплицираат во моделирање на меѓузависноста на системите на критична инфраструктура и тоа: влез-излез (I–O) и пресметлива општа рамнотежа (CGE). Покрај наведените пристапи, постојат и други видови пристапи за моделирање и анализирање на меѓузависноста на системите на критична инфраструктура, како што се: метод на хиерархиско холографско моделирање (HHM), методот базиран на архитектура на високо ниво (HLA), petri-net (PN) методот, метод на динамична контрола на системот (DCST), методот на Bayesian network (BN), итн.[163]

Методот на хиерархиско холографско моделирање (HHM) е холистичка методолошка рамка која има цел да се здобие и да ги претстави разновидните карактеристики и атрибути на системите на критична инфраструктура. Овој вид метод овозможува разбирање на ризиците на различни нивоа и доловува повеќеаспектна слика на одреден систем на критична инфраструктура во насока на идентификација на ранливостите. Основата на овој модел е преклопување помеѓу различните холографски модели во однос на објективните функции, ограничувања, варијабли на одлучување, како и односи на влез и излез помеѓу системите на критична инфраструктура. Со употреба на HHM моделот, може да се развијат и да се координираат повеќе математички модели за да се претстават

[162] Petit, F., Verner, D.: Critical Infrastructure Interdependencies Assessment. Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory. Computation Institute, University of Chicago https://www.osti.gov/servlets/purl/1400396 посетена на 27/11/2019.

[163] Abrishami, S., *et al*.: BN-SLIM: A Bayesian Network Methodology for Human Reliability Assessment Based on Success Likelihood Index Method (SLIM). Reliability Engineering & System Safety. Volume 193, January 2020, стр. 35-135. https://www.sciencedirect.com/science/article/pii/S0951832019305356, посетена на 4/12/2019.

повеќе димензии, визури и перспективи за меѓузависноста на системите на критична инфраструктура.[164]

Сепак, овој пристап е компликуван да се употреби во меѓузависните системи на критична инфраструктура поради: структурната сложеност, еволуцијата на мрежите, разноликоста во поврзаноста, динамичната комплексност, разноликоста во јазлите и меѓузависната комплексност.

Овие аргументи водат кон потешкотии и неможност да се обезбеди математички модел за одредени димензии, или визури и перспективи во системот.[165]

[164] Исто., стр. 35-135. https://www.sciencedirect.com/science/article/pii/S0951832019305356, посетена на 4/12/2019.

[165] Ani, U., D., *et al*.: A Review of Critical Infrastructure Protection Approaches: Improving Security Through Responsiveness to the Dynamic Modeling Landscape. PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT - 2019 преземена од: https://arxiv.org/ftp/arxiv/papers/1904/1904.01551.pdf, посетена на 4/12/2019.

глава III

КРИТИЧНА ИНФРАСТРУКТУРА – ЗАКАНИ И ЗАШТИТА

1. Закани за критичната инфраструктура

Функционирањето на системот на критична инфраструктура е под постојана закана од широк спектар безбедносни закани.[166] Во справување со потенцијалните закани, системот на критична инфраструктура вклучува мноштво елементи со различно ниво на важност, категоризирани во неколку нивоа и поврзани меѓусебно преку врски од разни видови и интензитет.[167] Ваквиот структурен аранжман води кон широка корелација помеѓу поединечните потсистеми, што го утврдува методот и интензитетот на ширење на влијанието од дефектите во системите на критична инфраструктура врз зависните потсистеми и општеството.[168]

Ефектите кои произлегуваат од овие закани врз критичната инфраструктура и нејзините потсистеми може да предизвикаат помали или поголеми проблеми кои можат да предизвикаат нарушувања и дефекти во различните потсистеми.[169] Тука првенствено, се мисли на нарушување на функционалните параметри кои предизвикуваат пад на изведбата на одредени елементи, каде падот е директно пропорционален на интензитетот на вонредната ситуација и степенот на отпорност на дадениот елемент на критичната инфраструктура.

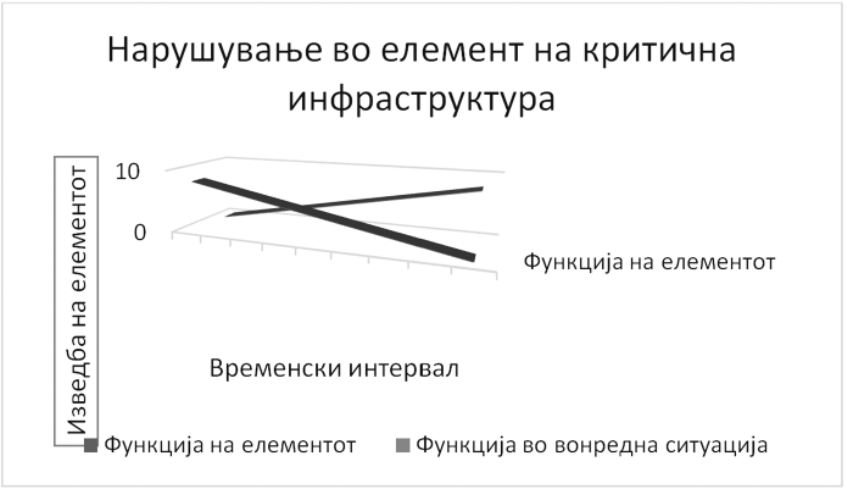
[166] Gregg, S., H.: Defining and Distinguishing Secular and Religious Terrorism. Perspectives on Terrorism. Vol 8, No. 2 2014. [article] http://www.terrorismanalysts.com/pt/index.php/pot/article/view/336/html, посетена на 22/12/2019.

[167] Good Progress on Tackling Hybrid Threats. European Commission Press Release. A_Europe_that_protects__good_progress_on_tackling_hybrid_threats.pdf, посетена на 21/12/2019.

[168] Failures in a Critical Infrastructure Systems. https://www.intechopen.com/books/system-of-system-failures/failures-in-a-critical-infrastructure-system посетена на 18/12/2019.

[169] Hybrid Conference: Critical Connections, Continuity and Supply – Assessing the Security of European Critical Infrastructure and Functions in a Hybrid Threat Context. https://eu2019.fi/en/events/2019-11-06/countering-hybrid-threats-critical-infrastructure-protection-security-of-supply, посетена на 19/12/2019.

Слика број 2: Нарушување во елемент на критична инфраструктура



Извор: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/336/html

Врз основа на изнесеното, вистински предизвик и императив е системите на критична инфраструтура да бидат разгледувани на сеопфатен начин, земајќи ги предвид неговите мрежни аранжмани каде поединечните подсистеми се меѓусебно поврзани преку различни видови врски. Основната структура на овие врски произлегува од нивниот карактер и вклучува еднонасочна поврзаност, што претставува влијание на зависност, и двонасочна поврзаност, што вклучува меѓузависност.

Генерално, меѓузависноста го зголемува ризикот од дефекти или нарушувања во повеќе инфраструктурни системи.[170] Следствено на тоа, во овој контекст е неопходно да се идентификуваат заканите и ризиците за 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);

[170] Rehak, D. & Hromada, M.: Failures in a Critical Infrastructure System. July 20, 2017. https://www.intechopen.com/books/system-of-system-failures/failures-in-a-critical-infrastructure-system, посетена на 17/12/2019.

- 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 синџирот 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).[171]

Овие закани мора да бидат анализирани во целост за да се утврди нивното потенцијално влијание врз инфраструктурата и колкава е веројатноста за нивно настанување.

Во оваа насока, може да се олесни идентификацијата на заканите и ризиците, како и ранливоста на системите на критична инфраструктура на локално, регионално, национално и на глобално ниво. За таа цел потребно да се направи:

- идентификација на засегнатите страни кои имаат удел и/или интерес во безбедноста и отпорноста на критичната инфраструктура;
- обезбедување акциони информации за заканите со цел сопствениците и операторите да можат да ги имплементираат плановите и да преземат соодветни активности;
- препознавање на важноста на реципроцитетот во размената на

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

информации – поради реалната ситуација во која сопствениците и операторите може да забележат сомнителни активности кои помагаат за идентификација и валидација на заканите;

- воспоставување и одржување на пристапни системи за споделување на информации за потребите на инволвираните страни за промовирање на рутински и брзи комуникациски канали за време на непланирани настани/вонредни состојби;
- информациите за заканите треба да бидат обработени за да се отстранат спецификите на изворите на податоци и методите за собирање, така што може да се споделат пошироко, особено со релевантните засегнати страни;
- информациите за сопствениците и операторите мора да бидат заштитени, во согласност со националното законодавство.[172]

Кога дискутираме за заканите на критичната инфраструктура тие еволуираат, а последиците од овие закани влијаат на оперативноста на системот на критична инфраструктура. Во однос на факторите на закани врз критичната инфраструктура, тие се многубројни, но сепак може да се каже дека 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).[173] Значи, заканите за критичната инфраструктура можат 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, поплави или други еколошки катастрофи. Исто така, критичната инфраструктура може да биде загрозена и од болести, пандемии, а сето тоа да влијае врз голем број критичен персонал.[174]

[172] 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 16/12/2019.

[173] Flammini, F., *Critical Infrastructure Security: Assessment, Prevention, Detection, Response,* 2012, стр. 9.

[174] Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.

2. ПРИРОДНИТЕ НЕПОГОДИ И КАТАСТРОФИ КАКО ЗАКАНИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

Природните (елементарни) непогоди и катастрофи можат да се случат во секое време и во секоја држава и можат да бидат со сериозни последици. Еклатантни примери за тоа се земјотресите кои имаат голема разорна моќ, големите поплави што можат да предизвикаат уништување на имот и на плодни земјишта и да нанесат човечки жртви, како и големи пожари предизвикани од запаливи агенси и слично.

Природните непогоди и масовните несреќи можат да се класифицираат во различни групи според различни критериуми. Секоја од овие групи има свои карактеристики и има свои специфичности. Овие специфики ја условуваат организацијата и начинот на работа во отстранување на последиците од одредени елементарни непогоди и масовни несреќи.

Природните непогоди и елементарните несреќи од катастрофите се разликуваат: по интензитет (број на жртви и степен на материјално уништување); по причина на појавување (пожар, вода, експлозиви, епидемии, итн.); по зафатеност на територијата (мала или голема територија, односно несреќи што ја покриваат непосредната или поширокаата територија).

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

Разгледувајќи ги елементарните и неелементарните непогоди, поплавите и пожарот ги ставаме во категорија на појави што можат да се контролираат и превентивно да се дејствува, додека земјотресот како елементарна непогода е појава што се јавува брзо и ненадејно, при што човекот не е во состојба да ја предвиди однапред појавата и да преземе мерки за превентивно дејствување.[175] Климатските промени во значителна мера се одразуваат на бројот на поплави и, секако, преку тоа врз појавата на земјотреси. Појавата на земјотресите и поплавите сериозно може да и се заканат на критичната инфраструктура и на тој

[175] Бакрески О., Милошевска Т. и Алчески Ѓ., Заштита на критична инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 96.

начин каскадно да предизвика ефекти на загрозување на безбедноста, меѓу другото и во доменот на енергетската безбедност. Многу е извесно дека поплавите и земјотресите може негативно да се одразат врз инфраструктурата што е поврзана со искористувањето или производството на енергија, но и врз инфраструктурата што обезбедува каков било сервис или е поврзана со енергетската безбедност.[176]

Анализата нè упатува на констатацијата дека природните катастрофи ќе бидат сè почести во сите делови на светот. Ако ги погледнеме податоците за настани што предизвикуваат големи штети, ќе видиме дека бројот на поплавите е зголемен неколку пати. Во осумдесеттите години на минатиот век, имало околу 100 големи поплави низ целиот свет, а бројот сега се зголеми на 350. Фреквенцијата на големи бури се зголеми за 2,5.[177] Државите ќе треба да се подготват за зголемената фреквенција и зголемениот интензитет на екстремните метеоролошки феномени.

2.1. Загрозеност од земјотреси

Џон Мишел (John Michell 1724-1793) бил англиски физичар и е прв кој дал добар опис за потресите во 1760 година. Според него: „земјотресите се бранови, во движење поставени со движечки карпести маси“. Исто така, тој посочува дека „земјотрес или потрес е природна појава, којашто е резултат на поместувањето на тектонските плочи или движење на Земјината кора, при што се ослободува голема енергија што води до потресување на земјата.“[178] Во 1855 година италијанскиот физичар Луиџи Палмиери (1807-1896) го создал првиот сеизмограф за проучување на овие бранови. Денес, постојат стотици сеизмографски станици на сите континенти, вклучувајќи и на Антарктикот, а вибрациите на поголемите земјотреси можат да се забележат на долги растојанија, практично насекаде на Земјата. Нашето уво е способно да ги почувствува примарните бранови со помал звук од 14 kHz (горниот звук до 24 kHz).

[176] Patrick Sawer, “Japan Earthquake: Nuclear Disaster Feared After Power Plant ’Explosion’“, *The Telegraph*, 12 Mar 2011, достапно на: http://www.telegraph.co.uk/news/worldnews/asia/japan/8377506/Japan-earthquake-nuclear-disaster-feared-after-power-plant-explosion.html.

[177] https://net.hr/danas/svijet/elementarne-nepogode-sve-ih-je-vise-i-sve-su-skuplje/ посетена на 19/12/2019.

[178] https://faktor.mk/shto-e-vsushnost-zemjotresot-i-kako-se-meri, посетена на 19/12/2019.

Но, тоа е мал дел од мноштвото бранови и не е доволно да се предвиди несреќа.[179]

Јачината на потресот зависи од повеќе фактори, како што се количината на ослободена енергија, длабочината на хипоцентарот, оддалеченоста од епицентарот и составот на Земјината кора. Земјотресот се манифестира со потрес или дислокација на земјишното тло. По целата планета има отприлика 13.000 земјотреси годишно. За среќа не се сите подеднакво со иста сила. Повеќето земјотреси може да се почуствуваат само со многу добро чуствителни сеизмолошки апарати. Големите земјотреси се јавуваат отприлика околу 16 пати годишно, а многу посилните уште помалку. Земјотресите не настануваат само поради поместувањето на карпестата маса. Така може и удар на метеорит да предизвика земјотрес, исто и вулканската ерупција, па дури и експлозија на атомска бомба. Вулканите често ќе ги најдеме на линиите на поместување, на места каде Земјината кора е многу тенка, така што притисокот таму придонесува за распрснување, при што вулканот потиснат со притисок надвор исфрла: гасови, пепел или течна магма.[180]

2.2. Загрозеност од поплави

Терминот поплава значи природен или вештачки начин на поплавување на теренот со излевање вода на несакано место. Со оглед на географските, геолошките и хидрографските карактеристики на земјата, има многу можности за поплави. Причини за поплавите се: обилни врнежи од дожд и покачување на нивото на водата; непристапност на водните патишта; уништување на брани или оштетување на резервоари, прелевање на реки и езера; теренско лизгање; топење на снегот, земјотреси.

Заштитата од поплави на населени места – градови, села и индустриски центри, како и земјоделски површини и патишта опфаќа активности на спроведување на разни градежни и технички мерки што се применуваат во заштитата од поплавување. Градежните и техничките мерки првенствено вклучуваат обезбедување на стабилен хидротехнички систем. Неградежните мерки вклучуваат, на пример, предвидување на поплави, додека градежните вклучуваат, на пример,

[179] https://www.znanje.org/i/i25/05iv02/05iv0210/zemljotresi%201.htm, посетена на 19/12/2019.

[180] https://faktor.mk/shto-e-vsushnost-zemjotresot-i-kako-se-meri/ посетена на 19/12/2019.

изградба на насипи, заштита од високи води и задржување на големи бранови на вода.

Мерките за заштита од поплави се спроведуваат од различни надлежни институции, претежно органи и тела задолжени за заштита и спасување од поплави. Во основа мерките се насочени кон: спасување луѓе и добиток во вода; спасување луѓе и материјални добра во поплавени места; транспорт на спасени луѓе и материјални добра на безбедни места и нивно дислоцирање итн.

2.3. Загрозеност од ветрови

Ветерот може да се опише како струење или циркулација на воздушните маси. Ветровите често се класифицираат според просторната скала, нивната брзина, причините кои ги предизвикуваат, географските региони во кои тие дуваат и според нивниот ефект. Иако ветерот сам по себе е самостоен временски феномен, тој може да се појави и како дел од некоја бура. Ветерот има големо значење за многу процеси и појави во природата, но влијае и врз човековите активности. Во човековата цивилизација, ветерот ја инспирирал митологијата, го променил текот на историјата, го проширил ланецот на транспорт и овозможил извор на струја за механичка работа, а се користи и за добивање електрична енергија и за рекреација. Според времетраењето ветровите ги делиме на постојани, периодични и локални. Ветровите се честа појава, особено во зимскиот период. Сепак, тие не се толку силни во некои држави како во определени делови на Европа и светот. Врз појавата, правецот и силата на ветровите најмногу влијае релјефот. Ветерот е одреден кога му се одредени правецот и брзината, односно јачината. Правецот на ветерот се одредува според страните на светот, а брзината се изразува во метри/секунда или километри/час. Мерка за јачина на ветерот е силината со која тој дејствува на разни предмети во природата (таква мерка е и Бофоровата скала). Инструментите за мерење на ветерот, со општо име се нарекуваат ветрометри или анемометри и можат да се поделат на две групи: инструменти кои го покажуваат правецот, односно брзината на ветерот или и двете компоненти; и инструменти кои непрекинато ги бележат вредностите за правецот и (или) брзината. Годишните честини и средните брзини на ветерот, по различни правци, може да се изразат и графички, со помош на т.н. *ружа на ветрови*.[181]

[181] На *ружата на ветерот*, најчесто се нанесени 8 правци, иако може да се состои и од 16, 32 или 36 правци. Должината на кракот од ружата во одреден правец,

Загрозеноста од ветрови е често присутен феномен. Најкарактеристични од ветровите се сепак ураганите и торнадата. Закана од ураган се применува за оние објекти лоцирани во регионите што може да бидат подложни на ураган. Временските информации може да се користат за да се идентификуваат оние региони што може да бидат под влијание на ваква циклонска активност. Историски податоци може да се користат за процена на фреквенцијата на вакви настани. Ураганите ја оштетуваат инфраструктура, како што се: цевководи, водоводна мрежа и слично (како на пр. ураганот „Ајк“ или ураганот „Катрина“). Параметрите на интерес што се поврзани со урагани вклучуваат: брзина на ветерот (на пример, категорија), бура, акумулација на дожд (длабочина и стапка), времетраењето и големината (земја – покриена површина).[182] За разлика од ураганот, заканата за торнадо се применува за оние области каде што постои потенцијалот за торнада или екстремни ветрови. Историските податоци можат да се користат за да се утврди можноста за нивна појава. Анализите треба да ја проценат веројатноста за торнада и екстремни ветрови и поврзаноста со брзината на ветерот, како и времетраењето.

зависи од честотата на ветерот, или пак од неговата брзина. За климатолошката обработка на ветерот, од особено значење се: среднодневната јачина на ветерот – се одредува како збир на терминските јачини (независно од насоката) поделен со бројот на термините, а се изразува во бофори; среднодневна брзина на ветерот – се добива кога збирот на брзините во термините се дели со три и се изразува во м/с; насока на ветерот – се означува со меѓународни ознаки, при што се земени почетните букви од англиските имиња на страните на светот. Насоката на ветерот укажува за доминантното струење на ветерот во одреден правец; зачестеност на ветерот – претставува број на јавувања на ветерот од дадената насока во проценти, каде што за 100 % се зема вкупниот број на сите насоки на ветерот и тишините набљудувани во целиот период (7, 14 и 21 часот). За месеците со 31 ден, вкупниот збир на сите насоки на ветерот и тишини, треба да изнесува 93, за месеците со 30 дена 90, а за февруари 84 односно 87 за престапните години; и средната брзина на ветерот – се добива кога ќе се подели сумата на брзини со сумата на честини на насоките за секоја поединечна насока. Пошироко види: Зиков М., Милевски И., Практикум по климатологија, 2001, Скопје, преземена од https://www.igeografija.mk/Portal/?p=3405, посетена на 19/12//2019.

[182] Holland, G., *Assessing Hurricane Impacts,* Willis Research Network and National Center for Atmospheric Research, достапно на: http://www.willisresearchnetwork.com/lists/publications/Attachments/55/WRN_Princeton_March%2009_Holland.pdf, accessed May 20, 2016.

2.4. Загрозеност од пожари

Пожарот како неелементарна непогода е неконтролиран процес на согорување, чија појава (пламен, топлина и производи од согорување) честопати го загрозува човечкиот живот и може да предизвика голема материјална штета. Најчести пожари се: на зелени и шумски површини; на станбени, јавни, комерцијални и други објекти; на објекти, инсталации и складишта на опасни материјали; на инфраструктурни објекти, инсталации и уреди. Шумски пожар се јавува во неколку форми, и тоа: слаб/мал или приземен пожар и зафаќа запалив материјал на земја и ниска вегетација, додека голем пожар се развива од слаб пожар кој постепено преминува кон поголем интензитет, а со него често се загрозени сите видови шуми. Подземниот пожар е многу ретка појава и се шири многу бавно. Како резултат на можни пожари од големи или од мали размери, може да се појават одредени последици: по населението што живее и работи во околината, по чуварите и спасителите, по работените и по објекти и инфраструктура.[183]

Пожарите варираат според локацијата, видот на материјалот за горење, волуменот, фазата на развој, итн. Според нивната локација тие се поделени на внатрешни и надворешни пожари. Според видот на горивото според европската класификација, пожарите се класифицираат во неколку класи: Класа А: вклучува пожари од цврсти материјали што горат со пламен и жар, како дрво, хартија и слични материјали. Класа Б: вклучува запаливи течности кои се незапирливи со вода, на пример, нафтени деривати, растворувачи, бои, лакови, масти, итн. Класа В: вклучува пожари од запаливи гасови, на пр. метан, пропан, бутан, ацетилен, итн. Класа Г: вклучува пожари на лесни метали како што се алуминиум, магнезиум и нивни легури.[184]

[183] https://www.osce.org/me/montenegro/282436?download=true, посетена на 17/12//2019.

[184] https://bonpet.ifixit.hr/klasifikacija-pozara/ посетена на 19/12/2019.

3. ХИБРИДНИ ЗАКАНИ ЗА СИСТЕМИТЕ НА КРИТИЧНА ИНФРАСТРУКТУРА

Хибридните закани се сметаат за закани кои ги таргетираат демократските држави и нивните процеси на донесување одлуки со повреда или поткопување на целта. Овие активности ги искористуваат сите видови ранливости во кој било домен којшто ќе биде експлоатиран од страна на противниците. Нивната магнитуда може да варира на оската и да влијае на оперативноста.

Хибридните закани кои произлегуваат од активностите на државни и не-државни актери продолжуваат да предизвикуваат сериозна и акутна закана за сите земји во светот.

Хибридните закани се мултидимензионални и се во комбинација со присилни и субверзивни мерки, во кои се употребаат конвенционални, но и неконвенционални методи и тактики.Тие се дизајнирани да бидат тешки за детектирање, или пак тешко да бидат поврзани со било кој поединец или група.

Во услови на хибридни напади и хибридно војување, честопати интересот на терористичките организации е изведување активности кои се под прагот со кој би се привлекло внимание и би се инцирале противмерки, за разлика од класичниот широко прифатен став дека терористичките активности без исклучок имаат потреба од медиумски публицитет. Основните прагови во оваа смисла се детекција, наведување и војна. Тоа подразбира – доколку не биде детектирана злонамерна активност, нема да има одговор. Доколку злонамерната активност биде детектирана, но нема наводи со кои може да се докаже (во недостаток на наведени докази), не може да се одговори со против-мерки. Многу поедноставно е ако е познато што е направено и кој е извршителот на одредено разорно и опасно дејствие, но доколку ова дејствие е под прагот на меѓународен вооружен конфликт, повторно ќе биде тешко да се одговори со воени средства.[185]

Базичните форми на терористички напади кои може да бидат извршени врз критичната инфраструктура вклучуваат:

- Бомбашки напади – што подразбира употреба на експлозиви на следниот начин: инсталација на експлозивна направа во или близу одредена локација на критична инфраструктура, самоубиствен напад, употреба на превозно средство за извршување на напа-

[185] Flynn, S., E.: The Future of Infrastructure and Resilience. Northeastern University Global Resilience Institute. Достапна на: http://www.oecd.org/gov/risk/Stephen%20Flynn_Keynote.pdf, посетена на 19/12/2019.

дот како што е воз, автомобил или авион, итн. Експлозивот исто така може да биде доставен до критичната инфраструктура преку пошта или преку синџирот за достава. Употребата на експлозив е најчестиот метод за извршување терористички напад. Експлозивите се „погодни" за употреба од страна на терористичките организации поради нивната разновидност, нивната достапност во одредени делови од светот, лесната употреба и спектакуларниот ефект при нивната употреба. Дополнително, покрај експлозивите и индустриската опрема, терористите исто така користат и импровизирани експлозивни направи. Изборот на методите и оружјето првенствено зависи од нивниот капацитет и способности. Методите, опремата и материјалите кои се употребуваат за производство на бомби и експлозивни направи исто така зависат и од културолошките традиции и услови, местото на настанот и потеклото на изведувачите.

- Употреба на мало оружје, минофрлачи, преносни противвоздушни ракетни комплети, итн.
- Земање заложници (киднапирање вработени) со цел да се изнуди поткуп или информација во однос на одредена критична инфраструктура.
- Изведување терористички напади со употреба на НХБР (нуклеарни, хемиски, биолошки и радиолошки) материјали директно или во близина на одредена критична инфраструктура.
- Сајбер-напади врз информатички системи за постигнување корист во форма на хакирање, кракирање, фишинг, логични бомби, вируси итн.[186]

Генерално, системот за заштита на критичната инфраструктура може да се смета за интероперабилен помеѓу три системи:

- ✓ Периферен заштитен периметар – отворениот простор на одреден објект.
- ✓ Заштита на имотот и систем на контрола на движењето на лицата во рамки на објектот и околината.
- ✓ Видеонадзор на јавни установи во градовите, стадионите, станиците, терминалите, шопинг-центрите, фабриките, итн.[187]

[186] Savolainen, J.: *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi).* November 22, 2019. https://www.hybridcoe.fi/publications/hybrid-threats-and-vulnerabilities-of-modern-critical-infrastructure-weapons-of-mass-disturbance-wmdi/ посетена на 19/12/2019.

[187] Improving the Security of International Infrastructures. OSCE Secretariat. https://www.osce.org/secretariat/107809, посетена на 20/12/2019.

3.1. Тероризмот како закана за безбедноста на критичните инфраструктури

Информацискатa револуција го помага создавањето и јакнењето на мрежните форми на организација и истовремено овозможува остварување нивни компаративни предности над хиерархиските форми. Тоа особено ќе придонесе за нови можности на недржавните актери, кои полесно ќе се трансформираат во мултиорганизициски мрежи во однос на традиционалните хиерархиски државни актери, со оглед на тоа дека недржавните актери побрзо се адаптираат на надворешните влијанија и попродуктивно ги користат информациите за унапредување на процесите за донесување одлуки.

Новите глобални терористички организации по својата внатрешна структура значително се разликуваат од традиционалните. Терористичките организации што биле активни во средината на XX век биле организирани во вертикален систем. Начелно, биле мали организации со мал број активни припадници со точно дефинирана улога, прецизна субординација и стационирани на одредено подрачје. Највисокото раководство на организацијата настојувало да престојува во подрачјата каде што ќе се реализираат терористичките акти, додека на територијата на други држави се дислоцирале, евентуално, поради безбедност. Раководителите биле задолжени за идеолошкото и оперативно раководење, додека каква било самоиницијативна активност не била допуштена.

Новите глобални терористички организации ги сочинуваат илјадници припадници што дејствуваат на глобално ниво. Структурата на овие организации е мрежеста и хоризонтална. Самостојните членови или малите групи имаат во рамки на организацијата висок степен на самостојност во одлучувањето. Раководството на организација се трансформира во оперативно ниво на раководење и станува верски-идеолошки лидер, односно елита што ја осмислува и ја дава политичката платформа на дејствувањето. Поради големиот број припадници на мрежата и нивната дисперзија, основната улога на лидерот е проектирање верска-идеолошка платформа, која со своите идеи и цели може да биде прифатена од сè поголемиот број потенцијални терористи. Непосредната подготовка на операциите, изборот на целите, времето на нападот, ангажирањето непосредни извршители (терористи-самоубијци) се препуштени на локалните или на регионалните структури на мрежата, освен кога станува збор за голем напад. Во тој случај, неопходно е одобрение од раководството. Како резултат на оваа структура и модалитети на дејствување, се изведуваат акции на локални верски фанатици (кои претходно немаат воспоставено формални врски со терористичката

мрежа) и, доколку се во склад со основните принципи на мрежата, ќе бидат дополнително прифатени како дел од поширока и координирана акција.[188]

Во многу аспекти, транснационалните врски се идеална организација за криминалните и за терористичките дејства во глобализираниот свет. Мрежите се распространети и, иако сите имаат свој центар, транснационалната распределба го отежнува процесот на државите да го нападнат нивниот центар на гравитација.

Резултатите од истражувањата на моделите и трендовите на активности ја потврдуваат хипотезата дека „новиот" тероризам еволуира кон мрежно дејствување – војување, со оглед на тоа дека:

- сè поголем број терористички организации ги прифаќаат мрежните форми на организација и притоа сè повеќе ја користат информацискатa технологија;
- терористичките организации (оние што се основани во осумдесеттите и деведесеттите години на XX век) се подлабоко вмрежени за разлика од терористичките организации со долга традиција;
- помеѓу степенот на активност на терористичките организации и степенот на прифаќање на мрежните форми на организација постои позитивна корелација;
- еднаква е веројатноста дека информацискатa технологија ќе се користи како организациска потпора и како средство за напаѓање при војување;
- поголема е веројатноста дека новорегрутираните припадници на терористичките организации се поопособени за користење нови технологии, што имплицира дека во иднина ќе бидат подлабоко вмрежени и повеќе ќе ја користат информатичката технологија.[189]

Причините поради кои новите информациски и комуникациски технологии го поддржуваат настанувањето на мрежните форми на организација се:

- Зголемената брзина на комуницирање (со зголемена пропустливост на мрежата и широка вмреженост). Новите технологии ја овозможуваат комуникацијата и координацијата меѓу раздалечените припадници на групите на терористичките организации.

[188] Милошевска Т., *Модели на поврзаност на тероризмот и на транснационалниот организиран криминал*, Филозофски факултет, Скопје, 2016.

[189] Милошевска Т., *Глобален тероризам*, Филозофски факултет, Мар-Саж, Скопје, 2018.

- Намалената цена на комуницирање. Новите технологии значително ги намалија трошоците за комуницирање, овозможувајќи одржливост на мрежниот облик на организација (со оглед на потребата за интензивна комуникација).
- Интеграцијата на комуникациските и на компјутерските технологии резултирала со зголемен опсег и сложеност на информациите што може да се споделуваат со помош на мрежата.[190]

Информацискатa револуција создава услови за формирање и за јакнење на мрежните облици на организација и истовремено овозможува остварување на нивните компаративни предности над хиерархиските облици. Информацискатa доба не влијае само на изборот на цели и на оружје на терористичките организации, туку и на нивниот начин на функционирање. Потенцијалната предност на мрежните организациски облици, во однос на традиционалниот хиерархиски поредок, се согледува преку мрежната структура на латерална контрола, авторитет и комуникација, за разлика од вертикалната комуникација.

Анализата на голем број дефиниции упатува на заклучокот дека тероризмот претставува закана за користење или реално користење на насилство (терор) за постигнување на политички цели. Не постои тероризам без терор, но од друга страна, секој терор, секој чин на насилство не мора да значи и тероризам. За одредена појава да се окарактеризира како тероризам, самиот чин на терор мора да има политичка цел.[191]

На прашањето кои се заедничките елементи на тероризмот, Интерпол одговара дека, генерално, тероризмот е криминал што го карактеризира насилство или заплашување, најчесто против невини жртви, во настојување да остварат политички или општествени цели.[192]

Голем број дефиниции ја истакнуваат политичката компонента на тероризмот, но постојат обиди да се додадат и некои други цели како што се криминалните. Пол Вилкинсон криминалниот тероризам го дефинира како систематско прибегнување кон терор поради стекнување приватна материјална корист.[193]

---

[190] Peter Monge, Janet Fulk, *Shaping Organizational Form: Communication, Connection, and Community*, Thousands Oaks, Sage, 1999, стр. 84.

[191] Schmid, P. Alex; Jongman, J.Albert, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature,* Amsterdam: North-Holland Publishing Company, 1988.

[192] Todd Sandler, Daniel G. Arce and Walter Enders, An Evaluation of Interpol's Cooperative-Based Counterterrorism Linkages, *The Journal of Law & Economics* Vol. 54, No. 1, Cambridge University Press, 2011.

[193] Wilkinson, Paul, The media and terrorism: a reassessment, *Terrorism and Political Violence,* 1997.

Во 2002 година, Шестиот комитет на ООН[194] се приближува кон генералната дефиниција кога објавува дека тероризмот претставува „криминални чинови/акти намерни или калкулирани да предизвикуваат општа состојба на терор во општеството, остварени од групи или од одредени личности, кои во политичка смисла се неприфатливи, без оглед на причините што ги користат да ги оправдаат, било да се поврзани за политика, филозофија, идеологија, расна, етничка, религиозна или за друга природа".

Согледувајќи ги сите наведени сфаќања за поимот тероризам, станува јасно дека тероризмот, во секој случај, претставува облик на криминална активност којашто ги содржи следниве карактеристики:

- извршување акти на насилство;
- застрашување или создавање чувство на страв;
- загрозување и повредување вредности како што се животот, здравјето, моралниот интегритет, имотот, јавната и државната безбедност и
- постоење посебен мотив за извршување, кој се согледува во остварување одредена политичка, социјална, национална, идеолошка или религиозна цел.

Концепцијата на мрежното војување е конзистентна со обрасците на случувања на Блискиот Исток, каде што е очигледно дека новите и активни терористички организации ја усвојуваат децентрализираната флексибилна мрежна структура, која им овозможува преобразба од формално организирани и државно спонзорирани терористички организации кон приватно финансирани неформални мрежи. Ако е повисоко нивото на мрежната организираност на терористичката организација, се јавува поголема веројатност информацискатa технологија да се користи како потпора во процесот на мрежно одлучување. Најновите достигнувања на информациските технологии им овозможуваат на вмрежените терористички организации побрз, поевтин и посигурен проток на информации. Преку прифаќање на информацискатa технологија за одлучување, се зголемува веројатноста дека терористичките организации ќе користат иста технологија како средство за напаѓање (со цел попречување на нормалното функционирање или уништување).[195]

Правењето разлика помеѓу политичкиот и обичниот криминал, во голема мера, ќе помогне за успешно планирање и изведување на

[194] Gerhard Hafner, Certain Issues of the Work of the Sixth Committee at the Fifty-Sixth General Assembly, *The American Journal of International Law*, Vol. 97, No. 1, Cambridge University Press, 2003.

[195] Милошевска Т., *Глобален тероризам*, Филозофски факултет, Мар-Саж, Скопје, 2018.

воените антитерористички акции што не претставуваат репресивно противзаконски воени и политички мерки. Единствената заедничка точка при дефинирањето на тероризмот претставува фактот што жртвите на терористичките акти се или убиени или повредени или, пак, врз нив се спроведуваат определени закани што се првенствено противзаконски.

Постојат четири доминантни модели за детерминирање на поимот тероризам, кои последователно резултираат со оформување на контратерористичката политика.

1. тероризам како вид криминал;
2. тероризам како форма на војување;
3. тероризам како борба за ослободување/осамостојување, кој се спроведува од репресивни малцински, политички или религиозни групи и
4. тероризам како насилна реакција.

Првите два модела се справуваат со тероризмот како криминален или воен проблем и вообичаено се пристапи на владините контратерористички политики. Третиот модел претпоставува идентификација со терористите и со другите што бараат промена на ситуацијата статус кво. Четвртиот модел го рефлектира разбирањето за политичките и социоекономските варијабли, кои комуницираат за да се создаде комплексност на политичко насилство и тероризам.

Формите на појавување на тероризмот во XXI век, во голема мера го надминуваат традиционалното сфаќање за тероризмот, ја отсликуваат неговата комплексност, динамичност и интензивност, но и неговата огромна опасност за националната безбедност на државите и на севкупната меѓународна безбедност.

Високиот степен на децентрализација и флексибилност во организациски поглед, поточно високиот степен на оспособеност на членовите на современата терористичка мрежа да применуваат современи технички иновации за обезбедување финансиски средства и водење сопствена пропаганда, способност за брзо приспособување на стратегијата и тактиките на дејствување кон глобалните еконономски и политички промени без промена на сопствените политички цели, ја прави новата меѓународна терористичка мрежа способна за брзо адаптирање и ефикасно дејствување во новото опкружување.

3.2. Специфични терористички закани за критичната инфраструктура

Заканите поврзани со тероризмот и нападите на критичната инфраструктура имаат повеќе димензии. Во основа, таквите закани се делат во зависност од нивната природа (физички наспроти сајбер),

според нивното потекло (инсајдер/внатрешни наспроти надворешни) и контекстот во кој тие се јавуваат (изолирани или мултиплицирани цели).

Физички версус сајбер закани. Физичките закани насочени кон критичната инфраструктура можат да имаат различни форми. Нивната заедничка карактеристика е што тие имаат цел да ја уништат инфраструктурата, да ја ослабнат или да ја направат неоперативна во целост или делумно со напади на нејзината физичка структура, механички компоненти, итн. Најинтуитивните физички закани за критичната инфраструктура вклучуваат употреба на експлозиви или запаливи средства, транспортни средства, ракети, гранати, па дури и едноставни алатки (на пр. Запалки за подметнување пожари), итн., за да се постигне целосно или делумно пропаѓање или уништување на инфраструктурата. Нападите може да вклучуваат и намерна модификација или манипулација со системите и процесите на критичната инфраструктура (на пр. вклучување на објектите и исклучување, отворање и затворање на цевководи, потиснување на процесни сигнали, сигнали за дефект или аларми).

Распоредувањето на хемиско, биолошко, радиолошко или нуклеарно оружје или супстанци претставува друг карактеристичен вид закана за критичната инфраструктура. Ова може да варира од ширење на заразни патогени во синџирите за снабдување со храна, водоводни цевки, итн, до употреба на отровен гас на клучните сообраќајни крстосници. Исто така е релевантно да се забележи дека нападот на критичен објект кој содржи хемиски, биолошки, радиолошки или нуклеарни материјали, исто така, може да резултира во ослободување на вакви материјали.

Во споредба со физичките закани, сајбер-заканите се разликуваат во голема мера, а крајниот резултат може да биде ист. Сајбер-заканите се разликуваат, но може да вклучуваат, на пример, напади кои: манипулираат со системите или податоците како што е малициозен софтвер што ги експлоатира ранливостите во компјутерскиот софтвер и хардверските компоненти неопходни за работа на критичните инфраструктурни системи; затворање на клучни системи како што се нападите на DoS (неодамнешен пример за напад на DoS, кој директно влијаеше на критичната инфраструктура беше нападот извршен врз данскиот систем за резервации на билети за железница на 14 мај 2018 година);[196] ограничување на пристапот до клучните системи или информации, како што се напади преку малициозен софтвер.

[196] The Local Dernmark's rail ticket systems targeted in digital attack, 2019, достапно на: https://www.thelocal.dk/20190902/denmarks-rail-ticket-system-targeted-in-digital-attack

Внатрешни версус надворешни закани. Додека заштитата на критичната инфраструктура од надворешни напади придонесува за значително ангажирање на национални и меѓународни регулаторни агенции, заканите од внатрешно потекло биле предмет на релативно помало внимание. Во споредба со надворешните актери, кои можат да добијат пристап до критичната инфраструктура преку насилни дејствија или, пак инсајдерите имаат неспорни предности, внатрешните извршители често се вработени во компанијата или се добавувачи. Тие можат да бидат главни заговорници или да дејствуваат како соучесници (на пр. информатори) на надворешните актери. Тие честопати се во состојба да ги набљудуваат процесите што не се нарушени во текот на еден временски период. Нивното знаење (или леснотијата со кое тие можат да се здобијат со знаење) за соодветната установа можат лесно да го искористат за криминални цели.

Имајќи го ова предвид, методологиите за спроведување процена на ризикот на специфични локации треба да вклучуваат разгледување на секоја улога во рамките на системот, а слабостите на инсајдерите не треба да се сметаат за посебна категорија. Наместо тоа, видовите закана треба да бидат земени предвид со инсајдерски елемент вклучен во секоја категорија. На пример, при разгледување на категоријата на закани, како што е лице со импровизирана експлозивна направа, која е користена за напад врз авиони, оние што вршат процена треба да размислат, одделно и за патник со импровизирана експлозивна направа за напад врз авион и за лице од екипаж и/или вработените со импровизирана експлозивна направа која може да се користи за напад на авиони. Во оваа област, клучна превентивна улога може да играат операторите на критичната инфрастрктура, почнувајќи од имплементација на ефективни процедури за селекција на персоналот и проверка.[197]

Изолирани версус мултиплицирани цели. Заканите против критичната инфраструктура може да бидат или изолирани и спорадични акти, или да се дел од поширок план за напад на инфраструктура во истиот сектор (на пр. нуклеарни централи), кои припаѓаат на идентичен сопственик/оператор, или сместени во иста географска област. Дејствијата мотивирани од терористи, насочени кон критичните инфраструктурни системи се на ист начин осмислени како што се случува индустриската шпионажа, каде сајбер-нападите се реализираат како кампањи или на-

[197] United Nations Office of Counter Terrorism, UN Counter-Terrorism Centre, INTERPOL (2018), *the protection of critical infrastructures against terrorist attacks: Compendium of good practices*.

пади во серија. На пример во 2011 година т.н. LURID[198] нападите имаа за цел, помеѓу останатите инфраструктурни системи, цел на напад да бидат и бројни дипломатски мисии и поврзани владини агенции во сајбер-просторот.

Идентификацијата на обрасците во слични сценарија честопати бара силни аналитички алатки и обработка на информации од огромни и хетерогени извори. ОБСЕ истакнува дека повеќето сајбер-напади поврзани со енергетскиот сектор не се објавуваат, бидејќи релевантните оператори не сакаат да ги обелоденат јавно овие инциденти.[199] Сепак, можноста да се препознае основната динамика и методи што е можно порано е клучна за да им се овозможи на властите да споделат информации. Ова го зголемува капацитетот за поефективно реагирање на тековните напади и превенирање на непосредни напади против веројатните жртви. Во некои случаи, она што се смета ини како изолиран напад може во реалноста да биде дел од поамбициозни и поединечни криминални стратегии.[200]

Критичната инфраструктура станува сè повеќе автоматизирана и меѓусебно поврзана, а со тоа се воведуваат нови слабости во однос на дефект на опремата, грешка во конфигурацијата, временските услови и други природни причини, како и физички и сајбер-напади. Изолацијата на мрежата веќе не е доволна за да се обезбеди сигурност на одредени објекти од критичната инфраструктура.[201] Заради тоа, критичната инфраструктура и понатаму е во опасност од постојано развивање на заканите во сајбер-просторот, на кои треба да се одговори преку холистички и ефикасен начин со цел да се заштитат економиите и општествата.[202]

---

[198] Nart Villeneuve, David Sancho, *The LURID Downloader*, Trend Micro Labs, 2011.

[199] OSCE (2013), Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, 2013, достапно на: www.osce.org/atu/103500?download=true

[200] Во заедничкиот Извештај на ДХС/ФБИ, издаден во 2017 година, се забележува дека одредени владини мрежи во секторот енергетика, нуклеарна енергија, вода, авијација се изложени на ризик од насочени напредни упорни закани (АПТ) активности. DHS, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, (2017), достапно на: www.uscert.gov/ncas/alerts/TA17-293A

[201] Kaspersky, Cyberthreats to ICS Systems, 2014, достапно на: http://media.kaspersky.com/en/ business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_ web.pdf.

[202] Tripwire. (2015). Cyberterrorists Attack on Critical Infrastructure Could be Imminent, достапно на: http://www.tripwire.com/state-of-security/securitydata-protection/security-controls/cyberterrorists-attack-on-criticalinfrastructure-could-be-imminent/.

„Театарот“ за закани сè повеќе се карактеризира со организирани групи или недржавни актери и лица кои прибегнуваат кон асиметрични напади овозможени со универзалната поврзаност што интернетот ја обезбедува и достапноста на потребните алатки и информации за напади. Губењето на контрола врз технологијата како резултат на глобализацијата, потребата од пристап до интернет и странската сопственост на критични инфраструктури исто така се дополнителни фактори кои ја зголемуваат ранливоста на критичната инфраструктура.[203]

Управувањето и функционирањето на критичните инфраструктурни системи ќе продолжи да зависи од сајбер-информациските системи и електронските податоци. Потпирањето на електричната мрежа и телекомуникациите, исто така, ќе продолжи да се зголемува, како и бројот на вектори на нападот и површината на нападот заради сложеноста на овие системи и повисоките нивоа на поврзаност заради паметните мрежи. Безбедноста на овие системи и податоци е од суштинско значење за довербата на јавноста и безбедноста.[204]

Експлоатацијата на постојните слабости, нулта денови и насочените фишинг напади ќе се зголемат и ќе продолжат да претставуваат закани против критична инфраструктура заради комплексната мешавина на наследни системи и нови компоненти во комбинација со потребата да се минимизираат деловните нарушувања и трошоците, што честопати ги одложува надградбите и ажурирањата. Вработените со привилегиран пристап до системот ќе останат клучни цели и ќе бидат предмет на напад на социјален инженеринг.[205]

Зајакнување на сајбер-безбедноста и справувањето со компјутерскиот криминал бараат комбинација на превенција, откривање, ублажување на инциденти и истраги.[206] Решавањето на слабостите на критичната инфраструктура бара соработка и пристап од јавниот и приватниот сектор и поврзување на националната и меѓународната димензија. Предизвикот за заштита на критичните инфраструктури бара

[203] EUROPOL. (2015), *The Interent Organised Crime Threat Assessment*, Hague, Netherlands.

[204] *NBC News*. (2015). Critical Infrastructure Is Vulnerable to Cyberattacks, Says Eugene Kaspersky, достапно на: http://www.nbcnews.com/tech/security/critical-infrastructurevulnerable-cyberattacks-says-eugene-kaspersky-n379631.

[205] Recorded Future. (2014). Real-Time Threat Intelligence for ICS/SCADA Cyber Security, достапно на: http://go.recordedfuture.com/hubfs/data-sheets/ics-scada.pdf, 2014

[206] *Infosecurity Magazine*. (2015). Destructive Cyber-Attacks Blitz Critical Infrastructure – Report, достапно на: http://www.infosecurity-magazine.com/news/destructive-cyberattacks-critical/.

управување, односно менаџирање со конкурентни барања помеѓу безбедноста и приватноста.[207]

Контролата на надзорот и стекнувањето податоци (SCADA), индустриските системи за контрола (ICS) и системите за автоматска идентификација (AIS) се комплексни системи составени од разни хардверски и софтверски компоненти, честопати од различни добавувачи. Тие честопати беа дизајнирани со помал акцент кон мрежната безбедност. Спојувањата и аквизициите, лошото управување со проценатa, отсуството на политики за управување и недостатокот на трансфер на знаење помеѓу персоналот, се причини кои можат негативно да влијаат на безбедносната мрежа каде може да се очекува постојан пораст на бројот на можности за експлоатација на ранливости.[208]

3.3. Мотиви за извршување на терористички напад врз критичната инфраструктура

Хетерогената природа на системите на критична инфраструктура, во комбинација со различниот географски и институционален аспект во кои се сместени и функционираат, предизвикува потешкотии во генералната дефиниција и утврдување на мотивите за извршување терористички акти врз критичната инфраструктура. Сепак, важно е да се истакне дека анализата на мотивите за терористичките напади е мошне потребна за спроведување процени и планирање на идните трендови и закани.[209] Исто така, анализата на терористичките мотивации може да обезбеди корисни придобивки, како дел од пошироките процени на закана, потребни според националните стратегии за заштита на критичната инфраструктура.

Во литературата диференцирани се неколку категории мотиви кои се особено важни за извршување терористички напади. Така, поделбата опфаќа неколку категории.

---

[207] Trend Micro. (2015). *Report on Cybersecurity and Critical Infrastructure in the Americas*, достапно на: http://www.trendmicro.com/cloud-content/us/pdfs/securityintelligence/reports/critical-infrastructures-west-hemisphere.pdf.

[208] Trend Micro. A Security Evaluation of AIS, 2015, достапно на: http://www.trendmicro.com/ cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-securityevaluation-of-ais.pdf.

[209] The Protection of Critical Infrastructure Against Terrorist Attacks: Compendulum of Good Practices. UN Counter-Terrorism Centre, United Nations Security Council CTED, Interpol, 2018. https://unrcca.unmissions.org/sites/default/files/eng_compendium-cip-final-version-120618_new_fonts_18_june_2018_optimized.pdf, посетена на 22/12/2019.

Во првата категорија мотиви, според емпириските податоци во оваа област се доаѓа до заклучок дека системите на критична инфраструктура претставуваат примамлива цел за терористичките групи и/или поединци. Имено, системите на критична инфраструктура претставуваат поволна цел поради нивната стратешка важност за општеството, особено во урбаните и развиените општествени центри. Идејата за интерференција во одреден систем на критична инфраструктура и можноста за предизвикување каскаден ефект би претставувала исполнета цел за терористичката идеологија и мотив, со максимизирање на последиците и предизвикување страв кај граѓаните.

Втората категорија мотиви произлегува од фактот дека со напад на одредена критична инфраструктура може да се постигне и ефект на прикажување немоќ кај соодветните институции кои во ситуации на извршен терористички напад ќе изгледаат неспособни да осигураат оптимално ниво на безбедност и веродостојни процени за степенот на загрозеност од закани. Во конкретни случаи, кога цел на напад се одредени мрежи на критична инфраструктура кои спроведуваат и доставуваат добра и услуги потребни за функционирањето на заедницата при што се нарушува или стопира нивната работа, доаѓа до израз ранливоста на управувачките тела на овие системи, без разлика дали се државни или приватни, како и ефективноста на владините политики и стратегии во насока на заштитата на критичната инфраструктура.

Третата категорија мотиви, во контекст на претходните две, ја подразбира желбата на терористичките групи и поединци да привлечат максимален публицитет врз нападот на критична инфраструктура, што не би имал толкав интензитет доколку била нападната „обична цел“.

Четвртата категорија мотиви се однесува на идејата за воспоставување сопствен легитимитет и општествена прифатеност. Освен нарушувањето и прекинот на проток на системите на критична инфраструктура, целта на терористичките организации е искористување на овие системи за свои потреби и овозможување пристап до нив со цел придобивање на своите следбеници и стекнување симпатии од страна на локалното население, со зголемување на бројот на припадници во своите редови. Дополнително, при напад на системите на критична инфраструктура кои обезбедуваат витални ресурси, како што се питка вода и други видови инфраструктурни елементи од водоснабдувачкиот сектор, според анализите на мотивите на терористите на ИСИЛ, мотивот не е единствено да се попречи движењето на трупите и борба со припадниците на вооружените сили, туку и зголемување на сопствената логистичка моќ. Според бихејвиористичките анализи, каде појдовна точка се мотивите за извршување терористички напади на системите

на критична инфраструктура може да бидат поимани во паралела со дејствата на индустриска шпионажа, каде нападите и сајбер-упадите се вршат во кампањи или сериски напади. Идентифкацијата на шемите на ваквите сценарија е мошне сложен аналитички метод за процесирање на податоци од разновидни извори. Така, способноста за рано откривање на динамиката и активностите на потенцијалните напаѓачи им овозможува на властите навремено споделување информации. На овој начин се зголемува капацитетот за ефективен и пре-емптивен одговор. А во одредени случаи, кога одреден напад изгледа како изолиран инцидент, може да се испостави дека е дел од поширока и поамбициозна криминална стратегија.[210]

3.4. Сајбер-тероризмот како закана за комуникациско-информациските системи

Новиот тероризам се одликува со воен карактер, екстремна бруталност, односно нов стил на дејствување, кој ќе биде поразорен и поубиствен во споредба со традиционалниот тероризам. Новите терористички организации постојано го усогласуваат своето дејствување со современите процеси, достигнување во науката и со техниката, особено со примената на комуникациските технологии и употреба на интернет за потребите на пропаганда, регрутирање, индоктринација, собирање средства и водење психолошка војна. Во економски зависен систем, новиот тероризам ги менува целите и стратегијата на сопственото дејствување. Неговата цел сè повеќе се поместува од едноставен психолошки ефект за креирање страв и несигурност кон цели за масовно разорување делови од светските економски, финансиски или технолошки мрежи.[211]

Во основа, ако војувањето со информации претставува начин за војување во иднината, тогаш и иднината на тероризмот ќе биде суштински детерминирана со појавата на сајбер-тероризмот. Терористите ги искористуваат придобивките на информатичката технологија, односно од поврзаноста на тероризмот и интернетот произлегува и една нова форма на тероризам – сајбер-тероризмот.

Сајбер-тероризмот е значаен потсистем на сајбер-војувањето, и е многу потежок за откривање и спротивставување, бидејќи е скоро

[210] Исто., The Protection of Critical Infrastructure against Terrorist Attacks: Compendulum of Good Practices. UN Counter-Terrorism Centre, United Nations Security Council CTED, Interpol, 2018.

[211] Милошевска Т., *Модели на поврзаност на тероризмот и на транснационалниот организиран криминал*, Универзитет „Св. Кирил и Методиј“, Филозофски факултет, МАР-САЖ Скопје, 2016, стр. 38-39.

неможно да се одреди политичката припадност или спонзорите на неговите извршители. Кога се зборува за поимот сајбер-тероризам, според Федералното истражно биро – ФБИ, овој феномен се дефинира како: „предумислени, политички мотивирани напади против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од страна на субнационалните групи или тајни агенти".[212] За разлика од сајбер- тероризмот, сајбер-војувањето е насочено кон информациите и информативните системи што даваат поддршка на цивилните и на воените структури на противникот. Тоа навлегува во сфера која е многу посуптилна од физичките напади и уништувања, односно дејствува врз протокот на информациите во мрежите и манипулира со нив (прекинува, видоизменува, додава и слично). Неговите активности се насочени првенствено кон информациите кои се пресудни за функционирање на цивилните и воените системи, како и контролата на авиосообраќајот, стоковите берзи, меѓународните финансиски трансакции, логистичките потреби и цели.

Дефиницијата која ја применува и Сојузниот криминалистички завод го опишува сајбер-тероризмот како „користење на сајбер-капацитети за изведување овластувачки, попречувачки или разорувачки милитантни операции и за инструментализирање на стравот преку насилство или закана со насилство, за да се предизвика политичка промена".

За Мишевски, сајбер-тероризмот е и насилен акт извршен со користење на интернет, преку кражба на доверливи и лични податоци со цел истите да бидат искористени за заплашување или принуда/присила поради остварување на одредени политички или општествени цели. Како акт на сајбер-тероризам се сметаат и активностите преку кои намерно се уништуваат голем број компјутерски мрежи, како и персонални компјутери поврзани на интернет, преку користење на алатки/програми како компјутерски вируси. Односно, сајбер-тероризмот уште може да се дефинира и како меѓународно користење на компјутер, мрежа, или јавен интернет за да се предизвика уништување или штета на персонални компјутери.[213]

Според Петровиќ, сајбер-тероризмот е конвергенцијата помеѓу сајбер-просторот и терористичките активности, на пример, политички мотивирано хакирање, кое има за цел да предизвика сериозна штета

[212] Hower S., *Cyberterrorism,* Santa Barbara, CA: Greenwood, 2011.

[213] Мишевски Д., Осигурување од сајбер ризици, *Осигурување*, Национално биро за осигурување-Македонија, бр.11, Скопје, 2017.

како загуба на човечки животи и/или сериозни економски последици. Основните карактеристики на хакирањето, се наведува во неговата аргументација, се: насилен планиран пристап, бидејќи станува збор за пробивање на заштитата на системот; неовластеното навлегување („упад“) во системот, кое се базира на високо професионално знаење; местото на „упадот“ е по правило оддалечено од местото каде што се наоѓа напаѓачот; при самото хакирање, напаѓачот истовремено врши и други дела: измами, кражба на идентитет, саботажа, дистрибуција на вируси и сл.; неовластени навлегувања можат да вршат поединци или групи, физички или правни лица.[214]

Во елаборацијата на Волкер стои дека сајбер-тероризмот е политички мотивирано користење на компјутери и информатичка технологија за да се предизвика поголема штета или општ страв во општеството. Сајбер-тероризам воедно претставува насилен акт извршен со користење на интернет, а кој резултира (или се заканува) со смрт или сериозни телесни повреди со цел преку заплашување да се остварат одредени политички цели.

Нападот на самонаречениот „сајбер-калифат“ врз француската телевизија TV5 Monde претставува вовед во ново ниво на сајбер-тероризмот. Акцијата во секој случај беше сајбер-напад кога истовремено беше прекината програмата на сите 11 канали на таа телевизија и беше преземена контролата врз профилите на „Фејсбук“ и „Твитер“, со импликации за техниката за производство на телевизиска програма. Со часови по нападот телевизијата можеше да емитува само претходно подготвени прилози.[215] Инцидентот не дојде ненадејно. Сојузниот криминалистички завод уште во 2014 година во една интерна анализа предупреди на терористичките закани од сајбер-просторот. И европската полициска агенција Европол во една анализа на ризиците во септември 2014 година укажа на опасностите од сајбер-тероризмот.

Сајбер-тероризмот претставува една од главните глобални закани на современата безбедност. Системи за заштита од ваков вид напади поседуваат меѓународните организации како НАТО и ЕУ и развиените држави како што се САД, Кина, Русија, Велика Британија и други. НАТО е единствената организација која на систематски и стручен начин се занимава со заштита од овој вид тероризам и поседува развиен систем на

[214] Петровиќ, Р.С., *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007.

[215] John Lichfield. TV5Monde hack: ‘Jihadist’ cyber attack on French TV station could have Russian link, Independent, London, United Kingdom, 2015.

сајбер-одбрана. За да останат во тек со рапидно променливите облици на закана и за да одржат високо ниво на сајбер-одбрана, НАТО усвои нова и напредна политика и Акционен план кој го поддржаа сојузниците на Самитот во Велс во септември 2014 година. НАТО силите за одговор на компјутерски инциденти (The NATO Computer Incident Response Capability (NCIRC) ја штитат сопствената мрежа, нудејќи 24-часовна поддршка во сајбер-одбраната на разни сајтови на НАТО. Кооперативниот центар за сајбер-одбрана на НАТО (The NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE)) во Талин во Естонија е најистакната и акредитирана од страна на НАТО институција за истражување и обука, која се занимава со образование, консултации, размена на лекции и развој во врска со сајбер-одбраната.[216] Целокупниот овој систем е токму фокусиран и лоциран во Естонија, кога во април 2007 година, се извршени напади врз информациско-комуникациските системи на Естонскиот парламент, во банките, во Владата, во медиумите, всушност, во сите значајни државни институции, при што предизвикале дестабилизација на државната безбедност, што од страна на мноштво експерти беше окарактеризирано како класичен пример за сајбер-тероризам. Ваквиот вид напад, сепак, не претставува напад со огромни последици и загуби, голема материјална штета или човечки жртви, но тоа беше првиот напад од такви размери за да се блокираат сите витални институции на државата, со што целиот систем и државата одат во насока на колапс. Многу пострашен исход би имал нападот кој би се состоел од навлегување во естонските компјутери и бази на податоци на здравствени или на криминални евиденции, исчезнување на банкарски сметки и сл.[217]

Кога се зборува конкретно за сајбер-терористички напади, веднаш се знае дека тие се насочени кон информациско-комуникациските системи, односно нападот е извршен со нивна помош, а се насочени кон критичните инфраструктури. Сајбер-терористот како цели за напад може да ги земе информациските системи и мрежи на болници, банки, влада, авиокомпании, поединци, и сл., при што ќе се бараат слабости и ранливости во тие системи, со цел да ги нападнат и уништат.

[216] Калач Ј., Сајбер тероризмот како закана кон безбедноста на државата, *Правдико*, 2017.

[217] Lewis, J., Cyber Attacks Explained, 2007, преземено од http://www.csis.org/tech/070615 cyber attacks.pdf.

3.5. Ранливост на критичната инфраструктура од терористички напади преку интернет

Истражувањата покажуваат дека терористичките организации ги сметаат нападите против критичната инфраструктура преку интернет како најпосакуван модус операнди. Група владини експерти за развој во областа на информациите и телекомуникациите во контекст на меѓународната безбедност во Извештајот од јули 2015 година констатирале дека употребата на информациите и телекомуникациите за терористички цели, регрутирање, финансирање, обука и поттикнување, вклучувајќи и за терористички напади против информациска критична инфраструктура или инфраструктура зависна од компјутерската технологија може да го загрози меѓународниот мир и безбедност.[218]

Следните констатации се неколку клучни заклучоци донесени од водечки истражувачки институции во врска со ранливоста на критичната инфраструктура од терористички напади извршени преку интернет:

- Критичната инфраструктура е ранлива на сите видови напади и сè повеќе напади се извршени преку интернет и сè повеќе е јасно дека ништо на интернет не е безбедно.[219]
- ИСИЛ веројатно нема да може да изврши спектакуларни напади преку интернет, како што е таргетирање на критична инфраструктура, но сепак, активно се обидува да регрутира лица способни за извршување напади преку интернет и најверојатно ќе може да го стори тоа.[220]
- Постои зголемена загриженост дека терористичките групи евентуално можат да развијат капацитети за користење на интернет и поширок интернет-простор за да спроведат деструктивни напади против критичната инфраструктура, со потенцијал да предизвикаат значителна штета.[221]

[218] A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. July 2015, достапно на: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/174

[219] World Economic Forum. White Paper. "*Global Agenda Council on Cybersecurity",* 2016, достапно на: http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

[220] STRATFOR, "The Coming Age of Cyberterrorism", 2015, достапно на: https://www.stratfor.com/weekly/coming-age-cyberterrorism

[221] ICT4PEACE Foundation. "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes," 2016, достапно на: http://ict4peace.org/wp-content/ uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes-2.pdf

- Капацитетот за извршување напади преку интернет не мора да доаѓа од ИСИЛ. Достапноста на алатки и услуги на компјутерскиот криминал на подземните криминални пазари веројатно ќе им овозможи на ИСИЛ и на други терористички организации уште повеќе да ги зајакнат постојните способности.[222] ИСИЛ се обидува да регрутира квалификувани лица способни да реализираат сложени напади преку Интернет.[223] Растот на црните пазари на ИКТ им отвора простор на „хакерите за изнајмување".[224]
- Очекуваниот раст на милијарди уреди преку интернет (индустриски „интернет на нештата") ќе донесе значителни безбедносни предизвици, вклучувајќи и употреба на IoT од страна на терористите за извршување напади против критична инфраструктура.[225]
- Cloud computing и криптирање ја зголемуваат комплексноста на предизвикот.[226]

Имајќи ја предвид ранливоста, заштитата на критичната инфраструктура од напади преку интернет, општо вклучува потенцијални терористички напади и во моментот се соочува со комплексни предизвици. Глобална агенда за компјутерска безбедност е насочена кон:

1. Меѓународна фрагментација: разликите во пристапот кон компјутерската безбедност, надлежноста на податоците и законското спроведување (како и културата, јазикот и политиката) преку јурисдикција и територијални граници можат да го отежнат ефикасното спречување, истрага и гонење на напади извршени преку интернет.

2. Меѓународно поставување на нормите: меѓународните политички разлики и агендите специфични за земјата можат да го отежнат развивањето на консензус норми во врска со компјутерската безбедност.

3. Улоги во однос на приватниот сектор: различните и понекогаш конфронтативни улоги што јавниот сектор мора да ги игра може да создадат тензии и намалување на довербата со приватниот сектор.

---

[222] STRATFOR, "The Coming Age of Cyberterrorism", 2015, достапно на: https://www.stratfor.com/weekly/coming-age-cyberterrorism.

[223] Ibid.

[224] STRATFOR, "Examining the Islamic State's Cyber Capabilities", 2015, достапно на: https://www.stratfor.com/analysis/examining-islamic-states-cyber-capabilities

[225] World Economic Forum, (2016), "Network Name ; "Industrial IoT.", достапно на: https://www.weforum.org/events/world-economic-forum-annual-meeting-2016/sessions/the-internet-of-thingsis-here/

[226] Council of Europe. Octopus Conference 2016 "Cooperation against Cybercrime. Key messages", достапно на: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMCon tent?documentId=09000016806be360

4. Погрешно усогласување на стимулациите за најдобра практика во компјутерската безбедност: Компаниите честопати не успеваат да преземат основни чекори за да ги заштитат своите системи и нивните корисници, затоа што тие се ставени во тешка позиција за балансирање на притисоците на пазарот за брза иновација против одржливите инвестиции во компјутерската безбедност, што може да ги зголемат трошоците или да ја одложат испораката на производите на пазарот.

5. Комплексности на екосистемите: Денешните софтверски и хардверски опкружувања се повеќе сложени екосистеми населени со мрежа на интерактивни уреди, мрежи, луѓе и организации. Ова значи дека решенијата за компјутерска безбедност честопати бараат доброволно ангажирање, соработка и инвестирање на многу независни субјекти, и покрај тоа што стимулациите и механизмите за преземање на вакви активности се дистрибуираат неконзистентно низ екосистемот.[227]

И покрај тоа што не постојат „брзи решенија за компјутерската безбедност", Белата книга ги идентификува чекорите што организациите можат да ги преземат за да започнат со решавање на предизвиците во врска со компјутерската безбедност, и тоа:

- ✓ донесување најдобри практики и сајбер хигиена;
- ✓ подобрување на системите за автентикација; и
- ✓ подготовка за напади (на пр, со подобрување на форензички способности, развој на планови за континуитет на деловните активности).[228]

Во делот на компјутерската безбедност значајно место му припаѓа на сајбер-просторот. Сајбер-просторот претставува глобален домен во областа на информациите и се состои од независна мрежа на информациски системи и инфраструктура, вклучувајќи интернет, телекомуникациски и компјутерски мрежи.[229] Со зголемување на зависноста од информатичката технологија, сите државни витални инфраструктури се ранливи на некој вид надворешен напад. Дури и ако експертите не се согласуваат за степенот и за природата на заканата, државите, сепак, треба да усвојат мерки за зајакнување на заштитата на информациските системи. Подигањето на свеста и поттикнувањето на обуката во областа на безбедноста на информациите и заштитата на

[227] World Economic Forum's, White Paper – Global Agenda Council on Cybersecurity, 2016, достапно на: http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

[228] http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

[229] Kissel R., (ed.). Glossary of Key Information Security Terms, 2011.

инфраструктурата ќе биде исклучително корисно. Тоа треба да вклучува тесна соработка изразена преку изведување заеднички вежби преку кои ќе се врши симулација и моделирање на способност за да се разбере влијанието на можен напад врз меѓусебно поврзаната и меѓусебно зависната информациска инфраструктура. Тоа ќе придонесе за развој на нови можности за детекција и идентификација на можните негативни импликации врз информациската инфраструктура.

4. САЈБЕР-ЗАКАНИ ВРЗ ИНДУСТРИСКИТЕ КОНТРОЛНИ СИСТЕМИ И КРИТИЧНАТА ИНФРАСТРУКТУРА

Критичната инфраструктура претходно се сметаше за нешто стабилно и конректно, било да се работи за физички или за информациони и комуникациски системи, но денес е актуелна холистичката перцепција на критичната инфраструктура која претставува збир на мрежи и системи кои се од витално значење за општеството како целина. Разликите во концептуализацијата и во дефинирањето на критичната инфраструктура во различни земји се резултат на различната перцепција на заканите и безбедносните ризици и разлики во географските и историските услови, но влијаат и социополитичките фактори.[230]

Следејќи ги глобалните трендови, постои реална можност во наредниот период јавниот и приватниот сектор да се соочат со зголемен број сајбер- напади, вклучувајќи и индустриска сајбер-шпионажа, сајбер-вандализам и идентификација на ранливости кај енергетскиот сектор, финансискиот сектор, здравствениот сектор, транспортните системи и други делови од критичната информациска инфраструктура и важни информациски системи. Притоа, може да се очекува различен пристап, од предизвикување на непосредни прекини во функционирањето на делови од критичната инфраструктура до целосно блокирање. Нефункционалноста на гореспоменатите системи може да има фатални последици, а поради висока хетерогеност на техничките решенија, подоцнежната техничка анализа е значително отежната.[231]

Информациските системи сè повеќе се соочуваат со закани и со изложеност на ризици од разни извори, вклучувајќи измами со помош

[230] Pursiainen C., *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6, 2009.

[231] Национална стратегија за сајбер-безбедност на Република Македонија (2018-2022), јули 2018, достапно на: http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf

на компјутер, шпионажа, хакерски упади или, пак, од т.н. малициозни програмски кодови, односно вируси, кои се сè покомплексни и пософистицирани.

Во листата која следува, нападите се распоредени според нивното влијание и тоа од наједноставни, до најдеструктивни и тоа:

- *Сајбер-шпионажа.* Претставува акт или практика на здобивање со тајни (осетливи, лични или класифицирани информации) од индивидуалци, конкуренти, ривали, влади и непријатели за стекнување на воена, на политичка или на економска предност користејќи нелегални методи за искористување на интернетот, мрежите, софтверот и/или компјутерите.
- *WEB вандализам.* Напади кои ги обезличуваат web-страниците, или напади со одбивање на услуга.
- *Пропаганда*. При овој вид напад можно е да се испраќаат политички пораки кон секој кој има пристап до интернет.
- *Собирање на информации*. Овој напад се користи со цел информациите кои не се чуваат безбедно да се пресретнуваат, па дури и да се модифицираат, овозможувајќи вршење на шпионажа од било кој дел од светот.
- *Напади со дистрибуирано одбивање на услуга*. Овој напад се карактеризира со можност за искористување на голем број компјутери во една или повеќе држави за лансирање на напад врз системите на државата од каде воопшто и не се лансира нападот.
- *Нарушување на функционирањето на опремата*. Жртви на овој напад се воените активности во кои за координација се искористени компјутери и сателити. Користејќи го овој напад, злонамерните можат да ги пресретнат или да ги изменат наредбите и комуникациите, со што војниците би се ставиле во ризична ситуација.
- *Напаѓање на критичната инфраструктура*. Со помош на овој напад, злонамерните можат да навлезат во системите за контрола на електрична енергија, водата, горивото, комуникациите, транспортот и слични клучни инфраструктурни елементи и да се обезбеди контрола врз истите со основна цел уценување, кражби, изнудувања, измама и слично.
- *Компромитиран фалсификуван хардвер*. Овој напад се однесува на заедничкиот хардвер искористен во компјутерите и мрежите кои имаат злонамерен софтвер скриен во софтверот, firmware-от или дури и во микропроцесорите.[232]

[232] Nickolov E., "Modern Trends In The CyberAttacks Against The Critical Information Infrastructure", ITU, Regional Cybersecurity Forum, Sofia, Bulgaria, 2008, до-

Нема дилема дека ако може да се каже дека компјутерските мрежи станаа нешто налик на „нервен систем“ на инфраструктурите на цивилниот и на воениот сектор, и онеспособувањето на овој „нервен систем“ ќе значи и парализа на целокупниот систем, односно на целата земја. Сајбер-нападите може лесно да бидат извршени од страна на криминалци, но може да бидат подготвени од терористички ќелии и меѓународно распространети групации. Ако еден насилен напад над државните инфраструктури го сметаме за акт на војна, тогаш зголемениот број на релевантни актери значи и дека војната не е повеќе базирана единствено на политичката рационалност. Цел на нападите може да бидат мали или големи системи, и може да се мотивирани од обичен вандализам, финансиски и политички придобивки, па сè до начин на докажување и заработување, но и престиж во очите на другите „сајбер-војници“. Географската оддалеченост и границите се исто така неважни, бидејќи една цел може да биде погодена од спротивната страна на светот за само неколку секунди.[233]

Како прв комбиниран напад на сајбер-напад и воена офанзива се бележи нападот врз Грузија. DDoS – напад од мали размери (напади со дистрибуиран прекин на услугите) врз грузиската интернет инфраструктура, биле регистрирани во јуни 2008 година, скоро два месеци пред петдневната војна помеѓу Русија и Грузија, во врска со прашањето за Јужна Осетија. На 20 јули 2008 година, фондацијата „Shadowserver“ регистрирала група чувари на интернет кои забележале повеќе DDoS напади насочени кон официјалната веб-страница на грузискиот претседател Михаил Сакашвили, кои резултирале со пад на веб-страницата повеќе од 24 часа. Утврдено било дека нападот бил координиран преку американски сервери, факт кој ја нагласува транснационалната природа на оваа закана. Според „New York Times“ нападите врз грузиската комуникациска мрежа кулминирале на 8 август 2008 година, првиот ден од војувањето, кога биле регистрирани напади на веб-страниците на Владата и медиумите. Како се заострувал конфликтот, така ескалирале и on-line нападите кои руските *хактивисти* ги вршеле над веб-страниците на претседателот, Парламентот, Министерството за одбрана, Министерството за надворешни работи, Грузиската народна банка и новински агенции. Грузија од сајбер-нападите претрпела мала штета бидејќи

стапно на: http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolovmodern-trends-sofia-oct-08.pdf.

[233] Thomas A. Johnson (ed)., *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015.

грузиската економија и виталната инфраструктура сè уште не биле интегрирани во е-општество. Сеедно, кампањата водена од страна на националистичките *хактивисти*, поттикнати на акција со помош на рускиот on-line хакерски форум, ефикасно ја пореметила дистрибуцијата на информации на Владата на Грузија, во клучните моменти на нападот.[234]

Овие сајбер-напади имаа три целни групи:

1. серверите задолжени за интернет-инфраструктурата на државата;
2. веб-страниците на владините институции и важни политичари во земјата и
3. провајдерите на приватниот сектор во земјата (банките, медиумите итн).

Оваа еволуција, или подобро речено револуција на сајбер-нападите, може да биде видена како модерна алатка за индиректна интервенција за тајно уништување на противничката мрежа и критичната воена инфраструктура, покажувајќи ја стратегиската важност на технолошката еволуција во сајбер-просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.

5. КРИТИЧНАТА ИНФРАСТРУКТУРА КАКО ЦЕЛ НА САЈБЕР-НАПАДИТЕ

Во време на модерен технолошки развој и целосна дигитализација на сите релевантни, лични, финансиски и други податоци и информации на физичките и правни лица, секако и сајбер-нападите станаа сè почеста појава со тенденција на постојан и рапиден пораст, а пак, штетата која ќе настане од таквите напади е значителна и тешко мерлива.

Нападите насочени кон критичната инфраструктура, без разлика дали зад нив стојат политички, верски, сепаратистички или други видови организации или станува збор за тероризам, индустриска шпиунажа, хакерски напади, претставуваат едни од најопасните глобални закани кои ја обележуваат денешницата. Новите облици на загрозување кои произлегуваат од сè посложените меѓународни односи и новите облици на невоените закани, кои се во согласност со променетиот концепт на безбедност, ги менуваат и концептите на меѓународната, а особено на

[234] Повеќе за ваквите напади во "Explaining Distributed Denial of Service Attacks to Campus Leaders," May 3, 2005, достапно на: http://www.uoregon.edu/~joe/ddos-exec/ddos-exec.pdf.

националната безбедност. Комплексноста и сложеноста на проблематиката која ја третира безбедноста на критичната инфраструктура, директно се врзува со стратегиите на националната безбедност на голем број држави каде што се добива поширока витална димензија, вклучувајќи економски, стопански, политички и еколошки прашања. Националната безбедност повеќе не подразбира исклучиво воени стратегии, туку сè почесто се настојува да се елиминираат невоените загрозувања со воочување на реалната опасност и ефикасна елиминација на истата. Често тоа претставува создавање стратегии на национална безбедност, низ еден деликатен и сеопфатен процес, вклучувајќи ја и безбедноста на критичната инфраструктура како составен дел на безбедносниот концепт на секоја држава.[235]

Критичните информациски инфраструктури може да бидат особено ранливи на напади од страна на хакери, криминалци и терористи. Главните алатки кои се користат за напад на критичните системи се малициозен софтвер (вируси, црви, тројански коњи), кои ги менуваат и ги уништуваат податоците или ги блокираат системите, кражба на идентитет (phishing) напади на веб- апликации (SQL напади), напади со откажување на услуги (DOS, DDoS), внатрешни напади (социјален инженеринг) и слично. Различни автоматски алатки овозможуваат напади од далечински систем, во рок и од неколку секунди. Ова претставува важна основа за поголем обем на активности поврзани со националната безбедност и подготвеност на комуникациите во време на кризни ситуации.

Информациското војување (приватни корисници – хакери или пак, одредени држави можат од различни причини да ги нападнат информациските системи во различни земји и да доведат до големи проблеми не само во функционирање на информатичката инфраструктура, туку и во многу други сектори, со оглед на фактот дека многу се потпираат на информациските системи. Голем дел од оваа инфраструктура е контролирана од индустриски контролни системи – ИКС, кои, исто така, се познати како „Надзорна контрола и стекнување со податоци“ (Supervisory Control and Data Acquisition – SCADA),[236] програми кои се ранливи на хакирање или DDoS-напади. Ако заканата не може да предизвика хакирање во системот, тогаш секогаш е можно да се пробие заштитата поради човечки фактор, т.е. корисничка грешка. Многу е полесно да се

[235] Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016.

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

напаѓаат корисниците (се мисли персоналот) отколку самата опрема. Кога нападот е успешен, опциите за извршување на посакуваниот удар се многубројни. Важно е да се напомене дека повеќето инфраструктурни системи имаат слични проблеми: исти оперативни системи, недостаток на средина во која би можело да се тестира моменталната сајбер-безбедносна состојба, локален менаџмент и нема присуство на надзор. Програмите се направени за специфични системи кои оригинално се поставени во затворени мрежи, па се направени со земање предвид на можноста за високи побарувања, но без заштита на доверливоста или интегрирани заштити.[237] Сопствениците на овие системи веруваат дека тие ќе бидат заштитени со тоа што се непознати за јавноста и никој нема да хакира во нивните системи. Исто така, тие се чувствуваат недопирливи, тргнувајќи од тоа дека нивните програми во кои целиот систем работи се специјално напишани само за нив, односно се уникатни со конкретни исполнувања кои ги бара специфичниот дизајн на хардверот. Повеќето од овие системи користат исти протоколи кои се развиени/напишани во истите програмски јазици како и сите останати програми на пазарот денес, со што е релативно лесно да се најдат ранливости во нив. Нападите против SCADA системите се дуплираа во 2014 година на повеќе од 160.000 напади.[238]

Ако погледнеме во критичната инфраструктура во полето на водоснабдувачкиот систем, на пример, потенцијалните терористи можат да навлезат во системите и да ги отворат вентилите/портите на браната и да предизвикаат поплави или да внесат хемикалии за пречистување до степен водата да стане отровна. Реалноста е дека сајбер-проблемите се исто толку важни како и другите проблеми со кои се соочуваат овие системи. Оваа еволуција, или подобро речено револуција на сајбер-нападите, може да биде видена како модерна алатка за индиректна интервенција за тајно уништување на противничката мрежа и критичната воена инфраструктура, покажувајќи ја стратегиската важност на технолошката еволуција во сајбер-просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.

[237] Edward G. Amoroso, *Cyber Attacks Protecting National Infrastructure*, Elsevier Inc, USA, 2011.

[238] Dell's, (2015) Annual Security Report, достапно на: http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html.

6. ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Заканите за критичната инфраструктура и другите поврзани ризици се идентификувани веќе неколку децении, и се смета дека зачетоците датираат од појавата на индустријализацијата и зголемената урбанизација. Веќе во последната декада од XX век, заштитата на критичната инфраструктура станува секуритизирано прашање што го привлекува вниманието на политичките раководства. Така, во 1997 година, заштитата на критичната инфраструктура станува прашање од национално значење во САД, откако претседателската комисија изготви извештај во кој се потенцира значењето на критичната инфраструктура.[239]

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

Во основа, државите се одговорни за заштита на населението и обезбедување на одредено ниво на социјална функционалност и безбедност, но факт е дека дел од критичната инфраструктура е во државна сопственост, а дел е во приватна сопственост (домашни или странски компании). Многу западни земји го имаат поголемиот дел од критичните инфраструктури во приватна сопственост, а државата со цел да обезбеди непречено работење и функционирање на критичните

[239] Rosslin John Robles, *et al*.: Common Threats and Vulnerabilities of Critical Infrastructures. International Journal on Control and Automation. http://article.nadiapub.com/IJCA/vol1_no1/3.pdf посетена на 11/12/2019.

инфраструктури[240] – вложува големи напори за да обезбеди соработка на државните структури и приватните лица. Заради испреплетените односи постојат сопственици кои не поседуваат исти вредности и ставови на обезбедување на системот на критичната инфраструктура. Оттука се наметнува потреба од еден мултиваријантен пристап на државата и на операторите.[241]

Овој мултиваријантен пристап треба да се заснова на искуства и најдобри практики помеѓу експерите и државите, првенствено поради различното ниво на развој на заштитата на критичната инфраструктура. Главните цели кои е потребно да се разгледаат со цел да се развијат ефикасни модели за заштита на критичната инфраструктура се следните:

- ✓ јавни-приватни партнерства во областа на заштитата на критичната инфраструктура;
- ✓ воспоставување механизам за размена на информации и податоци во однос на системите за заштита на критичната инфраструктура;
- ✓ воспоставување предуслови за основање центри за заштита на критична инфраструктура на национално ниво.[242]

Заштитата и резилиентноста на критичната инфраструктура се мерливи преку ранливоста на мрежите и на технологиите за критична инфраструктура.[243]

Во тековниот период, очевидна е и оправданата интензивирана загриженост и дебата околу заштитата на критична инфраструктура, особено во доменот на нивната ефективна заштита, имајќи ја предвид нивната витална позиција во социо-економските односи. Покрај оваа

[240] National critical infrastructure protection – regional perspective- Belgrade, December 2013 UDC726.9:75.041.5, ID176374796, Mihaljević B., Toth I., Stranjik A., Impact of Critical Infrastructure Ownership on the National Security of the Republic of Croatia.

[241] Во Германија 4/5 на критичната инфраструктура се во приватни раце. Во САД околу 85% од критичните инфраструктури се во приватна сопственост, но реалноста е дека пазарните сили сами за себе не се доволни да ја предизвикаат потребната инвестиција во заштитата во P. Auerswald, L.M. Branscomb, T.M. La Porte, E.Michel – Kerjan – *The Chalenge of Protecting Critical Infrastructure – issues in science and tehnology,* 2005, стр. 77.

[242] Resilience of Critical Infrastructure Protection. Guidelines. Humanitarian Aid and Civil Protection. https://ec.europa.eu/echo/sites/echo-site/files/recipe_guidelines.pdf посетена на 13/12/2019.

[243] Дирекција за безбедност на класифицирани информации http://www.dbki.gov.mk/?q=node/436 посетена на 13/12/2019.

оправдана загриженост, се истакнува и зголемениот акцент кој се става на потребата за подобрена ефикасност, изведба и продуктивност на системите на критична инфраструктура, како и импликациите кои произлегуваат од реалната состојба дека системите на критична инфраструктура речиси никогаш не функционираат и егзистираат одвоено и во изолација. Напротив, тие меѓусебно се суплементарни. Тенденцијата е овие системи да се трансформираат во тесно поврзани системи на (меѓу)зависни инфраструктури, конвергентни со информатичките и комуникациските технологии (the internet of things) и интернетот.

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

Заради тоа заштитата на овие инфраструктури е од исклучително значење со цел избегнување и намалување на негативните последици во случаи на нарушување на нивното функционирање и обезбедување континуиран нормален оперативен тек (при потенцијални закани од напади, грешки на нивните компоненти, или пак во случаи на природни непогоди) и осигурување на нивната непречена работа доколку настане некоја или комбинација од наведените настани.[244]

Критичната инфраструктура може да биде ефективно заштитена преку процена на заканите и ранливостите. Откако ќе се спроведе таа фаза, се развива и креира план со кој се елиминираат или минимизираат и ублажуваат заканите и ранливостите.

Во тој процес, потребно е да се спроведат неколку фази на активности во насока на заштита на критичната инфраструктура, и тоа:

1. Проценување на ранливостите на критичната инфраструктура од физички и сајбер-напади.
2. Развивање планови за елиминација на значителни ранливости.
3. Предлог на системи за идентификација и превенција на обиди за напад.
4. Развој на планови за предупредување, задржување и отфрлање напади во тек.

[244] O'Rourke, T., D.: Critical Infrastructure Interdependencies and Resilience. https://pdfs.semanticscholar.org/6c17/b35ec7555a9f27d5ccb6ca1d357a20b5ce0a.pdf, посетена на 21/11/2019.

5. Брза реконструкција на минималните и основни капацитети во случаи на извршен напад.[245]

Идентификацијата е неопходно потребна за понатаму да се креираат оптимални решенија. Основните чекори за идентификација и заштита на критичната инфраструктура вклучуваат:

- Спроведување на процени на ризик и приоритизација на објекти.
- Познавање на меѓузависноста на клучните инфраструктури.
- Анализа на меѓусекторските каскадни ефекти.
- Координација на јавните со приватните сектори и оператори за подобрување на заштитата и отпорноста.[246]

За имплементација на овој план, инфраструктурата може функционално да биде категоризирана во пет нивоа:[247]

- *Ниво 5* – управувањето со кризата на локално ниво, првенствено мора да се фокусира на објектите и субјектите кои се витални за локалната заедница, тука спаѓаат локалните сили за спроведување на законот, противпожарни станици, единици за одговор при катастрофи, итн.[248] Други локални објекти кои се критични за благосостојбата на локалната заедница се водоснабдувањето, системот за одвод и канализација, електрична енергија, болници и други здравствени установи, прехранбен ланец на набавка, комуникациски системи, банкарски услуги, спортски и образовни установи и други видови примарни ресурси на заедницата. Критериумите за утврдување ниво 5 на критичност се следните: 1. Број на жртви до 100 лица. 2. Економски последици од првата година по катастрофата. 3. Масовна евакуација со пролонгирано времетраење од една недела или подолго. Овие критериуми директно влијаат врз локалната економија и капацитетите.
- *Ниво 4* е категоризација на објекти со критичност за одреден регион. На ова ниво, неколку чекори се преземаат за да се обезбе-

[245] Assessing the Security of Internet Connected Critical Infrastructure (The CoMiFin Project Approach). https://www.nics.uma.es/pub/seciot10/files/pdf/ghani_seciot10_paper.pdf, посетна на 27/11/2019.

[246] Yosha, N.: Waking Up to Critical Infrastructure Threats. 2019, Threat Quotient, Inc. https://www.threatq.com › critical-infrastructure-threats, посетена на 18/12/2019.

[247] 4 Complex CIKR Systems. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, 2nd Edition by Ted G. Lewis https://www.oreilly.com/library/view/critical-infrastructure-protection/9781118817667/c04.xhtml/ посетена на 15/12/2019.

[248] Commercial Facilities as Targets. New Threats to Critical Infrastructure. Social Value Creation Report. https://www.nec.com/en/global/solutions/cybersecurity/publications/images/SocialValueCreationReport_en_Vol.1.pdf посетена на 20/12/2019.

ди добрата позиционираност на регионот за одговор на настани кои водат до катастрофи, како што се регионални недостатоци со снабдување со електрична енергија, дефицит на гориво, сајбер-напади, проблеми во транспортот, регионални проблеми со водоснабдување, како и други видови кризи. На пример, да се знае локацијата на големи резерви со гориво ќе помогне за време на недостиг на гориво. Критериумите со кои се утврдува ниво 4 на критичност се следните: 1. Повеќе од 100 жртви. 2. Значителни економски последици и загуби во периодот на првата година од инцидентот. 3. Масовни евакуации со времетраење повеќе од две недели.[249]

- *Ниво 3* на критичност е категоризација на објект со критичност на ниво на општина. Во овој сегмент важно е да се идентификуваат меѓусекторските зависности и каскадните ефекти за тоа како и зошто секој сектор е значаен за општината, засновано на каскадниот ефект. Во овие околности е неопходна силна основа за подготвеност на системите на критична инфраструктура, во согласност со секторската поделба од страна на државата. Преку фокусирање на највиталните сектори се креира план. Критериумите со кои се утврдува ниво 3 на критичност се следните: 1. Повеќе од 1.000 жртви. 2. Енормни економски загуби во текот на првата година. 3. Масовни евакуации кои траат повеќе од 3 недели.
- *Ниво 2* или *Ниво 1* се категории во случаи кога е погодена и националната економија. Националниот импакт од Ниво 2 се пресметува доколку системите на критична инфраструктура претрпат дефект или крах предизвикувајќи значителен голем број жртви на национално или на ниво на повеќе општини, опасности по јавното здравје, како и последици врз економијата и врз националната безбедност. Идентификацијата на Ниво 2 критичност е во случаи кога: 1. Оштетувањето или прекинот предизвикува повеќе од 2.000 жртви. 2. Економските последици се во вредност од милијарди долари во првата година по несреќата. 3. Масовните евакуации се пролонгирани за повеќе од еден месец. 4. Значителната штета и прекин во системите на критична инфраструктура предизвикува онеспособување на капацитетите за на-

[249] Infrastructure Systems: Developing a Critical Infrastructure and Key Resources Plan. Harris County Office of Homeland Security and Emergency Management.https://www.hsdl.org, посетена на 22/12/2019.

ционална безбедност, вклучително и одбранбените и разузнавачките функции, со исклучок на воените објекти.

- *Ниво 1* се идентификува како објект чија критичност доколку биде нарушена или прекината ќе резултира со најмалку од овие две последици: 1. Број на жртви над 5.000. 2. Повеќе десетици милијарди долари/евра загуба во првата година од катастрофата. 3. Масовни евакуации кои се во времетраење повеќе од 3 месеци. 4. Значително уништување на капацитетите за национална безбедност на државата за употреба на одбранбените и разузнавачки функции, со исклучок на воените објекти.[250]

Клучните елементи кои треба да бидат земени предвид за надминување на предизвиците поврзани со идентификација и заштита на критичната инфраструктура вклучуваат:

- ✓ развивање партнерства и координација со приватниот сектор кој е директно поврзан со заштитата на критичната инфраструктура;
- ✓ идентификација и утврдување на меѓузависностите;
- ✓ препознавање и разбирање на улогата на владата во заштитата на критичната инфраструктура.[251]

Идентификацијата на критичната инфраструктура со цел нејзина заштита, преку координација и интеграција на активностите во управувањето со ситемите на критична инфраструктура помеѓу широкиот опсег јавни и приватни менаџери и безбедносни партнери, придонесува за креирање план за заштита на елементите и системите на критичната инфраструктура и виталните ресурси во случаи на катастрофа или вонредна состојба во непосредниот домен на инцидентот на регионално и на национално ниво.[252] Планот за заштита на критична инфраструктура се состои од следните точки:

- ✓ Ги опишува улогите и одговорностите за подготвеност, заштита, одговор, опоравување, обновување и континуитет на операциите на координативните структури за заштита на критичната инфраструктура.

[250] Partnering for Critical Infrastructure Security and Resilience. Homeland Security. https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf, посетена на 18/12/2019.

[251] Johnson, L.: Critical Infrastructure Plan. Security Component Fundamentals for Assessment. Security Controls Evaluation, Testing, and Assessment Handbook, 2016.

[252] The Modern Attack Surface. Tenable [online] https://www.tenable.com/cyber-exposure, посетена на 18/12/2019.

- ✓ Воспоставува оперативен концепт за инцидентни операции за заштита на критичната инфраструктура, подготвеноста, заштитата, одговорот, опоравувањето и обновата.
- ✓ Ги потцртува активностите поврзани со инцидентот – пред одговорот и по одговорот во однос на споделување на информации и анализи на конкретните или потенцијални влијанија врз системите на критична инфраструктура и ги олеснува потребите за поддршка од страна на јавните и приватните планирачи

Веќе беше истакнато дека за да се обезбеди соодветното оптимално ниво на безбедност, потребно е да бидат ангажирани сите релевантни субјекти во врска со закани од потенцијални напади, реални напади или техники за опоравување, доколку се случил реален напад.[253]

Генерално, активностите на сите засегнати субјекти треба да бидат насочени кон: изградба на капацитети во справување со инциденти и во истражување на безбедносни појави, мониторинг на безбедноста, како и прибирање ИТ разузнавачки податоци; промовирање на соработка помеѓу клиентите во однос на ИТ безбедноста; одржување статистички апдејт на инциденти, промоција на стандарди и алатки за ИТ безбедност; промоција на стандарди за безбедност и управување со ризици; комуникација со цел зголемување на свесноста кај јавноста и добавувачите на услуги за безбедносни прашања; одржување модел за безбедност во согласност со аранжманите и аутсорсинг договорите и стимулирање производство и усвојување на соодветни стандарди и олеснителни можности на независни капацитети за заштита и безбедност.[254]

[253] Cismaru, D., *et al*.: CIP v5 Compliance Monitoring. October 25, 2017. https://www.aeso.ca/assets/Uploads/ARS-CIP-Compliance-Oct-25-2017-Final.pdf, посетена на 21.11.2019).

[254] Infrastructure Security. https://www.cisa.gov/infrastructure-security, посетена на 25/11/2019.

глава IV

БЕЗБЕДНОСТА И ИНФОРМАЦИИТЕ

1. ОПШТО ЗА ИНФОРМАЦИЈАТА

Информацијата несомнено е синоним на знаењето и таа е поширокатa основа на организираноста, на средената и на поврзаноста на деловите во системот, т.е. таа се идентификува со знаењето кое некој го употребува за да оствари одредена цел.

Располагањето со навремена, со точна и со издржана информација значи остварување на зацртаната цел, односно вистинската информација ако се искористи во вистинско време и на вистински начин тогаш таа може да биде најсилно оружје во рацете на тој што ја поседува. Со други зборови, постоењето на вистинска и на брза информација значи дека планираните задачи ќе се реализираат во целост и дека информацијата како своевиден податок за одредена состојба, селектирана, анализирана и интерпретирана ќе го има главниот збор при донесување на одредени одлуки. Значи, од информираноста, односно од неинформираноста во голема мера зависи ефикасноста на процесот на планирање. Оттука, не е сеедно каква информација ќе биде пласирана во одредена институција, ниту е небитен одговорот како соодветната институција откако ќе ја добие потребната информација ќе се однесува и како ќе ја искористи истата затоа што од овие претпоставки во голема мера зависи и одлуката за функционирањето на самата институција.

Информациите се предуслов за добро координирање и одлучување. Без потребните сознанија, податоци, параметри, невозможно е да се донесе координирана одлука. Од друга страна, резултатот на одлучувањето - одлуката како предуслов за акција, исто така, е информацијата. Оттука, секој систем, пред се човекот се бори да обезбеди точни, квалитетни, комплетни, навремени и корисни информации. Информацијата со вакви карактеристики ја намалува неизвесноста. Ако ја зголемува неизвесноста, тогаш таа е лоша, некорисна информација. Но постојат различни комбинации за карактеристиките на информациите. На пример, информациите можат да бидат точни, но некомплетни со што ќе го дезориентираат корисникот. Можат да бидат точни, но ненавремени со што нема да ја имаат очекуваната вредност за корисникот. Можат да бидат точни, но некорисни, доколку се претставени во поголем обем или пак на начин неприфатлив за корисникот итн.[255]

[255] Поповска З., *Управување со системите*, Економски факултет, Скопје, 2006, стр. 113.

За да го разбереме значењето на информацијата најнапред започнуваме со поширока елаборација на термините кои најчесто се користат како синоними. Тоа се термините: симболи, податоци, информации и знаење.[256] Симболите ги користиме најшироко како букви, бројки, кодови и други знаци. Потоа, следат податоците кои според некое правило претставуваат комбинација на симболите. Од семантички аспект, податок е сè она што е меморирано (чувано, регистрирано), но не е искористено, меѓутоа постои веројатност да се искористи. Кога податокот ќе се искористи, станува информација.[257] Доколку податокот има карактеристика на новост, тогаш се зборува за вест. По податоците следат информациите. На прашањето „Што се информациите?", се добиваат многубројни одговори. И покрај разликите во дефинициите, како суштествени за поимањето на информациите најчесто се вклучуваат новоста, корисноста и релевантноста. Доколку некој каже „економските науки не се исто со безбедносните науки, студентот по економија нема да прими информација, туку само сознание за апсурдноста на исказот". Но, ако некој му каже за правците на развојот на економската наука, тој ќе прими информација, бидејќи исказот содржи новост. Од друга страна, сè што се прима како новост, не се користи веднаш, бидејќи корисноста е поврзана со одредена промена, задача, цел. Информацијата е релевантна вест само кога носи знаење на корисникот за да може да го промени неговото однесување, став, мислење и да реши некоја задача.[258] Кога станува збор за знаењето, особено човековото знаење, тоа се создава низ перманентниот процес на креирање, пренесување, обработка, чување и користење на информациите. Знаењето се состои од пренослиби, но и од непренослиби информации, како и од кодифицирани, но и од информации кои не можат да се кодифицираат, бидејќи се резултат на високата експертска и имагинативна творечка сила на човекот. Затоа, најшироката дефиниција за знаењето која е и најсоодветна потенцира дека „знаење е она што служи за да биде искористено при одлучувањето."[259]

[256] Се смета дека најсоодветен хиерархиски редослед на термините е следниот: податоци на најниското ниво, следат информациите, потоа интелигенцијата (правила), знаењето (комбинација на податоците и информациите) и мудроста на највисоко ниво, во Barraba V., and Zaltman G., *Hearing the Voice of the Market,* Harvard Business School Press, 1990.

[257] *Податокот* се дефинира како неанализиран факт или настан врз кој се развива самата иформација. Врз основа на оваа рационална претпоставка податоците се средство за изразување на информациите.

[258] Поповска З., *Управување со системите*, Економски факултет, Скопје, 2006, стр. 111-112.

[259] Исто., стр. 112.

Може да се констатира дека информацијата е врвна општествена употребна вредност, основен стратегиски ресурс, главен инпут на секоја човекова дејност и главен развоен фактор, кој е поважен дури и од материјалниот фактор.[260] Како таква таа се прима заради некоја цел, односно таа е основа за донесување одлука која е во функција на координирачкиот процес. Доколку информацијата се прима за време на координирачкиот процес, тогаш таа има константно реална вредност, бидејќи овозможува реализација на целта во предвиденото време.

2. ПОИМ И ЗНАЧЕЊЕ НА ИНФОРМАЦИЈАТА

Современите информатички технологии драматично го променија начинот на кој информациите се собираат, се чуваат, анализираат и се споделуваат. Брзината, точноста и навременоста на информациите генерира создавање концепт на информациските операции.

Иако, нема теоретско објаснување за поимот информација, со сигурност знаеме дека таа е насекаде околу нас. Ја чувствуваме, ја гледаме, ја допираме, ја соопштуваме, ја примаме како нешто кое воопшто не сме го виделе или не сме го знаеле, а сепак знаеме дека е таму некаде и дека воопшто постои. Преку разни видови канали, средства за комуникација итн., информацијата стигнува до нас. Во денешно време информацијата е повеќе од секогаш присутна во нашите животи. До нас стигнуваат информации кои се намерни и ненамерни. Технологијата која секојдневно се усовршува нè принудува на некој начин да сме изложени на поголем степен на информираност – со наша или без наша согласност.[261]

Генерално, кога дискутираме за опфатот и за содржината во определување на поимот информација, дефиницијата за информација треба да го претстави феноменот информација преку една прецизна дескрипција на нејзината природа, преку воочување на разликата помеѓу информацијата и останатите поврзани концепти, како податокот, значењето, знаењето, а во исто време треба да ја воочи и суштинската разлика помеѓу овие концепти.[262]

---

[260] Стојановиќ П., *Теорија привредног развоја у мрежој технолошкој револуции*, Савремена Администрација, Београд, 1964, стр. 3-15.

[261] Herold R., Managing an Information Security and Privacy Awareness and Training Program, Press, Inc. Boca Raton, 2010, стр. 16-17.

[262] Losee, M. Robert - *„A Discipline Independent Definition of Information"* – Journal of the American Society for Information Science 48, Chappel Hill, 1998, стр. 6.

Поимот информација доаѓа од латинскиот глагол informare (поим, претстава, сознание),[263] а употребата на информацијата значи да се даде форма, или да се формира идеја за нешто. Тоа е општо етимолошко значење на самиот збор.[264]

За Келт, информациите се знаење за одреден предмет, проблем, настан или процес, и истите можат да се добијат од различни извори,[265] додека за Иглтон, дефиницијата за информации подразбира „вест или знаење добиено или дадено.[266]

Според Андерсон, информацијата е знаење изразено во сигнали, пораки, вести, известувања и сл. Секоја личност во светот е опкружена со информации од различни видови. Информацијата зависи и од тоа која е нејзината форма и во кој облик се прима.[267]

За Гачковски, информацијата може да се претстави како збир на вредности, како порака, како концепт, идеја, дизајн и слично, и токму затоа е многу тешко да се направи една комплетна дефиниција без да се изостави барем некој од овие елементи.[268]

Информацијата во одбранбениот речник е опишана како факт, податок или инструкции кои опстојуваат во некаков вид медиум или форма. Таа, исто така, може да се дефинира како смисла која човекот им ја доделува на податоци со помош на познати правила кои се употребуваат кога се претставуваат тие податоци,[269] додека за Албертс информацијата претставува термин кој често се употребува за да се посочат (покажат) многу различни точки во спектарот, почнувајќи од сурови податоци, завршувајќи со знаењето. Исто така, тој посочува дека информацијата е резултат на ставање индивидуални согледувања, повратни податоци

[263] Horić A., *Informacija – Povijest jednog pojma - O Capurrovom razumijevanju pojma informacije,* Zagreb, 2007, стр. 1.

[264] Смилевски В., Новинарски лексикон, Матица Македонска, Скопје, 2001, стр. 65.

[265] Kelt M., Smile by Imperial College, Glasgow Caledonian University, 2018, стр. 86.

[266] Игтон Т., Идеологија, Темплум , Скопје, 2005, стр. 43.

[267] Anderson J., Pew Research Center, Media Inquiries Washington, 2018, стр. 45-46.

[268] Gackowski, J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010, стр. 36.

[269] US Joint Publication 1-02., Department of defence dictonary of military and associated terms, November 2010, As Amended Through 15 January, достапно на: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

од сензорите (рецепторите) или податочни ставки, во некој контекст кој има (смисла) значење.[270]

Општоприфатените дефиниции според Урсул за информацијата говорат дека информацијата е акт од говорно или спознајно значење и е факт кој е научен за да има некоја корист, но е и знаење кое е добиено од некоја страна и претставува крвоток на животот во XXI век, како и моќ.[271]

3. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ НА ПОИМИТЕ ПОДАТОК И ИНФОРМАЦИЈА

Информациите, општо, се корисни податоци за одредена анализа, одлука или задача. Информациите мора да се секогаш соодветно заштитени без разлика на тоа како се чуваат, презентираат или пренесуваат. Значи, информацијата е податок кој има одредено значење или употребливост во определен контекст, односно за информација се смета обработениот податок кој ќе ни помогне да ги изградиме нашите ставови, процени и предвидувања.[272] Затоа, податокот е бескорисен се додека не пренесува одредена информација. Оттука, податок е претставување факти, концепти или инструкции на формализиран начин. Податокот треба да биде соодветен за комуникација, толкување или обработка од страна на луѓето или автоматизираните средства.[273]

Податоците се буквално секаде околу нас. Токму заради ваквата неорганизирана природа на податоците е неопходно тие да подлегнат на обработка со цел да бидат искористени. Во денешно време, кога има изобилство на податоци кои можеме да ги добиеме, споделуваме и мемориграме преку интернетот и другите форми на мрежни системи, проблемот не е дали има доволно податоци, туку дали може да се направи дистинкција на потребните од непотребните податоци.[274]

---

[270] David Alberts, *Understanding informaton age warfare*, 2001, достапно на: http://www.dodccrp.org/files/Alberts_UIAW.pdf

[271] Урсул А.Д.: Што е информација, во весник Московo универзитета, Сериа информатика, бр.2.1971, стр. 158-160.

[272] Metscher, Robert and Gilbride, Brion - *„Intelligence as an Investigative Function"*, International Foundation for Protection Officers, 2005, стр. 4.

[273] US Joint Publication 1-02, (2015), Department of defence dictonary of military and associated terms, November 2010, As Amended Through 15 January, достапно на: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[274] Metscher, Robert and Gilbride Brion - *„Intelligence as an Investigative Function"*, International Foundation for Protection Officers, 2005, стр. 3.

Мора да се нагласи дека податокот има своја примена во одредена информациска околина која претставува збир на поединци, системи и организации кои можат да прибираат, да обработуваат, и да дистрибуираат информации.[275] Според оваа дефиниција како дел од информациската околина, покрај системите и опремата која манипулира со информациите, се вклучуваат и поединците и носителите на одлуки. Луѓето и автоматските системи набљудуваат, се ориентираат, одлучуваат и дејствуваат врз основа на информациите во информациската средина. Поради тоа, информациската околина е главната околина на процесот на донесување одлуки.

Во основа, кога говориме за информациската околина таа е олицетворена во три димензии и тоа: физичка, информациска и когнитивна димензија.

Слика број 3: Три димензии на информациска околина

Извор: Милковски Н. и Богданоски М., Информацијата како стратешки ресурс од клучно значење за воените операции и одбраната на нацијата, *Современа македонска одбрана,* Министерство за одбрана на Република Македонија, година 15, бр. 28, јули 2015, стр 118.

[275] US Joint Publication 3-13. (2012). *Information Operations, Incorporating Change 1 20*, достапно на: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Во физичката димензија опстојуваат физичките платформи и комуникациските мрежи. „Во физичката димензија опстојуваат системите за командување и контрола, како и системот на комуникациска инфраструктура која им овозможува поддршка на поединците и организациите во воздух, на копно, на море и во вселената".[276] Како примери за физичката димензија може да ги земеме луѓето, местата и способностите како географски координати и комуникациска инфраструктура. Втората димензија е информацискатa димензија, каде што егзистираат информациите и информациските системи. Тука информацијата се креира, манипулира и споделува. Во оваа димензија се изведуваат активности како што се: собирање, складирање, објавување и заштита на информациите. Оваа димензија се состои од содржина и протокот на информации кои мора да бидат заштитени.[277] Когнитивната димензија претставува трета димензија на информацискатa околина. Човековата перцепција претставува „филтер" низ кој поминува целата содржина на когнитивната димензија. Овој филтер се состои од основните лични сознанија кои личноста ги внесува во ситуација, нивното искуство, обука и индивидуални способности (интелигенција, личен стил, способноста за перцепција и сл.). Денешната современа технологија ја прави лесна манипулацијата со податоците во информацискатa и физичката димензија. Колку што е полесно да се складираат, манипулираат и распределат податоците, толку се податоците поранливи при експлоатација. Но, когнитивната димензија сè уште не е лесно подложна на експлоатација, бидејќи современата технологија сè уште не може лесно да ги измени верувањата и предрасудите на луѓето.[278]

[276] US Joint Publication 3-13. (2012). Information Operations, Incorporating Change 1 20, достапно на: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, преземено од: Милковски Н. и Богданоски М., Информацијата како стратешки ресурс од клучно значење за воените операции и одбраната на нацијата, *Современа македонска одбрана,* Министерство за одбрана на Република Македонија, година 15, бр. 28, јули 2015, стр 115-125.

[277] Alberts D., *Understanding informaton age warfare*, 2001, http://www.dodccrp.org/files/Alberts_UIAW.pdf, преземено од: Милковски Н. и Богданоски М., Информацијата како стратешки ресурс од клучно значење за воените операции и одбраната на нацијата, *Современа македонска одбрана,* Министерство за одбрана на Република Македонија, година 15, бр. 28, јули 2015, стр 115-125.

[278] Милковски Н. и Богданоски М., Информацијата како стратешки ресурс од клучно значење за воените операции и одбраната на нацијата, *Современа македонска одбрана,* Министерство за одбрана на Република Македонија, година 15, бр. 28, јули 2015, стр 115-125.

4. МЕЃУЗАВИСНОТ НА ИНФОРМАЦИИТЕ И ИНФОРМИРАЊЕТО

Информацијата како поим и нејзината структура се во суштинска меѓузависност со информирањето.

Интеракцијата помеѓу информациите и информирањето е особено важна кога е придружена со меѓусебна зависност – степенот до кој членовите на групата се меѓусебно зависни едни од други за да се постигне зададената цел. Во некои случаи, а особено во работните групи, меѓузависноста вклучува потреба од заедничка соработка за успешно постигнување на една задача.[279]

Информациите и информирањето се неопходни и конзистентни во многу различни средини и претставуваат една од основните карактеристики на човечкиот род, а тоа е можноста субјективно да се процесираат спознанија и факти и да се генерира одредено знаење (разбирање, спознавање, перцепирање).[280] Информацијата и знаењето не мора да имаат исто значење.[281] Достапните информации сугерираат заклучоци формирани врз основа на позната шема и водат кон знаење.[282] Ако информаците се составени од зборови и фрази, тогаш информирањето е значењето и знаењето кои произлегуваат од тие зборови и фрази. Генерално, да се информира некој значи да му се пренесе одредено знаење. Информирањето може да се сфати како процес преку кој одреден човек или групација на луѓе се здобиваат со нови знаења преку информациите кои им се доставени или презентирани, односно се здобиле со ново знаење за одреден предмет на интерес.[283]

Во основа, информирањето е една од најважните активности во една организација.[284] Информациите кои се создаваат надвор од про-

[279] Извор: http://www.opentextbooks.org.hk/ditatopic/17339, посетено на 4/9/2019.

[280] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, стр. 2-4.

[281] US Joint Publication 1-02, (2015), Department of defence dictonary of military and associated terms, November 2010, As Amended Through 15 January, достапно на: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[282] Милковски Н. и Богданоски М., Информацијата како стратешки ресурс од клучно значење за воените операции и одбраната на нацијата, *Современа македонска одбрана,* Министерство за одбрана на Република Македонија, година 15, бр. 28, јули 2015, стр 115-125.

[283] Исто., стр. 2-4.

[284] Thomas E. Harris, Mark D. Nelson, Applied Organizational Communication, University of Alabama, 2009, стр. 67.

цесот на комуникацијата и работењето на организацијата, се засноваат на ефективни односи помеѓу поединци и групи. Внатрешната организациска комуникација, сметана како збир на процедури и организирана размена на комуникации, учествува во изградба на бројни проблематични ситуации кои се однесуваат на разбирањето и однесувањето на вработените, а сето тоа е услов за подобра размена на информациите. Затоа, комуникацијата не се одвива во стерилно и изолирано опкружување и е директно под влијание на поединците што ја сочинуваат размената на информации.[285]

Нема дилема дека информирањето има свој придонес во општественото живеење. Тоа претставува наука и уметност за преземање практични постапки кои ќе придонесат за зголемување на ефективноста, етичноста и/или ефикасноста во проширувањето на знаењето и контролата врз реалноста. За да биде сметано за наука, информирањето мора да биде ефективно и постојано. Тоа претставува една систематска студија на содржината и формата на реалноста (податоци и информации, и нивна меѓусебна релација), на резонирање и исходи, гледано од перспективата за целта и карактеристиките на информирањето.[286]

За да има успешно информирање, мора да постои размена на одредено значење (знаење) – мора да се разберат информациите кои се пренесуваат. Само ваквото разбирање може да биде гаранција дека постои информирање. Информирањето е истовремено многу едноставно и многу комплексно – едноставно во смисла на тоа што може да се разложи на специфични, одредени, квантитативни елементи кои овозможуваат прекин на процесот на информирање во кој било момент; а комплексно во смисла на тоа што сите овие елементи мора да бидат во целина и во одреден контекст, бидејќи информирањето е процес.[287]

Квалитетот на информацијата и информирањето е навистина важно прашање. Методолошки е неоправдано одвојувањето на квантитетот од квалитетот, бидејќи не е можно едното без другото. Исто така, кога се говори за квалитетот на информацијата и информирањето треба да се разликуваат два квалитети: техничкиот квалитет и содржински, односно благовремен квалитет на информацијата.

---

[285] Pipaş Maria Daniela, The Interdependence between Management, Communication, Organizational behavior and Performance, University of Cluj-Napoca, Romania, 2015, стр. 1561.

[286] Gackowski J. Zbigniew - *„Informing as a discipline – An initial proposal"*, Issues in Informing Science and Information Technology, Vol.13, California, 2010, стр. 169-179.

[287] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, стр. 4.

5. ТЕОРИСКИ МОДЕЛИ НА ИНФОРМИРАЊЕ

Теоријата на информациите е позната како математичка теорија. Неа ја поставил Клод Шенон, кој во 1949 година го објавил трудот „Математичка теорија на врски". Оваа теорија е премногу општа по својот обем, но е фундаментална според проблемите што ги третира и е класично моќна според резултатите што ги постигнува. Според Шенон, „*математичката теорија може да се примени во разни видови на кодови: од пишаниот јазик, преку нотите со кои се музицира и говорот, па сè до Морзеовата и Брајовата азбука*". Математичката теорија, всушност, се занимава со проблемите на пренесување на пораката во комуникациискиот процес. Теоријата на информациите може да се дефинира како наука која се занимава со изучување на механизмите на пренесување на пораката во универзален вид.[288]

Математичкиот модел на К. Шенон и В. Вивер, кој тие го имаат развиено во 1949 година, функционира на следниот начин:

Слика број 4: Математички модел на К. Шенон и В. Вивер

Во непосредното комуницирање (лице во лице) изворот на информацијата е мозокот чија порака органот за говор ја кодира, ја претвора во специјален вид сигнал, во зборови, кои преку каналот за врски – преку воздухот, се пренесува до соговорникот чиј орган за слух, заедно со одредени нерви, ги прима сигналите, ги декодира и пораката во првобитниот облик ја доставува до одредиштето, односно до мозокот на соговорникот (доколку станува збор за човек со човек, машина со човек) при преносот на пораката.[289] Според Клаус Кипендорф, преносот на информациите помеѓу машина со машина претставува „процес на пренос на структура помеѓу деловите на системот кои можат да се идентификуваат во времето и просторот".[290]

[288] Груевски Т. Комуникации и култура, Студентски збор, Скопје, 2004, стр. 31.

[289] Груевски Т. Комуникации и култура, Студентски збор, Скопје, 2004, стр. 31.

[290] Krippendorff K., Content Analysis: An Introduction to Its Methodology, Sage Publications, 2004, стр. 94-95.

Воопштено, моделот за информирање е составен од три делови: извор на информирањето (информатор), комуникациски (информирачки) канал/и и примач на информациите (информиран). 1) *Изворите на информирање* можат да бидат активни или пасивни. Активни извори за информирање се извори кои според својата природа служат за трансмисија, за дисеминација или за емитирање на информации. Ова се субјекти кои се активни и кои преку својата активност се трудат да го пренесат своето знаење (своите информации) на поширок круг луѓе. Пример за вакви извори се: научници, професори, политичари, новинари, борци за човекови права, проповедници и сл. Пасивните извори се извори кај кои информациите се добиваат преку опсервација, испитување, експериментирање, мерење, анализа и сл. Ова се историски и археолошки артефакти, временски прогнози, начини на однесување, лабораториски истражувања и сл. 2). *Каналите за информирање* ги поврзуваат изворите на информации и примачите на информации. Каналите за информирање (или комуникација) ги претставуваат начините на кои информацијата се пренесува од информирачот до информираниот. Трансферот на сигнали (информации) преку каналите за информирање го претставуваат процесот на информирање. Во однос на каналите за информирање, информирањето може да биде директно или индиректно. Во директното информирање, информацијата се пренесува директно од информирачот (изворот) до информираниот, односно преку персонален, непосреден контакт (лице в лице). Во индиректното информирање, информацијата се пренесува преку средства за посредна комуникација. Ваквата посредна комуникација може да се оствари на неколку различни начини (писмо, телефон, телефакс, компјутер и сл.). 3). *Примачи на информации* (јавноста, студентите, гласачите, донесувачите на одлуки) се оние кај кои информациите се пренесуваат. Информирањето како процес треба да предизвика проширување на знаењето или одредени промени во нивните ставови, однесувања и постапки. Примачите на информации можат да бидат едноставни или комплексни ентитети, да бидат индивидуални лица или организации, па дури и роботички уреди кои се контролираат нумерички или преку вештачка интелигенција.[291]

[291] Gackowski J. Zbigniew - *„Quality of Informing – Bias and Disinformation Philosophical Background and Roots"*, Issues in Informing Science and Information Technology, Vol.3, California, 2006, стр. 732 и Gackowski J. Zbigniew - *„Informing for operations – The first Principia"*, Issues in Informing Science and Information Technology, Vol.5, California, 2008, стр. 688.

Проучувањето на основните модели на информирање претставува темел за понатамошно разбирање на информациите од социолошки, математички и технички аспект.[292]

6. БЕЗБЕДНОСТ НА ИНФОРМАЦИИТЕ

Безбедноста на информациите подразбира заштита на информацијата од низа закани, со цел да се обезбеди континуитет на работењето, да се минимализира потенцијална штета, и да се максимизираат резултатите.[293] Значи, безбедноста на информациите е практика на заштита на информациите со ублажување на ризиците кои можат да ѝ наштетат на информацијата. Тоа е дел од управувањето со ризикот на информации. Обично вклучува спречување или барем намалување на веројатноста за неовластен и несоодветен пристап, употреба, откривање, нарушување, бришење, уништување, корупција, модификација, инспекција, евидентирање или девалвација, иако може да вклучува и намалување на негативните влијанија од инциденти. Примарниот фокус на безбедноста на информациите е урамнотежената заштита на доверливоста, на интегритетот и на достапноста на податоците.[294] Најчести закани за безбедноста на информациите се: самите вработени; ниската свесност за безбедносните аспекти на информациите; експанзија на користење компјутери и компјутерски мрежи; интернет и електронска пошта (e-mail); напади од хакери и од вируси; елементарни непогоди – пожар, поплава, земјотрес; и тероризам.[295]

Генерално, безбедноста на информациите е главен императив на информациската безбедност (Information Security), обезбедување информации или иформациска сигурност (Information Assurance) и сајбер-одбраната (Cyber Defence), или како и да ја наречеме оваа област која се занимава со сè поголемото нарушување на доверливоста, достапноста и интегритетот на информациите. Сите овие називи меѓусебно

[292] Golomb, Solomon W., Peile, Robert E., Scholtz, Robert A., Basic Concepts in Information Theory and Coding, Springer Publishing Company, 2010, стр. 62.

[293] Арсовски А., *Компаративна анализа и детален приказ на процесот на сертификација на информациски системи во државните институции на Република Македонија*, Универзитет Гоце Делчев, Штип 2017, стр. 26-27.

[294] Andress, J. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress, 2014, стр. 240.

[295] Национална стратегија за сајбер безбедност на Република Македонија 2018-2022, Верзија 1.2, Јули 2018.

се преклопуваат и делат еден заеднички предизвик, безбедност на информациите.[296]

Сите посочени термини имаат повеќе сличности отколку разлики во однос на начинот на перцепција на безбедноста на информациите и информациските системи. Но, сепак, постојат настојувања за нивно претставување како посебни дисциплини. Имено, информациската безбедност се претставува како подмножество на информациската сигурност. Исто така, информациската сигурност се претставува како подмножество на сајбер-одбраната, односно сајбер-безбедноста и обратно. Можноста од забуна произлегува од сличностите и фактот дека сајбер-безбедноста е релативно нова дисциплина.[297] Според тоа, се настојува да се прифати мислењето дека сајбер-одбраната го опфаќа само сајбер-просторот, или дека сајбер-одбраната, всушност, е информациската сигурност плус безбедноста на мрежите. Но, како и да е, зголемувањето на заканата од нападите врз безбедноста на информациите ги натера владите да ги земат предвид и ризиците од таквите напади на нивните комуникациско-информациски системи и другата критична инфраструктура. Исто така, се зголеми и вниманието во однос на вклучувањето на државите во информациското војување и можноста од колапс на комуникациската инфраструктура доколку таа не се брани.[298]

Криптографската заштита на комуникациско-информатичките системи во кои се процесираат класифицирани информации е дел од информатичката безбедност. Со примена на криптографски средства и методи се обезбедува сигурен и заштитен пренос на класифицирани информации помеѓу две точки преку неконтролиран простор. Со тоа значително се зголемува безбедноста на класифицираните информации, додека можноста за нивното компромитирање и нивна злоупотреба значително се намалува. При преносот на класифицираните информации по електронски пат надвор од контролираниот простор, задолжително се применуваат криптографски методи и средства, за зачувување на автентичноста, интегритетот и достапноста на класифицираната информација.[299]

---

[296] Kissel R. (ed.), *Glossary of Key Information Security Terms, 2011.*

[297] Withman E. M. Mattord J. H., *Principles of Information Security Fourth Edition, Course Technology, Cengage Learning, Boston, 2011.*

[298] Pindar J., Rigelsford J., *Cyber security and Information Assurance, The University of* Sheffield, 2011.

[299] Дирекција за безбедност на класифицирани информации, Информатичка безбедност на класифицирани информации, ИнфоЛист, достапно на: www.dbki.gov.mk

За постигнување соодветно ниво на безбедност потребно е да се создаде систем на информациска безбедност кој ќе обезбеди доверливост, интегритет и достапност на информацискатa инфраструктура, соодветно чување, обработка и пренос на податоците независно од нивната форма – електронска, печатена или некоја друга форма. Тоа ќе се постигне со прием на соодветни политики, едукација и тренинг на персоналот, зголемување на свесноста за ова прашање, како и примена на соодветни технологии.

Главните цели на безбедноста на информациите е да се заштити:

- ✓ Доверливоста: обезбедената информација да биде достапна единствено на оние кои се овластени за пристап и нема да бидат обелоденети на неовластени лица намерно или од небрежност.
- ✓ Интегритетот:сочувување на точноста и комплетноста на информацијата и на методите на процесирање. Информацискиот систем преку примена на соодветни мерки осигурува дека ќе се заштити од неовластени измени и дека содржи точни, целосни и веродостојни информации
- ✓ Достапноста: обезбедување овластените корисници да имаат пристап до информацијата кога е потребно.[300]

Во основа, ако кој било од трите принципи е повреден, тоа може да доведе до нарушување на безбедноста на системот, а тоа значи дека се случил безбедносен инцидент. Безбедносен инцидент значи секој успешен или неуспешен обид да се добие неовластен пристап, злоупотреба, објавување, модификација или уништување на информации и други средства на информациски системи, нарушување на нормалното функционирање на информацискиот систем или нарушување на кој било од принципите на информацискиот систем за безбедносна политика. Безбедносен инцидент е безбедносен настан кој резултира со штета, како што се изгубени податоци. Инциденти, исто така, може да вклучуваат настани кои не вклучуваат штета, но претставуваат остварливи ризици.[301]

Примери за безбедносни инциденти кои вработените треба да ги пријават се:

1. Загуба или недостаток на услуга, опрема, простории, ресурси или средства. Тука спаѓаат: пречки во телекомуникациите, исклучување од давателот на ИТ-услугите, недостаток/преки-

[300] Угриновска Н., *Безбедносни мерки за заштита на лични податоци*, Дирекција за заштита на личните податоци, Пропоинт, Скопје, 2018, стр. 46-47.

[301] Исто., стр. 46-50.

ни на електрична енергија, прекин во работата на критичната опрема за климатизација, инциденти/несреќи од природни катастрофи и инциденти од појава на пожари.

2. Системски пречки/преоптоварување, дефект на софтверот, хардверот или комуникациите како: продолжување на намалената ефикасност на апликациите, подолги прекини на софтверски решенија, попречена точност и комплетност на податоците на клиентите и трансакциите и грешки во обработката на податоците.
3. Човечки грешки, злоупотреби, отстранување и откривање на информации и ресурси. Тука спаѓаат: намерно грешење со опремата, неовластено откривање на доверливи информации (статус на сметка), откривање на лозинката, користење туѓа лозинка, откривање на лични податоци на клиентите на трети неовластени лица, грешки кои се резултат на нецелосни податоци, повреда на одредбите за физичка безбедност.
4. Неконтролирани системски промени и напади. Тука, пред сè се мисли на: хакерски напади, напади на вируси, напади на одбивање на услуга, малициозен програмски код, произволна инсталација на неодобрен софтвер или уред, неконтролирано менување на производството и конфигурацијата, несоодветно однесување на системот – индикација за напад.
5. Неовластен пристап до ресурси и информации. Тука се опфатени: неовластен пристап до компјутерска мрежа/апликација и неовластен пристап до функции во апликациите за кои работникот не е овластен.
6. Други нарушувања на безбедноста на информативниот систем вклучуваат странки или можна причина за инцидент, како: вработени, надворешни странки (консултанти, стажанти, студенти...) и даватели на услуги.[302]

[302] Исто., стр. 46-50.

7. ЕФЕКТИВНО СПОДЕЛУВАЊЕ НА ИНФОРМАЦИИ ЗА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Ефективноста на заштитата на критичната инфраструктура многу зависи од квалитетот и брзината на размена на разузнавачките информации и од информации кои се од значење, а се сензитивни. При поставувањето на оперативните рамки за размена на информации, стратегиите за заштита на критичната инфраструктура и сродните планови за имплементација треба да изнајдат законска основа во која ќе бидат опфатени три основни прашања:[303] „Кои информации треба да се разменуваат и зошто"?; „Како ќе се споделуваат информациите за која било задача"?; и „Меѓу кого информациите ќе бидат споделени"?.[304]

Информациите можат да се разменуваат на стратегиско, на техничко или на тактичко ниво. Од друга перспектива, информациите може да се поврзани со инциденти или да се дадени во општ контекст. Тоа исто така може да биде во форма на „реално време" што подразбира размена на информации во контекст на непосредна или тековна криза кога примателот се очекува да преземе итни мерки. Секогаш кога станува збор за овој последен вид информации, платформите за размена на информации (и приложените безбедносни карактеристики) ќе бидат структурирани многу поинаку отколку кога треба да се пренесат најдобрите практики или стратегиски совети.

Искуството покажува дека ефективноста на размената на информации за заштита на критичната инфраструктура зависи од два основни фактори, и тоа:

1) способност на водечките агенции да создадат доверба меѓу инволвираните чинители; и
2) обезбедување соодветно ниво на заштита за чувствителни информации чие споделување е поттикнато или овластено според аранжманите/договорите за заштита на критична инфраструктура.[305]

Важно е креаторите на стратегии за заштита на критична инфраструктура (и оние што се повикани да ги спроведат) да разберат како

[303] Попоска В., *Меѓународно-правни аспекти за заштита на критичната инфраструктура од современи безбедносни закани*, Универзитет „Гоце Делчев", Штип, 2019.

[304] INTERPOL. *The protection of critical infrastructures against terrorist attacks: Compendium of good practices, United Nations Office of Counter-Terrorism*, UN Counter Terrorism Centre, 2018.

[305] Исто., *The protection of critical infrastructures against terrorist attacks: Compendium of good practices.*

овие два фактори влијаат едни на други. Сепак, нивото на доверба ќе се намали ако информациите не се правилно заштитени, строгите нивоа на заштита на информации нема да создадат висок степен на доверба помеѓу учесниците. Создавањето вистинска доверба кај учесниците кон одреден аранжман за споделување информации може да биде временски напор и да бара активна посветеност од сите засегнати страни. Сепак, штом ќе се појави/заснова довербата, протокот на информации треба значително да добие и во квалитативна и во квантитативна смисла на зборот. Создавањето на средина на доверба за размена на информации зависи од поставувањето на јасни правни и оперативни рамки за заштита на чувствителната природа на споделените податоци. При дизајнирањето на такви рамки, сеопфатната цел е да се олесни циркулирањето на информациите. Заштитата на критичната инфраструктура секогаш треба да ја земе предвид потребата да се почитуваат применливите инструменти кои се занимаваат со правото на приватност и заштита на личните податоци.[306]

Секогаш не е неопходно да се споделат информации што се премногу специфични, на пример знаење за критични предмети/објекти и нивната локација или специфичните информации за ранливости или инциденти. За воспоставување доверба, треба да има континуитет кај лицата кои присуствуваат на состаноците за размена на информации. Учесниците треба да бидат назначени на лично ниво со доволно мандат и одговорност во сопствената околина. Генерално, не се дозволени замени. Состаноците за споделување информации се фокусираат на размената на информации: сите вклучени организации треба (во принцип) да дадат, односно да споделат информации. Давателот на услуги на информации ќе осигури дека дадените информации се со вистинско ниво на содржина и позадина. Засновано врз основа на информациите, примателите на информациите треба да можат да преземат соодветни активности во нивните организации или да бидат предупредени за новата закана. Давателот на информации останува сопственик на споделените информации и неговата сензитивна класификација. Ако не постои ниво на доверба, тогаш е многу тешко да се создаде високо ниво на доверба во електронското опкружување.[307]

Оперативно, голем број методи и решенија се достапни за да се заштити циркулацијата на чувствителните информации. Обично, овие методи и апликации се фокусирани на: процедури за безбедност и про-

[306] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[307] RECIPE, (2011), *Good Practices Manual for CIP Policies for Policy Makers in Europe*, достапно на: file:///Users/SM/Downloads/RECIPE_manual%20(1).pdf

верка; кодирање во боја системи; електронски алатки.[308] Сите три методи и решенија често се надополнуваат едни со други. Така, владите можат да обезбедат безбедносни проверки и дозволи за клучните засегнати страни кои имаат потреба од пристап до чувствителни информации за критичната инфраструктура. Според Директивата на Советот на Европската Унија „секоја личност која ракува со класифицирани информации потребно е да поседува соодветен степен на безбедносна проверка".[309] Платформите за споделување на информациите, исто така, можат да усвојат специфични критериуми за избор и за прием на нови кандидати, засновани на пример врз потребата постојните вработени да се согласат или во форма на скрининг на нивното минато, интервјуа со јавните органи надлежни за платформата за споделување информации, итн.[310]

8. КУЛТУРА ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИИТЕ

За разлика од традиционалните теории на безбедност кои не ја вклучуваат културната компонента во нивните анализи, современите интерпретации и гледишта на безбедноста и националната безбедност даваат посебен примат на културата и не се двоумат да ја направат дел од нивната анализа.

Културата и нејзината нормативна функција помагаат да се воспостават и развијат норми и правила кои се користат да насочат корисно и намерно однесување спречувајќи штетна и општествено неприфатлива акција. Културата креира различни средства на заштита и нејзината безбедносна и заштитна функција обично се заснова на антиципаторски и планирани активности кои имаат за цел навремено одредување кои средства мора да се користат и до кој степен.[311] Со цел да се дефинира културата за безбедност на информации, неизбежно е да се каже дека таа е составен дел од организациската култура во целост. Едноставно кажано, организациската култура определува како еден вработен ја гледа организацијата. Таа е карактеристика на организациите кои со текот на времето се менуваат и растат. Секако, раководството може да ја проекти-

[308] INTERPOL., *The protection of critical infrastructures against terrorist attacks: Compendium of good practices, United Nations Office of Counter-Terrorism*, UN Counter Terrorism Centre, 2018.

[309] EU Council Directive 2008/114/EC, Article 9.

[310] Stikvoort, Don (2009). ISTLP - Information Sharing Traffic Light Protocol.

[311] Станаревиќ С. Гачиќ Ј., Културата како на национален безбедбносен интерес, *Современа македонска одбрана*, бр. 26, Министерство за одбрана, Р. Македонија, 2014.

ра и да влијае врз организациската култура. Всушност, организациската култура претставува едно од главните средства за раководење. Двете клучни состојки на организациската култура се основните претпоставки и верувања. Организациската култура се состои од колективни вредности, правила и познавање на организацииите.[312]

Според „Поимникот за безбедносна култура", „под безбедносна култура може да се подразбира безбедносна активност што изразува подготвеност кон акции и однесувања во согласност со стекнатите знаења и вештини, како и во согласност со прифатени вредности". Исто така, безбедносната култура „се согледува во идентификување на опасностите, одговарање на нив со избегнување на опасност, со елиминирање на опасноста или упатување на оние субјекти кои професионално ќе ги зачуваат загрозените вредности".[313]

Роер во публикацијата „Формирање на безбедносна култура" истакнува дека безбедносната култура им помага и олеснува на корисниците да ја користат информациската технологија без опасности и закани.[314]

За Стајиќ, Мијалковиќ и Станаревиќ, безбедносната култура е збир на усвоени ставови, знаења, вештини и правила од областа на безбедноста, изразени како однесување и процес, за потребата, начини и средства за заштита на личните, општествените и меѓународните вредности од сите извори, форми и носители на закана, без разлика на местото или времето на нивната манифестација.[315]

Според нашиот пристап, безбедносната култура е динамична категорија која е условена од бројни безбедносно-културолошки фактори што влијаат на стабилноста на секое општество. Во согласност со промените кои се случуваат во самото општество и безбедносната култура се менува затоа што безбедносната култура е во тесна корелација со развојот на општеството. Исто така, безбедносната култура влијае на политичкото однесување во еден систем и карактеристично за неа е тоа што таа не се пропишува со одредени прописи од страна на државата или институциите.

Значи, согледувањето на проблемот на безбедносната култура единствено е можно само преку детално познавање на сложените, ис-

[312] Ulich, E. (2001). Arbeitspsychologie, vdf Hochschulverlag an der ETH Zürich.

[313] Stanarević S., Ejdus F., *Pojmovnik bezbednosne kultur*e, Centar za civilno-vojne odnose, Beograd, 2009, достапно на: *http://www.wbrc.rs/wp-content/uploads/2012/11/Pojmovnikbezbednosne-kulture-grupa-autora-2009.pdf*.

[314] Roer K., *Build a Security Culture*, IT Governance Publishing, United Kingdom, 2015.

[315] Stajić Lj., Mijalković S. Stanarević S., *Bezbednosna kultura mladih: kako živeti bezbedno*, Draganić, Beograd, 2006.

преплетени внатрешни односи, како и преку разгледување на клучните елементи кои ја имаат централната улога во креирањето на безбедносната култура, почнувајќи од средината, достигнатото ниво на образование, нивото на свеста, динамичноста и сложеноста на причинско-последичните односи во сферата на безбедноста, општествениот развој, повеќеструктурните форми на комуникација итн.

Во основа, безбедносната култура може да се разгледува на повеќе нивоа низ призмата на глобалното општество или како дел од општата култура на национално ниво, но и како култура на поединецот. Безбедносната култура на глобално ниво ги вклучува преференциите кои се однесуваат на последиците како резултат на односите во меѓународната заедница, дипломатијата, политиката итн. Безбедносната култура на ниво на национална држава и покрај амбивалентните погледи нè доведува до важни заклучоци кои укажуваат на развој и стабилност на државата, па оттука таа мора да биде добро изградена и добро прифатена од секој член на заедницата при што се остварува пред сè проактивна улога со цел зачувување на вредностите на едно општество.

Според презентираните објаснувања и дефиниции, постојат три главни елементи кои заедно формираат безбедносна култура: технологија, политика (правила) и нивни корисници. Овие три елементи комуницираат едни со други и секој директно влијае на другите два. За воспоставување елементи на безбедносната култура во организациите, неопходно е да се спроведат и имплементираат пет клучни компоненти на безбедносната култура (Слика број 5).

Слика број 5: Пет клучни елементи на безбедносна култура

Извор: Zoran Milanović, Radovan Radovanović. (2015), Informaciono-bezbednosna kultura-imperativ savremenog drustva, *Nauka, bezbednost, policija*, Vol. 20, iss.3, Kriminalisticko-policijska akademija, Beograd

Во продолжение ќе бидат елаборирани петте клучни елементи на безбедносната култура и тоа:

1) Информативна култура – организацијата собира и анализира релевантни податоци и активно дистрибуира безбедносни информации и совети засновани на таа анализа.

2) Култура на доверба – подразбира признавање на природните ограничувања на човековите перформанси. Културата на доверба укажува на тоа дека грешките и небезбедните активности на корисникот нема да бидат казнети доколку биле ненамерни. Сепак, оние што постапуваат несовесно или неоправдано преземаат одредени ризици, ќе бидат дисциплиниско казнети.

3) Култура за пријавување, т.е. култура за известување, претставува создавање атмосфера во која луѓето имаат доверба да известуваат за безбедносни проблеми без страв од вина, па дури и се охрабрени и наградени за обезбедување на информации поврзани со безбедноста. Вработените треба да знаат дека ќе се постигне култура на доверба и ќе се постапува по доставената информација, во спротивно тие ќе решат дека нема корист од нивното пријавување.

4) Културата за учење потврдува дека организацијата е во состојба да учи од своите грешки и е подготвена да направи промени. Целта на културата за учење е луѓето да ги разберат процесите на системите за управување со безбедноста преку личен пример.

5) Флексибилната култура е онаа во која организацијата и луѓето се способни ефикасно да се прилагодат на променливите барања.[316]

Во основа, културата за безбедност на информациите не е ништо друго туку субкултура во организациската култура. Затоа, таа е клучен фактор во воспоставувањето на безбедност на информации. Културата за безбедност на информациите се однесува на знаењето, претпоставките и верувањата на вработените за безбедноста на податоците. Организациите кои имаат добро развиена и применета безбедносна култура може да ги претворат вработените во безбедносна вредност наместо закана.[317] Сепак, дури и со таква култура во практиката постојат некои компромиси кои мора да се направат и судир на интереси кои треба да

[316] Milanović Z., Radovanović R., Informaciono-bezbednosna kultura-imperativ savremenog drustva, *Nauka, bezbednost, policija*, Vol. 20, iss.3, Kriminalisticko-policijska akademija, Beograd, 2015.

[317] Solms Von B., 'Information security – the third way?', Computers and Security, vol. 19, no. 7, 2000, стр. 615-620, Nicholson, A, Webber, S, Dyer, S, Patel, T & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare, Computers and Security, vol. 31. no. 4, стр. 418-436, и Siponen, MT. (2001). 'Five dimensions of computer security awareness', Computers and Society, vol. 31, no. 32, стр. 24-29.

се разрешат. Имајќи предвид дека вработените се една од најголемите закани за безбедноста на податоците, културата за безбедност на информациите мора да ги информира и образува за чувањето на сигурноста и тајноста на податоците.[318]

Безбедносната култура на корисниците на информатичка технологија се рефлектира, директно или индиректно, врз нивната целокупна безбедност и заштита од ризиците на кои се изложени. Создавањето на култура на информации и безбедност на информации во рамките на организацијата е преку имплементирање на информативен и безбедносниот аспект на секој вработен како рутина во секојдневната работа.[319]

8.1. Компоненти на културата за безбедност на информации

Информациската безбедносна култура претставува императив на современото општество. Ефективната информациска култура во организациите зависи од три компоненти: луѓето, процесите и технологиите.[320] Културата за безбедност на информации е еден од клучните поставки за општото информациско безбедносно ниво на една организација. Техничките мерки, чувањето од неовластените лица, се бескорисни ако заканата за безбедноста на информациите потекнува од внатрешноста на организацијата.[321] Луѓето го посочуваат човечкиот фактор, додека може да има позитивно или негативно влијание врз раководењето со безбедноста на информациите, т.е. тој е „движечка сила“ или „силата за запирање“.[322] Со цел да се добие позитивно влијание од овие фактори, неопходно е да се воспостави позитивна култура за безбедност на информации. Безбедноста на информациите е повеќе од едноставно

[318] Mitnick, K & Simon, WL., The art of deception: controlling the human element of security, Indianapolis: Wiley Publishing, 2002.

[319] Solms Von B., 'Information security – the third way?', Computers and Security, vol. 19, no. 7, 2000, стр. 615-620

[320] Aliti, A & Akkaya, D., Employees' Role in Improving Information Systems Security, Master's Thesis, Linnaeus University, School of Computer Science, Physics and Mathematics, Växjö, Sweden, 2015, http://lnu.diva-portal.org/smash/get/diva2:434613/FULLTEXT01.pdf.

[321] Alex Fagerström, *Creating, Maintaining and Managing an Information Security Culture, Information and Media Technology*, ARCADA 2013.

[322] Fahey P., 'Human Factors in Information Security Management Systems', Infosec Institute, 2013, достапно на: http://resources.infosecinstitute.com/human-factors-informationsecurity-management-systems.

аплицирање на физичка и техничка контрола.[323] Покрај овој факт, голем број организации сè уште се фокусираат едноставно на техничките аспекти на информациската безбедност, занемарувајќи ја едукацијата на вработените и информациската безбедносна култура.[324] Сепак, многу е важно да се разбере културата на организацијата и практиката која влијае врз постапките на вработените со цел да се изгради култура на безбедност на информации.[325]

Мартинс и Елоф наведуваат дека културата за безбедност на информации се однесува на претпоставките за прифатливо однесување во однос на безбедноста на информациите,[326] додека Закариа и Гани тврдат дека културата за безбедност на информации може да дејствува како „човечки заштитен ѕид“ за да се заштитаат информациските средства на организацијата.

Безбедноста на информациите може да се перципира како натпреварувачка предност, ако е соодветно имплементирана и одржувана,[327] односно потребно е да се набљудува холистички и сите вработени треба да се свесни за можните закани за безбедноста на организацијата, особено за внатрешните безбедносни инциденти. За да се надминат овие закани, организацијата треба да ја поттикнува колективната одговорност меѓу сите вработени, а не само на техничкиот персонал за спроведување на безбедносните активности. Културата за безбедност на информациите, исто така, ќе го обликува однесувањето на вработените кон безбедносните проблеми.

Истакнувањето на нетехничките аспекти може да помогне во негувањето на безбедноста на информациите како клучен дел на секојдневната рутина на секој вработен во организацијата. Меѓутоа, безбедносната култура ќе се развие и ќе успее само ако има вклучување на сите нивоа на вработени.

---

[323] Thomson K.L., Solms R., Louw L., *Cultivating an organizational information security culture.* Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa, 2006.

[324] Fagerström A., *Creating, Maintaining and Managing an Information Security Culture, Information and Media Technology*, ARCADA, 2013.

[325] Leach J., 'Improving user security behaviour', Computers & Security, vol. 22, no. 8, 2003.

[326] Martins A & Eloff J., 'Information Security Culture', MA Ghonaimy (ed.), Security in the Information Society: Vision & Perspectives, Kluwer Academic, 2002.

[327] Kosunen P., Yrityksen henkilöstö – merkittävä tietoturvauhka. Bsc. Thesis (in Finnish). Information Technology, Haaga-Helia University of Applied Sciences, Helsinki, 2013, преземено од Fahey R., 'Human Factors in Information Security Management Systems', Infosec Institute, 2013, достапно на: http://resources.infosecinstitute.com/human-factors-informationsecurity-management-systems.

Во основа, елементите на културата за безбедност на информации може да се гледаат како елементи на организациската култура, а таа опфаќа: артефакти, постигнати вредности, споделени претпоставки и знаење, и истите можат да се претстават на следните нивоа:

- Ниво 1: Артефакти претставуваат работи кои можат да се видат, слушнат или почувствуваат во организацијата.[328] Тие вклучуваат процеси и организациската структура. Артефактите се всушност она што се случува во организацијата.[329]
- Ниво 2: Официјалните гледишта, стратегиските документи, мисијата и визијата на организацијата претставуваат усвоени вредности. Усвоените вредности се вредностите според кои организацијата сака да се води.[330]
- Ниво 3: Споделените претпоставки се однесуваат на начинот на постигнување успех. Тие се имплицитни, споделени од вработените и истите се формираат со години на организациско искуство.
- Ниво 4: Знаење. Вработените е неопходно да имаат задолжително знаење да ги реализираат на безбеден начин нивните секојдневни задачи.[331]

Слика број 6: Нивоа за култура на безбедност на информации

Извор: Van Niekerk, JF & Von Solms, R. (2010). 'Information security culture: A management perspective', *Computers and Security*, vol. 29, no. 4.

[328] Schein, EH. *The corporate culture survival guide*. Jossey-Bass Inc, 1999.

[329] Niekerk Van, JF & Solms Von, R., 'Information security culture: A management perspective', *Computers and Security*, vol. 29, no. 4, 2010, стр. 45-145.

[330] Исто., стр. 45-145.

[331] Fagerström A., *Creating, Maintaining and Managing an Information Security Culture, Information and Media Technology*, ARCADA, 2013.

Сите овие елементи се заеднички за организациската култура воопшто, како и за субкултурите. Ова, исто така е случај и со културата за безбедноста на информациите. Сепак, кај културата за безбедноста на информациите, знаењето ги поддржува сите три нивоа на организациската култура, односно без соодветно знаење, не може да се обезбеди безбедноста на информациите, така што предлагаат знаењето да биде четвртиот елемент на културата за безбедност на информации.

Постојат бројни активности кои раководството треба да ги извршува ако очекува соодветна култура во организацијата. Комуникацијата меѓу вработените и раководството треба да биде јасна, концизна и достапна. Освен тоа, секој поединец мора да ги знае каналите за комуникација. Вработените треба да се поттикнуваат да учат за безбедната и сигурна употреба на податоците.[332] Раководството треба да воспостави програми за подигнување на свеста, а сите вработени кои работат со класифицирани податоци треба посебно да се образуваат за употребата на податоците.[333]

[332] Радојевиќ К. Љуштина А., Улогата на безбедносната култура во заштитата на СНПП-мрежите, *Современа македонска одбрана*, Министерство за одбрана, Р. Македонија, 2015.

[333] Schlienger T. Teufel S., Information security culture – from analysis to change. *South African Computer Journal*, 2003.

глава V

САЈБЕР-БЕЗБЕДНОСТА И КРИТИЧНАТА ИНФРАСТРУКТУРА

1. САЈБЕР-БЕЗБЕДНОСТ

Сајбер-безбедноста сè повеќе претставува еден од врвните приоритети во организациите, особено на оние во критичниот национален инфраструктурен сектор.[334]

Терминот сајбер-безбедност својата основа ја влече од терминиот сајбер-простор. Наједноставно кажано, тоа е безбедност во сајбер-просторот. Сепак, терминот има малку подлабока историја. Етимолошки, основата на зборот е од старогрчкиот термин „кибернетик“ (κυβερνᾶν) што се користел за да го определи терминот управител во смисла на владение (политичко управување – владеење со луѓето). Современото значење на терминот се применува подоцна и првпат е искористено во книгата на математичарот Норберт Винер насловена како „Кибернетика: или контрола и комуникација помеѓу животните и машините“.[335]

Термините како сајбер-криминал, сајбер-шпионажа, сајбер-тероризам, сајбер-војување и сл, се термини што повеќе или помалку ја формираат контурата на она што го предизвикува организирањето на терминот сајбер-безбедност во современа општествена смисла. Денес, за овој термин има различни видувања. Некои академски и експертски организации се на став дека терминот сајбер-безбедност е општ и поширок, и опфаќа сет мерки, постапки и активности што се однесуваат на дигиталниот свет креиран од интернетот. Од друга страна, често овој поим се поистоветува со поимот на информациска безбедност. Тоа е и разбирливо, ако се знае дека во основата на сајбер-светот е информацијата. Сепак, кога се зборува за безбедноста на информацискатa технологија (доаѓа од „IT Security“) се мисли на заштита на сите информации (независно дали се во тврда или дигитална – електронска форма).[336]

---

[334] Walker-Roberts S, Hammoudeh M, Dehghantanha A., A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access 1–1*, 2018.

[335] Wiener N., *Cybernetics: or Control and Communication in the Animal and the Machine*, MIT Press, USA, 1965.

[336] Hadzi-Janev M. Bogdanoski M., *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*“, IGI Global, 2016, достапно на: https://www.igi-global.com/book/handbook-research-civil-society-national/129591

Фокусот и интересот кон сајбер-безбедноста во последните неколку години драстично се зголеми како резултат на негативните ефекти по безбедноста (почнувајќи од индивидуалната безбедност преку безбедноста на бизнис-заедницата, па сè до националната безбедност).

Така, основната поделба вклучува:

- закани од сајбер-криминалот (индивидуални, групни – организирани, од терористички побуди – за терористички цели, корпоративни цели, (САД, Австралија, Велика Британија, Германија и некои други држави сметаат дека сајбер-криминалот е закана за националната безбедност);
- закани од сајбер-шпионажа (која може да биде од економски побуди-натпревар помеѓу корпорации во економски контекст и за воени цели – закана за националната безбедност);
- закани од користењето на сајбер-просторот од страна на терористите и потенцијална расправа за сајбер-тероризам; и
- закана од т.н. сајбер-конфликт како најекстремна форма на закана од сајбер-просторот.[337]

Во основа, сајбер-безбедноста значи обезбедување на безбедноста на сајбер-просторот од закани кои можат да имаат различни форми, од злонамерен софтвер, преку „спамови“, „фишинг“, па сè до софистицирани вируси кои можат да го „исфрлат од функција“ целиот општествен систем. Крадењето тајни информации од националните компании и владините институции, напаѓање на инфраструктурата од витално значење за функционирањето на една нација или напад на приватноста на еден државјанин, се екстремни примери на широкиот спектар на закани во сајбер-просторот, каде што почнувајќи од владите, преку компаниите, па сè до обичните граѓани, никој не е сигурен.

Покрај ова, сторителите на напади на сајбер-просторот се професионалци кои сега работат за владите, хактивистички организации или високоорганизирани криминални банди, а сè помалку се тинејџери во потрага за краткотрајна слава како што беше порано. Компаниите и владите склучуваат договори, унапредувајќи го државно-приватното партнерство за да го направат сајбер-просторот побезбедно и посигурно место. Но, тоа е само едната страна од медалот. Од друга страна, компаниите блиски до владите, како што се веб-пребарувачите и социјалните мрежи, прибираат јавни податоци од интернет-просторот за граѓаните, а потоа им ги продаваат на компаниите за комерцијални и маркетинг-цели

[337] Исто, https://www.igi-global.com/book/handbook-research-civil-society-national/129591

или им ги стават во раце на разузнавачките агенции за доминација на државите во сајбер-просторот.[338]

Напредната перзистентна закана (АПТ)[339] е најпредизвикувачката закана, ако не и една од најпредизвикувачките закани за безбедноста општо и за безбедноста на критичните национални инфраструктури.[340] АПТ нападите станаа тешки за решавање затоа што за разлика од другите сајбер-напади кои зависат од автоматско скенирање и искористување на познатите ранливости, АПТ се софистицирани и во многу случаи човечки насочувани напади, со специфични цели.[341]

Она што го прави АПТ уште покомплицирано е фактот дека тие често се под радарот, насочени и многу фокусирани сајбер-напади и кога поединец или група добиваат неовластен пристап до IoT (интернет на нештата) мрежа тие можат да останат неоткриени подолг временски период.[342] АПТ групите се состојат од експерти кои вршат разузнавачки информации со отворени извори и методи за социјално инженерство да ги компромитираат владините и трговските субјекти на систематски начин.[343] За да бидат неоткриени АПТ групите ги искористуваат ранливостите што вообичаено не се познати пред јавноста, и тие користат шифрирана комуникација, злоупотреби на стандардни протоколи, и пронајдени слабости во текот на денот.[344]

АПТ групите претставуваат огромен ризик за многу инфраструктури на одредени организации заради природата на нивните напади.[345] АПТ

[338] Славески С., *Сајбер-безбедност*, Министерство за одбрана на Р.С. Македонија, 2015.

[339] Advanced Persistent Threat (APT)

[340] Haddad Pajouh H, Dehghantanha A, Khayami R, Choo KKR., A deep recurrent neural network based approach for internet of things Malware threat hunting, future generation computer system. *Futur Gener Comput Syst* 85, 2017, стр. 88–96.

[341] Ussath M, Jaeger D, Cheng F, Meinel C., *Advanced persistent threats: behind the scenes.In: 2016 Annual Conference on Information Science and Systems* (CISS), 2016.

[342] Azmoodeh A, Dehghantanha A, Choo K-KR., Robust malware detection for internet of (Battlefield) things devices using deep Eigenspace learning. *IEEE Trans Sustain Comput* 1–1, 2018.

[343] Min M, Xiao L, Xie C, Hajimirsadeghi M, Mandayam NB (2017), Defense against advanced persistent threats: a Colonel Blotto game approach. In: 2017 IEEE international conference on communications (ICC)

[344] Hopkins M, Dehghantanha A., Exploit kits: the production line of the cybercrime economy? In: 2015 second international conference on Information Security and Cyber Forensics (InfoSec), 2015.

[345] Conti M, Dehghantanha A, Franke K, Watson S., Internet of things security and forensics: challenges and opportunities. *Futur Gener Comput Syst*, 2017.

групите имаат тенденција да го прилагодат својот Malware за да нападнат одредена цел. Овие малициозни софтвери не се обични и не можат да се откријат со употреба на традиционални безбедносни механизми,[346] односно бараат употреба на напредни техники како што се „длабоко учење", машинско учење и анализа на шема. Сите овие носат големи компликации во однос на тоа каква заштита една организација може да искористи за да се брани од напади на АПТ, бидејќи различни групи на АПТ користат различни тактики, техники и процедури.[347]

Во продолжение ќе се анализираат три специфични групи на АПТ, главно насочени кон таргетирање на критичната национална инфраструктура на западните земји. Имено, станува збор за: АПТ28 (APT28), Регин (Regin) и Црвен октомври (Red October).

АПТ28 (APT28) претставува руска група која е позната и по многу други имиња[348] која се фокусира на собирање на разузнавачки информации за руската влада.[349] Од 2007 година, движењето АПТ28 се насочува кон напади на националната критична инфраструктура во САД, Европа и земјите од поранешниот Советски Сојуз, вклучувајќи ги владите и војската, безбедносните организации, медиумите и дисиденти и субјекти кои со во судир со сегашната руска влада.

АПТ28 краде внатрешни податоци откако ќе ја загрози жртвата и понекогаш ги објавува тие информации.[350] До сега, оваа група е вклучена во Сирискиот конфликт, односите помеѓу НАТО и Украина, бегалската и мигрантската криза во Европската Унија, Олимпијадата од 2016 година, јавните обвинувања во врска со руското државно спонзорирање на хакерството и претседателските избори во САД во 2016 година.

АПТ28 применува четири главни тактики за компромитирање на планираните цели. Овие вклучуваат испраќање фишиниг е-маил пораки и доставуваат документ што распоредува малициозен софтвер врз системите на корисникот или содржи злонамерна URL наменета да ги преземе ингеренциите за е-пошта на примачите и да обезбеди пристап

[346] Haughey H, Epiphaniou G, Al-Khateeb H, Dehghantanha A, *Adaptive traffic fingerprinting for darknet threat intelligence,* vol 70, 2018.

[347] Conti M, Dargahi T, Dehghantanha A., *Cyber threat intelligence: challenges and opportunities*. Springer, Cham, 2018.

[348] Fancy Bear, Strontium, Pawn Storm, Sofacy, Sednit, Tsar Team. Lemay A, Calvet J, Menet F, Fernandez JM, Survey of publicly available reports on advanced persistent threat actors. Comput Secur 72: 2018, стр. 26–59.

[349] FireEye (2014) FireEye releases report on Cyber Espionage Group with possible ties to Russian Government.

[350] FireEye, APT28: a window into Russia's cyber espionage operations?, 2014.

до нивните сметки. АПТ28, исто така, компромитираше и позицонираше малициозен софтвер на легитимни веб-страници со цел да ги направи заразни посетителите на одредени страници и се здоби со пристап до организации преку компромитирање на нивните мрежни сервери.[351]

Регин (Regin) е групата АПТ што користеше уникатен малициозен софтвер наречен Regin. Групата создаде исклучително комплексен малвер што може да се модифицира со широк опсег на разни способности што можат да бидат распоредени во зависност од целта.[352] Може да издржат долгорочни процеси за собирање разузнавачки информации без да бидат откриени. Може да се скрие себеси и неговите активности на компромитирани компјутери.

Клучна цел на Регин е собирање разузнавачки информации и поддршка на други видови напади. Групата е користена за собирање податоци од владини организации, финансиски институции, инфраструктурни оператори, деловни активности, академици и приватни поединци.[353]

Прецизната техника што се користи за примарното компромитирање е сè уште мистерија, иако постојат бројни теории, како што е употреба на човечки напади во средина со експлоатирања на прелистувачи browser zero-day.[354] Во бројни инциденти, заразените машини биле исто така контролори на домен на Windows. Насочување на администратори на системот преку експлоатирања врз основа на веб е лесен начин за постигнување на инстант административен пристап до целата мрежа.[355]

Црвен октомври (Red October) е исто така руска група. Тие главно се насочени кон амбасадите и дипломатските претставништа, универзитети и истражувачки фирми, бизнис-компании, нуклеарни неенергетски лаборатории, нафтени и гасни компании, воздушни институции, воени служби во различни земји, главно поврзани со регионот на Источна Европа, поранешни членки на СССР, и земји во Централна Азија.[356]

---

[351] Dimitris Gritzalis, Marianthi Theocharidou, George Stergiopoulos (ed.), *Critical Infrastructure Security and Resilience Theories, Methods, Tools and Technologies*, Springer Nature Switzerland AG., 2019.

[352] Symantec, Regin: top-tier espionage tool enables stealthy surveillance symantec security response 2015.

[353] Kaspersky Lab., The regin platform nation-state ownage of GSM networks, 2014.

[354] Symantec, Regin: top-tier espionage tool enables stealthy surveillance symantec security response, 2015.

[355] Kaspersky Lab., The regin platform nation-state ownage of GSM networks, 2014.

[356] Chavez R, Kranich W, Casella A., Red October and its reincarnation. Bost. Univ. | CS558 Netw. Secur, 2015.

Оваа група има за цел да краде класифицирани информации, да се здобие со геополитички информации, како и продажба на класифицирани информации на црниот пазар.[357] Тие користат spear phishing за да создадат почетна инфекција и да се насочат кон одредена цел или организација заснована на познати информации. Тие ги користат познатите слабости на различни апликации како што се Microsoft Office, PDF и Java.[358] Малициозен софтвер се користи да ја зарази жртвата-машина откако злонамерна датотека ќе се отвори, потоа се инсталира основна компонента и комуникација со команда и серверот за контрола (C&C) и се воспоставува преку модул backdoor по кој шифрирана комуникација е воспоставена помеѓу машината-жртва и серверот C&C. Повеќе од 60 различни домени се кодирани со код на малициозен софтвер, за да комуницираат со C&C сервери. Злонамерниот софтвер содржи компоненти што инфицираат машини на истата локална мрежа без првичен напад на фишинг.[359]

Компјутерската и комуникациска безбедност се есенцијален дел од информатичката безбедност во заштита на комуникациско-информатички сиситеми во кои се процесираат класифицирани информации. Со примена на безбедносни мерки од сајбер и комуникациската безбедност се постигнуваат следните ефекти:

- ✓ идентификација на лицата кои пристапуваат во системот;
- ✓ контрола и евиденција на пристап до објектите на системот врз основа на дадено право за пристап од дефинирана база на податоци;
- ✓ обезбедување на сигурен начин за означување на степенот на класификација;
- ✓ идентификација и сигурна евиденција на корисникот за отпечатениот, пресниментиот, модифицираниот, копираниот или избришаниот класифициран документ;
- ✓ заштита на важните технички и програмски елементи, системски можности и функционалност на системот;
- ✓ контрола и менаџмент на ракувањето и преносот на преносни мемориски медиуми на кои се запишуваат класифицирани информации;

[357] Kaspersky Lab, Red October: an advanced cyber-espionage campaign targeting diplomatic and government institutions, 2013.

[358] Chavez R, Kranich W, Casella A, Red October and its reincarnation. *Bost. Univ. | CS558 Netw. Secu,* 2015.

[359] Kaspersky Lab, Red October: an advanced cyber-espionage campaign targeting diplomatic and government institutions, 2013.

- ✓ планирање, конфигурирање, управување и контрола на мрежни уреди.[360]

Во основа, кога станува збор за изнаоѓање ефикасни мерки за заштита, треба да постои јасна стратегија на сајбер-безбедноста. Затоа, сајбер- безбедноста се темели на јасна стратегија. Општо земено, стратегијата за сајбер-безбедноста е насочена кон остварување на неколку цели како: сајбер- отпорност, сајбер-капацитети и култура за сајбер-безбедност, справување со сајбер-криминал, сајбер-одбрана и соработка и размена на информации.

Во продолжение ќе бидат претставени неколкуте важни цели, и тоа:

1. *Сајбер отпорноста* обезбедува доверливост, интегритет и достапност преку идентификација, заштита и воспоставување на претходна состојба од сајбер-инциденти. Јавниот и приватниот сектор мора да имаат навремени и точни информации и предлози за подобрување на сајбер-безбедноста и да бидат во можност меѓусебно да соработуваат во случај на сајбер-инциденти.
2. *Сајбер-капацитети и култура за сајбер-безбедност* е цел која е насочена кон промовирање на свесноста за сајбер-закани и се фокусира на градење капацитети за сајбер-безбедност помеѓу засегнатите страни со активности во оваа област. Промовирањето на култура за сајбер-безбедност значи поттикнување на одговорност и разбирање за сајбер-ризиците во сите сфери на општеството, преку развивање на информирана доверба на корисниците во електронските сервиси, како и подобрување на знаењето како тие притоа да ги заштитат нивните лични податоци. Постигнувањето на оваа цел значи креирање вештини, знаења и решенија за заштита, притоа обезбедувајќи поголема отпорност од злонамерни сајбер активности.
3. *Справување со сајбер-криминал* е најчесто широко толкувано и во теоријата не постои една широко прифатена и унифицирана дефиниција за сајбер-криминалот. Она што како елемент се јавува во скоро сите дефиниции е тоа дека сајбер-криминалот е криминал кој е овозможен од, или е насочен против компјутери. Сајбер-криминалот може да опфати кражба на интелектуална сопственост, злоупотреба на патент, трговска тајна, и сл., но исто така вклучува и напади против компјутери со цел намерно нарушување на нивното функционирање или недозволено копирање на класифицирани информации складирани во

[360] Дирекција за безбедност на класифицирани информации, Информатичка безбедност на класифицирани информации, *ИнфоЛист,* достапно на: www.dbki.gov.mk

компјутерските системи.[361] Еден од условите за формирање на ефикасна национална *сајбер-одбрана* е сите организации кои нудат услуги во сајбер-просторот континуирано да ги усогласуваат оперативните планови за одбрана од сајбер-закани во согласност со националните сценарија, со цел заштита на критичната информациска инфраструктура. Цивилно-воената соработка на меѓународно ниво се базира на ресурсите со кои располага државата и кои функционираат соодветно и во сајбер-просторот – во однос на предупредувањето, превенцијата, заштитата, одвраќањето, детекцијата и активната одбрана.

4. *Соработката и размената на информации* е особено важна за секоја организација и поединец која треба самостојно да се грижи за начинот и одговорноста во користењето на најновите технологии. Сепак, доколку сакаме да имаме безбеден сајбер- простор на национално ниво потребно е да се дефинираат ефикасни и ефективни процедури за соработка и размена на информации помеѓу сите засегнати страни. Од оваа причина, потребно е да се зајакнат капацитетите, процедурите и процесите помеѓу засегнатите страни преку постојана соработка. Меѓународната соработка е еден од клучните сегменти во заложбите за зголемување на капацитетите за справување со заканите во сајбер-просторот. Во голем дел од случаите, Македонија би се соочила со сајбер-напади кои се делумно или во целост организирани и реализирани од злонамерни корисници кои се надвор од физичките граници на нашата држава. Во овој случај, успехот на преземените мерки за намалување на ефектите на регистрираните сајбер-инциденти и пронаоѓање и преземање соодветни мерки против сторителите на кривичното дело во основа зависи од воспоставената соработка на билатерално, регионално и на меѓународно ниво. Со цел да се обезбеди целосна оперативност на државните институции и надлежните органи одговорни за справување со ризиците и инцидентите во сајбер-просторот потребни се интернационални партнерства на тие институции со други држави и организации. Активното меѓународно учество во справување со глобалниот предизвик од сајбер-заканите ќе придонесе за зголемување на државните капацитети за справување со сајбер-ризиците.[362]

[361] Wilson, C. Botnets, *Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* 2008.

[362] Национална стратегија за сајбер безбедност на Република Македонија (2018-2022), јули 2018, достапно на: http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf

Истражувањето има цел да ги изнајде применливите правила за заштита на критичната инфраструктура од современите безбедносни закани во светот што се менува; да ги истражи пристапите на меѓународните организации; да ги лоцира причинско-последичните врски и главните двигатели на промената, како и да ги испита тенденциите на развој, можните решенија и потенцијалните фактори на ризик или успешноста во контекст на поставување на соодветна инфраструктура во меѓународен контекст.

2. САЈБЕР-БЕЗБЕДНОСТА, КРИТИЧНАТА ИНФРАСТРУКТУРА И МЕЃУНАРОДНИТЕ ОРГАНИЗАЦИИ

Сајбер-безбедноста и сајбер-криминалот се проблеми коишто тешко можат да бидат раздвоени во ова глобално општество. Со развојот на интернетот како глобална структура за бизнис и како нова алатка за политика, за шпионажа и за воени активности, сајбер-безбедноста стана централна тема во националната и во меѓународната безбедност. Оттука, голем број држави донесоа свои национални сајбер-безбедносни доктрини или стратегии. Освен на национално ниво, и меѓународните организации активно се занимаваат со оваа проблематика. НАТО, ЕУ и другите релевантни институции преземаат сериозни напори и чекори за спречување и справување со овие негативни предизвици. Сајбер-одбраната станува сериозна и реална потреба како компатибилен дел од целокупната сајбер-безбедност. Во продолжение на главата ќе се задржиме на приодот на ООН, на НАТО, на ЕУ и на ОБСЕ кон овој проблем.

2.1. Приодот на ООН кон сајбер-безбедноста

Организацијата на обединетите нации (ООН) решаваат прашања во врска со безбедноста на информациите преку својата канцеларија за работи за разоружување од 1998 година, кога Руската Федерација претстави нацрт-резолуција на состанокот на Првиот комитет на Генералното собрание на ООН.[363] Таа беше усвоена без гласање и оттогаш генералниот секретар доставува годишни извештаи до Генералното собрание со

[363] United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/.

ставовите на земјите-членки за ова прашање.[364] Покрај тоа, Институтот на Обединетите нации за истражување на разоружувањето, обезбедува градење капацитети ориентирани кон политика на национално, регионално и мултилатерално ниво, како и релевантно истражување и анализа. Институтот, исто така работи на подигање на свеста за интеракцијата помеѓу иницијативите за сајбер-прашања насочени кон обезбедување на хармоничен раст и развој на стабилно компјутерско опкружување. За таа цел, Институтот на ООН досега спроведе процена на националните способности, доктрини, организирање и транспарентност и градење доверба за компјутерска безбедност, и организираше работилници за компјутерска безбедност, но и конференции за меѓународна безбедност и стабилност. Исто така, ги поддржува владините експертски групи на Обединетите нации кои работат на прашања во врска со сајбер-просторот.[365] Владината експертска група за развојот на полето на информациите и телекомуникациите во контекст на меѓународната безбедност, формирана е на иницијатива на земјите-членки, и ги испитува постојните и потенцијалните закани од сајбер-сферата и можните мерки за соработка за нивна борба. Главните достигнувања на Владината експертска група вклучуваат: воспоставување глобална агенда за безбедност и воведување на принципот „меѓународното право“ да се применува на дигиталниот простор. Досега, пет владини експертски групи постигнаа напредок во постигнување на консензус и објавување на три извештаи за развојни информации и информации во телекомуникациите во контекст на меѓународната безбедност. Работата на Групата на владини експерти од својот прв извештај во 2010 година до денес ја позиционираше како клучен меѓународен механизам за дискутирање за донесување стандарди и мерки за градење доверба во сајбер-просторот, што треба да се сфати сериозно од државите. Сепак, иднината на оваа рамка сè уште е неизвесна по неуспехот да се постигне консензус во Петтата група на владини експерти, кои разгледаа, меѓу другото, постојни и нови закани, градење капацитет, градење доверба, препораки за примена на стандарди, правила и принципи за одговорно однесување на државите, примена на меѓународното право за употреба информатички и комуникациски технологии, како и заклучоци и препораки за идна работа.[366]

Меѓународната унија за телекомуникации на ООН (ITU) го објавува Глобалниот индекс за компјутерска безбедност во светот, кој

[364] Developments in the field of information and telecommunications in the context of international security. United Nations Office for Disarmament Affairs.

[365] Исто.

[366] Исто.

ја мери компјутерската безбедност во светот. Тоа е извештај базиран на истражувања што ја мери посветеноста на земјите-членки за безбедноста во сајбер-безбедноста и се состои од петте столба на Глобалната агенда за компјутерска безбедност на ИТУ: правни прашања, технички проблеми, организациски проблеми, градење на капацитети и соработка.[367]

2.2. Приодот на НАТО кон сајбер-безбедноста

НАТО ги промовира вредностите за заштита на критична инфраструктура, со вршење ревизија на степенот на подготвеност на земјите членки во однос на планирање и мапирање на инфраструктурата, при што Алијансата не навлегува во директно регулирање на областа, но формулира програми за поддршка на националните планови, во смисла на промовирање високи стандарди за подготвеност и подобрена интероперабилност во менаџирање на евентуални последици.

Студиите и активностите на НАТО од областа на критичната инфраструктура ги вршат специјализирани тела и комитети кои во организациската структура потпаѓаат под Senior Civil Emergency Planning Committee (SCEPC), коешто е главното одлучувачко тело на НАТО за полето на Civil Emergency Planning (CEP).

Во 2003 година (SCEPC) утврдува посебен Концепт-документ за заштита на критична инфраструктура, заедно со road map, за поттикнување на развој на механизми кои нациите ќе може да ги употребат за да се подготвуваат, односно да ги координираат можните инциденти на критичната инфраструктура. Препознаени императиви во документот на НАТО се: идентификување на критичната инфраструктура, размена на информации, развој на програми за едукација и тренинг на персоналот, идентификување на истражувачки и развојни проекти, како и рационализирање на заштитата на критичната инфраструктура преку теренски вежби.[368]

На Самитот на НАТО во Рига во ноември 2006 година, шефовите на држави и влади ја потврдија улогата на Алијансата повторувајќи ја нивната „решеност да заштити популации, територии, инфраструктура и сили против последиците од терористичките напади“, истакнувајќи

[367] Global Cyber security Index (GCI), ITU, International Telecommunication Union, Generva, Switzerland, 2018, достапно на: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01- 2018-PDF-E.pdf.

[368] Правна рамка за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Стеда графика, Скопје, 2016.

дека „безбедносните интереси, исто така, можат да бидат засегнати од нарушување на протокот на виталните ресурси“. Слична заложба се појавува и во Сеопфатната политичка насока, исто така одобрена од шефови на држави и влади во Рига.

Во јануари 2008 година НАТО ја усвои својата прва политика кон сајбер-одбраната и според тоа разви соодветен акционен план за дејствување во кој се трасира јасната визија за опасноста и за потребата од реакција кон таквата опасност од сајбер-заканите. Меѓутоа, во многу случаи, изборот на заштитни мерки исто така зависи од видот на инфраструктурата. Така, на пример, одредени сектори во голема мера зависат од фиксни инфраструктури (на пример, транспорт, енергија), додека други се потпираат на мрежни инфраструктури (на пример, информации и комуникација). Во првиот случај, заштитата најверојатно ќе се фокусира на зацврстување на овие фиксни инфраструктури, додека во вториот, мерките за заштита ќе имаат за цел да обезбедат дека мрежата може да продолжи да ја извршува својата функција. Во согласност со Извештајот, мерките за заштита може да се класифицираат во четири широки категории, во зависност од кој аспект на инфраструктурата се насочени:

1) *мерки за физичка заштита* – кои се насочени кон физичките компоненти на инфраструктурата;
2) *електронски или сајбер-мерки* за заштита – чија цел е заштита на ИКТ инфраструктурата од напади;
3) *мерки за заштита на човечкиот капитал* или персоналот – кои се насочени кон вработените во инфраструктурата и другите категории на луѓе кои имаат директен однос со инфраструктурата; и
4) *организациски мерки* – кои се однесуваат на начинот на кој се управува инфраструктурата.[369]

Мерките за заштита може да бидат постојани / долгорочни или тие можат да бидат флексибилни, односно постепено да се спроведуваат според различните нивоа на ризик и на опасност. Ова укажува на фактот дека стратегијата за заштита на критичната инфраструктура треба да се организира како процес на постојана ревизија за да обезбеди тековно приспособување на мерките за заштита.

Неколку фактори се идентификувани за ефикасна стратегија за заштита на критичната инфраструктура: прво, дека заштитата на критич-

[369] Извештај на специјалниот известувач за парламентарното собрание на НАТО (2007), достапно на http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pd

ната инфраструктура е многу чувствителна област, и затоа е важно да се обезбеди високо ниво на доверливост во однос на најкритичните елементи на стратегијата, вклучувајќи го и пописот на критичните инфраструктури. Исто, споделувањето на информации помеѓу засегнатите страни од приватниот сектор до јавниот сектор и обратно - е од клучно значење, тоа често е многу деликатно прашање. Затоа, ефикасно споделување информации ќе се случи само ако соодветни правила гарантираат дека информациите се споделуваат строго врз основа на неопходност, врз зададен основ и во целосно безбеден режим. Второ клучно прашање е потребата да се даде приоритет меѓу можните заштитни мерки. Сеопфатната заштита од сите опасности за сите критични инфраструктури е речиси секогаш невозможна, не само од технички причини, туку и поради други ограничувања, особено високите трошоци.[370]

Во стратегискиот концепт од Лисабон во 2010 година особено се издвојуваат сајбер- заканите по критичната инфраструктура и заштитата на енергетската критична инфраструктура, што го детерминира фокусот на Алијансата кон развој на заштитата посебно кон овие два аспекти.[371] Значи, сајбер-одбраната беше претставена како еден од најважните предизвици на Алијансата во иднина. Особено беше истакната важноста од заштита на информацискатa и комуникацискатa инфраструктура на НАТО. Во таа насока, покрај националниот предизвик за заштита на информациите, заштитата на информацискиот систем на НАТО претставува интегрален дел во функционирањето на Алијансата. По случувањата во Естонија во мај и април 2007 година, кога беше нападната информацискатa инфраструктура на земјата, НАТО започна со континуиран развој и подобрување на заштитата на своите комуникациски и информациски системи од напади и од неовластен пристап. Алијансата, исто така, ги насочи своите активности во поддршка на индивидуалните напори за заштита на информацискатa инфраструктура на секоја земја-членка. НАТО-центарот за сајбер-одбрана во Естонија е акредитиран од Алијансата. Тоа е меѓународна воена институција која се фокусира на различни аспекти поврзани со сајбер-одбраната, како што се образование, анализи, консултации, научени лекции, истражување и развој. Иако Центарот не е под директна командна линија на НАТО, неговата мисија е да се

[370] Извештај на специјалниот известувач за парламентарното собрание на НАТО (2007), достапно на http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.

[371] НАТО Стратешки концепт, достапен на https://www.nato.int/lisbon2010/strategic-concept-2010- eng.pdf, 2010.

зголеми способноста, соработката и размената на информации помеѓу НАТО и земјите од НАТО и партнерите во доменот на сајбер-одбраната.

Новиот стратегиски концепт и декларацијата донесена на Самитот во Чикаго 2012 година препознаа дека сајбер-нападите се сè пософистицирани и затоа дизајнирањето на ефективна сајбер-одбрана е една од најприоритетните задачи за НАТО. Изнаоѓањето на ефективен одговор мора да биде преку пристап кој е базиран на интензивна координација, преку што ќе се зајакне отпорноста на системот на одбрана. Сепак, комплексноста на овие закани наметна низа предизвици и од доменот на капацитетите и од начините на справување со нив. Тие во голема мера можат да предизвикаат контрадикторни ситуации кои му пркосат на меѓународното право општо, и дел од човековите права посебно.

Зголемениот број сајбер-напади, стратегиите и технологиите за компјутерско војување водат кон создавање стручни сајбер-центри. Центрите се формираат во приватни компании (како Lockheed Martin, Сајбер-центар за извонредност - CoE, отворен во 2015 година), национални субјекти/ентитети како што се германскиот Национален центар за компјутерска заштита и меѓународни субјекти како што е Кооперативниот сајбер НАТО Одбранбен центар за извонредност - CCDCOE во Естонија и Европската организација за компјутерска безбедност во Белгија.[372] Исто така, заради подобро функционирање и размена на податоци во НАТО воспоставен е Ситуацискиот центар на НАТО кој е дизајниран за алармирање и за давање на ситуациска свест на Северноатлантскиот совет и Воениот комитет, за да им помогне да ги исполнат своите функции во време на мир, напнатост и криза, како и за време на вежби на високо ниво. Тоа го прави преку примање, размена и ширење на информации од сите можни внатрешни и надворешни извори што се достапни.[373] Преку користењето на апликациите и програмите на НАТО можат да се утврдат проблематичните подрачја или да се утврдат областите што се интересни подрачја за безбедносни истражувања. Притоа, може да се направи систематска процена и да се увиди значењето, односно предностите или негативностите за конкретен објект или план.[374]

Политиката на НАТО ги дефинира начините за продолжување на активностите за подигање на свеста, едукацијата, обуката и поттик-

[372] Wilson R. J., *The Shadowy World Of Cyber Warfare*, Military & Aerospace Electronics, Vol. 27, Issue 12, 2016.

[373] *Situation Centre (SITCEN)*. NATO. (2015), достапно на: https://www.nato.int/cps/en/natohq/topics_57954.htm.

[374] Чековиќ Т., *Повеќедимензионалните придобивки и ефекти од пристапувањето кон НАТО,* Институт за Европска Политика-Скопје, Релатив, 2018.

нува понатамошен напредок во различни иницијативи за соработка, вклучувајќи ги и оние со земјите-партнери и меѓународни организации. Исто така, таа предвидува зголемување на соработката на НАТО со индустријата, вклучувајќи и за размена на информации и за размена на најдобри практики. Сојузниците, исто така, се залагаат за подобрување на размената на информации и заемната помош во спречување, ублажување и обновување од сајбер-нападите. Политиката на НАТО за сајбер-одбрана е надополнета со акциски план со конкретни цели и временски рамки за спроведување на голем број теми од развојот на способностите, образованието, обуката, вежбите и партнерствата.

Сојузниците на Самитот во Варшава во 2016 година ветија дека ќе ја зајакнат и ќе ја подобрат сајбер-одбраната на националните мрежи и инфраструктури, како приоритетни задачи.[375]

Соединетите Американски Држави се консултираа со своите сојузници и претседаваа со експертската група на НАТО за да разговараат за новиот стратегиски концепт. Меѓу другото, заклучено е дека сајбер-нападите со различен степен на сериозност се една од трите најверојатни закани за земјите-членки на НАТО до 2020 година. Сојузниците на САД, особено Велика Британија, ги поддржаа иницијативите. Британскиот министер за одбрана, Ник Харви, повика на можност за колективно дејствување во случај на агресивен чин во сајбер-просторот, повикувајќи се на Членот 5 од Колективниот договор.[376]

Сајбер-одбраната стана составен дел од процесот на планирање на одбраната на НАТО преку олеснување на заедничкиот пристап кон развојот на способноста. Воспоставувањето на засебно дефинирани целни области за развој на способност што ќе биде во согласност со брзите промени во оперативните и во технолошките закани, се клучни за политиката на НАТО. Способноста за одговор на инциденти на НАТО[377] обезбедува соодветно ниво на одговор на сајбер-напади, додека другите иницијативи започнаа да се обликуваат, создавајќи стабилна и ефикасна платформа за одбрана.[378]

Во овој контекст, Организацијата на Северноатлантскиот договор (НАТО) ги насочува повеќето од своите сајбер-активности во сферата на

[375] *Cyber defence*. (2018), NATO, достапно на: https://www.nato.int/cps/en/natohq/topics_78170.htm.

[376] Stevens T., *Contemporary Security Policy A Cyberwar of Ideas? Deterrence and Norms in* Cyberspace, Contemporary Security Policy, Vol.33, No.1. 2012.

[377] (Computer Incident Response Capability – NCIRC)

[378] Mahon T., *Cyber - the 21st Century Threat*, *Military Technology*, Vol. 39 Issue 5, 2015.

одбраната. Откако НАТО ја прогласи *сајбер-сферата* за петти домен[379] на војната во јули 2016 година,[380] проблемите со компјутерската одбрана станаа дел од задачата на колективната одбрана на оваа организација и земјите-членки се обврзаа на сајбер-одбрана, односно да го развијат и зајакнат целосниот спектар на националните можности за компјутерска одбрана.[381]

Земјите-членки на НАТО, генерално, ги прифаќаат активностите на Алијансата во однос на заштитата на критичната инфраструктура, но останува фактот дека сепак предметната проблематика е одговорност и е обврска првенствено на национално ниво.

2.3. Приодот на Европската Унија кон сајбер-безбедноста

Новите размислувања одат во насока дека комплексните инфраструктурни системи е потребно да се разгледуваат како отворени, ранливи системи со многу внатрешни проблеми.[382]

На ниво на ЕУ, преземени се бројни активности за заштита на клучните информациски инфраструктури со цел да се зголеми нивната безбедност.

Акцискиот план, донесен на 30 март 2009 година е заснован на пет столба од Европската комисија:

1) подготвеност и превенција;
2) откривање и одговор;
3) ублажување и одговор;
4) меѓународна соработка; и
5) критериуми за европски критични инфраструктури.[383]

---

[379] Вклучувањето на сајбер-доменот како петти домен на војување значи дека сајбер-нападите сега спаѓаат во Членот 5 од принципот на колективна одбрана.

[380] Warsaw Summit Communique issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. 9.7.2016. North Atlantic Treaty Organisation. https:// ccdcoe.org/sites/default/files/documents/ NATO-160709-WarsawSummitCommunique.pdf.

[381] Cyber Defence Pledge. 8.7.2016. North Atlantic Treaty Organisation. https:// www.nato.int/cps/en/natohq/ official_texts_133177.htm

[382] Lundborg, T., Vaughan-Williams, N., Resilience, Critical Infrastructure and Molecular Security: the Excess of Life in Biopolitics, *International Journal Political Sociology*, vol. 5, no. 4, 2011, стр. 369.

[383] CIIP Action Plan in its Communication on Critical information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and cyber-disruptions: enhancing preparedness, security and resilience' – COM (2009), достапно на: http:// eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Европската програма за заштита на критичната инфраструктура (EPCIP)[384] ја поставува севкупната рамка на активности насочени кон подобрување на заштитата на критичната инфраструктура во Европа – низ сите држави на ЕУ и во сите релевантни сектори на економската активност. Заканите на кои Програмата треба да одговори не се ограничени само на тероризмот, туку вклучуваат и криминални активности, природни катастрофи и други причини за несреќи. Клучен столб на оваа програма е Директивата за европски критични инфраструктури од 2008 година.

Европската програма за заштита на европската критична инфраструктура се фокусира на четири главни столба:

1) Создавање процедура за идентификување и процена на критичната инфраструктура на Европа и учење како подобро да се заштити истата. Оваа постапка е воспоставена за енергетски и за транспортни сектори во Директивата за идентификација и одредување на Европската критична инфраструктура.
2) Мерки за помош на заштитата на инфраструктурата, вклучувајќи и експертски групи назначени од ЕУ и создавање на Информативна мрежа за предупредување за критични инфраструктури (CIWIN) – комуникациски систем базиран на интернет за размена на информации, студии и најдобри практики.
3) Финансирање на повеќе проекти за критична инфраструктурна заштита од 2007 година па натаму. Овие проекти се фокусираа на различни прашања, вклучувајќи ги националните и европските системи за размена на информации и алармирање, развој на начини за процена на меѓузависноста помеѓу електронските и мрежите за пренос на електрична енергија и создавање прирачник за „добри практики“ за креаторите на политики.
4) Меѓународната соработка со земјите од Европската економска област и земјите од Европската слободна трговска зона, како и експертски состаноци помеѓу ЕУ, САД и Канада.[385]

Во март 2009 година, Иницијативата за заштита на критична информациска инфраструктура[386] го основа Европското јавно приватно-

[384] Европска програма за заштита на критичната инфраструктура, достапно на https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786

[385] European Commission, достапно на: https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[386] Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on

партнерство за еластичност[387] како координативно тело за европскиот одговор на сајбер-закани за критична информациска инфраструктура. Улогата на работните групи формирани од ова Партнерство беа да ја поттикнат размената на информации и добрите практики, по моделот на постојните национални механизми за јавно-приватно партнерство; да го прави можно разгледувањето на приоритетите, целите и мерките на јавните политики во оваа област; и да ги идентификуваат основните предуслови за безбедност и еластичност во Европа.

Во Талин на 27-28 април 2009 година се одржа Министерска конференција на ЕУ за заштита на критичната национална инфраструктура каде се констатирало дека и покрај напредокот постигнат на ниво на ЕУ и земји-членки, мора да се зголеми нивото на безбедност, подготвеност и еластичност на информациските критични инфраструктури. Беше наведено дека треба да се направат напори за подобрување на координацијата и соработката со поддршка на Европската агенција за безбедност на мрежа и информации (ENISA).[388]

Европската агенција за безбедност на мрежи и информации е формирана за да обезбеди високо ниво на мрежна и информациска безбедност на ниво на Европската Унија. Покрај мрежата ENISA, критичната инфраструктурна информациска мрежа (CIWIN),[389] им помага на земјите-членки, институциите на ЕУ, корисниците и операторите на критична инфраструктура кои играат важна улога во заштитата на информациските критични инфраструктури на ниво на ЕУ и кои разменуваат информации за закани и ранливости и градат соодветни мерки и стратегии за намалување на ризиците и заштита на клучните информациски инфраструктури.

Европската комисија на 31 март 2011 година го усвои соопштението „Достигнувања и следни чекори: кон глобална сајбер-безбедност"'. Во изјавата се дадени следните чекори планирани за секоја европска и меѓународна акција. Фокусот е ставен на глобалната димензија на одговорот и на важноста од соработката помеѓу

Critical Information Infrastructure Protection. „Protecting Europe for large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". 30.3.2009. COM (2009) 149 final.

[387] European Public Private Partnership for Resilience (EP3R). ENISA, достапно на: https://www. enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/ european-public-private-partnership-for-resilience-ep3r

[388] European Network and Information Security Agency – ENISA (2009). European Union Ministerial Conference on Critical Information Infrastructure Protection, Tallinn.

[389] Critical Infrastructure Warning Information Network – CIWIN.

земјите-членки и приватниот сектор на национално, на европско и на меѓународно ниво.[390] Особено важен сегмент е заштитата на критичната информатичка инфраструктура, која е опфатена со посебната стратегија за сајбер-безбедност на ЕУ која ги идентификува активностите кои дополнително ќе придонесат за сајбер-резилиентност и безбедност на критичната инфраструктура во сајбер-секторот. Предлозите на стратегијата вклучуваат: координирани превентивни механизми, подобрена подготвеност и вклучување на приватниот сектор.

Стратегијата за сајбер-безбедност на Европската комисија и на високиот претставник од 2013 година е првиот сеопфатен документ за политиката на Европската унија во оваа област.[391] Крајниот рок за национално транспонирање од страна на земјите членки на ЕУ беше 9 мај 2018 година. Директивата има три дела кои се однесуваат на:

1. Градење на национални капацитети, во секоја земја-членка одделно.
2. Прекугранична соработка: прекугранична соработка помеѓу земјите на ЕУ.
3. Национален надзор на критичните сектори: земјите-членки на ЕУ треба да ја надгледуваат сајбер-безбедноста на критичните пазарни оператори во нивната земја: Ex-ante надзор во критични сектори (енергетски, транспорт, вода, здравство и финансиски сектор), ex-post надзор за критични набавувачи на дигитални услуги (точки за размена на интернет, системи за имиња на домени итн.).

Во Стратегија за сајбер-безбедност на ЕУ јасно е зацртана визијата на Европската Унија: да обезбеди силна и ефективна заштита и промоција на правата на граѓаните за да ја направи онлајн-средината на ЕУ како најбезбедна во светот. За остварување на визијата, ЕУ предвидува исполнување на пет стратегиски приоритети:

1. Постигнување на сајбер-отпорност – со зголемување на способностите, подготвеноста, соработката, размената на информации и подигање на свеста во областа на мрежната и информацискатa

[390] Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" – COM (2011), достапно на: http://ec.europa.eu/information_society/ policy/nis/strategy/activities/ciip/index_en.htm

[391] Европски Парламент (2016) Директива за безбедност на мрежите и информатичките системи достапна на https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

безбедност за јавниот и за приватниот сектор и на национално и на ниво на ЕУ.

2. Драстично намалување на сајбер-криминалот – преку зајакнување на стручноста на оние кои се задолжени за истражување и гонење на овие казнени дела, со донесување на покоординиран пристап помеѓу спроведувањето на законот во рамките на ЕУ, како и преку подобрување на соработката со другите актери.
3. Развој на сајбер-безбедносната политика и способностите поврзани со Заедничката безбедносна и одбранбена политика (ЗБОП).
4. Развој на индустриските и на технолошките ресурси за сајбер-безбедност за да имаат корист од единствениот дигитален пазар. Ова ќе помогне да се стимулира појавата на европската индустрија на пазарот за обезбедување на информатичко-комуникациска технологија, а тоа ќе придонесе за раст на конкурентноста на економијата на ЕУ.
5. Воспоставување кохерентна меѓународна политика на сајбер-просторот на ЕУ и промовирање на основните вредности на ЕУ – дефинирање на нормите за одговорно однесување, заложби за примена на меѓународното право во сајбер-просторот и да им се помогне на земјите надвор од ЕУ во градењето на сајбер-безбедносните капацитети.[392]

Директивата поврзана со Стратегијата на ЕУ за сајбер-безбедноста, поставува поспецифични насоки за земјите-членки за мерките на заштита на критичната информатичка инфраструктура, вклучувајќи го и поставувањето на национални компјутерски центри за одговор во итни ситуации (CERTs). Во исто време, Агенцијата за безбедност на мрежата и информациите на Европската Унија (ЕНИСА) е задолжена за следење на спроведувањето на мерките за заштита на критичната информациска инфраструктура и обезбедување мерки и ресурси за градење капацитети.

Агендата за безбедност на ЕУ, усвоена во 2015 година, ги наведува видовите компјутерски криминал како еден од трите клучни приоритети за кои е потребна итна акција, заедно со тероризмот и со организираниот криминал. Во овој поглед, сајбер безбедноста е дефинирана како „предна линија на одбраната“ против компјутерскиот криминал и повикува на брзо усвојување на сеопфатна рамка за регулирање на безбедноста на мрежите и информациите во Европската Унија.[393]

[392] Славески С, Сајбер-безбедност, Современа македонска одбрана, Министерство за одбрана, 2015.

[393] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the

Во 2016 година беше донесена Директива за мерки за високо заедничко ниво на безбедност на мрежните и информациските системи на ЕУ (Директива NIS), три години по комплицираните преговори меѓу Комисијата, Европскиот парламент и Советот на Европа. Директивата ги повикува сите земји-членки да ги утврдат основните безбедносни стандарди за националните мрежни и информациски системи, што ќе бидат дефинирани од надлежниот национален орган, да формираат функционални центри за спречување на ризик од безбедност во ИКТ системите и да усвојат национални стратегии и планови за соработка во оваа област. Во согласност со одредбите на оваа Директива, националната стратегија за безбедност на информациите треба да се осврне на следните прашања дадени во вид на цели и приоритети:

- надлежности и одговорности на релевантни државни органи и други актери;
- мерки за подготвеност, реакција и обновување, вклучувајќи и соработка на јавниот и приватниот сектор;
- индикација за планирани програми за образование, програми за подигнување на свеста и обука;
- упатство за планови за истражување и развој;
- план за процена на ризикот за идентификување на потенцијалните ризици;
- список на актери вклучени во спроведувањето на стратегијата.[394]

Во однос на критичната инфраструктура за информации, Директивата NIS предвидува дека земјите-членки се одговорни за воспоставување на *критична инфраструктура* во областа опфатена со Директивата.

Директивата NIS, всушност, признава два вида субјекти: оператори на ИКТ систем кои обезбедуваат оператори на основни услуги (анг. operators of essential services) и даватели на дигитални услуги (анг. digital services providers). Анексите II и III содржат список на услуги што спаѓаат во првата група, врз основа на која може да се утврди дали одреден давател на услуги е еден од давателите на услуги што е особено релевантен за одржување на клучните социјални и економски активности. Списокот

Regions. The European Agenda on Security. 28.4.2015. European Commission. COM(2015) 185 final

[394] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union L 194/1.

на услуги всушност ја изедначува оваа група со критични оператори во инфраструктурата, што ги вклучува следните сектори:

- ✓ енергетски сектор (електрична енергија, нафта и гас);
- ✓ транспортен сектор (воздушен, железнички, воден и патен транспорт);
- ✓ банкарски сектор;
- ✓ инфраструктури на финансискиот пазар;
- ✓ здравствен сектор (здравствени установи, вклучувајќи болници и приватни клиники);
- ✓ набавка и дистрибуција на вода за пиење;
- ✓ дигитална инфраструктура (IXP, провајдери на DNS и регистрирани домени на TDL). (Анекс II);
- ✓ интернет пазар;
- ✓ интернет прелистувач и
- ✓ служба за компјутерски облак (анг. cloud computing) (Анекс III). [395]

Директивата NIS утврдува специфични принципи кои се однесуваат на развој на дополнителни правила и / или упатства за подготвеност на критичните сектори за реакција на компјутерскиот ризик. За таа цел, на земјите-членки им беше советувано да развијат национална стратегија што ќе ги вклучува сите релевантни димензии на општеството и на економијата, а не само на секторите и дигиталните услуги опфатени со Анекс II и Анекс III од Директивата. Ова ќе придонесе кон усвојување закони кои обезбедуваат повисоко ниво на безбедност за мрежните и информатичките системи и опфаќаат сектори што не се наведени во анексите на Директивата.

Како дел од најновите чекори кон воспоставување на систем за отпорност на ЕУ во сајбер-просторот, Комисијата планира да спроведе процена на ризик од сајбер-инциденти во високо меѓусебно зависни сектори во и надвор од националните граници, особено во секторите опфатени со Директивата NIS. Покрај тоа, *Европскиот одбранбен фонд* предвидува поголема инвестиција во компјутерската безбедност, меѓу другите. Поточно, Европскиот инвестициски фонд треба да го зголеми својот придонес во безбедносната и во одбранбената агенда на ЕУ, вклучувајќи и инвестиции во прашања како што се технологии со двојна употреба и компјутерска безбедност, заедно со финансирање за цивил-

[395] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union L 194/1.

на инфраструктура за заштита и биоодбрана. Европскиот одбранбен фонд, исто така, работи на зголемување на уделот на кооперативни проекти за одбрана во вкупното трошење на одбраната, како и да ја испита комплементарноста со цивилната употреба и релевантните европски програми за граѓанска поддршка. Во овој поглед, потребна е комплементарност главно во однос на безбедносните политики на ЕУ, вклучувајќи ја и сајбер-безбедноста. Затоа, може да се очекуваат понатамошни зголемувања на инвестициите во сајбер-одбраната на земјите-членки на ЕУ, насочени првенствено за постигнување интероперабилност и ефикасност преку комплементарност и споделување ресурси.[396]

Генерално, прашањата за безбедноста на сајбер-просторот од интелектуална сопственост, културна разновидност и заштита на лични податоци до борба против терористичка пропаганда и радикализација на интернет, а особено борба против сајбер-нападите се на четврто место. Тие беа дури и пред миграцијата, еден од најголемите предизвици со кои се соочува ЕУ од неодамна. Осврнувајќи се на бројките кои покажуваат дека во 2016 година имало повеќе од 4.000 напади на ден преку уценувачки софтвери (анг. Ransomware) и повеќе од 80% од европските компании искусиле барем еден инцидент во врска со компјутерската безбедност, претседателот на Европската комисија Јункер претстави предлог за развој на нови алатки на ENISA.[397]

Покрај тоа, предвидено е воспоставување мрежа за компјутерски капацитети на ЕУ, со оглед на тоа што активностите на ЕУ се насочени кон еластичност, одвраќање и одбрана, при што приоритет е воспоставување на стратегиска рамка за спречување конфликти и сајбер-стабилност во нејзините билатерални, регионални, мултикарактер и мултилатерални ангажмани со давање приоритет на соседните држави и земјите во развој. Мрежата ќе ги обедини Европската служба за надворешни работи, властите на земјите-членки кои се занимаваат со компјутерска безбедност, агенциите на ЕУ, услугите на Комисијата, академската заедница и граѓанското општество. За да се одговори на сајбер-нападите, улога и одговорности имаат клучните три столбови во ЕУ: мрежната и

[396] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Launching the European Defence Fund. 7.6.2017. European Commission. COM (2017) 295 final.

[397] President Jean-Claude Juncker's State of the Union Address 2017. 13 September 2017. European Commission. SPEECH/17/3165

информациската безбедност, органите кои го спроведуваат законот и одбранбените агенции.[398]

Заокружувајќи го циклусот на надворешната политика во сајбер-просторот, ЕУ има развиено и „алатки за сајбер дипломатија", со кои се утврдени конкретни мерки според Заедничката надворешна и безбедносна политика.[399] Тие, исто така вклучуваат рестриктивни мерки што можат да се користат за зајакнување на реакцијата на ЕУ на активности што негативно влијаат на нејзините политички, безбедносни и економски интереси, воспоставувајќи основа за ЕУ и земјите-членки да развиваат капацитети за предупредување и одговор. За таа цел, алатките за сајбер-дипломатија ги утврдија принципите врз основа на кои ЕУ и нејзините земји-членки треба да одговорат на злонамерните сајбер-активности, дејствувајќи како рамка за заеднички дипломатски одговор на ЕУ.[400]

За таа цел, нова платформа за компјутерска безбедност/одбрана, образование, обука, евалуација и вежбање се усвои во септември 2018 година.[401] Европскиот колеџ за безбедност и одбрана (ESDC) ќе има задача да управува со координирање на образованието, на обука, на евалуација и на вежбите во компјутерската безбедност/одбрана.

Усвоената стратегија за Западен Балкан јасно ја нагласува потребата за проширување на оперативната соработка за борба против разни видови организиран криминал за да се вклучи овој регион во рамките на постојниот циклус на политика. За таа цел, Стратегијата предвидува зголемена поддршка за градење капацитетите во областа на компјутерската безбедност и во борбата против сајбер-криминалот, преку зајакнување на соработката со релевантни агенции, како што се Европол и ЕНИСА (Европска агенција за безбедност на мрежи и информации).[402]

---

[398] Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN (2017) 450 final.

[399] Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN (2017) 450 final.

[400] Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption. 7 June 2017. Council of the European Union. 9916/17.

[401] New EU cyber platform to boost cyber security capabilities across Europe. 14.2.2018. European Union External Action Service.

[402] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A credible enlargement perspective for and enhanced EU engagement with the Western Balkans. 6.2.2018. European Commission. COM(2018) 65 final

2.4. Приодот на ОБСЕ кон сајбер-безбедноста

Во рамките на активности фокусирани на безбедноста и други теми како што се контрола на оружјето, мерки за безбедност и градење доверба, човекови права и др., Организацијата за безбедност и соработка во Европа (ОБСЕ), исто така, се осврнува на проблемите со сајбер безбедноста во форма на справување со тероризам и со компјутерски криминал. Сепак, во 2012 година, ОБСЕ одлучи да ги зголеми индивидуалните и колективните напори за решавање на безбедносните проблеми при употреба на информатички и комуникациски технологии (ИКТ) на сеопфатен и на меѓудимензионален начин.[403] За таа цел, формирана е неформална работна група за сајбер безбедност која предложи серија мерки за градење доверба за зајакнување на меѓудржавната соработка, транспарентност, предвидливост и стабилност, намалување на ризиците од погрешна перцепција, ескалација и конфликт што може да биде резултат на користење на ИКТ.

Државите на ОБСЕ усвоија серија мерки за градење доверба. Првиот пакет мерки за транспарентност од 2013 година воспостави, меѓу другото, и официјални точки за контакт и комуникациски линии до спречување на можни тензии како резултат на сајбер-активности. Во 2013 година, земјите-членки на ОБСЕ го усвоија првиот пакет мерки за градење доверба за да се намали ризикот од конфликт предизвикан од употреба на информатички и комуникациски технологии.[404] Пакетот со 11 мерки вклучува, меѓу другото: размена на информации за сајбер закани, за национални рамки, за стратегии и за терминологија; безбедност на ИКТ системите и нивна употреба; одржување консултации за намалување на ризикот од погрешна перцепција и можна појава на политички или воени тензии или конфликти што можат да произлезат од употреба информациска компјутерска технологија и да се заштити националната и меѓународната критична инфраструктура; размена на информации за преземените мерки за да се обезбеди отворен и безбеден интернет; назначување на национални точки за контакт; и улогата на ОБСЕ како платформа за дијалог.[405]

[403] Decision No.1039. Development of Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies. 26.4.2012. Organisation for Security and Cooperation in Europe. PC.DEC/1039.

[404] Organization for Security and Co-operation in Europe. (2013). Permanent Coucil Decision, No. 1106, достапно на: www.osce.org/ pc/109168).

[405] Decision No.1106. Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication

Вториот пакет мерки, усвоен во март 2016 година, се темели на претходните упатства со додавање на пет нови. Покрај подобро дефинираните принципи за споделување на податоците, новите упатства директно ги повикуваат земјите-членки да ги промовираат и да ги зајакнат механизмите на јавно-приватно ниво партнерства за заедничка реакција на заканите. Вториот сет (2016 година) се фокусираше на натамошно зајакнување на соработката помеѓу државите учеснички - вклучувајќи, на пример, ефективно ублажување на сајбер-нападите врз критичната инфраструктура кои можат да влијаат на повеќе од една земја-учесник.[406] Покрај тоа, претпоследното упатство (бр. 15) се занимава со заштита на критична инфраструктура што зависи од функционирањето на ИКТ и обезбедува неколку модели на соработка во оваа област.[407]

Под покровителство на ОБСЕ, 57-те земји-учеснички на Организацијата продолжуваат да работат на теренот на креирање на збир мерки за градење доверба за намалување на ризиците од конфликт кои произлегуваат од употреба на ИКТ. Тие се дизајнирани да го направат сајбер-просторот попредвидлив и да понудат конкретни алатки и механизми за да се избегнат и да се решат потенцијалните недоразбирања, вклучувајќи:

- механизам за здружување на државите за консултации околу потенцијални инциденти за безбедност во сајбер/ИКТ за децентрализирање на зголемувањето на тензиите;
- платформа за размена на ставови, национални безбедносни политики за сајбер / ИКТ и пристапи за да им се овозможи на државите подобро да си „ги читаат“ намерите едни на други во сајбер-просторот;
- предмети за соработка, вклучувајќи и можност за заштита на информацискатa критична инфраструктура како дел од зајакнувањето на мрежната еластичност во регионот на ОБСЕ во корист на сите.

Technologies. 3.12.2013. Organisation for Security and Cooperation in Europe. PC.DEC/1106.

[406] Organization for Security and Co-operation in Europe. (2016). Permanent Coucil Decision, No. 1202, достапно на: www.osce.org/ pc/227281.

[407] Decision No.1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 10.3.2016. Organisation for Security and Cooperation in Europe. PC.DEC/1202.

Одделот за транснационални закани на Секретаријатот на ОБСЕ[408] им помага на државите учесници во нивните напори да ја зајакнат компјутерската/ИКТ безбедност. Поточно, назначено лице за компјутерска безбедност помага во спроведување и развој на нови пристапи за сајбер / ИКТ безбедност, нудејќи насоки и совети за политика, како и координирање на организациските резултати во ова поле. Одделот за транснационални закани исто така нуди конкретни активности дизајнирани за подобрување на капацитети за справување со заканите поврзани со безбедноста преку интернет и ИКТ, индивидуално и кооперативно. Ваквите активности се движат од вежби за промовирање соодветни национални одговори на потенцијални сајбер-напади врз критични инфраструктури, до работилници за борба против употребата на интернетот за терористички цели и обука за истраги и гонење на компјутерски криминал.[409]

[408] OSCE Secretariat Transnational Threats Department (2019), Transnational Threats Department Cyber/ICT Security, Vienna, Austria, достапно на: www.osce.org/secretariat/cyber-security.

[409] Пример за работилница реализирана на 20 ноември 2019 година во Скопје: Регионална работилница во Југоисточна Европа за заштита на критична инфраструктура од терористички напади. Работилницата беше во организација на Единицата против тероризам на Одделот за транснационални закани на ОБСЕ, со поддршка на Мисијата на ОБСЕ во Скопје и во партнерство со Извршниот директорат на Комитетот за борба против тероризмот на ООН (УНКТЕД), ИНТЕРПОЛ и Канцеларијата на ООН за борба против тероризам (УНОКТ). Работилницата имаше цел да ги поддржи земјите-учесници на ОБСЕ во спроведувањето на резолуцијата 2341 (2017) на Советот за безбедност на ООН, која ги повикува земјите-членки да се справат со опасноста од терористички напади против критична инфраструктура и да разгледаат мерки за развој на национални стратегии и политики, покрај другите релевантни резолуции. Настанот се реализира со цел да се даде преглед на пејзажот на закани за различни критични сектори, вклучувајќи ги таканаречените „меки" цели, потенцирајќи ги и физичките и сајбер-заканите.

глава VI

АНАЛИЗА ЗА БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И КРИТИЧНАТА ИНФРАСТРУКТУРА

1. КАКВИ СОГЛЕДУВАЊА НУДИ АНАЛИЗАТА

Безбедноста како динамична, комплексна и мултидимензионална категорија е витална човекова потреба и клучен општествен и државен интерес, односно таа е присутна во целокупното опкружување на нашето живеење. Таа е и референтната категорија во рамките на интерпретативната мисла на бројни автори кои ја конкретизираат, стилизираат и валоризираат преку систематска анализа и егзегеза во нивните трудови. Преку конкретната концептуализација и експозициска интонација, како и експликацискатa стипулација на идиомот безбедност ние со сигурност знаеме дека овој тема – референцијал е насекаде околу нас. Ја чувствуваме, ја гледаме, ја примаме, ја доживуваме како сеприсутен феномен кој постои за нас, за социјалните групи, за државата воопшто.

Подробниот опис на безбедноста се совпаѓа со откривањето и реконструирањето на слоевите на значењата за безбедноста кои се искажуваат отворено, со нагласување на контекстот на безбедносниот текст во кој се опишуваат општествено-безбедносни настани, состојби, однесувања и институции од безбедносниот сектор кои се ситуационо значајни да стипулираат, да нормираат и да одговорат на својата намена.

Безбедноста е во функција на заштита на критичната инфраструктура, која 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 ослабнувачки 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.

Заштитата на критичната инфраструктура е сериозен предизвик за безбедносниот сектор во едно општеството и е голема грижа за сите релевантни субјекти затоа што станува повеќе од очигледно дека критичната инфраструктура е изложена на безбедносни закани. Оттука,

секојдневно се преземаат чекори од страна на безбедносниот сектор за заштита на критичната инфраструктура која секогаш имала големо значење за функционирањето на државата. Затоа, потребно е да се обезбеди интегритивен пристап кој ги соединува сите компоненти на безбедносниот сектор и ги поврзува одвоените аспекти на организирањето.

Заштитата на критичната инфраструктура е предуслов, претпоставка за заштитата на други пошироки општествени вредности. Оттука, критичната инфраструктура претставува „крвоток" за непречено функционирање на базичните елементи на општеството, и аналогно на тоа нивната заштита претставува приоритет за секое општество, затоа што таа е и неопходна и суштинска и секако животно важна. Затоа, самата критична инфраструктура може да се смета за инструментална и средствена вредност. Тоа подразбира дека критичната инфраструктура би можеле да ја одредиме како нешто што е од суштествено значење за економијата, за државата и за општеството, најчесто идентификувани како сложени материјални и нематеријални системи, чие нарушување во функционирањето или уништувањето би можело да создаде долгорочни штетни последици врз основните вредности на економијата, на државата и на општеството во целина.

Значи, концептот на заштита на критичната инфраструктура е широко прифатен концепт кој се однесува на подобрување на начините на работа и функционирање на одделните сектори, односно вклучува широка платформа за реализација и конкретизација на одредени задачи за подобрување и заштита на виталните инфраструктурни објекти.

Анализата супстанционално потврди дека заштитата на националната критичната инфраструктура претставува исклучива одговорност на националните држави. Во нашата држава, во ситуација кога нема направено сериозен исчекор во регулирањето на критичната инфраструктура, треба да се направи еден сеопфатен исчекор, односно да се примени т.н. „широк и сеопфатен" („comprehensive and wide") концепт кој ќе ги обедини заедничките напори за институционален одговор. Тоа ќе овозможи да се направи солиден механизам со кој се оформуваат активностите во сферата на заштита на критичната инфраструктура.

Во таа насока, идните чекори треба да бидат насочени кон:

- регулирање на критичната инфраструктура како концепт кој ги спојува преференците на државата и на соодветните оператори со што нема да се понуди еднодимензионален пристап кој дава ексклузивитет на државата или државна контрола со регулаторно преземање, туку е повеќедимензионален поврзувачки механизам со соодветна симболична и институционална моќ која ќе ја направи јасната синергија и дијалектика помеѓу засегнатите страни;

- разбирање на елементите на критичност и ранливост на објектите од витален критичен инфраструктурен интерес;
- унифицирана имплементацијата на секторскиот и на потсекторскиот пристап кон заштита на критичната инфраструктури, со што треба да се воспостави заедничка листа на сектори, што ќе овозможи кохерентна имплементација на мерките и на постапките за заштита на критичната инфраструктура;
- идентификацијата на критичната инфраструктура со цел нејзина заштита, преку креирање план за заштита на елементите и на системите на критичната инфраструктура. Планот за заштита на критичната инфраструктура треба: да ги опише улогите и одговорностите за подготвеност, заштита, одговор и континуитет на операциите за заштита на критичната инфраструктура и да се воспостави оперативен концепт за инцидентни операции за заштита на критичната инфраструктура;
- артикулација на концептуализациите на идиомот критична инфраструктура воопштена, синтетизирана и елаборирана, како и егзимплифицирана во анализираниот контекст за да се согледа референцијалната корелираност на безбедноста, безбедносните појави и нивната поврзаност со критичната инфраструктура, особено, со безбедноста на информациите итн.;
- длабинско согледување на информациите и нивното значење. Издржаноста, веродостојноста и валидноста на самата интерпретација на важни од помалку важни информации несомнено е нејзината генерална слабост изразена во конзистентноста на сопствената интерпретација да ја промовира во крајна цел.

Критичната инфраструктура се соочува со бројни закани и ризици, кои се зголемуваат речиси експоненцијално. Тоа се должи на фактот дека безбедноста на овие мошне значајни, но кршливи системи е ранлива поради опасности од надворешни манипулации. Оттука, современите закани за критичната инфраструктура се постојан предизвик, и аналогно на тоа, зголемувањето на отпорноста на системите на критичната инфраструктура е приоритет не само на операторите, туку и на државата.

Што се однесува до заканите и ризиците врз критичната инфраструктура во урбаните средини, нема дилема дека заканите се директно поврзани со глобалните безбедносни предизвици, вклучувајќи го и современиот тероризам. Оттука, потребно е преземање соодветни чекори во однос на превенција, подготвеност и одговор на терористичките напади врз критична инфраструктура во урбаните средини, што ќе бидат во согласност со Европската програма за заштита на критичната инфраструктура.

Експоненционалната анализа супстанционално потврди дека во заштитата на критичната инфраструктура мора да постои логичен след на активности во кој ќе постојат строго дефинирани правила на игра, а одредувањето на постапките ќе значи: идентификација на критичните точки; создавање на критични мапи со инфраструктура; размена на информации; координаран пристап на постапување. Ова е особено важно ако се знае дека повеќето системи на критична инфраструктура се географски дислоцирани, а сепак, физичката локација на критичната инфраструктура е во непосредна близина меѓусебно. Но, истовремено, тоа подразбира и дека системите на критична инфраструктура се симултано ранливи на нарушување од ист, или последователен регионален настан/инцидент. Во вакви околности, за да се обезбеди потребната функционалност потребен е интегративен пристап со вклучување на: министерствата, агенциите и дирекциите што функционираат во рамките на државата; локалните власти; инфраструктурните оператори; релевантните субјекти кои ги третираат засегнатите критични инфраструктури итн.

Општествата се ранливи поради тоа што силно се потпираат и зависат од соодветното функционирање на сложените и меѓусебно зависни системи на критична инфраструктура. Овие системи може да бидат оштетени и уништени со физички и сајбер-методи. Овие системи се основата на пазарната економија, а компаниите постојано изнаоѓаат решенија за оптимални решенија за квалитетен краен продукт и редукција на трошоците.

Безбедноста на информациите и информациските системи во технолошки сè поразвиениот свет е од примарна важност и веќе претставува висок приоритет на секоја држава. Опасноста од напади на информациските системи и, воопшто, на информациската инфраструктура е постојано присутна, со што се зголемува и веројатиоста да се наруши достапноста, интегритетот, доверливоста или, пак, автентичноста на информацијата која се пренесува. За да се спречи сето ова, се користат безбедносни сервиси кои, користејќи повеќе безбедносни механизми, кои обезбедуваат заштита на информациите во системите базирани на информациските технологии.

Во согласност со нивните утврдени обврски, државите се должни да ги заштитат своите граѓани од надворешни закани од трети страни, вклучително и од терористички организации. Оваа обврска особено се истакнува во заштитата на критичната инфраструктура од вакви видови закани, чие влијание директно се однесува на обезбедувањето витални социетални функции. Обврските и задачите на државата да превенира, спречи и казни вакви видови криминални активности се со цел да се

заштитат човековите права и националната и меѓународната безбедност. Истовремено, со цел да бидат преземени соодветни мерки за превенција на терористички закани, одредени права може да бидат повремено под рестрикции, во согласност со меѓународното хуманитарно право, бегалските права и меѓународните човекови права. Тероризмот, како глобална закана, ја загрозува не само безбедноста на државите поединечно, туку и меѓународната заедница. Сепак, државите се тие кои најсилно ги чувствуваат последиците од нападите врз критичната инфраструктура и вредностите кои се штитат (во смисла загуба на човечки животи, материјална штета, политички импликации, итн.). Ризиците од заканите за критичната инфраструктура се во подем, земјаќи го предвид неизоставниот домино ефект кој произлегува од овие закани за системите на критичната инфраструктура.

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 кои се 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 во однос на критериумите, евалуацијата и веројатноста. Затоа, зголемената улога која ја добиваат безбедносните субјекти претставува дел од генералното интензивирање на безбедносните активности низ општествените сегменти. Овие процеси неретко 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.

2. ДЕФИНИЦИСКО-ПОИМЕН РЕЧНИК

Информациите се дефинираат како корисни податоци за одредена анализа, одлука или задача. Информациите мора секогаш да се соодветно заштитени без разлика на тоа како се чуваат, презентираат или пренесуваат.

Информациски систем е систем со кој се прибираат, снабдуваат, чуваат, обработуваат, прикажуваат и испорачуваат информациите, со цел да бидат достапни и употребливи за секој што има право и потреба да ги користи.

Информатичка и комуникациска технологија (ИКТ) се сите физички уреди и/или средства што се користат за автоматско прибирање, обработка, чување и презентација на информацијата.

Информатичката инфрастуктура ја опфаќа целата информатичка комуникациска опрема во одреден ентитет – државен орган, организација, компанија или друг правен субјект во рамките на кои се создаваат, чуваат и обработуваат информациите.

Критична информациска инфраструктура (КИИ) – е кои било информациско-комуникациски системи чиешто одржување, сигурност и безбедност се критични за националната безбедност, економијата, јавната безбедност и здравјето. Националната критична информациска инфраструктура е дел од критичната инфраструктура (КИ).

Информатичката безбедност на класифицирани информации вклучува интегриран сет на меѓузависни мерки и активности чија цел е да ги заштитат класифицираните информации кои се процесираат во комуникациско-информатичките системи.

Безбедноста на информациите се однесува на заштитата на информациите (приватни и лични податоци) и информативни средства од сите видови на закани, без разлика дали се внатрешни или надворешни, намерни или случајни.

Сајбер-безбедност – претставува активности и мерки за заштита на информациските системи кои го формираат сајбер-просторот од напади, обезбедување доверливост, интегритет и достапност на информации и системи, откривање на напади и сајбер-безбедносни инциденти, активирање на механизми за контраодговор и обновување на системите до состојба во која се наоѓале пред сајбер инцидентот.

Сајбер-војна – акт на војна во и околу виртуелниот простор со средства кои се предоминантно поврзани со информатичката технологија.

Сајбер-закана – потенцијалната причина за инцидент во сајбер-просторот што може да предизвика оштетување на некоја институција или систем.

Сајбер-инцидент – еден или повеќе настани поврзани со сајбер-безбедноста кои предизвикуваат повреда на доверливост, интегритет или достапност на информациите и ја нарушуваат безбедноста на информацискиот систем.

Сајбер-криза – настан или настани во сајбер-просторот кои би можеле да предизвикаат или веќе предизвикале значително нарушување во општествениот, во политичкиот и во економскиот живот во државата. Ваквата ситуација може да влијае на безбедноста на граѓаните, демократскиот систем, политичката стабилност, економијата, животната средина

и другите национални вредности, односно националната безбедност и одбраната воопшто.

Сајбер-криминал – опфаќа противправни активности кои се вршат во сајбер- просторот, односно криминал кој може да се изврши само преку користење на ИКТ уреди и системи, каде што уредите и системите или се користат како средства за извршување на криминал, или се примарни цели на криминалните активности; или криминал овозможен од сајбер-просторот, како што се традиционалните криминални активности и материјали за злоупотреба на деца, што се зголемува со сè поголемото користење на компјутерите, компјутерските мрежи или други форми на информациско-комуникациска технологија.

Сајбер-простор – е простор во кој се остварува комуникацијата помеѓу информациските системи. Оваа дефиниција го опфаќа интернетот и сите информациски системи поврзани со него, како и независни информациски систем.

Сајбер-напад – операции кои лицата и / или информациските системи намерно ги вршат на кое било место во сајбер-просторот со цел да се загрозат доверливоста, интегритетот или достапноста на информативните системи во националниот сајбер- простор.

Сајбер-одбрана – проактивна мерка за откривање или добивање информации во врска со сајбер-упад, сајбер-напад или сајбер-операција или за утврдување на потеклото на операцијата што вклучува инволвирање, превентивна или сајбер-контраоперација против изворот.

Сајбер-отпорност – способноста да се подготви, да се прилагоди, издржи и брзо да се закрепне од пореметувања што произлегуваат од намерни напади, несреќи или природни закани или инциденти во сајбер просторот.

Сајбер-ризик – потенцијален ризик од предизвикување штета со користење на слабости во еден или повеќе информациски субјекти.

Сајбер-саботажа – сајбер-напад насочен против интегритетот и достапноста на ИКТ системите.

Сајбер-шпионажа – сајбер-напад насочен против доверливоста на ИКТ системите.

БИБЛИОГРАФИЈА:

1. Amoroso, E. G., *Cyber Attacks Protecting National Infrastructure*, Elsevier Inc, USA, 2011.
2. Anderson J., *Pew Research Center*, Media Inquiries Washington, 2018.
3. Antunovic B., Varga I, Kralik G, Baban M, Poljak V, Njari B, Pavlovic Z, Mackic S: Racunalna simulacija kao alat za procjenu rizika od teroristickih napada u lancu proizvodnje hrane – *Krmiva* 53 Zagreb 1.
4. Arquilla Johan and David Ronfeldt (eds)., *Transnational Criminal Networks, in Networks and Netwars*, Santa Monica, CA: RAND, 2001.
5. Azmoodeh A, Dehghantanha A, Choo K-KR, Robust malware detection for internet of (Battlefield) things devices using deep Eigenspace learning. IEEE Trans Sustain Comput 1–1, 2018.
6. Baldwin, D., The Concept of Security, *Review of International Studies*, Vol 23, No 1, Aberystwyth, 1997.
7. Barraba V., and Zaltman G., *Hearing the Voice of the Market*, Harvard Business School Press, 1990.
8. Бакрески, О., Драган, Т., Митевски, С., *Корпорациски бебедносен систем*, Комора на Република Македонија за обезбедување лица и имот, Скопје, 2012.
9. Бакрески О. и Милошевиќ М., *Современи безбедносни системи – Компаративна анализа на земјите од Југоисточна Европа*, Аутопринт Т.А., Скопје, 2010.
10. Бакрески О. Милошевска Т. и Алчески Ѓ., *Заштита на критична инфраструктура,* Комора на РМ за приватно обезбедување, Скопје, 2017.
11. Бакрески О., Ахиќ Ј., и Наќ И., *Приватен безбедносен сектор во ЈИЕ*, Комора на РМ за приватно обезбедување, Скопје, 2019.
12. Бакрески О., Данчиќ М., Кешетовиќ Ж. и Митевски С., *Приватна безбедност: теорија и концепт*, Комора на Република Македонија за приватно обезбедување, Скопје, 2015.

13. Бакрески, О., и други: *Безбедноста низ призмата на приватната безбедност. Комора на Република Македонија за приватно обезбедување*. Скопје, 2018.

14. Бузан Б.„*Луѓе, Држави и Страв: Проблемот со националната безбедност во меѓународните односи"*; Академски печат; Скопје, 2010.

15. Beraković, M., *Voda-vječna tajna prirode*, Zagreb, Antibarbarus, 2015.

16. Blomstrom Magnus, Hettne Bjorn, *Development Theory in Transition: The Dependency Theory and Beyond -Third World Responses*, Zed Books, London, 1998.

17. Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era*, Second Edition, Lynne Riener Publishrs, Boulder, Colorado, 1991.

18. Buzan, B., Waever, O., and de Wilde, J.: *Security: A New Framework for Analysis*, Lynne Rienner Publishers, London, 1998.

19. Čaleta, D., Radović, S.: *Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection*. Belgrade, IOS Press, 2015.

20. Čelebić, G. i Rendulić, D., I.: *ITdesk.info – načrtovanje računalniškega e-izobraževanja s prostim dostopom* - Priročnik za digitalne pismenosti, Zagreb, 2012.

21. CJ Asberg and P Wallensteen, "New Threats and New Security: The Post-Cold War Debate Revisited", in Peter Wallensteen (ed.), *Preventing Violent Conflicts: Past Record and Future Challenges*, Uppsala: Uppsala University, 1998.

22. Ванковска Б., *Меѓународна безбедност – критички пристап*, Филозофски факултет, Скопје, 2011.

23. Conception de la sécurité, Série d`études 14, Publication des Nations Unise, 1986.

24. Conti M, Dargahi T, Dehghantanha A, *Cyber threat intelligence: challenges and opportunities*. Springer, Cham, 2018.

25. Conti M, Dehghantanha A, Franke K, Watson S , Internet of things security and forensics: challenges and opportunities. *Futur Gener Comput Syst*, 2017.

26. Conway, M. et al.: *Terrorist's Use of the Internet: Assessment and Response*. Dublin, IOS Press, 2017.

27. Cox, L., A.: *Breakthroughs in Decision Science and Risk Analysis*. John Wiley & Sons Inc., 2015.

28. Critical Infrastructure Security and Protection The Public-Private Opportunity- White Paper and Guidelines by CoESS And its Working Committee Critical Infrastructure December, 2010.

29. Curran, K., Al-Masri, A.: *Smart Technologies and Innovation for a Sustainable Future.* Proceedings of the 1st American University in the Emirates. Dubai, Springer, UAE, 2017.

30. Danchev, Dancho, *Coordinated Russia Vs Georgia Cyber Attack In Progress* | Zdnet, Zdnet, 2008.

31. Dannreuther R. "*International Security; the contemporary agenda*", Polity Press, Cambrige, 2007.

32. Das, K., S., et al.: *Handbook on Securing Cyber-Physical Critical Infrastructure. Foundations and Challenges*. Elsevier, Waltham, MA, USA, 2012.

33. Dawson, M., et al.: *Developing Next Generation Countermeasures for Homeland Security Threat Prevention*. IGI Global, 2016.

34. Dimitrijević, V., *Pojam bezbednosti u međunarodnim odnosima*, Savez udruženja pravnika Jugoslavije, Beograd, 1973.

35. Dimitris Gritzalis, Marianthi Theocharidou, George Stergiopoulos (ed), *Critical Infrastructure Security and Resilience Theories, Methods, Tools and Technologies*, Springer Nature Switzerland AG, 2019.

36. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union.

37. Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption. 7 June 2017. Council of the European Union. 9916/17.

38. Edwards, M.: Critical Infrastructure Protection. NATO Advanced Workshop on Critical Infrastructure Protection. Ankara, IOS Press, 2012.

39. Energy Sector-Specific Plan, 2015, стр. VII.

40. EU Council Directive 2008/114/EC, Article 2(d).

41. EU Council Directive 2008/114/EC, Article 9.

42. European Network and Information Security Agency – ENISA (2009). European Union Ministerial Conference on Critical Information Infrastructure Protection, Tallinn.

43. EUROPOL, The Interent Organised Crime Threat Assessment, Hague, Netherlands, 2015.

44. Fagerström, A.: *Creating, Maintaining and Managing an Information Security Culture, Information and Media Technology*, ARCADA, 2013.

45. Fancy Bear, Strontium, Pawn Storm, Sofacy, Sednit, Tsar Team. Lemay A, Calvet J, Menet F, Fernandez J., M. Survey of publicly available reports on advanced persistent threat actors. *Comput Secur* 72: 2018.

46. Fischer, D., *Nonmilitary Aspects of Security: A System Approach*, Aldershot: United Nations Institute for Disarmament Research, 1993.

47. Fischer, J.R., Halibozek E. and Green G., *Indroduction to Security*, Elsevier Inc., New York, 2008.

48. Fruhlinger, J.: What Is Stuxnet, Who Created It And How Does It Work, 2017.

49. Gackowski, J. Zbigniew - „Subjectivity Dispelled: Physical Views of Information and Informing*", Informing Science: the International Journal of an Emerging Transdiscipline* Vol.13, California, 2010.

50. Gallie W.B., Essentially contested concepts, *Proceedings of the Aristotelian Society,* 56, 1956.

51. Garver, E.: Rhetoric and Essentially Contested Arguments, *Philosophy and Rhetoric,* Vol.11, No.3, (Summer 1978).

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

53. Global Business Expansion: Concepts, Methodologies, Tools and Applications. Information Resources Management Association, USA. IGI Global, 2018.

54. Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005, COM, (2005), 576 final, Annex II.

55. Johnson Brian, *Principles of Security Management,* Pearson Prentice Hall, New Jersey, 2005.

56. Haddad Pajouh H, Dehghantanha A, Khayami R, Choo KKR. (2017), A deep recurrent neural network based approach for internet of things

Malware threat hunting, future generation computer system. *Futur Gener Comput Syst* 85.

57. Hafner, G.: Certain Issues of the Work of the Sixth Committee at the Fifty-Sixth General Assembly, *The American Journal of International Law*, Vol. 97, No. 1, Cambridge University Press, 2003.
58. Haughey H, Epiphaniou G, Al-Khateeb H, Dehghantanha A., *Adaptive traffic fingerprinting for darknet threat intelligence*, vol 70, 2018.
59. Hewedy Amin, *Militarization and Security in the Middle East*, Printer Publishers, London 1989.
60. Herold Rebecca, *Managing an Information Security and Privacy Awareness and Training Program*, Press, Inc. Boca Raton, 2010.
61. Правна рамка за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Стеда графика, Скопје, 2016.
62. Hopkins M, Dehghantanha A., Exploit kits: the production line of the cybercrime economy? In: 2015 second international conference on Information Security and Cyber Forensics, 2015.
63. Horić A., *Informacija – Povijest jednog pojma - O Capurrovom razumijevanju pojma informacije,* Zagreb, 2007.
64. Ian Loader and Neil Walker, *Civilizing Security*, Cambridge: Cambridge University Press, 2007.
65. *Infosecurity Magazine*. Destructive Cyber-Attacks Blitz Critical Infrastructure – Report, 2015.
66. Jovanović S. Milovanović S. Mandić J. i Jovović S., Sistemi zdrastvene zastite, *Engrami,* vol. 37 januar-mart 2015.
67. Jusufranić,I., *Osnove drumskog saobracaja*, Tehnologija – Organizacija– Ekonomika – Logistika – Upravljanje, Травник, 2007.
68. K. Roer. *Build a Security Culture*, IT Governance Publishing, United Kingdom, 2015.
69. Kaspersky Lab., Red October: an advanced cyber-espionage campaign targeting diplomatic and government institutions, 2013.
70. Kissel R. (ed.), *Glossary of Key Information Security Terms, 2011.*

71. Korkali, M.; Veneman, J.G.; Tivnan, B.F.; Bagrow, J.P.; Hines, D.H. *Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependence*. Sci. Rep. 2017.

72. Kruszka, L., et al.: *Critical Infrastructure Protection. Best Practices and Innovative Methods of Protection*. NATO Science for Peace and Security Series D: Information and Communication Security. Vol. 52. IOS Press, 2019.

73. Klaić, Z., S. Mandžuka, P. Škorput, Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama, 18. *Telekomunikacioni forum Telfor*, Beograd, 2010.

74. Klemen, Groselj, *Critical Infrastructure Protection and the Energy Sector Counter – Terrorism Challenges regarding the Processes of Critical Infrastructure*. Ljubljana, September, 2011.

75. Kostadinov, Venceslav, *"Vulnerability Assessment. New Nuclear Power Plants Universal Methodology for Terrorism Threats and Natural Disasters Analyses and Predictions*", in Denis Caleta, Paul Shemella, Iztok Podbregar, Branko Lobnikar, Ljubljana. Institute for Corporative Studies-ICS, Monterey. Center for Civil-Military Relations, 2011.

76. Kostić, V., *Zapalive I druge opsne materije*, Udruzenje publicista Beograd, 1980.

77. Krajcar, S., *Energetska sigurnost i kritčna infrastruktura.* Sveučiliše u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb 2009.

78. Lazari, A.: *European Critical Infrastructure Protection*. Springer International Publishing Switzerland, 2014.

79. Leach, J., 'Improving user security behavior', *Computers & Security*, vol. 22, no. 8, 2003.

80. Lichfield, John, TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link, Independent, London, United Kingdom, 2015.

81. Stajić Lj., Mijalković, S. Stanarević S., *Bezbednosna kultura mladih: kako živeti bezbedno*, Draganić, Beograd, 2006.

82. Lopez, J., et al.: *Critical infrastructure Protection: Advances Information Infrastructure Models, Analysis and Defense*. Springer, Verlag, Berlin, Heidelberg, 2012.

83. Lopez, J., Setola, R., Wolthusen, S., *Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defense*, Springer, 2012.

84. Losee, M. Robert - „A Discipline Independent Definition of Information" – *Journal of the American Society for Information Science* 48, Chappel Hill, 1998.

85. Luard, E., *Basic texts in International Relations*, St. Martin's Press, New York, 1993.

86. Luiijf, E, *Understanding Cyber Threats and Vulnerability*. Researchgate, 2017.

87. Lundborg, T., Vaughan-Williams, N., Resilience, Critical Infrastructure and Molecular Security: the Excess of Life in Biopolitics, *International Journal Political Sociology*, vol. 5, no. 4, 2011.

88. Mahon T., Cyber - the 21st Century Threat, *Military Technology*, Vol. 39 Issue 5, 2015.

89. Makwana R., *Multinational corporations: Beyond the profit motive*, 2006.

90. Management of Defence, Democratic and Civilian Control, Including Integration of Security Sector, 2010.

91. Mangold, P., *National Security and International Relationsm*, Rotledge, London and New York, 1990.

92. Marion Kelt, *SMILE by Imperial College*, Glasgow Caledonian University, 2018.

93. Martin van Creveld. *The Transformation of War*, New York, NY: The Free Press, 1991.

94. Martins A. & Eloff J., 'Information Security Culture', MA Ghonaimy (ed.), *Security in the Information Society: Vision & Perspectives*, Kluwer Academic, 2002.

95. Masleša R., *Teorije i sistemi sigurnosti*, „Magistrat" Sarajevo, 2001.

96. Mayre, D., *Voda od nastanka do upotrebe*, Zagreb, Prosvjeta, 2004.

97. Metscher, Robert and Gilbride, Brion - „Intelligence as an Investigative Function", International Foundation for Protection Officers, 2005.

98. Michael Genser, *A Structural Framework for the Pricing of Corporate Securities: Economic and Empirical Issues*, Springer-Verlag New York, LLC, 2005.

99. Michael Kenney, When Criminals Outsmart the State: Understanding the Learning Capacity of Colombian Drug Trafficking Organizations, *Transnational Organized Crime* 5/1, 1999.

100. Mikulandra A., 22. ožujka obilježavamo Svjetski dan voda, Osnovna škola Čazma, 2014.

101. Miletiћ S., *Policijsko pravo*, Policijska akademija, Beograd, 1997.

102. Min M, Xiao L, Xie C, Hajimirsadeghi M, Mandayam NB., Defense against advanced persistent threats: a Colonel Blotto game approach. In: 2017 IEEE international conference on communications (ICC), 2017.

103. Mitnick, K & Simon, WL. The art of deception: controlling the human element of security, Indianapolis: Wiley Publishing, 2002.

104. Milanović, Zoran, Radovan Radovanović. Informaciono-bezbednosna kultura-imperativ savremenog drustva, *Nauka, bezbednost, policija*, Vol. 20, iss.3, Kriminalisticko-policijska akademija, Beograd, 2015.

105. Monge, Peter, Janet Fulk. *Shaping Organizational Form: Communication, Connection, and Community*, Thousands Oaks, Sage, 1999.

106. Mostashari, A.: An introduction to Non-Governmental Organizations (NGO) Managemanent – Compliled by– Indian Studies Group at MIT, June 2005.

107. Moteff, J., Parfomak, P., *Critical Infrastructure and Key Assets: Definition and Identification*, Congressional Research Service, the Library of Congress, 2004.

108. Nart Villeneuve, David Sancho, The LURID Downloader, Trend Micro Labs, 2011.

109. National Critical Infrastructure and Key Resources, Cansas City Regional Tew, Interagency Analisys Center.

110. New EU cyber platform to boost cyber security capabilities across Europe. European Union External Action Service, 2018.

111. Norbert Wiener. *Cybernetics: or Control and Communication in the Animal and the Machine*, MIT Press, USA, 1965.

112. Nyamuya Maogoto, Jakson Sheehy Benedict, *Private Military Companies & International Law: Building New Leaders of Legal Accountability & Responsibility*, 2009.

113. Paunović Ž., Nevladine organizacije, *JP Službeni glasnik*, Beograd, 2006.

114. Pescaroli, G. and Alexander, D.:Critical infrastructure, anarchies and the vulnerability paths of cascading disasters, *Nat. Hazards*, vol. 82, no. 1, 2016.

115. Pindar J., Rigelsford J. *Cyber security and Information Assurance, The University of Sheffield, 2011.*

116. Post R.S., *Security Administration: An introduction*. Cincinnati: Anderson, 1970.

117. Pursiainen, C. Critical infrastructure resilience: A Nordic model in the making? *Int. J. Disaster Risk Reduction*, 2018.

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

119. Reid, Peter, *How to Land a Top-Paying Corporate securities research analysts Job*, Emereo Pty Ltd, 2012.

120. Rinaldi, S., Peerenboom, J., Kelly, T., „Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies“, *IEEE Control Systems Magazine*, Vol. 21, No. 6, 2001.

121. Rosenau, James, *Turbulence in World Politics*, Princeton, NJ: Princeton University Press, 1990.

122. Sandler, Todd, Daniel G. Arce and Walter Enders, An Evaluation of Interpol's Cooperative-Based Counterterrorism Linkages, *The Journal of Law & Economics* Vol. 54, No. 1, Cambridge University Press, 2011.

123. Schmid, P. Alex; Jongman, Albert J., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Amsterdam: North-Holland Publishing Company, 1988.

124. Sills L.David, Merton K. Robert (eds), *Internacional Encyclopedia of the Social Sciences,* vol.XI, MacMillan Publishing Company, New York 1968.

125. Škuliħ Milan, *Organizovani kriminalitet*, Dosije, Beograd 2003.

126. Slaveski S., *Bezbednosen sistem*, Evropski univerzitet, Skopje, 2009.

127. Paoli Letizia, Fijnaut Cyrille, „Organised Crime in Europe: General Introduction“, in: Paoli Letizia, Fijnaut Cyrille (eds.), *Organised Crime in Europe: Manifestations and Policies in the European Union Beyond*, Springer, Dordrecht NL, 2003.

128. Stallings William, *Network and Internetwork Security – Principles and Practices*, Prentice Hall, Englewood Cllifs, New Jersey 1995.

129. Stamper, A., Versuch einer sicherheits-analytischen Bewertung der inneren Konfliktsituationen in unserer Zeit, *Kriminalistik,* 2/1981.

130. Steele, W.E.; Hussey, K.; Dovers, S. What´s Critical about Critical Infrastructure? *Urban Policy Res*. 2017.

131. Stevens T. Contemporary Security Policy A Cyberwar of Ideas? Deterrence and Norms in Cyberspace, *Contemporary Security Policy*, Vol.33, No.1. 2012.

132. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the White House Washington February 2003.

133. Thomas A. Johnson (ed). *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare,* CRC Press, 2015.

134. Thomas C Shelling, Arms and influence, New Haven CT: Yale University Press, 1967.

135. Ulich, E. Arbeitspsychologie, vdf Hochschulverlag an der ETH Zürich, 2001.

136. UN (United Nations). World Urbanization Prospects: The 2018 Revision, Key Facts. 2018.

137. United Nations Development Program, Human Development Report 1993, Oxford University Press, New York.

138. Ursic H.S. and Pagano L.E., *Security Management systems*: illinous, Charlies C.Thomas, 1974.

139. Ussath M, Jaeger D, Cheng F, Meinel C (2016), Advanced persistent threats: behind the scenes.In: 2016 Annual Conference on Information Science and Systems (CISS).

140. Van Niekerk, JF & Von Solms, R. ‘Information security culture: A management perspective’, *Computers and Security*, vol. 29, no. 4. 2010.

141. Vebster's New international dictionary, second edition 1934.

142. Alibabić V. Mujić I., *Pravilna prehrana i zdravlje, Veleučilište, Rijeka, 2016.*

143. Von Solms, B. 'Information security – the third way?', *Computers and Security,* vol. 19, no. 7. 2000.

144. Nicholson, A, Webber, S, Dyer, S, Patel, T & Janicke H., SCADA security in the light of Cyber-Warfare, *Computers and Security*, vol. 31. no. 4, 2012.

145. Vreg F., *Demokratsko komuniciranje*, NUB BiH, Sarajevo, 1991.

146. Vukadinović R., *Teorije o međunarodnim odnosima*, Zagreb, 1978.

147. Walker-Roberts S, Hammoudeh M, Dehghantanha A. (2018), *A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure.*

148. Wilkinson, Paul, The media and terrorism: a reassessment, *Terrorism and Political Violence*. 1997.

149. Williams Phil, Non-*State Threats and Future Wars*, in Robert J. Bunker (eds), Frank Cass & Co. Ltd, 2003.

150. Williams Paul, *Security Studies: An Introduction*, Routledge, 2008.

151. Wilson R. J. The Shadowy World Of Cyber Warfare, *Military & Aerospace Electronics*, Vol. 27, Issue 12. 2016.

152. Wilson, C., Botnets. *Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* 2008.

153. Withman E. M., Mattord J. H. *Principles of Information Security, Fourth Edition, Course Technology, Cengage Learning, Boston. 2011.*

154. Zoli, C.; Steinberg, L.J.; Grabowski, M.; Hermann, M. Terrorist critical infrastructures, organizational capacity and security risk. *Saf. Sci.* 2018.

155. Zorić D., *Privatna bezbednost razvijenih i zemalja u tranziciji*, Fakutet za bezbednost i zastitu, Banja Luka.

156. Виоти, П. Каупи, М. *Меѓународни односи и светска политика. Безбедност, економија, идентитет*, Скопје, Академски печат, 2009.

157. Вукадиновиќ, Р., *Нови проблеми сигурности у европи, Међународна политика*, Београд, 1991.

158. Ејдус Ф., *Међународна безбедност: теорије, сектори и нивои,* Службени гласник, Београд, 2012.

159. Здравковски Б., *Сообраќајна инфраструктура*, Скопје, 2010.

160. Зиков М., Милевски И., *Практикум по климатологија*, 2001.

161. Ивановски, З., Ангелески, М., *Безбедносни системи*, Европски универзитет, Скопје, 2005

162. Игтон Тери, *Идеологија*, Темплум, Скопје, 2005.

163. Јасмин Калач. Сајбер тероризмот како закана кон безбедноста на државата, *Правдико*, 2017.

164. Jakovljević V., Gačić J., Zastita kriticne infrastructure u kriznim situacijama, 2012.

165. Jarlsvik, H., Castenfors, K., *Security and Preparedness in the EU*, Stockholm, 2004.

166. John Sullivan, *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*, John Wiley & Sons, Inc., 2007.

167. Johnson, A. Thomas (ed.), *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015.

168. Jurišić, D., *Critical Infrastructure Protection in Bosnia and Herzegovina and the Role of Military*, 2013.

169. Јованов, Д. Ј., Џон Лок и право на отпор, во Зборник радова Правног факултета у Новом Саду, Правни факултет у Новом Саду, Нови Сад, 2015.

170. Lok, Dž., *Dve rasprave o vladi*, Knjiga 2, Beograd, 1978.

171. Клајд Вилкокс и Барбара Норандер, *Разбирање на јавното мислење, Вашингтон*, 2002.

172. Мала политичка енциклопедија, Савремена администрација, Београд, 1966.

173. Милиќ Д., Биотероризам и употреба биолошког оружја – Центар за безбедносне студије, *Ревија за безбедност* - стручни часопис о корупции и организованом криминалу, Београд, број 2, 2010.

174. Милошевска Т. *Модели на поврзаност на тероризмот и на транснационалниот организиран криминал*, Универзитет Св. Кирил и Методиј, Филозофски факултет, МАР-САЖ Скопје, 2016.

175. Милошевска Т., *Глобален тероризам,* Филозофски факултет, Мар-Саж, Скопје, 2018.

176. Мишевски Д, Осигурување од сајбер ризици, Осигурување, Национално биро за осигурување-Македонија, бр.11, Скопје, 2017.

177. Мојаноски, Ц, За поимот наука за безбедноста, *Годишник на Факултетот за безбедност*, Скопје, 2010.

178. Петровић, Р, С. *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007.

179. Поповска З., *Управување со системите*, Економски факултет, Скопје, 2006.

180. Попоска. В. Меѓународно-правни аспекти за заштита на критичната инфраструктура од современи безбедносни закани, Универзитет „Гоце Делчев“, Штип, 2019.

181. 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.

182. Савић А., *Национална безбедност*, Криминалистичко-полицијска академија, Београд, 2007.

183. Смилевски В., *Новинарски лексикон*, Матица Македонска, Скопје, 2001.

184. Спасески, Ј., Аслимоски, П., Безбедност одбрана мир, Институт за истражување на туризмот, Факултет за туризам и угостителство, Охрид, 2001.

185. Стајић Љ. и Гаћиновић Р., *Увод у студије безбедности*, Драслар партнер, Београд, 2007.

186. Стојановић П., Теорија привредног развоја у мрежој технолошкој револуции, *Савремена Администрација*, Београд,1964.

187. Thomson, K.L., von Solms, R., Louw, L. (2006). *Cultivating an organizational information security culture*. Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa.

188. Темјановски Р., *Транспортните коридори: предизвици и ограничувања во економскиот развој,* 2012.

189. Угриновска Н., Б*езбедносни мерки за заштита на лични податоци,* Дирекција за заштита на личните податоци, Пропоинт, Скопје, 2018.

190. Урсула Д.: Што е информација, во весник Московo универзитета, Сериа информатика, бр.2.1971.

191. Хаг, Р., Хароп, М., *Компаративна анализа на власта и политиката*, Академски печат, Скопје, 2009.

192. Чековиќ Т., *Повеќедимензионалните придобивки и ефекти од пристапувањето кон НАТО*, Институт за Европска Политика-Скопје, Релатив, 2018.

193. Џ. Бејлис., С.Смит., П.Овенс., *Глобализација на светската политика. Вовед во меѓународни односи*, Скопје, Табарнакул, 2009.

194. Čaleta, D., Radović, S., *Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection*. Belgrade, IOS Press, 2015.

195. Conway, M. et al., *Terrorist's Use of the Internet: Assessment and Response.* Dublin, IOS Press, 2017.

196. Curran, K., Al-Masri, A., Smart Technologies and Innovation for a Sustainable Future. Proceedings of the 1st American University in the Emirates. Dubai, Springer, UAE, 2017.

197. Das, K., S., et al., *Handbook on Securing Cyber-Physical Critical Infrastructure. Foundations and Challenges.* Elsevier, Waltham, MA, USA, 2012.

198. Edwards, M., *Critical Infrastructure Protection. NATO Advanced Workshop on Critical Infrastructure Protection*. Ankara, IOS Press, 2012.

199. Hokstad, P., Utne, B., I., Vatn, J, *Risk and Interdependencies in Critical Infrastructures. A Guideline for Analysis*. Springer, Verlag-London, 2012.

200. Lazari, A, *European Critical Infrastructure Protection*. Springer International Publishing Switzerland, 2014.

201. Hokstad, P., Utne, B., I., Vatn, J, *Risk and Interdependencies in Critical Infrastructures. A Guideline for Analysis.* Springer, Verlag-London, 2012.

ИНТЕРНЕТ ИЗВОРИ

1. http://www.uoregon.edu/~joe/ddos-exec/ddos-exec.pdf.
2. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/174
3. https://www.sciencedirect.com/science/article/pii/S0951832019305356
4. http://lnu.diva-portal.org/smash/get/diva2:434613/ FULLTEXT01.pdf.
5. https://arxiv.org/ftp/arxiv/papers/1904/1904.01551.pdf
6. https://www.nics.uma.es/pub/seciot10/files/pdf/ghani_seciot10_paper.pdf
7. https://edition.cnn.com/2018/10/03/uk/uk-russia-cyber-attacks-intl/index.html.
8. https://books.google.mk/books?id=IMPMBQAAQBAJ&pg=PA79&dq=critical+infrastructure+definition&hl= ge&q=critical
9. https://www.cisecurity.org/cyber-pledge/tools.cfm
10. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf
11. http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=
12. https://www.aeso.ca/assets/Uploads/ARS-CIP-Compliance-Oct-25-2017-Final.pdf
13. http://ec.europa.eu/information_society/ policy/nis/strategy/activities/ciip/index_en.htm
14. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMCon tent?
15. https://www.dhs.gov/cisa/critical-infrastructure-and-key-resources-support-annex
16. https://www.nato.int/cps/en/natohq/topics_168104.htm?
17. https://ehs.unu.edu/research/critical-infrastructures-resilience-as-a-minimum-supply-concept-kirmin

18. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx
19. https://www.cpni.gov.uk/critical-national-infrastructure
20. https://www.nato.int/cps/en/natohq/ official_texts_133177.htm
21. https://www.nato.int/cps/en/natohq/topics_78170.htm.
22. https://www.merriam-webster.com/dictionary/cybersecurity
23. http://hachhst.com/technical-library
24. http://www.dodccrp.org/files/Alberts_UIAW.pdf
25. http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html.
26. http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolovmodern-trends-sofia-oct-08.pdf.
27. https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure
28. https://www. enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/ european-public-private-partnership-for-resilience-ep3r
29. https://www.researchgate.net/publication/257391861_System-of-systems_approach_for_interdependent_critical_infrastructures
30. http://resources.infosecinstitute.com/human-factors-informationsecurity-management-systems.
31. https://www.sciencedirect.com/topics/computer-science/critical-infrastructure-and-key-resource
32. https://www.sciencedirect.com/topics/computer-science/critical-infrastructure-protection
33. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01- 2018-PDF-E.pdf.
34. http://folk.ntnu.no/jvatn/pdf/FrontMatter.pdf
35. Holland, G., Assessing Hurricane Impacts, Willis Research Network and National Center for Atmospheric Research, достапно на: http://www.willisresearchnetwork.com/lists/publications/Attachments/55/WRN_Princeton_March%2009_Holland.pdf, accessed May 20, 2016.
36. http://ec.europa.eu/finance/general-policy/index_en.htm
37. http://studenti.mojsajt.rs/uploads/20177/documents/1_deoishrana.pdf

38. http://www.batut.org.rs/download/aktuelno/briga%20o%20zdravlju/Bolesti%20koje%2.
39. http://www.inst-antonatrstenjaka.si/gerontologija/slovar/1029.html
40. http://www.iph.mk/svetski-den-na-vodata-2015-vodata-i-odrzliviot-razvoj
41. http://www.merriam-webster.com/dictionary/critical
42. http://www.pilar.hr/kritina-infrastruktura-u-hrvatskoj#sadržaj
43. https://bonpet.ifixit.hr/klasifikacija-pozara
44. https://borefor.wordpress.com/2011/05/24/hemijska-industrija/
45. https://faktor.mk/shto-e-vsushnost-zemjotresot-i-kako-se-meri/
46. https://medicalcg.me/zdravstveni-sistem-u-crnoj-gori-realnost-i-perspektive/
47. https://net.hr/danas/svijet/elementarne-nepogode-sve-ih-je-vise-i-sve-su-skuplje/
48. https://www.dhs.gov/information-technology-sector
49. https://www.forbes.com/sites/niallmccarthy/2017/08/31/private-security-outnumbers-the-police-in-most-countries-worldwide-infographic/#219af810210f
50. https://www.moore-serbia.rs/sectors/sample-sector-(7)
51. https://www.osce.org/me/montenegro/282436?download=true
52. https://www.researchgate.net/publication/5223115
53. https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.
54. https://www.znanje.org/i/i25/05iv02/05iv0210/zemljotresi%201.htm
55. https://www.zzjzfbih.ba/svjetski-dan-voda-voda-i-energija/
56. http://ict4peace.org/wp-content/ uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes-2.pdf
57. https://www.cisa.gov/infrastructure-security
58. https://www.britannica.com/topic/input-output-analysis
59. http://www.globalresearch.ca/the-role-of-private-military-and-security-companies-in-modern-warfare/32307

60. http://media.kaspersky.com/en/ business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_ web.pdf.
61. http://resources.infosecinstitute.com/human-factors-informationsecurity-management-systems.
62. https://books.google.mk/books?id=1f6qDQAAQBAJ&pg=PA249&dq=critical+infrastructure+traffic&hl=en&sa=X&ved=0ahUKEwjw
63. http://www.csis.org/tech/070615 cyber attacks.pdf.
64. https://www.unisdr.org/files/66506_f415finallewisandpetitcriticalinfra.pdf
65. https://traffic.fpz.hr/index.php/PROMTT/article/view/3106
66. https://www.igi-global.com/book/handbook-research-civil-society-national/129591
67. http://www.infosecwriters.com/text_resources/pdf/Improving_Security_from_the_Inside_Out_ NSI.pdf
68. http://www.nbcnews.com/tech/security/critical-infrastructurevulnerable-cyberattacks-says-eugene-kaspersky-n379631.
69. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
70. https://pdfs.semanticscholar.org/6c17/b35ec7555a9f27d5ccb6ca1d357a20b5ce0a.pdf
71. www.osce.org/atu/103500?download=true
72. www.osce.org/secretariat/cyber-security.
73. https://s3.amazonaws.com/academia.edu.documents/39898015/2014_Review_on_modeling_and_simulation_of_interderpendent_critical_infrastructure_systems.pdf?response-content-disposition=inline
74. http://www.telegraph.co.uk/news/worldnews/asia/japan/8377506/Japan-earthquake-nuclear-disaster-feared-after-power-plant-explosion.html.
75. https://www.osti.gov/servlets/purl/1400396
76. https://www.dhs.gov/cisa/protecting-critical-infrastructure
77. http://go.recordedfuture.com/hubfs/data-sheets/ics-scada.pdf
78. https://ec.europa.eu/echo/sites/echo-site/files/recipe_guidelines.pdf
79. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.2276&rep=rep1&type=pdf

80. http://article.nadiapub.com/IJCA/vol1_no1/3.pdf
81. http://www.wbrc.rs/wp-content/uploads/2012/11/Pojmovnikbezbednosne-kulture-grupa-autora-2009.pdf.
82. https://www.nato.int/cps/en/natohq/topics_57954.htm.
83. https://www.thalesgroup.com/en/activities/security/critical-infrastructures
84. https://www.stratfor.com/analysis/examining-islamic-states-cyber-capabilities
85. https://www.hsdl.org/?abstract&did=805457
86. https://www.thelocal.dk/20190902/denmarks-rail-ticket-system-targeted-in-digital-attack
87. https://www.mprest.com/blog/item/the-need-for-an-intelligent-grid-management-system-of-systems-part-2
88. http://www.trendmicro.com/cloud-content/us/pdfs/securityintelligence/reports/critical-infrastructures-west-hemisphere.pdf.
89. http://www.tripwire.com/state-of-security/securitydata-protection/security-controls/cyberterrorists-attack-on-criticalinfrastructure-could-be-imminent/.
90. http://www.brooklyn.cuny.edu/web/aca_centers_casegk12/MuirWebDescriptionExamples.pdf
91. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
92. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
93. https:// ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf.
94. https://www.forcepoint.com/cyber-edu/cybersecurity
95. https://digitalguardian.com/blog/what-cyber-security
96. https://www.next-kraftwerke.com/knowledge/derms
97. https://www.weforum.org/events/world-economic-forum-annual-meeting-2016/sessions/the-internet-of-thingsis-here/
98. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf
99. www.uscert.gov/ncas/alerts/TA17-293A

100. www.dbki.gov.mk

101. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786

102. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

103. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pd

104. http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_3-2015/67-2015-3-14-Skero.pdf

105. https://www.igi-global.com/book/handbook-research-civil-society-national/129591

106. https://www.nato.int/lisbon2010/strategic-concept-2010- eng.pdf.

107. http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf