УНИВЕРЗИТЕТ „СВ.КИРИЛ И МЕТОДИЈ“
ФИЛОЗОФСКИ ФАКУЛТЕТ – СКОПЈЕ

Институт за безбедност, одбрана и мир

Последипломски студии од областа на корпоративна безбедност и безбедносен менаџмент

Магистерски труд

Сајбер напади како закана за критичната информациска инфраструктура

Ментор:
Проф. д-р Тања Милошевска

Изработил:
Ратко Стефковски
индекс: 5272/19

Скопје, 2021 година

Содржина

1. Вовед

1.1 Проблем на истражување

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

Нападите насочени кон критичната инфраструктура, без разлика дали позади нив стојат политички, верски, сепаратистички или други видови организации или станува збор за тероризам, индустриска шпионажа, хакерски напади, претставуваат едни од најопасните глобални закани кои ја пратат денешницата. Новите облици на загрозување кои произлегуваат од сé 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 националната безбедност.[1]

Реалноста е дека сајбер-проблемите се исто толку важни како и други 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 критична воена инфраструктура, покажувáќи ја стратегиската важност на технолошката еволуција во сајбер-просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.

„Театарот" за закани сé 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

[1]Милошевска, Т. *Глобален тероризам*, Универзитет Св. Кирил и Методиј, Филозофски факултет-Скопје, Мар-Саж, Скопје, 2018.

и странската сопственост на критични инфраструктури истотака се дополнителни фактори кои ја зголемуваат ранливоста на критичната инфраструктура.[2]

Управувањето и функционирањето на критичните инфраструктурни системи ќе продолжи да зависи од сајбер-информациските системи и електронските податоци. Потпирањето на електричната мрежа и телекомуникациите, истотака, 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.[3]

Критичната инфраструктура станува сè повеќе автоматизирана и меѓусебно поврзана, а со тоа се воведуваат нови слабости во однос на дефектна опрема, 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.[4] Заради тоа, критичката 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.[5]

За превенција на вакви и слични напади на националната критична инфраструктура, било тоа да е физички или сајбер-напад, секоја држава треба да има стратегиски план за превенција, брз одговор и брзо отстранување на последиците, и враќање во нормален работен тек на нападнатата критична инфраструктура, што опфаќа:процена на слабостите што би довеле до физички или сајбер-напад;план за отстранување назначајните слабости; развивање системи за идентификување и спречување на обидите за напад; сигнализација за евентуален

[2] EUROPOL. *The Interent Organised Crime Threat Assessment*, Hague, Netherlands, 2015.
[3]*NBC News*. Critical Infrastructure Is Vulnerable to Cyberattacks, Says Eugene Kaspersky, 2015, достапнона:http://www.nbcnews.com/tech/security/critical-infrastructurevulnerable-cyberattacks-says-eugene-kaspersky-n379631.
[4] Kaspersky, Cyberthreats to ICS Systems, 2014, достапнона: http://media.kaspersky.com/en/ business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_ web.pdf.
[5] Tripwire. Cyberterrorists Attack on Critical Infrastructure Could be Imminent, 2015, достапнона: http://www.tripwire.com/state-of-security/securitydata-protection/security-controls/cyberterrorists-attack-on-criticalinfrastructure-could-be-imminent/.

напад и отпорна нападот и обновување на работните способности на нападнатиот систем од критичната инфраструктура.[6]

Земајќи ги предвид анализите направени од најрелевантните светски институции во доменот на безбедноста и одбраната, несомнено е дека во последните години сајбер заканите се меѓу најзначајните безбедносни закани врз современите општества, што е основна причина истите да се третираат како интегрален дел од националната и меѓународната безбедност.

1.2 Предмет на истражување

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 критично информацискатa структура. Притоа, може да се очекува различен пристап, од предизвикување на непосредни прекини во функционирањето на делови од критичната инфраструктура до целосно блокирање.[7]

Критичните инфраструктури во својот развој сè повеќе користат информациони технологии, со оглед на тоа дека тие стануваат достапни на пошироката јавност. Како резултат на интензивното користење информатички технологии од страна на разни сектори, доаѓа до формирање голема меѓузависност меѓу различните инфраструктурни сектори. Во тој контекст, особено е забележителна и значајната зависност на речиси сите инфраструктурни сектори од информационите технологии (што прераснаа во еден критичен, а најверојатно и најкритичен инфраструктурен сектор). Оттука постоењето голема меѓу поврзаност

[6]Бакрески, О, Милошевска, Т, Алчески Ѓ. *Заштита на критична инфраструктура*, Комора на Република Македонија за приватно обезбедување, Стеда-графика, Скопје, 2017.
[7]Национална стратегија за сајбер безбедност на Република Македонија 2018-2022, Верзија 1,2, Министерство за информатичко општество и администрација, Министерство за внатрешни работи и Министерство за одбрана, јули 2018.

на инфраструктурата е еден од најголемите проблеми воуправување со инфраструктурата.[8]

Функционирањето на системот на критична инфраструктура е под постојана закана од широк спектар безбедносни закани.[9]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.[10]

Ефектите кои произлегуваат од овие закани по критичната инфраструктура и нејзините подсистеми може да предизвикаат помали или поголеми проблеми кои можат да предизвикаат нарушувања и дефекти во различните подсистеми.[11]

Ефективноста на заштитата на критичната инфраструктура многу зависи од квалитетот и брзината наразмена на разузнавачките информациии од информации кои се од значење, а се сензитивни. Припоставувањето на оперативните рамки за размена на информации, стратегиите за заштита на критичната инфраструктура и сродните планови за имплементација треба да изнајдат законски основ во кој ќе бидат опфатени три основни прашања:[12] „Кои информации треба да се разменуваат и зошто“?; „Како ќе се споделуваат информациите за било која задача“?; и „Меѓу кого информациите ќе бидат споделени“?.[13]

Информациите можат да се разменуваат на стратегиско, техничко или тактичко ниво. Од друга перспектива, информациите може да се поврзани со инциденти или да се дадени во општ контекст. Тоа истотака може да биде во форма

---

[8]Li, H., et al, *Strategic Power Infrastructure Defense*, Proceedings ofthe IEEE, 2005.
[9] Gregg, S., H.: Defining and Distinguishing Secular and Religious Terrorism. *Perspectives on Terrorism*. Vol 8, No. 2 2014, достапно на: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/336/html, посетена на 10/03/2021.
[10] Good Progress on Tackling Hybrid Threats. European Commission Press Release, достапно на: A_Europe_that_protects__good_progress_on_tackling_hybrid_threats.pdf, посетена на 10/03/2021.
[11] Hybrid Conference: Critical Connections, Continuity and Supply – Assessing the Security of European Critical Infrastructure and Functions in a Hybrid Threat Context, достапно на: https://eu2019.fi/en/events/2019-11-06/countering-hybrid-threats-critical-infrastructure-protection-security-of-supply, посетена на 10/03/2021.
[12]Попоска В. *Меѓународно-правни аспекти за заштита на критичната инфраструктура од современи безбедносни закани*, Универзитет „Гоце Делчев“, Штип, 2019.
[13] INTERPOL. *The protection of critical infrastructures against terrorist attacks: Compendium of good practices, United Nations Office of Counter-Terrorism*, UN Counter Terrorism Centre, 2018.

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 тип информации, платформите за размена на информации (и приложените безбедносни карактеристики) ќе бидат структурирани многу поинаку отколку тогаш 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.[14]

Справувањето со безбедносните сајбер закани бара специфицирани знаења и мултидисциплинарен пристап.

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 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 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.

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

Од претходно наведените причини, зајакнувањето на националните капацитети за справување со сајбер заканите и зголемувањето на сајбер безбедноста станаа еден од клучните предизвици за Македонија.

1.3 Досегашни истражувања

Во научната литература во Македонија се проучуваат одредени аспекти на сајбер заканите и напади по критичната информатичка инфраструктура, анализи изработени од автори што се однесуваат на поврзаност со сајбер тероризмот. Сепак има мал број на истражувања во научната литература во Македонија кои содржат анализи за влијанието на сајбер нападите по критичната информациска инфраструктура.

Општо земено, критичната инфраструктура претставува средство или систем, кој суштински придонесува за одржување на виталните општествени функции. Оштетувањето на критичната инфраструктура, уништувањето или прекинот на функционирањето на овие системи, предизвикано од природни катастрофи, малициозно однесување, криминални активности и тероризам може да предизвика значајни последици по безбедноста на луѓето, општествата и меѓународниот поредок.[15]

Идејата за истражувањето е резултат на поттикот да се дојде до одредени научни и практични сознанија, како и да се осознаат начините и методите кои придонесуваат кон една комплетна анализа, за да се дознае што всушност се прави на тоа поле, за да се формира целосна слика за сајбер заканите по критичната информациска инфраструктура. Ова истражување кое е планирано да се спроведе, ќе го заземе вистинскиот аспект во однос на зголемување на истражувањата во оваа чувствителна област. Поради фактот што проблематиката е актуелна, а севкупноста на сите елементи е во корелација со последните настани во светот, нејзината динамика како истражувачки проблем го заслужува потребното внимание.

[15]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 13/03/2021.

Со оглед на недостатокот на научна опсервација за сајбер нападите од оваа перспектива и на недостиг на анализа на начините на кои овој проблем го покажува (и на тој начин влијанието што таков приказ може да го има врз колективната свест на општеството), анализата на импликациите од сајбер заканите врз критичната информациска инфраструктура е основна определба на овој труд за да понуди свој придонес кон постојните истражувања.

1.4 Цели и задачи

Општата цел на ова истражување е научна дескрипција, анализа и идентификација на сајбер нападите и нивните импликации врз критичната информациска инфраструктура.

Посебни цели:

- Анализа на податоци за видовите на сајбер закани врз критичната информациска инфраструктура.
- Да се определат новите начини/модалитети на реализација на сајбер напади.
- Да се согледа како се идентификува критичната инфраструктура во македонската држава.
- Утврдување на безбедносните последици од сајбер заканите по критичната информатичка инфраструктура.
- Да се види каква е моменталната заштита на критичната информациска инфраструктура во Македонија.
- Воспоставување на стандардни оперативни процедури во Македонија за справување со сајбер нападите врз критичната информациска инфраструктура.

Со оглед на целите, основни **задачи** на истражувањето се следниве:

- Да се утврди дали е потребна поголема соработка помеѓу разузнавачките агенции и организации во делот на сајбер напади врз критичната информациска инфраструктура.

— Да се идентификува динамиката на манифестирање на сајбер заканите врз критичната информациска инфраструктура.
— Да се утврди нивото и степенот на загрозеност на информациската критичната инфраструктура.
— Да се одговори на дилемата која е причината и покрај развиените современи методи, да се реализираат сајбер напади врз критичната информациска инфраструктура.
— Да се подобри непосредната комуникација помеѓу директните извршители кои што учествуваат во справување со сајбер заканите врз критичната информациска инфраструктура.

1.5 Дефинирање на основните поими

➢ Информација

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,[16] 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 од сензорите (рецепторите) или податочни ставки, во некој контекст кој има (смисла) значење.[17]

[16]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
[17]David Alberts, *Understanding informaton age warfare*, 2001, достапнона: http://www.dodccrp.org/files/Alberts_UIAW.pdf

- **Безбедност на информации**

Безбедноста на информациите подразбира заштита на информацијата од низа закани, се со цел да се обезбеди континуитет на работењето, да се минимализира потенцијална штета, и да се максимизираат резултатите.[18]

- **Сајбер напад**

Сајбер напад претставуваат операции кои лицата и/или информатичките 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**

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 контра операција против изворот.[19]

- **Сајбер-простор**

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.[20]

---

[18]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.
[19]*Национална стратегија за сајбер безбедност на Република Македонија 2018-2022*, Верзија 1,2, Министерство за информатичко општество и администрација, Министерство за внатрешни работи и Министерство за одбрана, јули 2018.
[20]Kissel R., (ed.). *Glossary of Key Information Security Terms*, 2011.

- **Сајбер саботажа**

Сајбер саботажа – сајбер напад насочен против интегритетот и достапноста на информациско комуникациските системи.

- **Сајбер-криминал**

Сајбер криминал, познат и под називот електронски криминал, компјутерски криминал и слично, кој опфаќа криминални активности спроведени со користење на компјутери и интернет, најчесто финансиски мотивирани. Компјутерскиот криминал вклучува кражба на идентитет и измама, меѓу другите активности. Компјутерскиот криминал се разликува од другите форми намалициознисајберактивности, кои имаат политички, воени или мотиви на шпионажа.[21]

Сајбер-криминалот може да опфати кражба на интелектуална сопственост, злоупотреба на патент, трговска тајна и сл, но истотака вклучува и напади против компјутери со цел намерно нарушување на нивното функционирање или недозволено копирање на класифицирани информации складирани во компјутерските системи.[22]

- **Сајбер-тероризам**

Сајбер-тероризмот е конвергенцијата помеѓу сајбер-просторот и терористичките активности, на пример, политички мотивирано хакирање, кое има за цел да предизвика сериозна штета како загуба на човечки животи и/или сериозни економски последици.[23]

[21]Достапно на https://www.newamerica.org/cyber-global/compilation-of-existingcybersecurity-and-information-security-related-definitions/
[22]Wilson, C., Botnets, *Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, January, 2008, стр. 7
[23]Бакрески, О, Милошевска, Т, Алчески Ѓ. *Заштита на критична инфраструктура*, Комора на Република Македонија за приватно обезбедување, Стеда-графика, Скопје, 2017.

- **Сајбер војна**

Сајбер војна или „наменска употреба на компјутерски системи со цел да се прекинат активностите на непријателска земја или нападна нејзините комуникациски системи “[24].

- **Сајбер безбедност**

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 контра-одговор и обновување на системите до состојба во која се наоѓале пред сајбер инцидентот.

- **Инфраструктура**

„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. “[25]

- **Критична инфраструктура**

Критичната инфраструктура претставува средство или систем, кој суштински придонесува за одржување на виталните општествени функции. Оштетувањето на критичната инфраструктура, уништувањето или прекинот на функционирањето на овие системи, предизвикано од природни катастрофи, малициозно однесување, криминални активности и тероризам може да предизвика

[24]Достапно на https://www.newamerica.org/cyber-global/compilation-of-existingcybersecurity-and-information-security-related-definitions/

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

значајни последици по безбедноста на луѓето, општествата и меѓународниот поредок.[26]

- **Критична информациска инфраструктура**

Критична информациска инфраструктура е кои било информациско-комуникациски системи чие што одржување, сигурност и безбедност се критични за националната безбедност, економијата, јавната безбедност и здравјето. Националната критична информациска инфраструктура е дел од критичната инфраструктура.[27]

1.6 Основна хипотетичка рамка

Врз основа на општиот пристап на проблемот за сајбер нападите како закана за критичната информациска инфраструктура и врз основа на веќе поставените цели во ова истражување ќе ја поставам следнава општа хипотеза:

Прекузајакнувањенакапацитетитезапревенција и заштитаодсајбернападиќе се дејствува во насока на безбедно и отпорно дигитално опкружување со цел заштита на критичната информациска структура.

Посебни хипотези:

- ✓ Меѓу-институционалниот и мулти-дисциплинарниот пристап со вклучување на сите засегнати страни е од клучно значење за да се обезбеди ефикасен одговор на сајбер нападите.
- ✓ Унапредувањето на соработката со регионалните и меѓународните организации е од суштинско значење за справување со сајбер напади.

[26]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.

[27]Бакрески, О, Милошевска, Т, Алчески Ѓ. *Заштита на критична инфраструктура*, Комора на Република Македонија за приватно обезбедување, Стеда-графика, Скопје, 2017.

- ✓ Воспоставување ефикасни процедури за пријавување и истражување на сајбер нападите ќе резултира со намалени негативни импликации на критичната инфраструктура.
- ✓ Преку соработка на сите засегнати страни за унифицирање безбедносни норми,стандардизирање на соработката ќе се воспостави задолжително ниво на заштита за субјектите кои управуваат со критичната информациска структура.
- ✓ Создавање на национална платформа/систем за размена на информаци и во врска со закани, инциденти и непосредните опасности ќе резултира кон подобрување на заштитата на критичната информациска структура.
- ✓ Примена на соодветен модел за заштита на критичната информациска инфраструктура во голема мера ќе ја обезбеди адекватна заштита на инфраструктурата.

Варијабли

Предикторска варијабла (независна варијабла)

-Критична информациска структура.

Критериумска варијабла (зависна варијабла)

-Постигнати резултати во спречување на сајбер нападите.

1.7 Научна и општествена оправданост на истражувањето

Научната оправданост на ова истражување се согледува во придонесот на верификување на научно недоволно познати и проучени специфични факти и насока на подобрување на меѓународната соработка и изнаоѓање на нови форми и методи за превенирање и сузбивање на сајбер нападите по критичната информациска инфраструктура.

Општествената оправданост се состои во тоа што истражувањето би помогнало да се согледаат можностите на заедничко дејствување во насока на намалување на бројот на потенцијални сајбер напади.

1.8 Методи и техники на истражувањето

Во контекст на современите научно-методолошки пристапи на истражување со комбинирање на повеќе истражувачки методи, во истражувањето ќе настојувам со примена на неколку методолошки постапки на собирање, анализа и интерпретација на податоците да се добие една систематизирана целина.

Компаративниот метод на анализа се користи со цел да се изврши делумна квалитативна и квантитативна селекција и анализа на прибраните податоци и врз основа на тоа да се воопштат релевантните факти за потврдување или негирање на поставените тези. Овој метод се користи за споредување на сите податоци добиени со претходно користење на статистички методи и анализа на содржината кои се однесуваат на бројните показатели за состојбата на сајбер заканите врз критичната информациска инфраструктура. Покрај квалитативната анализа на релевантни теориски извори, како основна методолошка постапка односно техника за собирање на податоци ќе се користи анализа на содржина на публикации, извештаи, конференциски материјали, статистички показатели, извештаи и анализи на невладини организации, агенции за испитување на јавното мислење, тинк-тенкови и државни институции итн., а како методолошки постапки за анализа и интерпретација на податоците ќе се применат аналитичко-синтетички метод и компаративен метод на анализа. Преку анализа и интерпретација на податоците во ова истражување се очекува да се добијат квантитативни и квалитативни податоци, со кои преку соодветна обработка ќе се добие верификација на хипотезите и ќе се оствари целта на истражувањето.

2. Поим за критична инфраструктура

Постојат многу трудови што го разработуваат проблемот на критичната инфраструктура и тие се важен сегмент на националната безбедност и безбедноста воопшто. Луѓето се свесни дека не можат секогаш да штитат се, и дека мора да одлучат која инфраструктура е клучна за нив и зошто. Заштитата на критичната инфраструктура е на крстосница меѓу политиката, бизнисот, технологијата и ризикот. Сите се свесни за важноста на критичната инфраструктура, но се уште не постои листа или дефиниција на критичната инфраструктура и тоа доведува до различни пристапи кога е во прашање и самата заштита на критичната инфраструктура. Во основа, критичната инфраструктура како витална, комплексна и меѓусебно структурно поврзана целина е од исклучителна важност и значење занепреченото функционирање на државата. Таа е јасна дијалектика и синергија што ги поврзува индустрискиот сектор, комуникациските системи, енергетскиот сектор и другите сектори, системи и мрежи што се од големо значење за државата бидејќи со неа се обезбедува потребната стабилност. Оттука нарушувањето или прекинот на работата на одредени сектори/системи може да доведе до сериозни последици што може да имаат и ослабувачки ефект на безбедноста на државата, на националната економија, на економскиот развој и просперитет, на стабилниот енергетски сектор, односно нарушувањето или прекинот на работата на само еденод наведените сектори може да доведе до сериозни последици врз другите критични сектори.[28]

Критичката инфраструктура е важна компонента на националната безбедност на секоја земја затоа што нејзиното загрозување го доведува во прашање нормалниот тек на животот и безбедноста на граѓаните и функционирањето на државата.[29] Критичката инфраструктура е збир на сите објекти, мрежи и функции

[28]Бакрески О. Милошевска Т. Алчески Ѓ, *Заштита на критична инфраструктура*, Комора на РМ за приватно обезбедување, Скопје, 2017.
[29]Mikac, Cesarec & Larkin, 2018:23 (преземено од *Критична инфраструктура-концепт и безбедносни предизвици,* Марина Митревска и др., Скопје, 2019, стр.21).

што се важни за опстанокот на државата, чие што уништување ќе влијае негативно врз безбедноста, националната безбедност, јавното здравје и сл.[30]

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 ги опфаќаат: енергетскиот сектор, секторот за управување со води, прехранбениот сектор, транспортниот сектор, телекомуникациите, здравството, банкарството и финансиите итн. Сепак, важно е да се напомене дека не постои универзално прифатена дефиниција и секоја држава ги дефинира во согласност со своите интереси.[31]

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, за што ќе стане збор понатаму во трудот.[32]Критичната инфраструктура претставува средство или систем кој суштински придонесува за одржување на виталните функции. Оштетувањето на критичната инфраструктура, уништување или прекин на функционирањето на овие системи, предизвикано од природни катастрофи, малициозно однесување, криминални активности и тероризам може да предизвика значајни последици по безбедноста на луѓето, општествата и меѓународниот поредок.[33]

Заштитата на критичната инфраструктура на национално ниво е една од приоритетните задачи. Вклучува различни чекори како што се вовлекување, приоритизација и заштита на оние инфраструктури и услуги кои се од витално значење за благосостојбата на општеството. Иако некои сектори, потсектори и услуги се чини дека се многу круцијални за сите земји, други може да се

[30] Dawson, Omar, 2015:97 (преземено од *Критична инфраструктура-концепт и безбедносни предизвици*, Марина Митревска и др., Скопје, 2019, стр.21).
[31]Critical National Infrastructure. CPNI. https://www.cpni.gov.uk/critical-national-infrastructure-0
[32]Бакрески О., Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура*, Дирекција за безбедност на класифицирани информации, Скопје, 2021, стр.35
[33]Kravcov, A., *et al. Durability of Critical Infrastructure, Monitoring and Testing*: Proceedings of the ICDCF 2016. Springer Nature Singapore, 2017, достапна на:https://books.google.mk/books?id=1f6qDQAAQBAJ&pg=PA249&dq=critical+infrastructure

разликуваат по нивното значење врз основа на специфични економски, еколошки и социјални карактеристики на секоја земја.

Според Европскиот Совет, терминот критична инфраструктура значи систем или дел од систем што е суштински за соодветна операција на виталните општествени функции, што се однесуваат на здравјето, безбедноста, економската и социјалната благосостојба на луѓето.[34] Неуспехот да се одржи поднослив ниво на одржливост, или уште полошо целосниот колапс на КИ би имал значително влијание врз индивидуално, социјално, економско и национално ниво. Бизнисот и индустријата и од приватните и од јавните сектори, во голема мера зависат од КИ, за нивните витални функции. Типични примери на КИ вклучуваат информатичка и комуникациска технологија (ИКТ), енергија, транспорт, економија (финансиски сектор), здравство, одбрана, храна, водоснабдување и владини услуги.

Критичката инфраструктура може да се моделира како сајбер-физички системи, каде што информациите (сајбер) делот, ги контролира физичките компоненти и основните структури, да ги управуваат, контролираат и оптимизираат целите и функционалноста на КИ. На пример, контрола на физичките компоненти на електраната (на пример, генератори или дистрибутивни елементи) може да се изведат преку интерактивни сензори и активатори,кои периодично го проверуваат статусот, пренесуваат информации до централни информациски контролни системи и прифаќаат мрежни команди за да се измени статусот на физичките компоненти соодветно. Идентификувањето и евалуацијата на КИ е предизвик, додека процесоти методологиите што се користат за идентификување и оценување на критичната инфраструктура, особено оние што можат да влијаат на луѓето и системите на национално ниво, може да се разликуваат од една земја во друга.[35]

[34]Gullasch D, Bangerter E, Krenn S. Cache games–bringing access-based cache attackson AES to practice. In: *Security and Privacy (SP*), IEEE Symposium onIEEE, 2011, pp 490–505.
[35] GritzalisD., Theosharidou M., Stergiopoulos G., *Critical Infrastructure Security and Resilience*, 2019 p.18

3. Класификација на критичната инфраструктура

Критичната инфраструктура опфаќа широк спектар на витални сектори како што се сообраќај, транспорт, производство и дистрибуција на енергија, информациски и комуникациски системи, здравствени служби, системи за снабдување со вода и храна, финансиски служби, државна инфраструктура и сл. Делумното или целосното откажување на овие инфраструктури може да го загрози општеството, националната безбедност и да доведе до најразлични проблеми.

Развиените земји, а во последно време и помалку развиените, настојуваат да ги идентификуваат и анализираат критичните сектори, потсектори, процеси и објекти, преку користење на различни методолошки и политички пристапи. Неверојатна комплексност на инфраструктурните системи е дефинитивно најголем заеднички проблем на сите земји кои се впуштиле во анализирање и идентификување на критичната инфраструктура како и оние кои се обидуваат да формираат политика на заштита на критичната инфраструктура.[36] Зголемената меѓузависност на критичната инфраструктура и поголемата оперативна сложеност ја прави критичната инфраструктура особено ранлива на природни катастрофи и природни опасности, човечки грешки и технички проблеми, како и нови форми на сајбер криминал, тероризам. Секој од овие настани може да доведе до сериозни последици по критичната инфраструктура, па дури и до целосно уништување на критичната инфраструктура. Има голем број инфраструктурни сектори кои истовремено опфаќаат поголем број на потсектори, гранки на индустријата, услуги, производствени области и имаатспецифична вертикална структура. Некои мислења укажуваат на опасност од идентификување на сите инфраструктури како критични поради нејасната граница помеѓу критична и некритична инфраструктура. Заедно укажуваат на зголемување на меѓусебната поврзаност на критичната инфраструктура (меѓусекторско поврзување).

[36]Lewis, T., *Infrastructure Protection in Homeland Security, Defending a Networked Nation*, Wiley Interscience, 2006.

Генерално, голем број експерти се согласуваат дека голем број ризици и закани треба да се идентификуваат пред да се определи критичната инфраструктура.[37]

Анализирајќи ги различните пристапи на дефинирање и класификација на критичната инфраструктура, може да се заклучи дека таа опфаќа посебно:

- Храна
- Вода
- Стопанство
- Здравствени служби и службата за итна помош
- Енергија
- Сообраќај
- Информации и телекомуникации
- Банкарство и финансии
- Хемиски постројки
- Безбедносна индустрија
- Пошта и дистрибуција на стока и
- Национални споменици и други културни вредности.

Сајбер безбедноста може да означува физичка заштита на сајбер средствата. Пружање физичка и сајбер безбедност на критичната инфраструктура бара широк напор што може да варира, додека различни поединци или политики може да зборуваат за други активности. Во текот на 2004 година, група научници направија компаративна анализа на критичните инфраструктури во шеснаесет земји, која може да се претстави на следниов начин:

- банкарство, финансии, телекомуникации, енергија, информации и телекомуникациските системи наведуваат 14 земји;
- транспорт, логистика, дистрибуција во нејзините листи од 13 земји;

[37]Moteff, D.J., Parfomak, P., *Critical Infrastructure and Key Assets: Definition and Identification,* Congressional Research Service, Library of Congress, 2004.

- здравствените услуги и водоснабдувањето во нивните списоци наведуваат 12земји;
- листа на 11 земји од централната влада / владините служби; - службите за спасување за итни случаи наведуваат 10 земји во нивните списоци;
- снабдувањето со нафтени производи наведуваат 9 држави во своите списоци;
- информативни услуги, медиуми (радио и ТВ), јавна администрација наведува 8 земји,
- други области - зајакнување на законодавството, судството, националниот јавен ред и безбедност, управување со отпад, полиција, заштита, војска и воени објекти, системи за осигурување, социјални услуги, управување со водоснабдувањето, нуклеарните централи во нивните списоци наведуваат 6 земји.

Со анализа на овие осум групи приоритети во однос на критичната инфраструктура, може да се заклучи дека дефиницијата за критична инфраструктура и нејзината содржина не може да биде идентична во секој дел од светот и затоа логично е дефиницијата и содржината да се одредуваат на национално ниво.

4. Методологии за идентификација и евалуација на критичната инфраструктура

Идентификацијата на националната критична инфраструктура е регулирана со различна национална и меѓународна правна рамка. Во рамките на националната програма за заштита, секоја земја-членка на ЕУ треба да ги идентификува „националните критични области/сектори“, да ги евидентира и ги оценува нивните системи или компоненти како и да ја евидентира и оценува потенцијалната поврзаност и зависност меѓу идентификуваните КИ. Исто така, треба да развие и ажурира оперативен безбедносен план и план за итни случаи за да ги заштити своите критични инфраструктури. Бидејќи во повеќето случаи, сопствениците на КИ и операторите се приватни субјекти, било во процес за идентификување на националните КИ и секој процес под програма за национална заштита, бара размена на информации меѓу вклучените страни, во согласност со принципот на соработка со засегнатите страни, посебно јавното-приватно партнерство.[38]

Европскиот совет дава понатамошни насоки во идентификација на националните КИ за секоја земја членка, со што ги обврзува земјите членки да идентификуваат потенцијална Европска критична инфраструктура на нивна територија. Често штетите и загубите на КИ во една земја членка, може да има негативни последици во неколку други земји членки.[39] Директивата се однесува на енергијата и транспортот, додека остава отворено вклучување на други сектори во својот опсег, давајќи приоритет на секторот за информатичка и комуникациска технологија (ИКТ). Неопходен услов за имплементација на Директивата кај секоја земја членка е, според тоа, идентификација на критичната инфраструктура во секоја земја –членка.[40]

[38]Public Private Partnerships (PPP) – Cooperative models (2017) ENISA. Достапно на ENISA: https://www.enisa.europa.eu/publications/public-private-partnerships-pppcooperative-models
[39]European Commission, *European programme for critical infrastructure protection*, 2007.
[40]EU Commission. *Review of the European Programme for Critical InfrastructureProtection* (EPCIP), 2012.

За секој национална КИ, идентификувана како ЕКИ, секоја земја -членка е одговорна, меѓу другото, за собирање информации за безбедносни ризици, закани и ранливости по ИЕК. Крајната цел од Директивата е да се имплементираат, во сите назначени ЕКИ, планови за безбедност на операторот (OSP) со цел да ги заштити на ниво на оператор, во рамките на заедничка Европска стратегија.

4.1 Идентификација на критичната инфраструктура

Точната дефиниција за критичната инфраструктура варира од земја до земја. Општо земено, критичните инфраструктури се инфраструктури чие нарушување, неуспех или уништување би имало значително влијание врз јавното здравје, животната средина, безбедноста, социјалната и економската благосостојба. Покрај разлики во дефиницијата, често постојат диференцијации на посуштинско ниво, со влијание врз идентификацијата на КИ. Во Германија, на пример, КИ е поделена на витална техничка инфраструктура и витална социо-економска инфраструктура.[41]

Во Велика Британија[42], инфраструктурите сеподелени на критични национални инфраструктури и други критични инфраструктури. Врз основа на релевантната литература и широко користените меѓународни практики, може да се спроведе формален процес за идентификување и означување на националните КИ во четири последователни фази:

- Идентификација на критичните сектори/потсектори.
  Во оваа фаза, се идентификуваат секторите и/или потсекторите кои се перцепираат за круцијални за националните интереси.
- Идентификација на критичните услуги.
  Критичните услуги на секторот/потсекторот се идентификуваат за секој критичен сектор.
- Означување на критичната инфраструктура.

[41]National Strategy for CIP. Federal Republic of Germany, 2009.
[42]National Security Strategy and Strategic Defence and Security Review, UK Government, 2015, достапно на:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

За секоја критична услуга, критичните средства/компоненти кои се состојат од КИ се идентификувани и означени.

- Заштита на критичната инфраструктура.

  Се спроведуваат процедури за заштита и безбедност за секоја критична инфраструктура.

4.2 Идентификација на критичните сектори и потсектори

Во фаза на идентификување на критичните сектори, секоја земја-членка изготвува почетна листа на нејзините национални критични сектори, односно секторите што постојат во рамките на географските граници на нејзината територија и кои вклучуваат потенцијална критична инфраструктура. Процесот на изборот на националните критични сектори и потсектори не е секогаш директен. Сите национални сектори не се подеднакво витални/критични во секоја земја. Некои сектори можат да бидаткласифицирани како критични, а некои како помалку критични или помалку важни. Покрај тоа, не сите услуги на секторот/подсекторот се подеднакво критични, што го отежнува идентификувањето на почетната листа на критични сектори на стратешко ниво. Европската комисија ја препознава разновидноста на националните критични сектори во секоја земја-членка, т.е. тешкотијата да се идентификуваат критичните сектори/потсектори во секоја земја и на идентификувањето, назначувањето и давање приоритет на КИ во секој критичен сектор. Меѓутоа, во поглед на создавање заедничка рамка за Европската програма за заштита на критична инфраструктура (EPCIP), заедничка листа на критични сектори/потсектори, се прават големи напори. Неколку земји-членки ја усвоија оваа листа за да ги идентификуваат национални критични домени. Во согласност со широко користената методологија за идентификација на КИ по сектор, ENISA[43] предлага варијација на индикативната табела на Зелената книга[44] и го вклучува концептот на услуга по потсектор.

[43]Lückerath D et al. *The RESIN Climate Change Adaptation Project and its Simple Modeling Approach for Risk-Oriented Vulnerability Assessment*. In: Workshop 2018ASIM/GI-Fachgruppen (ASM 2018), Proceedings of ASIM workshop, Hochschule Heilbronn, Germany, March 8–9, 2018, pp 21–26.
[44]Connelly A et al. RESIN Glossary, Deliverable D1.2. EU H2020 Project RESIN, The University of Manchester, Manchester, United Kingdom, 2016.

Концептот на услуга често се користи како синоним за терминот инфраструктура, како што се интегрира натаму на ниво доволно апстрактно и доволно описно за концептот на збир од средства/производи и процеси на кои (во крајна линија) им е потребна заштита.

4.2.1 Идентификација на критичните услуги

Во литературата може да се најдат два главни пристапи за идентификување на националните критични услуги по сектори[45] накратко опишани подолу.

1) Државен пристап

Во овој пристап, Владата има водечка улога во дефинирањето и давањето приоритет на критичните услуги - преку координативно тело - или надлежен орган за заштита на КИ. На централно ниво, се составува списокот на индикативни национални услуги од критичниот сектор. Алтернативно, список на национални критични услуги е составен на меѓусекторско (или попречно) ниво. Тогаш критичните услуги се оценети, со специфични критериуми и дадени приоритети за да се понуди конечната листа на национални критични услуги. За секоја критична услуга, се составува листа на засегнати страни-оператори, од кои (или во соработка со) листа на најкритични стоки, производи и системите што ја поддржуваат оваа услуга, се сумираат. Овој пристап е искористен во земји како Швајцарија, Естонија, Холандија и Чешка.[46]

[45]Klaver M. *Good practices manual for CIP policies, for policy maker's in Europe*. Brussels: RECIPE, 2011, достапно на: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPE_manual.pdf
[46]Ibid

2) Пристап управуван од оператор

Во пристапот управуван од операторот, водечка улога им се доделува на операторите на критична инфраструктура. Особено, според националните критични сектори/потсектори идентификувани на централно ниво (врз основа на јавно-приватно партнерство-ЈПП), е составена листа на засегнати страни-оператори на КИ, исто така познати како витални оператори (ВО), од кои се бара да ги идентификуваат и оценат критичните услуги и најкритичните средства/системи што ги сочинуваат. Во неколку европски земји, оваа одговорност е доделена на релевантнно тело за витални операции, одговорно зарелевантен критичен сектор (на пример, релевантното министерство). Треба да се нагласи дека според овој пристап виталните операции одат во преден план, за разлика од концептот на критична услуга што доминира во пристапот управуван од државата. На некој начин, виталните операции се клучно средство на кое му е потребна заштита.

Овој пристап се користи во земји како што се Франција и Обединетото Кралство. Секој пристап бара спроведување на метрика за проценка и приоритет на критичноста на секое средство (на пример, услуги, стоки, системи и сл.) на критичен сектор. Овој процес, и покрај неговата важност, не е очигледен, особено затоа што, скоро секогаш, критериумите за критичност на вклучените податоци се разликуваат од земја до земја. Покрај тоа, инфраструктурата може да биде критична поради меѓузависностите помеѓу услугата што ја поддржува инфраструктурата и други услуги во ист или различен сектор.

4.2.2. Зависности и меѓузависности

Средство (на пример, инфраструктура, услуга или подсектор) може да биде критично не само поради директното влијание што може да го предизвика поради неговата неисправност или загуба (исто така познато како ефект од прв ред), но исто така и поради влијанието врз другите критични средства, познати како ефекти од втор ред. Ефектите од прв ред ја одразуваат директната виталност на критично

средство за општеството[47], на пр. според меѓусебните критериуми споменати погоре, додека ефектите од повеќе намени ја одразуваат индиректната виталност на средството за други критични средства. Обично, ефектите од втор ред се подразбираат или како зависности, каде што критичниот елемент зависи од друг елемент или како меѓузависности каде два критични елементи меѓусебно се засегнати на национално или и транснационално ниво.[48] Забележано е дека зависностите или меѓузависностите може да постојат или во рамките на секторот/потсекторот во кој се дава услуга или помеѓу два или повеќе сектори/потсектори на национално ниво или помеѓу два сектори/потсектори кои работат во различни земјиж-членки.

[47]Luiijf E, Burger H, Klaver M, Marieke H. *Critical infrastructure protection in theNetherlands: a Quick-scan*. EICAR Denmark, Copenhagen, 2003.
[48]Rossella M, Cédric L-B. *Methodologies for the identification of critical information infrastructure assets and services*. Guidelines for charting electronic data communication networks, European Union agency for network and information security. ENISA, Heraklion, 2014.

5. Практиката на одделни држави

Во последниве години, повеќето земји-членки на ЕУ, се во процес на дизајнирање, конзистентни сајбер безбедносни политики за КИ[49]. ЕУ ја истакнува потребата од користење на најдобри практики и методи за заштита на КИ. Засновано на јавни извори и литература, разгледуваме некои најдобри практики што се имплементирани во земјите на ЕУ, за идентификување и заштита на европските КИ. Поради важноста на заштитата на информатичката критична инфраструктура, за повеќето национални критични сектори денес, (интерполирани),ниво 2 е додадено за да ги опфати повеќето национални критични сектори за да ги вклучи земјитекои иако немаат или ја немаат завршено стратегијата за заштита на критична инфраструктура, веќе изготвија стратегија за сајбер-безбедност за заштита на нивнатакритична инфраструктура за информации и комуникација.

Следните неколку случаи ја опишуваат критичната инфраструктура во Франција, Германија и Велика Британија и САД. Некои од овие земји се пионери во медолошкиот дизајн на критичната инфраструктура и се добра пракса за анализа на проблемот.

5.1 Франција

Франција е една од првите европски земји што дизајнираше и спроведе политика за идентификација и заштита на КИ. Франција дефинираше 12 витални сектори,[50]кои се поделени во 3 главни области како што следува:

1) Државни сектори (јавни услуги, воени операции, судски функции и истражување).
2) Сектори за цивилна заштита (здравство, водостопанство, храна).

[49]EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, BSA – the software alliance, 2015, достапно на:http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[50]The Critical Infrastructure Protection in France. Paris: Secrétariatgénéral de la defenseet de la sécuriténationale (SGDSN), 2017, достапно на:Secrétariatgénéral de la défense et de lasécuriténationale: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

3) Области на економскиот и социјален живот на нацијата (енергија, електронски комуникации,аудиовизуелни и информациски системи, транспорт, економија, индустрија).

Како дел од стратегијата за национална безбедност, се следи националниот државен пристап за идентификување на националната критична инфраструктура. Особено, владата, дефинира список на витални оператори,каде што секој оператор е поврзан со еден критичен сектор. Администраторот на секој витален оператор е должен да:

• Назначи службеници за безбедност, на централно и локално ниво.

• Спроведување на проценка на ризик за да се идентификуваат критичните средства/системи и поставување Оперативен безбедносен план (ОСП) за да го заштити.

• Идентификување на средствата/системите што ќе бидат предмет на ОСР, што треба да се имплементираатпод водство на операторот, како и план за надворешна заштитаспроведена од одговорното јавно тело.

5.2 Германија

Според германскиот Устав, државна задача е да се гарантира јавна безбедност и да се обезбеди заштита на основните добра и услуги. Федералната канцеларијаза цивилна заштита и помош при катастрофи (ББК) е одговорна за стимулирање наоператори на критични инфраструктури за проактивно обезбедување на КИ и подготвување ефективнипланови за управување со кризи. Според тоа,[51] следните инфраструктури и секторисе дефинирани како критични во Германија: енергија (електрична енергија, гас, минерали масло), вода (снабдување), храна (индустрија за малопродажна храна, прехранбена индустрија), култураи медиуми (радиодифузија, печатени медиуми, културни средства),

[51]BKK Annual Report, 10–13. Germany: federal office of civil protection and disaster assistance (BKK), 2015.

информации (телекомуникации,информатичка технологија), финансии (даватели на финансиски услуги, осигурувања,банки, берзи), здравје (здравствена заштита, лаборатории, лекови, вакцини), транспорт (авијација, превоз, железница, патишта, логистика) и држава/администрација (Парламент, влада, судство, итни служби).

Од 2009 година, Германија ја усвои Националната стратегија за заштита на критичната инфраструктура (СИП стратегија). Стратегијата ги вклучува федералните, локалните нивоа и владата за да ја зајакнат и имплементираат заштитата на КИ во нивните области. Ги содржи следните пакети, кои делумно се имплементирани паралелно, и се базира на пристапот за соработка усвоен од федералната администрација со вклучување на другите главни играчи, т.е. оператори и релевантни здруженија:

1. Дефиниција на целите за општа заштита.

2. Анализа на закани, ранливости и способности за управување.

3. Проценка на вклучените закани.

4. Приоритизирање на цели за заштита, земајќи ги предвид сите постојни мерки.

5. Имплементација на мерките за постигнување на целите првенствено преку: специфични здруженија, решенија и внатрешни прописи; развој на концепти за заштита од страна на компаниите.

6. Континуиран, интензивен процес на комуникација.

5.3 Велика Британија

Во Велика Британија, националната инфраструктура е дефинирана како објекти, системи, локации или мрежи потребни за работа на земјата и обезбедување основни услуги на кои се потпира секојдневниот живот на луѓето во Обединетото

Кралство[52]. Некои средства на националната инфраструктурата се нарекуваат критични во смисла дека нивната загуба би довела до значителни економски или социјални последици или жртви. Овие критични средства ја сочинуваат Националната критична инфраструктура. НКИ во Велика Британија се состои од 13 национални инфраструктурни сектори: сектор за хемикалии, цивилни нуклеарни комуникации, одбрана, служби за итни случаи, енергија, финансии, храна, влада, здравство, простор, транспорт и вода. Неколку сектори имаатдефинирани „подсектори“; Службите за итни случаи, на пример, може да се поделат на полиција,Брза помош, противпожарна служба и крајбрежна стража.Секој сектор има еден или повеќе одговорни владини оддели за секторот и обезбедување заштитна сигурност за критичните средства. Всушност, секое министерство е одговорно за својот сектор/подсектор што е надлежно, дефинира листа на критични оператори (СО) на услугите што го сочинуваат сектор/подсектор, и секој СО, од своја страна, ги идентификува најкритичните средства/системикои ги сочинуваат услугите. Во исто време, Центарот за заштита на националните инфраструктури (CPNI), како одговорно јавно тело, самостојно спроведува сопствена студија за проценката на потенцијалната КИ, според критериумите за вкрстена проценка за влијанието врз британското општество.

5.4 Соединети Американски Држави

САД се првата земја што разви иницијативи за заштита на КИ. Во согласност со Национален план за заштита на инфраструктурата,[53] ЦИ е дефиниран како системи и средства, физички и виртуелни, кои се толку витални за САД што секоја недостапност или уништување би имало значително влијание врз безбедноста, економијата, јавното здравје, или секоја нивна комбинација.

[52]National Security Strategy and Strategic Defence and Security Review (2015) UK Government, достапно на:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
[53]Austin Smith. *Presidential Policy Directive 21: Implementation: an interagency security committee white paper*. Interagency Security Committee, 2017.

Директивата за претседателската политика[54] го дефинира Министерството за внатрешна безбедност како одговорно тело за критична инфраструктурна безбедност преку Канцеларијата за Инфраструктурна заштита. Американското министерство за внатрешна безбедност идентификуваше 17 критични сектори. За секој сектор, Агенција специфична за сектор била назначена како координатор. Овие сектори се: хемиски сектор, комерцијални капацитети, комуникации, критично производство, брани, служби за итни случаи, информатичка технологија, нуклеарни реактори, материјали и отпад, храна и земјоделство, одбранбена индустриска база, енергија, здравствена заштита и јавно здравство, сектор за финансиски услуги, системи за вода и отпадни води, владини капацитети и транспортни системи.

Кога се разгледува класификацијата на критичната инфраструктура, често се користи Извршната наредба 13010[55], што ја потпишал Клинтон во 1996 година, според која е воспоставена претседателска комисија за заштита на критичната инфраструктура, која се однесува на она што одредена инфраструктура ја прави критична: Одредени национални инфраструктури што се толку витални што нивното попречување или уништување има ефект на слабеење на одбранбената и економската безбедност на САД.[56] Според оваа извршна наредба, оваа инфраструктура опфаќа:

- Телекомуникации
- Системите на електрична енергија
- Складирање и транспорт на нафта и гас
- Банкарство и финансии
- Транспорт
- Системи на снабдување со вода
- Итни системи

[54]Critical Infrastructure Security and Resilience – PPD-21 (2013) Washington DC. Достапно на: https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf
[55]Executive Order 13010 - Critical Infrastructure Protection, Federal Register, Vol. 61, No. 138. pp. 37347-37350, 1996.
[56]Ibid. стр. 37347.

- Континуитет на власта.

Извештајот на комисијата ги дефинирал инфраструктурите на секој сектор што е споменат во извршната наредба:

- Банкарство и финансии-ентитети како што се малопродажба и комерцијални организации, инвестициски институции, брокерски куќи, трговски куќи и системи за резерви и придружни оперативни организации, владини операции и активности за поддршка што се вклучени во сите аспекти на монетарните трансакции, вклучувајќи штедни влогови, инвестиции, безготовински исплати и исплати во форма на заеми и други финансиски инструменти.
- Системи за електрична енергија- Електраните и мрежите за пренос и дистрибуција што произведуваат и снабдуваат електрична енергија до крајните корисници така што тие постигнуваат и одржуваат номинална функционалност, вклучувајќи транспорт и складирање на гориво што е неопходно за овој систем.
- Итни служби- медицински, полициски, противпожарни служби и системи за спасување како и лица што се на располагање тогаш кога поединецот или заедницата се соочени со вонредни ситуации. Овие услуги главно се даваат на локално ниво. Освен тоа, државните и федералните планови имаат функција на давање поддршка во текот на реагирање на вонредни ситуации и санирање на последиците.
- Производство, складирање и транспорт на нафта и гас- постројките за производство и складирање на природен гас, сирова и преработена нафта и нафтени деривати, постројки за рафинирање и преработка на овие горива и нафтоводи, бродови, камиони и железнички системи за транспорт на овие производи до крајните корисници.
- Информации и комуникации-Компјутерската и телекомуникациската опрема, софтвер, процеси и луѓе што поддржуваат: собирање, обработка, складирање и пренос на податоци и информации, процеси и луѓе што од податоците создаваат информации, а од информациите, знаење.

- Транспорт- системи за физичка дистрибуција што значајно придонесуваат за националната безбедност и економската благосостојба, вклучувајќи системи за националниот воздушен сообраќај, воздушни линии, воздухоплови и аеродроми, патишта и автопати, копнени возила, пристаништа, водени патишта и пловила, јавен сообраќај, железнички и автобуски, нафтоводи, вклучувајќи ги и оние за природен гас, нафта и други опаани материјали, товарна и патничка железница и сл.
- Системи за снабдување со вода-Извори на вода, резервоари и постројки за складирање, водовод и други транспортни системи, системи за филтрација на вода, прочистување и третман, цевководи, системи за ладење и други механизми кои обезбедуваат вода за домаќинствата и индустријата, потрошувачи, вклучувајќи системи за управување со отпадни води и заштита од пожари.

Примарна цел на основната политика на САД е да се зајакне безбедноста и издржливоста на критичните инфраструктури против физичките и сајбер-заканите.

6. Јавни-приватни партнерства во заштитата на критичната инфраструктура

Јавно-приватното партнерство (ЈПП) овозможува јавниот и приватниот сектор да бидат ангажирани во испорака на стоки и услуги кои се генерално одговорни на јавниот сектор, со што се олеснуваат строгите буџетски ограничувања за јавните расходи. Иако ЈПП имаат потенцијал да овозможат побрза имплементација на политиките и да гарантираат добри стандарди за одржување, Утврдено дека проектите опфатени со ревизијата не биле секогаш ефикасно управувани и дека не даваат соодветна услуга. Потенцијалните придобивки од ЈПП често не биле реализирани затоа што биле обележани со одложувања, зголемување на трошоците и ниска искористеност, што резултирало со неефикасни расходи од 1,5 милијарди евра, од кои 0,4 милијарди евра се од фондовите на ЕУ. Дополнителна причина е недостатокот на соодветни анализи, стратешки пристапи за користење на ЈПП и институционални и правни рамки. Бидејќи само неколку земји –членки имаат соодветно ниво на искуство и експертиза во имплементација на успешни проекти за ЈПП, постои висок ризик дека ЈПП, како што се очекуваше, нема да придонесат за целта за зголемување на учеството на финансирањето од ЕУ што се користи во мешани проекти, вклучувајќи ЈПП. Постигнувањето ефективни јавни-приватни партнерства е долг и макотрпен процес, кој вклучува отстранување на многу пречки и проблеми и воспоставување на поинаква перспектива кон самите безбедносни проблеми што постојат во релевантните министерства и приватното обезбедување.[57] Од 1990-тите, 1.749 ЈПП во вкупна вредност од 336 милијарди евра се финансиски затворени во ЕУ. Повеќето проекти за ЈПП беа имплементирани во областа на транспортот, што во 2016 година претставуваше една третина од инвестициите во текот на целата година, а потоа следуваа областите на здравството и образованието. Меѓутоа, досега беше малку искористено финансирањето на ЕУ за ЈПП. Иако политиката на Комисијата веќе неколку години ја охрабрува употребата на ЈПП (на пр. Стратегија Европа 2020) како можно ефективно средство за

[57]S. V. N., Bhushan N. Critical Infrastructure: Defense Industrial Base Sector. In: Shapiro L., Maras MH. (eds) *Encyclopedia of Security and Emergency Management*. Springer, Cham, 2020.

спроведување проекти, откриено ер дека во периодот 2000-2014 година имало само 84 ЈПП, со вкупни трошоци за проектот-29,2 милијарди евра, со финансирање од ЕУ од 5,6 милијарди евра. Грантовите од структурните и кохезионите фондови беа главниот извор на финансирање од ЕУ, проследено со финансиски инструменти, честопати во соработка со Европската инвестициска банка (ЕИБ).[58] Судот испита 12 ЈПП кои се кофинансирани од ЕУ во Франција, Грција, Ирска и Шпанија во областа на патниот транспорт и информатичката и комуникациската технологија (ИКТ). Околу 70% од вкупните трошоци за проектот (29,2 милијарди евра) за ЈПП кои добија поддршка од ЕУ отпаѓаат на посетените земји -членки. Судот оцени дали проектите опфатени со ревизијата можат да ги постигнат придобивките што се очекуваат од ЈПП, дали овие проекти се засноваат на анализи и соодветни пристапи и дали севкупните институционални и правни рамки на посетените земји -членки се соодветни за успешна имплементација на ЈПП проекти. Генерално, Судот го утврди следново:

- ЈПП им овозможија на јавните власти да набавуваатголеми инфраструктурни проекти во рамките на една постапка, но го зголемија ризикот од недоволна конкуренција и на тој начин ги ставија договорните органи во послаба преговарачка позиција.
- Споделувањето на ризикот помеѓу јавните и приватните партнери честопати беше несоодветно, неконзистентно и неефикасно, додека високите стапки на повратт (до 14%) за ризичниот капитал на приватниот партнер не секогаш ги одразуваа ризиците што ги носи тој партнер. Покрај тоа, за повеќето од шесте ИКТ проекти опфатени со ревизијата, не беше најсоодветно да се склучат долгорочни договори, бидејќи овие проекти се засегнати од брзите технолошки промени.

Имплементацијата на успешни проекти за ЈПП бара значителен административен капацитет што може да се гарантира само со соодветни институционални и правни рамки и долгогодишно искуство во имплементација на проекти за ЈПП. Судот утврди дека ова во моментов е достапно само во неколку

[58] https://op.europa.eu/webpub/eca/special-reports/ppp-9-2018/hr/

земји -членки на ЕУ. Затоа, оваа ситуација не е во согласност со целта на ЕУ да ги искористи повеќето од фондовите на ЕУ во мешани проекти, вклучително и ЈПП.

Комбинацијата на средства од ЕУ и ЈПП е поврзана со дополнителни барања и неизвесности. Покрај тоа, способноста да се евидентираат проекти за ЈПП како вонбилансни ставки игра важна улога во изборот на опција за ЈПП, но таквата практика е исто така причина за ризик од оштетување што може да се реализира со вложените пари и транспарентност.

Според Европскиот центар за знаење -приватно партнерство (ЕПЕК), 1.749 ЈПП во вкупна вредност од 336 милијарди евра се финансиски склучени на пазарот на ЈПП во ЕУ помеѓу 1990 и 2016 година. Пред финансиската и економската криза, пазаротна ЈПП доживеа нагло зголемување на обемот, но од 2008 година бројот на нови проекти за ЈПП значително се намали. Во текот на 2016 година, комбинираната вредност на 64 ЈПП финансиски склучени на пазарот во ЕУ изнесуваше 10,3 милијарди евра. Најголем дел од проектите беа од транспортниот сектор, којво 2016 година изнесува една третина од вкупните инвестиции во ЈПП, а потоа следуваат здравствените и образовните сектори.

сл.1 Пазарот на ЈПП во ЕУ од 1990-2016

извор:Европски ревизорски суд според податоците од ЕПЕК

Пазарот на ЈПП во ЕУ е главно концентриран во Обединетото Кралство, Франција, Шпанија, Португалија и Германија, каде што 90% од вкупните проекти

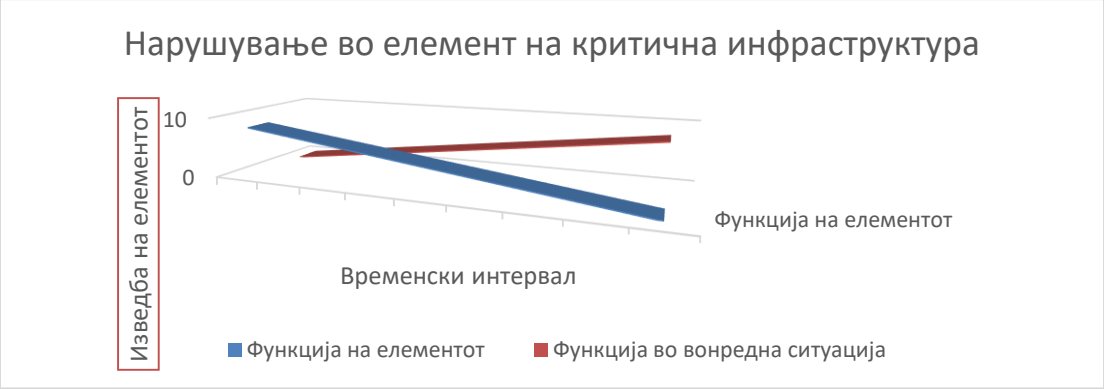
на пазарот беа спроведени помеѓу 1990 и 2016 година. Додека голем број проекти за ЈПП се имплементирани во некои земји -членки, како што е Обединетото Кралство со над 1000 проекти за ЈПП во вредност од речиси 160 милијарди евра спроведени во тој период, потоа Франција со 175 ЈПП во вредност од речиси 40 милијарди евра. Помалку од пет ЈПП проекти се имплементирани во 13 од 28 земји -членки. Тешкотиите што може да се сретнат при реализацијата на јавните-приватни партнерства може да имаат квалитативен и квантитативен карактер. Квалитативните потешкотии произлегуваат од фактот дека државата со своите безбедносни служби прави монолит, каде што нема доволно критична маса дел од одговорностите глатко да се пренесат на приватните компании, освен ако претходно не се трансформирале. Квантитативната содржина на потешкотиитекои произлегуваат од јавните-приватни партнерства извираат од фактот дека во одредени случаи, приватните компании немаат доволно експертиза да се справат со широкиот спектар на безбедносни услуги.[59] Заштитата на критичната инфраструктура е една од најоптималните области за воспоставување партнерства помеѓу јавниот и приватниот сектор, сооглед на нивниот многу чест јавен/национален или локален карактер, што може дасе преведе од јавна сопственост или јавно управување, или пак, јавни цели. Во таа насока, неприфатливо е да се прави разлика помеѓу јавниот иприватниот безбедносен сектор затоа што приватниот безбедносен сектор има комерцијален карактер затоа што услугите се наплатуваат. Како и да е, и услугите на безбедносните служби во јавниот сектор се наплаќаат и тие трошоци се на државна сметка.

Во Европската унија има трендови во врска со прераспределбата на одговорностите на јавниот сектор во корист на приватниот безбедносен сектор, што несомнено ги претставува насоките за понатамошен развој на приватниот безбедносен сектор. Факт е дека во секоја европска земја постојано расте присуството на приватни компании за безбедност во јавните служби за заштита.[60]

[59]Critical infrastructure Protection. Science Direct, достапно на: https://www.sciencedirect.com/topics/computerscience/critical-infrastructure-protection
[60]Mihaljević, B. Protection of Critical National Infrastrucutre: Challenges for the Private Security Sector. *Ann. Disaster Risk Science*. 2018, 1, 47-56

7. Закани и ризици по критичната инфраструктура

Функционирањето на системот на критична инфраструктура е под постојана закана од широк спектар безбедносни закани.[61] Во справувањето со потенцијалните закани, системот на критична инфраструктура вклучува многу елементи со различно ниво на важност, категоризирани во неколку нивоа и поврзани различно и со различен интензитет. Ефектите што произлегуваат од овие закани по критичната инфраструктура и нејзините потсистеми можат да предизвикаат помали и поголеми проблеми кои можат да предизвикаат нарушувања и дефекти во различни потсистеми.[62] Нарушувањето се однесува на функционалните параметри што предизвикуваат паѓање на одредени елементи и тој пад е директно пропорционален на интензитетот на вонредната ситуација и степенот на отпорност на елементот од критичната инфраструктура.[63]



сл.2 Нарушување во елемент на критична инфраструктура.[64]

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

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

[63]Бакрески О. Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура*, Дирекција за безбедност на класифицирани информации, Скопје, 2021, стр.63.

[64]Terrorism and Media including Internet- 2016 достапно на: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/336/html

Потребно е да се идентификуваат заканите и ризиците по системите на критична инфраструктура и нивната зависност. Некои од нив може да се однесуваат на национално, а некои на глобално ниво.[65] Тоа се следните:

- климатски и атмосферски влијанија (екстремни температури, суша, шумски пожари)
- хидролошки несреќи (поплави);
- метеоролошки појави (тропски циклони, силни конвективни бури, екстремни зимски бури);
- геофизички настани (земјотреси, цунамија, вулканскиерупции);
- 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, кинетички напади);
- сајбер инциденти (напад со одбивање на пристап, малициозенсофтвер, фишинг)
- нападврзланецотза набавка (експлоатација на ранливостите за предизвикување на системски и/илимрежен дефект);
- операции со странско мешање (ширење дезинформации и поткопување на демократски процеси);
- несигурни инвестиции (потенцијално да им се даде на странски инвеститори и непотребно влијае врз националната критичка инфраструктура).[66]

[65]Бакрески О., Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура*, Дирекција за безбедност на класифицирани информации, Скопје, 2021, стр.63.
[66]CISA. Critical Infrastructure Sectors, достапно на: https://cset.inl.gov/Lists/Critical_Infrastructure_Sectors/DispForm.aspx?ID=1&Source=

Заради полесна идентификација на заканите и ризиците по критичната инфраструктура како на локално, национално така и на глобално ниво, најпрво треба да се преземат следните чекори:[67]

- 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 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.

Идентификација и проценка на ризикот во критичната инфраструктура е најважниот чекор во креирањето на успешна стратегија за подобрување на безбедноста и нивната заштита. Идентификацијата на ризикот го вклучува процесот на пронаоѓање, пропишување и карактеризација на елементите на ризик релевантни за целите на управување, односно проценка на ризикот. Неопходно е да се идентификуваат изворите на ризик, настани или околности, како и нивните потенцијални последици. Сеопфатна идентификација и регистрација на ризикот е

[67]Federal Ministry of the Interior, Building and Community. Critical infrastructure Protection, достапно на:https://www.bmi.bund.de/EN/topics/civil-protection/critical-infrastructure-protection/critical-infrastructure-protection-node.html

од суштинско значење за понатамошна анализа. Идентификацијата треба да ги вклучува сите ризици без оглед дали се под контрола или не.

Кога зборуваме за ризици во критичната инфраструктура, дефинитивно се инволвирани фактори кои можат да го загрозат безбедното функционирање на критичната инфраструктура. Потребно е извршување на должностите од страна на операторите, како и сопствениците на КИ, социјална клима и интерперсонални односи меѓу сите луѓе неопходни за функционирање на КИ, како и безбедност на објектите технички и информатичко-комуникациски системи и други средства, и правилата за функционирање на самиот процес на КИ. Исто така, треба да се внимава ризиците меѓусебно да бидат условени и испреплетени и при промена на временски, просторни и еколошки фактори, односно средините доведуваат до појава на нови и промена на постојните ризици. Со други зборови, ризиците се променлива категорија, така што се намалуваат видовите ризици кои може да доведат до појава на нови или да се зголеми веројатноста за реализација на друг ризик, кој не треба да се занемари во процесот на анализа, идентификација и класификација на ризиците.

Можни опасности и проценка на ризик од природни катастрофи и други несреќи се класифицираат, во зависност од причината, на: сеизмички, хидросферски, атмосферски метеоролошки, биосферски и техничко-технолошки. Се врши евидентирање на карактеристиките на потенцијалните опасности, за секоја потенцијална опасност одделно, и според можните големини, според следново:

- Големина 1 - минимална опасност,
- Големина 2 – мала опасност,
- Големина 3 - средна опасност,
- Големина 4 - голема опасност и
- Големина 5 - максимална опасност.

По завршување на прелиминарната анализа на потенцијалните опасности од природни непогоди и други несреќи, се врши анализа на ризик, која резултира со

одредување на нивоата на ризик. Ниво на ризик, кое може да се движи од минимум 1 до максимум 25, се добива како производ на степенот на веројатност и степенот на последица. Степенот на веројатност што одговара на скалата на степенот на веројатност,се изведува на следниов начин:

1 - невозможно, 2 - неверојатно, 3 - веројатно, 4 - речиси сигурно и 5 - сигурно.

Степенувањето на последиците што одговара на големината на последиците, се врши според следното:

1-минимално, 2-мало, 3-умерено, 4 –сериозно и 5-катастрофално.

Врз основа на одредено ниво на ризик, класификацијата на ризикот се врши во категории од најниската (прва) до највисоката (петта) и потоа одредува кои ризици се прифатливи, а кои не. Прифатливите ризици се ризици од првата, втората и третата категорија, додека ризиците од четврта и петта категорија се неприфатливи. Врз основа на листата на прифатливи и неприфатливи ризици, дефинирана е листа на приоритети за третирање.

Класификација на безбедносните закани и ризици по критична инфраструктура може да се направи на неколку начини. Така, на пример, можно е врз основа на потеклото да се поделат во изолирани категории:[68]

Елементарните непогоди, грешките надвор од системот, може да се поделат на:

- Оние што се предизвикани од човечки фактор- лошо планирани активности во рамките на секторот, непромисленост на операторот на критичната инфраструктура, неадекватна соработка или координација на активности и
- оние предизвикани од техничко – технолошки причини, откажување на машини, дефектен драјвер или грешка во софтверот што се користи во рамките на некој инфраструктурен сектор.

[68]La Porte, T.R., *Critical Infrastructure in the Face of a Predatory Future: Preparing for untoward Surprise,* Vol. 15, No.1, 2007.

Нападите врз критичната инфраструктура се поделени на физички (директни терористички напади и саботажа) и виртуелни (сајбер-напади).

7.1 Природните непогоди и катастрофи закана по критичната инфраструктура

Овој вид катастрофи се случуваат во секое време и насекаде и можат да бидат со сериозни последици. Најчест вид се земјотресите кои имаат голема разорна моќ, потоа поплавите што можат да предизвикаат уништување на плодни почви и имот и да нанесат човечки жртви, а и големите пожари предизвикани од запаливи материи и сл. Овие природни несреќи се класифицирани во различни групи, според различни критериуми. Секоја од овие групи има свои карактеристики што ја условуваат организацијата и начинот на остранување на последиците од масовните несреќи. Тие се разликуваат и според интензитетот и причината за појавување, по опфатеноста на просторот.

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 не елементарни непогоди за кои е одговорен човекот, неговата работа (пожари, експлозии, техничко-технолошките катастрофи и сл.).[69]

Поплавите и пожарите се во категоријата појави што можат да се контролираат и да се дејствува превентивно, додека земјотресите се елементарни непогоди што се јавуваат брзо и ненадејно и човекот не е во состојба да ги предвиди однапред и да преземе превентивни дејства. Појавата на земјотресите и поплавите сериозно може да и се заканат на критичната инфраструктура и на тој начин каскадно да предизвика ефекти на загрозување на безбедноста, меѓу другото и во

[69]Бакрески О., Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура*, Дирекција за безбедност на класифицирани информации, Скопје, 2021, стр.66.

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.[70]

7.2 Хибридните закани по системите на критична инфраструктура

Хибридните закани се оние што чија мета се демократските држави и нивните процеси на донесување одлуки со повреда или поткопување на метата. Овие активности ги искористуваат сите видови ранливости во било кој домен кој ќе се најде 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 се позиционираат како сериозна и акутна закана за сите земји во светот.

Хибридните закани се мултидимензионални, и се во комбинација со присилни и субверзивни мерки, за кои се употребаат конвенционални, но и неконвенционални методи и тактики. Тие се дизајнирани да бидат тешкиза детектирање, или пак комплицирано е да бидат поврзани со било кој поединец или група.[71]

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

1) Периферен заштитен периметар – отворениот простор на одреден објект.
2) Заштита на имотот и систем на контрола на движењето на лицата во рамки на објектот и околината.
3) Видео надзор на јавни установи во градовите, стадионите, станиците, терминалите, шопинг центрите, фабриките, итн.[72]

---

[70]Бакрески О., Милошевска Т. и Алчески Ѓ., *Заштита на критична инфраструктура*, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 96.
[71]Бакрески О. Милошевска, Т,*Безбедноста на информациите и критичната инфраструктура*, Дирекција за заштита на класифицирани информации, Скопје, 2021, стр.69
[72]Improving the Security of International Infrastructures. OSCE Secretariat, достапно на: https://www.osce.org/secretariat/107809

Критичната инфраструктура станува сè повеќе автоматизирана и меѓусебно поврзана, а со тоа се воведуваат нови слабости во однос на дефектна опрема, 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. Заради тоа, критичката 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 дасе заштитат економиите и општествата.

8. Критичната инфраструктура во Република Северна Македонија и нејзина заштита

Критичната инфраструктура во Република Македонија е релативно нова област којашто сè уште е законски нерегулирана, односно сè уште не постои правна рамка за дефинирање, идентификација и заштита на критичната инфраструктура, а со тоа нема формална утврдена листа на критична инфраструктура. Сепак, треба да се нагласи дека идентификацијата на критичната инфраструктура нема да започне од почеток, затоа што е реално да се таа да се заснова на некои постојни акти што ја препознаваат оваа област. Овде треба да се нагласи проблематиката на задолжително обезбедување која е препознаена во глава 4, член 25 во првиот закон за обезбедување на имот донесен во 1999 година.[73] Имено во овој член е децидно пропишано дека „Владата определува кој правни лица се должни да имаат обезбедување на лица и имот за свои потреби, ако вршењето на нивната дејност е поврзана со ракување на радиоактивни материи или другии опасни материи за луѓето и околината; со предмети и објекти од историско и културно значење; како и во други случаи кога тоа е во интерес на обезбедност односно одбраната“.Во посебна глава IV во член 25 е пропишано „Владата на Република Северна Македонија определува кои правни лица се должни да имаат обезбедување на лица и имот и свои потреби, ако вршењето на нивната дејност е поврзано со ракување: со радиоактивни материи или други опасни материи за и околината; со предмети и

[73]Службен весник на РМ бр.80/99,66/07,51/11

објекти од особено културно и историско значење како и во други случаи кога тоа е во интерес на безбедноста, односно одбраната на Северна Република Македонија.“ Новиот Закон за приватно обезбедување во својата содржина ги следи суштинските определби на Законот за обезбедување лица и имот и издвојува посебна глава V, за уредување на темата „Задолжително приватно обезбедување“, која во Член 44, став 1 и натаму ја делегира обврската за определување на правните лица на Владата на Република Северна Македонија и ги набројува веќе утврдените дејности со претходното решение. Значајна интервенција Законот за приватно обезбедување врши со определувањето дека приватното обезбедување може да биде организирано или за сопствени потреби или може да се склучи договор за услуги. Во однос на пропишаното значајни се две карактеристики. Прво, и одредбите на Законот за приватно обезбедување укажуваат на тоа дека има одреден континуитет во насока на препознавање на критичните сектори и вториот значаен елемент на севкупното третирање на оваа значајна проблематика е дека во периодот од 10 години од донесување на Законот не постоеше акт што ги пропиша конкретните правни лица.[74]Затоа, Владата донесе Одлука за определување правни лица што се должни да имаат обезбедување на лица и имот за свои потреби.[75]

Со одлуката се дефинирани три групи правни лица. Двете групи се формулирани според дејноста на правните лица, а првата група врши дејност поврзана со ракување со радиоактивни материи или други по луѓето и околината опасни материи, а втората група правни лица врши дејност поврзана со ракување со предмети и објекти од особено културно-историско значење.Одлуката пропишува трета група правни лица што се должни да имаат приватно обезбедување врз основа на посебен критериум што е во интерес за безбедноста и одбраната на државата. Покрај Законот за приватно обезбедување[76], во законските решенија се препознаваат одредени елементи со кои се идентифика критичната инфраструктура. Законот за одбрана, во Глава 6 која ги дефинира субјектите од

[74] Правна рамка за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр. 43
[75] Правна рамка за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр. 43
[76] „Сл.весник на РМ“ бр. 166/2012, 164/2013, 148/2015, 193/2015, 55/2016

значење за одбраната, за какви што се сметаат јавните претпријатија и трговските друштва од областа на енергетика, сообраќајот, врските, комуналните дејности и градежништвото.[77]

Потребна е соработка меѓу релевантните субјекти заради заштита на критичната инфраструктура. Затоа познавањето на механизмите на приватниот безбедносен сектор треба да се заснова на целосно разбирање и разграничување заради избегнување на било какви импровизации, а соработката меѓу секторите е од голема корист.Одредена состојба може да стане проблематична, ако се направи лоша проценка и координација, но и недостаток на навремени информации што укажуваат на постоење опасност и неподготвеност на субјектите да се справат со безбедносните предизвици. Од голема важност е носењето на одлука на вистински начин и во вистинско време како и постоење на потребната координација меѓу релевантните субјекти, што често пати е ненавремена. Секоја избрзана или задоцнета одлука може да биде пресудна во заштита на критичната инфраструктура.[78]

Македонија треба да презема чекори за кохерентна имплементација на мерките за подобрување на заштитата на критичната инфраструктура и дефинирање на обврските на сите субјекти засегнати со оваа проблематика. Спроведувањето на мерките е директно поврзано со постоење, односно непостоење на соодветна процена која треба да укаже или да претпостави на одредена закана. Проценатa на ризици врз самите критични инфраструктури претставува процес во кој се анализираат собраните безбедносни информации со определување на приоритети по однос на критериумите, евалуацијата и веројатноста. Што се однесува до заканите и ризиците врз критичната инфраструктура нема дилема дека централната улога му припаѓа на приватното обезбедување во нашата држава. Оттука потребно е преземање соодветни чекори во однос на превенција, подготвеност и одговор на заканите врз критична инфраструктура со која ќе се обезбеди адекватна заштита и врвните приоритети во заштита на критичната

[77] Закон за одбрана, „Службен весник на РМ “, бр. 185 од 30.12.2011 година (член 90-96).
[78]Бакрески О., Милошевска Т., и Алчевски Ѓ., *Заштита на критична инфраструктура*, Комора на РМ за приватно обезбедување, Скопје, 2017, стр. 192.

инфраструктура. Во координацијата во безбедноста за заштита на критичната инфраструктура, во нашата држава треба да претходат фази на подготовка, планирање и усвојување и адаптација на подзаконски акти од различни закони, меѓу кои: законот за енергетика, законот за заштита и спасување, законот за приватно обезбедување, законот за одбрана, закон за безбедност на мрежи и информациски системи, понатаму Националната стратегија за сајбер-безбедност, Стратегијата за одбрана и други.[79]

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

9. Дефинирање на сајбер криминалот

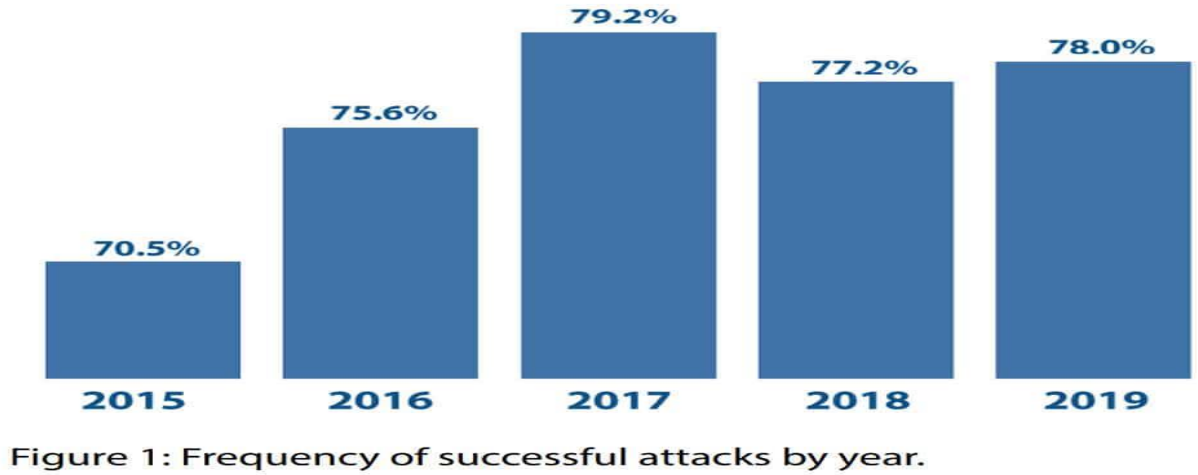
Еден од најголемите проблеми е немање единствена дефиниција за новите облици на криминалитет, така што ниту сајбер криминалот не е исклучок, и иако постојат повеќе дефиниции, не постои дефиниција за сајбер криминалот што е општо прифатена. Тешко дека со една дефиниција може да се опфатат, сите кривични дела што спаѓаат под овој вид криминал, поради големата различност на овој облик на криминогено однесување. Сајбер криминалот е само форма од која произлегуваат различни облици на криминална дејност. Се работи посебен вид криминалитет насочен против компјутерските системи, или еден дел, каде што на различни начини и со различни средства со намера за себе и за другите да прибават било каква корист или да нанесат штета на друг.[80] Во литературата постои став дека сајбер криминал е дел од стопанскиот криминал, но и сфаќање дека се работи за имотен криминал и дека компјутерските кривични дела по својот карактер се најблизу до имотните кривични дела.

Најсеопфатната дефиниција го дефинира сајбер криминалот како збир на сите деликвентни однесувања со кои уредитеза електронска обработка на податоци се користат како средство за постигнување на казниви дејства или како директна цел за казнување на дејството.[81] Во Прирачникот на кривичното правосудство на САД од 1979 година, дадена е првата дефиниција за сајбер криминал и според кој претставува секој нелегален акт за чие што успешно гонење е неопходно добро познавање на компјутерска технологија. Работната група на експерти од ОН на 11 Конгрес за превенција на криминалитетот и кривичното правосудство одржано во 2005 година во Банкок го дефинирала сајбер криминалот како општ поим што опфаќа кривични дела што се вршат со помош на компјутерскиот систем или мрежи, во компјутерскиот систем или мрежи или против компјутерскиот систем или мрежи. Комисија на Европската Унија во 2001 година го одредила поимот сајбер криминал во најширока смисла, така што под сајбер криминал се подразбира

[80] Donn B. Parker. *Fighting computer crime*, New York (USA), 1983, str.70.
[81] S. Konstantinović-Vilić, V. Nikolić-Ristanović, *Kriminologija*, Niš, 2003, str.178-179.

секое кривично дело што на било кој начин подразбира употреба на информатичка технологија.[82]

Најшироко прифатена и употребувана дефиниција е дека сајбер криминал е општествено опасна појава за чие остварување, сторителот користи знаења од компјутерската технологија така што компјутерскиот систем е сфатен во најширока смисла што се користи како средство или како објект за криминален напад или заедно.[83] Од дефинициите може да се сфати дека опсегот на криминални дејства е е широк и дека под сајбер криминал се смета секое дејство што се врши со помош на компјутер, компјутерски мрежи и програми. Покрај дејството што е насочено кон прибавување на противправна имотна корист, сајбер криминалот опфаќа и активности што се прават со друга цел како и создавање и дистрибуција на вируси, објавување на доверливи лични и деловни податоци на интернет и сл.[84]



сл.3 Статистика на сајбер криминал во светот[85]

[82] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN.
[83] B.Simonović, K*riminalistika*, Pravni fakultet u Kragujevcu, Kragujevac, 2004, str. 665
[84]Ţ.Aleksić i M.Škulić, *Kriminalistika,* Beograd, 2007, str. 46-63.
[85]300+Terrifying Cybercrime and Cybersecurity Statistics (2021 EDITION) достапно на:https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

9.1 Историјат на сајбер криминалот во светот

За првпат зборот “hack” бил употребен во 1960 година во група за правење на модели на возови на МИТ, во врска со начинот на манипулирање со моделите на возови. Во 1970 година почнало појавувањето на првите телефонски “криминалци” т.н. phreaks. Тие се занимвале со провала во телефонските централи од каде извршувале бесплатни повици. Најпознат од оваа категорија на криминалец (phreaker) е John Draper (Captain Crunch). Тој е креатор на “blue box” – електронска направа која произведува звуци со одредена бранова должина со кои може да се остваруваат бесплатени телефонски повици. Исто така во оваа категорија спаѓаат и Steven Wozniak и Steve Jobs (основачите на Apple), кои започнуваат сериско производство на вакви направи.

Во 1983 година е снимен филмот “War Games” кој претставува како инспирација за голем број луѓе низ целиот свет, да станат хакери. Истата година била фатена група со име “414” , која во рој од 9 дена, провалила над 60 компјутери меѓу кои спаѓале и компјутерите на “Los Alamos National Labaratory” – фирма која се занимавала со делови за нуклеарно вооружување. 1984 год. се појавува првиот хакерски магазин “2600”1986 год. бил донесен првиот закон за компјутерски криминал кој бил со многу недостатоци за лица кои се компјутерски криминалци. Во 1988 год. бил создаден првиот црв (worm). Креатор на овој црв бил Robert T.Morris кој бил студент на Cornell University и син на главниот научник во NSA (National Security Agency). Тој го тестира својот “црв” на ARPAnet и тој се проширил на 6000 компјутери. Тој добива 3 години условна казна и 10.000’ парична казна. Во 1990 год. операцијата “Sundevil” во 14 града низ САД, тајната служба врши апсење на членови од BBS (Bulletin Board Systems). Обвинението на членовите на BBS се: злоупотреба на телефони и телефонски системи, неовластено користење на кредитни картички и слично. Во 1993 год. Kevin Poulsen (повеќе познат како Dark Dante) провалува во телефонска централа во Los Angeles за да биде единствениот кој што ќе може да се јави во радио емисија каде што главната награда било: автомобил Порше и две патувања. За ова дело тој добива казна затвор 5 години. Во 1995 год. била извршена голема компјутерска кражба вредна 10 милиони долари.

Одговорноста за ова дело е на Владимир Левин, водач на руска хакерска група. Тој успева да "извлече" од CityBank 10 милиони долари и да ги префрли истите на сметки во Финска и Израел. Од 10-те милиони долари, 400.000 долари никогаш не се пронајдени. За овој случај тој добива 3 години затвор. 1995 год. уште е запаметена по апсењето на Кевин Митник, еден од најдобрите хакери на сите времиња. Тој имаше безброј обвинениј меѓу кои се: крадење на 20.000 кредитни картички, упад и неовластено користење на бројни компјутерски системи во USA, како на приватни фирми така и во државни институции. Заради ова тој 4 години во затвор ја чекал судската пресуда, а таа била: уште 4 години затвор. Во 2003 година Кевин Митник почнува да се занимава со компјутерска безбедност. Тој е основач на Defensive Thinking во Лос Анџелес, фирма која се занимава со компјутерска безбедност и денеска претставува еден од најпознатите експерти на тоа поле. Во 2000 год. се случуваат најголемите DOS (Denial Of Service) напади. Притоа хакерите прават најголеми напади на: eBay, Yahoo, Amazon и други поголеми компании. Истата година хакери провалуваат во Microsoft мрежа и го крадат source code-от за најновите верзии на Windwos i Office. Исто така во 2001 година Microsoft станува жртва на DOS напади и блокирање на DNS адреси. Резултатот на тоа е: милиони луѓе немаат пристап до Microsoft сајтот 2 дена.

Во 2002 год. меѓу позначајните компјутерски криминали се смета делото на Британецот Garry McKinnon кој неавторизирано пристапува во компјутерската мрежа на NASA и во американската воена мрежа и причинува штета околу 900.000 долари. Според статистиките за 2006 година на Институтот за компјутерска сигурност во САД, беше проценето дека просечната штета на компјутерска измама изнесува 150,000 американски долари, додека просечната штета од физички кражби изнесува 10,000 долари.Оваа статистика е објаснета со примерот дека сајбер криминалец ќе направи измама и ќе добие пристап до кредитни картички, има поголем пристап до средства отколку оној криминалец кој ќе украде прирачник. Хакерот кој ќе добие неовластен пристап до комерцијален веб сајт може да добие пристап до илјадници разни кредитни картички. Сепак за скоро се постои превентива и секоја приказна има две страни. Во случајот на компјутерски криминал, со цел да се заштитиме од самите себе, но овој пат во дигиталниот свет,

мораме да развиеме нови системи за превенција и детекција на сајбер криминални активности. Мора да се создадат специјални одреди кои ќе ги истражуваат нелегалните активности, но истите, заради проблемите со анонимноста и човечките права, наскоро се соочија со големи проблеми заради нарушување на приватноста – битка која сеуште се води. Единствениот поголем прболем зошто превенцијата на сајбер криминалот не е толку ефективна е бидејќи детекцијата и заштита од истиот се навистина скапи.

9.2 Интеграција на контролен систем со корпоративна мрежа

Историски гледано, проблемот со индустриската сајбер безбедност беше поедноставен отколку денес, затоа што индустриските мрежи беа „зафатени со воздух“. Терминот „воздушен јаз“ доаѓа од деновите пред сеприсутната безжична комуникација. Во таа ера, „воздушниот јаз“ значеше дека не постоеше онлајн конекција од кој било вид помеѓу индустриската мрежа и јавната мрежа. Безбедноста и сигурноста на контролните системи што работат на овие големи индустриските сајтови беа безбедни од онлајн, далечински мрежи. Напаѓачот требаше или физички да добие пристап до сајт, или преку измами легитимен вработен, изведувач или посетител во извршување на нападот или извршување на нападот на местото. Воздушните празнини започнаа да исчезнуваат во голем број во средината на 1990 тите години.Тоа беше почеток на “IT/OT integration –термин што беше широко прифатен. Како што контролните системски мрежи се користеа на исти компјутети, оперативните системи, софтвери и мрежните компоненти како информатичко – технолошки системи, тие ја одделија ИТ технологијата и организацијата на оперативната технологија немаше повеќе цел. Интеграцијата на ИТ и ОТ тимовите и процесите беше поврзана со зголемената интерконекција на ИТ и контролните мрежни системи. Од средината на 90-тите индустриите ги откриј бенефитите од користење на податоците од контролните системи како дел на бизнис процесите (пр. кога корпоративните компјутерски системи се подготвени да разберат точно колку долго и тешко е користено секое скапо парче индустриска опрема, тие системи можат да го одложат одржувањето. Оваа функција на „предвидливо одржување“ го одложува скапото одржување на опремата доколку

индустриската опрема не се користи 100% од неговиот капацитет за целиот период од претходното закажано одржување. Надвор од апликации на високо ниво, интеграција на ИТ / ОТ мрежа е предвидливо и само одржувањето кое ги намалува трошоците за работа на големите индустриски локации околу 3-7%. На некои сајтови, ова е целата оперативна маргина на профитот на страницата. Постојат многу други примери, вклучувајќи пристап во реално време до материјали и производи, мерења на квалитетот, производство по нарачка и прилагодување во реално време, распоредот за производство за да се дојде до продажбата. Сите овие профитабилни апликации за споделување информации обезбедуваат привлечни бизнис мотивации за интегрирање на ИТ и ОТ мрежи. Проблемот со ИТ / ОТ мрежната интеграција, наспроти интеграција на ИТ / ОТ тим или деловен процес на интеграција, дали мрежната интеграција воведува нови ризици за сајбер безбедност. Во отсуство на каква било заштита од сајбер -безбедност, напаѓачите едноставно би можеле да се поврзат со мрежи на корпорации преку Интернет.[86]

9.3 Карактеристики на сајбер криминалот

Во однос на традиционалните облици на криминалитет, сајбер криминалитет брзо ги менува формите и обликот на дејствување, границите меѓу државите како и видот на оштетување. Овие кривични дела се вршат прикриено, често без видлива и блиска поврзаност на сторителот на делото и жртвите. Најчесто тешко се откриваат и уште потешко се докажуваат, а долго време остануваат практично неоткриени се' додека оштетениот не претрпи некоја штета што е видлива во компјутерскиот систем.[87]

Значајна карактеристика на сајбер криминалот е неговата феноменолошка разновидност и големата динамика на развојот.[88] Бројот на облиците на сајберкриминалот е огромен и во постојан пораст, благодарение на постојаниот развој на технологијата секојдневно се појавуваат нови и посложени форми на

[86]Robert M. Clark, Simon Hakim, *Cyber-Phisical Security*, Switzerland, 2017,p.69
[87] Igor Ţ. Ţivkovski, *Otkrivanje i razjašnjavanje kompjuterskog kriminaliteta*, 2012, Beograd, str.162-165.
[88] Alisdair A. Gillespie. *Cybercrime: Key Issues and Debates Florence*, Kentucky (USA), 2015.

сајбер криминал. Како што компјутерската технологија наоѓа примена во сите сфери на животот, можностите за злоупотреба се поголеми секојдневно и се јавуваат значително поопасни облици на криминално однесување што порано не биле познати во криминалната пракса.

Втора значајна карактеристика на сајбер криминалот е што не ги познава границите меѓу државите и континентите. Извршителот може од било кое место на светот да нападне одреден компјутерски систем без оглед каде се наоѓа, овозможено од големата брзина на работа на компјутерите како и просторната и временската рамка што немаат никакво значење кај повеќето облици на сајбер криминал.

Со сајбер криминал се занимаваат лица што многу добро ја познаваат информацискатa технологија. Во првите години од развојот на информацискатa технологија, високата стручност била предуслов за ракување со компјутери, а тоа доведувало до тешко разоткривање на сторените кривични дела. Денес состојбата е променета, достапноста и едноставноста во користењето на компјутерите и ширењето на информатичката писменост овозможиле ширење на употребата на компјутерите што се составен дел на секојдневниот живот, а со тоа е намалено и времето што е потребно за стекнување на неопходните знаења и вештини за извршување на кривични дела од областа на сајбер криминалот.

Мал е ризикот за откривање на сторителите, а фактот дека овие дела се извршуваат во информациско опкружување, овој вид кривични дела дава одредена карактеристика, а тоа е дека овие кривични дела се вршат брзо, полесно, на разни начини каде што сторителот е анонимен затоа што современата информатичка технологија дава идеални услови на сторителите да ги прикријат своите криминални дејствија.Затоа е тешко да се соберат прецизни податоци за распространетоста на сајбер криминалот, за структурата на кривичните дела како и за нивните последици, така што бројката е огромна. Според некои проценки се движи од 90-99%.[89] Еден од основните проблеми во спречување и сузбивање на овој вид на криминал е и фактот дека само мал број извршени кривични дела се прибавени и расветлени од страна на полициските и правосудните органи.За

[89]D. Dimovski. *Kompjuterski kriminalitet*, Niš, 2010, str.205.

бројката на сајбер криминал карактеристични се следниве факти: малата веројатност на откривање, неуреденост во известувањето за извршените дела, неодговорна заштита, пораст на бројот на компјутери кој условува пораст на потенцијални извршители, тешко пронаоѓање на материјални траги за извршени кривични дела.[90]

Во текот на различните злоупотреби само мал број оштетени лица се свесни дека се жртви на кривични дела па така изостанува и поднесување на кривични пријави иако и дојде до откривање на делото, во повеќето случаи предоцна е да се преземат некои мерки. Карактеристично е и кога оштетените ќе откријат дека биле жртви на кривично дело, тие често не поднесуваат пријава и не ги известуваат надлежните органи. Во голем број случаи раководните оштетени субјекти настојуваат да ги сокријат овие овие кривични дела и да претрпат штета отколку да пријават при што ризикуваат да биде нарушена довербата. Ако дојде до неовластено влегување во информацискиот систем на некоја банка, и ако тоа се објави, клиенти со право стравуваат дека нивните податоци не се во сигурни раце и би побарале друг деловен партнер.

9.4 Цели на сајбер криминалот

За да се одредат целите на сајбер криминалот, претходно мора да се одредат основните поими. Компјутерскиот систем може да се дефинира како секој поединечен компјутер или група компјутери што се меѓусебно поврзани од кои во зависност од програмот за управување, еден или повеќе и се врши автоматска обработка на собраните податоци.

Компјутерските податоци можат да се дефинираат како секое изложување на податоци или концепти во облик што е погоден за нивна обработка во компјутерскиот систем, вклучувајќи и соодветна програма на основа на која компјутерскиот систем ја врши својата функција.[91]

[90] I.Feješ, *Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti*, 2000, str. 378.
[91] Član 1. Konvencije o visokotehnološkom kriminalu, Savet Evrope, Budimprešta, 2001. god

За потенцијални цели на компјутерскиот криминал можат да се земат хардверот, софтверот, програмите, податоците, заштита, услугите. Бројни активности што можат да имаат карактер на криминално дејство можат да се групираат на следниот начин:[92]

- Напад на хардвер (уништување, оштетување или отуѓување на компјутерски систем или негови компоненти).
- Напад на софтверот (уништување, оштетување, отуѓување и неовластена измена, објавување или користење на програмски производи).
- Напад на податоци (уништување, оштетување, отуѓување и неовластена измена, објавување или користење на податоци).
- Напад на заштита на системот (нарушување или пробивање на системот на заштита).
- Напад на услуги (неовластено користење на информатичките ресурси).

Компјутерската технологија воведе драстични промени во сите сфери на современиот живот. Тие промени донеле позитивни промени и низа проблеми поврзани со појава и ширење на сајбер криминалот, разни облици, форми и видови и тие можат да се сведат на следново: нови форми на вредност, концентрација на податоци, нов амбиент на делување, нови методи и техники на делување, ширење на географскиот простор, мобилност и стабилност на ризикот.[93]

Малициозниот софтвер што ги вклучува вирусите, тројанските вируси, адвер и спајвер ги напаѓа компјутерите преку добивање пристап до системи, следење активности и прибирање податоци, бот мрежи или киднапирани компјутери кои вршат задачи на далечина без знаење на нивните корисници и скратување на услуги кои се насочени кон исцрпување на достапните ресурси во мрежа, апликација или услуги за да се спречи пристапот на корисниците во нив. Физичките лица можат да претрпат финансиски загуби, но можат да бидат и жртви на кражба на лични податоци како и на идентитетот. Фирмите, жртви на сајбер нападите се соочуваат со потенцијални финансиски загуби како и загуби на чувствителни

[92] Slobodan R. Petrović, Kompjuterski criminal, Ministarstvo unutrašnjih poslova Republike Srbije, "*Bezbednost" - "Policajac*", Beograd 2000, str.45–46
[93] D. Littlejohn Shinder, M. Cross. *Cybercrime*, Burlington, MA, United States, 2002, str. 2.

деловни информации, податоци за патенти и лични податоци на нивните клиенти и корисници што може да доведе до сериозни последици по репутацијата на фирмите. Јавни и непрофитни организации можат да станат жртви на изнуда или кражба на личните податоци на корисниците на нивните услуги.

Сајбер просторот е местото за извршување на кривични дела како што е недозволена трговија со дрога, оружје и со чувствителни податоци и информации, трговија со луѓе и други платени убиства, физички напади и други форми на насилство. Договорите се случуваат на тн. даркнет каде што корисниците делуваат целосно анонимно. Со користење на даркнет, поединци и криминални организации користат енкриптивни алатки за праќање пораки и крипто валути за вршење финансиски трансакции, со што следењето и идентификацијата се тешки. Блек хет хакери се технички експерти што го користат потенцијалот на дарк нетот и анонимно реализираат продажба на сите оние што бараат начини за злоупотреба на конкретни системи.

Генерално сајбер-овозможениот криминал е во брз пораст и во развиените земји и во земјите во развој. По својата природа сајбер криминалот е меѓународен криминал којги преминува државните граници. Сторителите не мораат да бидатво истата држава како и жртвите или полицијата која што ги гони. Ова е еден одклучните предизвици во борбата против сајбер криминалот, бидејќи разликите воправните системи и пракси на различните вклучени држави можат да влијаат врзефикасноста и изводливоста на соработката, како и на размената на оперативнисознанија и докази. Одреден број на полициски служви во светот имаат капацитет независно да се соочатсо случаи на сајбер криминал, иако многу од нив имаат посебни единици за сајберили „компјутерски“ криминал. Како и со другите форми на малициозни активностиво сајбер просторот постои очигледнаасиметрија на вклучените трошоци. Како резултат на тоа, традиционалниот пристап на полициската работа со кривичните дела во одредена мерка се менува во сајбер сферата. Наместо непосредно апсење на сторителите, полициските единици за сајбер криминал главно се фокусираат на прекинување на тековни сајбер кривични дела и решавање на безбедносните пропусти кои биле злоупотребени. Поради еднаквата распространетост на предизвикот на атрибуција во целиот сајбер спектар

и долгите и напорни истражни постапки, вклучувајќи го и форензичното испитување на податоци, доаѓањето до правосилни пресуди е исто така побавно во споредба со традиционалните кривични дела. На државно ниво борбата против сајбер криминалот бара соработка од сите страни.

Приватниот сектор е најчестата мета на сајбер криминалците и неговите искуства и интереси треба да се земат во предвид при планирањето на стратегии за борба против сајбер криминалот. Експертите за сајбер криминал од приватниот сектор, како и академската заедница и граѓанското општество, истотака можат да придонесат во планирањето на политики за борба против сајбер криминалот со технички капацитети и знаење. За ефективна борба против сајбер криминалот, владите мораат да негуваат јавно – приватна соработка и да го поддржуваат воспоставувањето на мрежи на доверба. Подеднакво важна е превенцијата на сајбер криминалот и заштитата на индивидуалните корисници. Преку општо подигање на свеста и градење на капацитети, корисниците требаат да научат како да препознаат потенцијал но измамнички емаил пораки, малициозни содржини и потенцијално лажни контакти. Дури и релативно едноставни активности можат да имаат големо влијание во спречувањето на сајбер криминалот, како на пример обуки,за корисниците да одржуваат основна сајбер хигиена и користат силни лозинки, ажуриран лиценциран софтвер и енкрипција.

На меѓународно ниво постигнат е напредок со усвојување на Конвенцијата за компјутерски криминал на Советот на Европа[94], која исто така се нарекува Будимпештанска конвенција. До денес, Будимпештанската конвенција е единствениот обврзувачки меѓународен инструмент за сајбер криминал кој пропишува упатства за државите за развивање на сеопфатни национални законодавни рамки во борбата против сајбер криминалот и воспоставување на рамка за меѓународна соработка меѓу земјите потписнички. Меѓутоа, со шеесет и една потписничка и уште десет закони се очекувада се приклучат, истата се уште не е универзален глобален документ. Сепак во последните години можат да се забележат случаи на меѓународна соработка. На пример, меѓународните

[94] Конвенција за компјутерски криминал. Совет на Европа. Договор бр. 185.

организации за полициска соработка, првенствено Интерпол и Европол, се вклучени во активности насочени кон јакнење на меѓународните капацитети и создавање на рамки за преку гранична соработка меѓу различните полиции. Поради претходно споменатите потреби за одржување на националните единици за борба против сајбер криминал, овие рамки можат да ги надоместат ограничените национални капацитети, вклучително и преку развојот на јавно – приватни партнерства и мрежи надоверба меѓу експертите од различните сектори на општеството.[95]

9.5 Облици на сајбер криминал

За сајбер криминалот се смета секое незаконско однесување насочено кон електронските операции на компјутерските системи и податоци што се обработуваат. Во поширока смисла, сајбер криминалот се поврзува со секое незаконско однесување поврзано за компјутерскиот систем и мрежите, вклучувајќи и незаконско поседување, нудење и дистрибуција на информации преку компјутерските системи и мрежи. Наведени се неколку конкретни облици на овој вид криминал:

- Неовластен пристап до компјутерскиот систем или мрежа преку кршење на мерките за заштита.
- Оштетување на комјутерските податоци или програми.
- Компјутерска саботажа.
- Неовластено пресретнување на комуникации.
- Компјутерска шпионажа.

Сајбер криминалот во поширока смисла најчесто се појавува во следните облици:

- Компјутерски фалсификати.
- Технички манипулации на уреди или електронски компоненти на уредите.

[95] Клопфер, Ф. *Вовед во управувањето со сајбер безбедност* – прирачник за пратеници, Geneva Centre for Security Sector Governence, Женева, 2019 стр.7

- Злоупотреба на системот на плаќање како што е кражба на електронски кредитни картички или користење на лажни шифри во незаконити финансиски активности.

Терминот сајбер-криминал, најчесто е мошне широко толкуван и во теоријата не постои една широко прифатена и унифицирана дефиниција за него. 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 компјутерските системи.[96]

Одредени автори укажуваат на постоење на четири основни класи на меѓузависност, кои меѓусебно не се исклучуваат:

- Физички, како резултат на физички врски помеѓу инфраструктурите. Output на една инфраструктура е input за другите и обратно;
- Сајбер, како зависност на податоци разменети преку информационата инфраструктура;[97]
- Географски, настанати како резултат на просторната близина за кои нерегуларни настани може да создадат корелација и промени во соседните инфраструктури;
- Логичка, кога зависноста не се изразува преку физички, сајбер и географски механизми.[98]

[96] Wilson, C., Botnets, *Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, January,2008, p. 7

[97]Во голем степен функционирањето на современите инфраструктури зависи од компјутерските контролни системи.

[98]Rinaldi, S., Peerenboom, J., Kelly, T., „Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies “, *IEEE Control Systems Magazine*, Vol. 21, No. 6, Dec 2001, стр. 11-25.

10. Сајбер нападите како закана за критичната инфраструктура

Сајбер закана, сајбер криминал и сајбер простор се термини кои често се користат денес. Терминот компјутерски криминал е понов, бидејќи компјутерот првично се користеше само за научни цели и при размена на податоци преку Интернет. Подоцна, како извор на податоци почнува да се користи во повеќе различни гранки на економијата. Покрај добрите намери, создава и проблеми, кои ги користат и злоупотребуваат криминалните групи. Интернетот поедноставува многу правни операции помеѓу ентитети од различни држави.[99] Денес, државите го обучуваат персоналот за користење технологии кои ќе можат да ги следат во работата и да соработуваат на глобално ниво со цел да би можеле да разменуваат информации, со цел да се спречат овие модерни форми на криминал. Глобалната поврзаност, која доколку се користи на соодветен начин може да обезбеди и целосна анонимност, ги зголемува можностите на злонамерните корисници за пристап, кражба и злоупотреба на чувствителни информации. Голем дел од злонамерните корисници и криминални организации го препознаа сајбер просторот како можност за брза добивка, притоа овозможувајќи им намален ризик од нивно откривање. Глобализацијата и анонимноста им овозможуваат на злонамерните корисници полесни напади кон претходно точно дефинирани жртви, но воедно и реализирање на многу поголеми операции и напади од многу поголеми размери.

10.1 Извори и закани против сајбер криминалот

Клучен извор се странските разузнавачки служби, кои преку сајбер закани вршат дестабилизација и заплашување на одделни држави. Ова е обично се случува кога конфронтираните разузнавачки служби, особено ривалските, „се хранат“ со дезинформации и гласини заради заплашување, кое понекогаш може да се претвори во вистинско сајбер ривалство. Кога станува збор за нарушување на

[99]Ментюкова, М. А. & М.М. Дубровина.
Эволюцияуголовнойответственностизадоведениедосамоубийства с использованием сети Интернет. *Журнал Вопросысовременной науки и практики,* (44), 2013, 81-86.

приватноста и безбедноста на поединци кои претставуваат закана, тие полесно се откриваат. Голем проблем е што државните органи во многу случаи го прават тоа без судска наредба и демократска контрола. Во глобалниот свет, големите корпорации можат да се поврзат со криминал, и добро обучени хакери за саботажа и шпионажа. Корпорациите собираат голема количина на лични податоци, со што се загрозуваат човековите права, во зависност од интересите што ги имаат, ги делат со индивидуални криминални организации и владите кои соработуваат со нив. Хакерите се извор на закани, бидејќи со помош на Интернет можат да предизвикаат напад на сајтови. Средствата за напад се подобри од ден на ден, така што резултатите од софистициран напад се поочигледни. Во последно време, веб - страниците што нанесуваат политичка штета на противникот, сé повеќе се напаѓаат. Инсајдерите обично го знаат системот на жртвата, така што лесно можат да пристапат до него. Во Америка, според информациите најчесто се случуваат напади однадвор од државата.

Со оглед на фактот дека постои време кога има тајни и отворени конфликти, се формираат групи за тероризам кои имаат капацитет за сајбер напад. На подземната сцена на пазарот се ботнет оператори кои, всушност, ги претставуваат хакери кои запленуваат сé поголем број компјутери, преку кои се подготвуваат за нови напади. Сето ова е измама и спамирање. Спамирањето вклучува испраќање спам (е-пошта), а фишерите се поединци или мали групи кои извршуваат казни за идентитет со што се стекнуваат со големи количини на незаконски заработени пари. Користење спам или софтвер за шпионажа, се реализира преку испраќање на лажни информации, а нивната цел е да ги продадатнивните производи, да дистрибуираат малициозен софтвер, со што се извршуваат напади врз разниорганизации. Посебна закана во овој вид криминал претставуваат педофилите кои со помош Интернетот шират податоци (фотографии, видеа) со сексуална злоупотреба на деца, користејќи интернет простории за разговор.[100]Една од најголемите закани во светот е сајбер тероризмот, кој денес е во пораст. Тука мислиме на напади врз информациите на компјутерските системи,

[100]United States Government Accountability office, 2009., P.G.; Wulf &Jones, 2009.; 943; Golumbic, 2007

различнипрограми и податоци. Според Вулетиќ, сајбер тероризмот е „криминално дело извршено so компјутеришто резултира со насилство, смрт и / или уништување, создавајќи терор за да ја убеди владата да се променинејзината политика.[101]

Во време на големи технолошки разлики, особено помеѓу развиените и силните индустријализирани земји и сиромашни земји, кога нема можност да се води војна противмногу супериорен ривал, следуваат сајбер војни со сајбер тероризам. Овие терористи ги постигнуваат своите намери со помош на логички бомби, тн. тројански коњи, црви, со помош на разни вируси итн. Треба да се истакне исаботажатасо употреба на компјутерска технологија, упад во компјутерите на нуклеарните централии исклучување на големи електронски системи, блокирање компјутерски мрежи итн. Користејќи ги овие методи, на различен софтвер, овие актери можат да ја саботираатработата на берзите, го нарушуваат воздушниот сообраќај, односно контролата на летање, влијаат на промената на притисокотво гасоводи, како и попречување на државните органи и предизвикување штета на институциите.

Сајбер тероризамот се разликува од стандардните форми на тероризам во начинот на имплементација. Тоа е поприврлечно за терористите,бидејќи се прави без употреба на оружје. Овој вид тероризам е многу поекономичен, затоа што еполесно е да се најде хакер, да се плати и да се изврши задача со него, за разлика од конвенционалните терористи кои треба да се подготват, обучат итн., што бара големи ресурси, како и ризик од откривањеи изведување пред лицето на правдата. На овој начин, мисиите за самоубиство се избегнуваат, и тоа привлекува зголемување на медиумското внимание благодарение на начинот на извршување.

Постојат многу организации во светот кои реагираат на овие сајбер закани. Овие се:Apek-Tel, Enisa, Nato- Специјален координативен центар за сајбер-одбрана CCDCOE, ARSEAN,OAS, Тим за реагирање на компјутерски инциденти, Форум за управување со Интернет, Меѓународна телекомуникациска унија итн. Покрај наведените има и невладини организации: Human Rights Watch, Amnesty

[101]Vuletić, D. Napad na računarske sisteme, *Vojnotehnički glasnik*, Vol. 60, (1), 2012, 235-249.

International, Репортери без граници, итн. Најпознати од индустриските организации се: Конзорциумза промоција на безбедноста на Интернет (ICASI) итн.

10.2 Сајбер војна

Дефиницијата за сајбер војната е всушност чин на војување во сајбер просторот или преку сајбер просторот. Тоа е специфичен начин на војување што користи информатичко-комуникациски технологии за постигнување на воени цели и ефекти во физичките, информатичките и сајбер домени. Не постои меѓународен договор за тоа како треба да се дефинираат содржината, методите, техниките, средствата и целите на сајбер војувањето. Меѓународната заедница се уште се нема согласено околу мерките за градење на националните капацитети и меѓународната доверба или како да го примени постојното меѓународно право на сајбер војувањето, односно, заостанува и способноста на меѓународната заедница да изнајде решение за регулирање на сајбер конфликтите. Сторителите на сајбер нападите се прикриени, а ефектите имаат одложено дејство. Напаѓачите можат да бидат владини тела или органи, приватни компании, криминални организации, терористи или неформални групи и поединци. Повеќето земји немаат доволно капацитети за:

- Прецизно откривање на сајбер нападите
- Идентификација и атрибуција на напаѓачите
- Навремена прецизна реакција на сајбер нападите.

Недостатокот на правни прописи остава простор за потенцијална злоупотреба на сајбер нападите, која што може да доведе и до појавата на меѓународни и регионални кризи, особено во региони обременети со хронични политички тензии. Меѓународната заедница се уште се обидува да постигне договор околу начините за регулирање на сајбер војувањето. Постојат различни предлози, од кои еден е Прирачникот од Талин, подготвен од група академици во НАТО Центарот за заедничка сајбер одбрана во Талин, Естонија.[102] Одговорот во

[102] Клопфер, Ф. *Вовед во управувањето со сајбер безбедност*- прирачник за пратеници, Женева 2012 стр.13

меѓународни рамки е усвојувањето и примената на мерки за градење на капацитетите и довербата на национално, регионално и меѓународно ниво.

ООН создала гурпа на владини експети за новитетите на полето на информации и телекомуникации во рамките на меѓународната безбедност. Групата се има состанато пет пати во периодот меѓу 2004 и 2017 година за да разгледува постојни или потенцијални закани; норми, правила и принципи на одговорно однесување на државите; и мерки за градење на капацитетите и довербата.

Во Извештајот од 2013 година, ГВЕ заклучи дека „Меѓународното право, а особено Повелбата на Обединетите нации, е применливо и суштинско во одржувањето на мирот и стабилноста и промовирањето на отворено, безбедно, мирно и пристапно ИКТ опкружување"[103] Организацијата за безбедност и соработка во Европа (ОБСЕ) вложи дополнителни напори преку усвојувањето на Мерките за градење на доверба за зачувување на меѓународниот мир и стабилност (МГД).12 МГД се фокусираат на размена на информации и дијалог; заштита на критичните инфраструктури и националната безбедност; и промовирање и подобрување на соработката меѓу јавниот и приватниот сектор. Меѓутоа, обете иницијативи се доброволни (не се задолжителни за земјите членки на ОН и ОБСЕ) и нивното постоење не е директна и цврста гаранција за постигнување на мир и безбедност во сајбер просторот на меѓународно ниво.

Можно решение можат да бидат билатерални и мултилатерални договори меѓу различните држави. Овие договори можат да ги дефинираат нормите, стандардите и принципите на мирно однесување; да воспостават правила и процедури во случај на сериозни сајбер инциденти; да ја олеснат соработката и создавањето на заеднички капацитети за откривање на сајбер напади, идентификација на напаѓачите и атрибуција.[104]

[103]Извештај на Групата на владини експерти за новитетите во полето на информации и телекомуникаци и контекстот на меѓународната безбедност, 24 јуни 2013 година, Генерално собрание на ОН. Резолуција A/68/98

[104] Клопфер, Ф. *Вовед во управувањето со сајбер безбедност*- прирачник за пратеници, Женева, 2012 стр.14

10.3.Сајбер шпионажа

Сајбер шпионажата се дефинира како акт на тајно преземање и користење на сајбер капацитетите за собирање на податоци и ннформации со цел да се пренесат на спротивната страна. Пристапот е достапен кога лицето лажно се претставува како легитимен корисник или преку користење софистицирани напади, со кои се манипулира легитимниот корисник, им се отвара пристап на лицата кои имаат за цел да добијат неовластен пристап. Основната карактеристика на сајбер шпионажата е единствената асиметрија на вклучени трошоци. Трошоците за заштита се диспропорционално високи во споредба со трошоците на напаѓачот што треба да открие и злоупотреби една единствена слаба точка. Сајбер шпионажата е ефективна офанзивна алатка за извлекување на информации од системи, процеси и поединци. Се проценува дека потребното време за откривање упад е меѓу еден и три месеци кога напаѓачот може да добие пристап до огромни количини чувствителни информации. Предизвикот е да се направи разлика меѓу активностите на собирање на информации и активностите со малициозни намери кои може да се сметаат за чин на агресија. Според тоа, тенка е границата меѓу чиновите чија примарна цел е сајбер шпионажата и оние кои можат да се сметаат за непосредни сајбер напади. Поради ова исклучително е тешко да се утврдат меѓународни принципи и режими со кои се регулира идејата за сајбер шпионажа која, за сега, останува релативно нерегулирана.

Од безбедносна гледна точка се смета дека сајбер шпионажата може потенцијално да се преклопи со идејата за сајбер криминал. Во таа смисла, сајбер криминалците можат да бидат најмени од трети страни да вршат и/или овозможат дела на шпионажа со задача да продрат во владини и/или корпоративни системи и извлечат чувствителни информации.[105]

Уште еден предизвик е значаен, а тоа се државни спонзорирани кампањи за сајбер шпионажа каде што државите спонзорираат страни кои имаат капацитет за

[105] Клопфер, Ф. *Вовед во управувањето со сајбер безбедност*- прирачник за пратеници, Женева, 2012 стр.16

продирање во системите на нивните противници. Хакерите станаа потенцијални приватни шпионски армии во дигитална доба на располагање на најбогатиот купувач. Преку вклучување во сајбер шпионажа, државите сега се во можност да развијат хибридни односи со своите противници. Тоа ефективно значи дека односите во реалниот свет остануваат нормални, додека непријателските активности и судири се случуваат во дигиталниот домен преку користење на сајбер шпионажа заедно со хакирање и хактивизам, сајбер криминал и офанзивни сајбер активности. Сајбер шпионажата не мора секогаш да се врши од страна на државите или државно спонзорираните актери. Таа може да биде искористена и од сајбер криминалците, како и од приватниот сектор за едноставно добивање на финансиска добивка. Најдобра одбрана против сајбер шпионажата е одвраќањето. Тоа наведува до зголемување на реалните или претпоставените трошоци од потенцијалниот напад за противникот. Покрај градењето на посилна одбрана, ова исто така значи и промовирање на билатерална и мултилатерална соработка за постигнување на договори и/или кодекси на однесување со кои се регулира прашањето на сајбер шпионажа, покрај другите видови на однесување во сајбер просторот. Навидум успешен пример на ова е договорот од 2015 година меѓу САД и Кина за економска шпионажа, кој утврдува дека ниту една држава нема да врши или свесно да поддржува сајбер овозможени кражби на интелектуална сопственост со цел обезбедување на конкурентски предности на фирми или сектори во стопанството. Меѓутоа, сајбер шпионажата со цел добивање на разузнавачки информации за национална безбедност се уште не е регулирана. Поради оваа причина, постојат сé повеќе иницијативи од државите за дискусии во поглед на правото на „одмазда", или повратно хакирање кога ќе се открие упад во системот, како поубедлива форма на одвраќање. Една од земјите која им се приклучи на овие дискусии е Германија, каде што државната разузнавачка заедница бара да и биде дадено правото да користи активна одбрана. Ова имплицира право на уништување податоци кои се украдени или преместени од германски сервери, како и компромитирање на странски сервери за зајакнување на националните капацитети

за надзор. Идејата за овие иницијативи е одвраќање на потенцијалните напаѓачи преку заканата од одмазда.[106]

10.4 Сајбер тероризмот како закана за комуникациско – информациските системи

Сајбер тероризмот е значаен подсистем на сајбер војувањето, и е многу потежок за откривање и спротивставување, бидејќи е скоро неможно да се одреди политичката припадност или спонзорите на неговите извршители. Кога се зборува за поимот сајбер тероризам, според ФБИ[107], овој феномен се дефинира како: „обмислени, политички мотивирани напади против информации, компјутерски системи, компјутерски програми и податоци што резултираат со насилство против цели кои не се воени од страна на суб – националните групи или тајни агенти".

За разлика од сајбер тероризмот, сајбер војувањето е насочено спрема 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".[108]

---

[106] Клопфер, Ф., *Вовед во управувањето со сајбер безбедност*- прирачник за пратеници, Женева, 2012 стр.17

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

[108]Бакрески О. Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура, Скопје,*Дирекција за заштита на класифицирани информации, 2021, стр.81

Според Мишевски, сајбер тероризмот е насилен акт извршен со користење на интернет, преку кражба на доверливи лични податоци со цел истите да бидат искористени за заплашување или принуда/ присила поради остварување на одредени политички и општествени цели.[109]

Според Петровиќ, сајбер тероризмот е конвергенција меѓу сајбер просторот и терористичките активности што имаат за цел нанесување на сериозна штета како загуба на човечки животи или економски последици. Се изразува преку насилен планиран пристап, неовластено навлегување во системот, по правило оддалечен од местото што се наоѓа напаѓачот и сл. Кога се зборува конкретно за сајбер-терористички напади, веднаш се знае дека тие се насочени кон информациско-комуникациските системи односно нападот е извршен со помош на нив, а се насочени конкритичните инфраструктури. Сајбер-терористот како цели за напад може да ги земе информационите 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.[110]

Сајбер тероризмот е поврзана со сé поголемата зависност на општеството од интернетот и заканата од меѓународен тероризам.[111] Анонимноста и нерегулираната правна природа на интернетот го изложува на експлоатација и злоупотреба од страна на терористички организации и други недржавни страни. Сепак користењето на интернетот за тероризам е голем проблем за меѓународната заедница и секогаш се изнаоѓаат нови средства за борба против тероризмот.[112] Не постои универзална дефиниција за сајбер тероризам, повеќето дефиниции се однесуваат за напад што користи електронски средства за да се навлезе и сериозно да се попречи функционирањето на критичната национална инфраструктура.

---

[109]Мишевски Д. Осигурување од сајбер ризици, *Осигурување*, Национално биро за осигурување-Македонија, бр.11, Скопје, 2017.
[110]Бакрески О. Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура*, Дирекција за заштита на класифицирани информации, Скопје, 2021, стр.83.
[111] Ленц, Кристофер Е. Ленц. Обврска на државата да спречи и одговори на чинови на сајбер тероризам, *Чикаго журнал на меѓународно право*, 10 бр. 2, 2010.
[112] Клопфер, Ф. *Вовед во управувањето со сајбер безбедност*- прирачник за пратеници, Женева, 2012, стр.18.

ОБСЕ го дефинира сајбер тероризмот како сајбер поврзан тероризам или терористички напади врз сајбер инфраструктурата, а особено на контролните системи на критичната ненуклеарна енергетска инфраструктура.[113]

Сценаријата вклучуваат парализирање на важни урбани подрачја, секторот за јавно здравство или нарушување на финансискиот сектор со менување на неколку единици или нули.[114] Развојот на интернетот придонесе терористичките организации да ги искористат за реализирање акти на сајбер тероризам. Има многу терористички организации што го користат интернетот за вршење кривични дела како што е измама, неовластен пристап и недозволено мешање во компјутерски систем. Резолуцијата 1566 на Советот за безбедност на ОН нуди упатства во тој поглед. Кривични дела, вклучително и против цивили, извршени со намера да се предизвика смрт или тешки телесни повреди, или за земање заложници, со цел предизвикување на состојба на терор [...], застрашување на населението или принудување на влада или меѓународна организација да изврши или да се воздржи од извршување на некое дејство, што претставува прекршок во рамките на и според дефинициите во меѓународните конвенции и протоколи кои се однесуваат на тероризмот.[115]

Дополнително, терористичките организации го користат интернетот секојдневно за различни активности како што се пропаганда (вклучувајќи и радикализација, наведување на тероризам, врбување), финансирање, обука и планирање (вклучувајќи и преку тајни комуникации и информации од отворени извори), како и извршување на сајбер напади.[116] Додека употребата на интернетот за пропагандни цели зема голем замав во меѓународната заедница, повикувањето на посилни партнерства, вклучително и со технолошката индустрија, како и

[113] Добри пракси за заштита на ненуклеарната критична енергетска инфраструктура од терористички напади со фокус на закани кои доаѓаат од сајбер просторот, Организација за безбедност и соработка во Европа. бр. 16, 2013.
[114] Ген. Вотел, Јозеф Л. Разбирање на тероризмот денес и утре. *ЦТЦ Сентинел* 8. Издание 7, 2015, стр. 2–6.
[115] Одлука на Советот за безбедност 1566 (2004) за Заканите по меѓународниот мир и безбедност предизвикани од чинови на тероризам. 8 октомври 2004. Совет за безбедност на Обединетите Нации. Резолуција S/RES/1566. Оп. став 3.
[116]Употребата на интернетот за терористички цели, Канцеларија на Обединетите нации задроги и криминал, 2012.

предизвикотна употребата на интернетот за финансиски цели доста често се занемарува. Во меѓувреме, со општиот премин кон употребата на технологија во меѓународната трговија го трансформираше интернетот во средство за перење пари и пренос на средства на терористичките организации.[117]

Генерално, активностите за борба против тероризам кои го вклучуваат интернетот можат да имаат влијание врз повеќе човекови права (вклучувајќи ја приватноста и слободата на изразување, здружувањето, мирното собирање и религија или вера).

Во поглед на употребата на интернетот за пропагандни цели, владите усвоија нови мерки од побивање на активностите за оправдување или величање (апологетика)на терористички чинови до законски забрани за наведување на вршење на истите.[118] Меѓутоа, треба да се забележи дека говорот кој е морално одбивен, шокантен, вознемирувачки или навредлив не претставува сам по себе кривично дело; но „такви се барањата на плурализмот, толеранцијата и слободоумноста без кои не постои демократско општество".[119] Меѓутоа, предизвикот е во идентификација на точката во која полемиката или критиката се претвораат во говор на омраза, величање (апологетика) или наведување на вршење терористички чинови. Не е секогаш лесно да се идентификува оваа точка. Во суштина, важно е владите јасно да ги дефинираат релевантните кривични делаво кривичните законици на нивните држави, за да им се овозможи на граѓаните да ги предвидат последиците поврзани со одредени активности и да се избегне преголемото регулирање на човековите права. Гаранциите за исполнување на соодветниот процес, како што се пресумпција на невиност и правото на фер судење, се клучни во осигурувањето дека мерките за борба против тероризмот се ефективни и го почитуваат владеењето на правото. Понатаму, ефективниот надзор над страните во јавниот сектор вклучени во борбата против тероризмот (на интернет и

[117]Џејкобсон, Мајкл. Јуни Финансирање на тероризмот преку интернет. *ЦТЦ Сентинел* 2. Издание 6, 2009, стр. 17–20

[118] Побивање на приказните на терористите. 2017. Совет за безбедност на Обединетите нации S /RES/2354 (2017). Преамбула став 12, и Забрана за наведување на терористички чинови. 2005. Совет за безбедност на Обединетите нации S/RES/1624 (2005). Преамбула став 4 и оперативен став 1(а).

[119] Хендисајд против Обединетото Кралство. 4 ноември 1976. Совет на Европа: Европски суд за човекови права. 5493/72, оп. цит., став 49

вон него) се суштински во промовирањето на реформски процеси во борбата против тероризмот кои ги почитуваат човечките права.

Развојот на информатичките системи придонесува за севкупниот развој на општеството. Тој напредок го создава сајбер криминалот со кој треба да се соочиме, и кој зазема примарно место во структурата на кривичните дела во современиот свет. Самиот зборот сајбер на грчки значи некој што владее или владеење, а значењето на терминот е невидливо, незабележително и неограничено. Сајбер криминалот претставува професионално, посебно знаење и познавање за да се изврши кривично дело. Со намалување на можноста за контрола, националната безбедност се среќава со нови и опасни видови криминал, па се поставува прашањето- како да се обезбеди демократски метод на контрола на прописите што се поврзани со интернетот, како и заштита од овој вид на криминал, односно хакерска дејност.

Во современиот свет, сајбер пропагандата често е претходница на војните, револуциите и воените акции. Сајбер нападот тешко се открива, а разузнавачките агенции ги попречуваат овие откривања, насочувајќи ја својата активност на парализирање на службите кои вршат заштита и контрола. Тешкотии се јавуваат и на меѓународно ниво, затоа што проблемите за решавање како законската регулатива се различни од земја во земја, па сеуште нема прописи што би можеле да се применуваат на глобално ниво. Со создавање на Г8 може да се каже дека се направени почетните чекори на сопирање на овој вид криминал на меѓудржавно ниво. Но, може да се каже дека големите сили во светот, имале решавачко влијание така што нивните интереси избиле на прв план.

Со оглед на тоа дека поголемиот дел од земјите во светот немаат основна ИТ структура, постојат бројни фактори што вршат влијание, а тоа се: политички, правни, психолошки, технички итн. Овие фактори можеме да ги поделиме на:

- Правни, ако се однесуваат на кривично-правната регулатива како и откривање на кривични дела и нивно процесуирање и
- Социјални, ако влијаат на суштината на овој облик на криминал, како и опасноста од овој облик на кривични дела во едно општество.

Се поставува прашањето, со кои демократски процеси или правни стандарди треба да се раководи во текот на донесувањето одлуки за евентуална реакција? Ова е доста важно затоа што некои фактори драматично ја намалуваат транспарентноста на сајбер војната во однос на другите типови конфликти.[120] Може да се каже дека поединци и помали компании вршат злоупотреба на националната територија за создавање на хакерски напади. Нападнатите фирми не сакаат да даваат информации, од аспект на безбедноста и ги чуваат како тајни. Државите немаат многу начини да ги откријат фактите за преземените мерки. Повеќето земји во светот не се свесни и не знаат дека од нивните територии, поединци и разни компании лансирале хакерски напади. Тешкотија за разузнавачките служби е големата количина кои поединечно не претставуваат опасност, туку заедносо дејствување предизвикуваат вистинска штета. Ниту самата законска регулатива во тој домен не е опширна и добро објаснета за да може власта законито да реагира и спроведува како превентивни така и репресивни мерки, односно за да адекватно реагира на употреба на софтвер, што ќе детектира напад.

Во правната регулатива не постои начин да се дознае кој може да сподели сознанија и информации и со кои лица. Одговорноста, посебно во приватниот сектор, треба да се решава побрзо и поефикасно. Во ваква ситуација тешко може да се зборува за координирани акции и реакции заради спречување на овој облик на криминалитет. Во суштина, таа координација не постои или постои во многу мал обем, давајќи на тој начин можност и шанса за ваков вид на криминалитет.

Демократската власт кога станува збор за сајбер тероризмот подгрева додатни проблеми. Првиот е дисперзија на одговорност. Поради големото групирање на самостојните актери често е тешко да се утврди кој е задолжен за конкретната област. Затоа постои потреба да се премостат некои поединечни улоги во министерствата и механизми на закана и реагирање. Ова е посебно случај кога е во прашање вештачката поделба на безбедноста на државата и други државни

[120]Buckland, B., Schreier, F. & Winkler, T. *Demokratsko upravljanje*: izazovi Sajber bezbednosti, Beograd: Forum za bezbednosti demokratiju, 2010.

мрежи со различни улоги и одговорности.[121] Општеството мора да биде одговорно и сериозно да се спротивстави на сите облици на кривични дела, затоа што пристапот кон тоа е многу важен заради сузбивање на сајбер криминалот, што претставува одговорност на општеството, па е дефинирана како етичка идеологија каде што ентитетот има обврска да делува со загриженост и свест за влијанието на своите акции на други.[122]Што се однесува до индивидуалната одговорност, таа се однесува на секој поединец и неговата поединечна одговорност во однос на заедницата, додека кај корпоративната одговорност се однесува на почитување на меѓународните норми. Со развојот на технологијата настанува и проблем за усовршување и развој на информациските закани што е опасност за целото општество, односно човештвото. Значајно место заземаат истражувањата за проблемите, особено мултидисциплинарното решавање на прашањата за безбедноста на информациите. Треба да се постави прашањето дали безбедносните органи можат да ја следат преписката, така што во современиот свет многу земји ја следат и следат комуникацијата на разни терористички групи и криминални организации. Прашањето за приватност е значајно прашање.
Во компјутерите постојат податоци за луѓе достапни ширум светот. Колку што технологијата не ја загрозува приватноста на луѓето, луѓето се оние кои ја злоупотребуваат технологијата за сајбер криминал, лична контрола на приватноста. Затоа на секое општество му е потребна посилна контрола и сузбивање на овој вид криминал. Единствено преостанато место за колонизација се независните медиуми. Ова е нова област за човечка интеракција, економска експанзија и социјални и политички махинација.[123] Речиси и да нема влада во светот што може да ги принуди компаниите да преземат акции кога станува збор за безбедност, бидејќи најголемо влијание имаат транснационалните сили и поединци кои имаат свои интереси и цели. Сајбер безбедноста понекогаш наидува на пречки, а тоа се правото на приватности слободата на изразување. Проблемот е поврзан со технолошките знаења. На тоа може да се додаде јавно- приватната

[121]Buckland, B., Schreier, F. & Winkler, T. *Demokratsko upravljanje*: izazovi Sajber bezbednosti, Beograd: Forum za bezbednosti demokratiju, 2010.
[122]Mamić, D. D*ruštvene mreže kao omogućitelji društvene (ne) odgovornosti*, Zagreb: Fakultet elektronike i računarstva, 2012.
[123]Rushkoff, D. *Media Virus*. New York: Ballantine Books, 1996.

соработка од која произлегува сајбер безбедноста што е дисперзивна и излегува од рамките на агенциските овластувања.

10.5 Сајбер напади врз индустриските контролни системи и критичната информациона структура

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.[124]

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.[125]

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

[124]Pursiainen C., *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6, 2009.
[125]Национална стратегија за сајбер-безбедност на РепубликаМакедонија (2018-2022), јули 2018, достапнона: http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf

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 несечуваат 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 наголем 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 клучниинфраструктурни 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-отили дури и во микропроцесорите.[126]

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 истотака неважни, бидејќи една цел може да биде погодена од спротивната страна на светот за само неколку секунди.[127]

Како прв комбиниран напад на сајбер-напад и воена офанзива себе лежи нападот врз Грузија. DDoS – напад од мали размери (напади со дистрибуиран прекин на услугите) врз грузиската интернет инфраструктура, биле регистриран и 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 „Shadow server“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

[126]Nickolov E., “Modern Trends in The CyberAttacks against the Critical Information Infrastructure”, ITU, Regional Cybersecurity Forum, Sofia, Bulgaria, 2008, достапно на: http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolovmodern-trends-sofia-oct-08.pdf.
[127]Thomas A. Johnson (ed)., *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015.

кулминирале на 8 август 2008 година, првиот ден одвојувањето, кога биле регистрирани напади на веб-страниците на Владата и медиумите. Како се заострувал конфликтот, така ескалирале и on-line нападите кои руски те*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 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 хакерскифорум, ефикасно ја пореметила дистрибуцијата на информации на Владата на Грузија, во клучните моменти на нападот.[128]

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, медиумитеитн).

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 развојна иднатасајбер-војна.

10.6 Реализирани сајбер напади врз критичната информациска инфраструктура

Кога критичната инфраструктура ќе стане нефункционална, негативните ефекти можат да бидат широко распространети и катастрофални. Сајбер нападите се значајна закана за јавната и приватнатра инфраструктура. Само во изминатата година, 56% од енергетските комунални капацитети пријавиле барем еден сајбер -

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

напад што предизвикало загуба на податоци или исклучување на операциите. За да дадеме перспектива за трошоците за само еден напад - неодамнешниот хакер на SolarWinds, во кој беа откриени над 18.000 податоци за приватни и владини клиенти, ќе чини околу 100 милијарди долари за да се опорави. Пред да навлеземе во неодамнешни напади, прво вреди да се сфати што точно претставува критичната инфраструктура. Агенцијата за компјутерска безбедност и инфраструктура ги дели видовите инфраструктури што се сметаат за критични на 16 сектори:[129]

- комуникациски сектор
- комерцијален сектор
- критичен производен сектор
- одбранбен индустриски сектор
- услужен сектор
- енергетски сектор
- финансиски услужен сектор
- сектор за храна и земјоделие
- владин сектор
- јавен здравствен сектор
- информатичко – технолошки сектор
- сектор за нуклеарни реактор и отпад
- сектор за транспортни системи
- сектор за водниот потенцијал.

Се поставува прашањето, зошто сајбер нападите на критичната инфраструктура се зголемуваат? Како што луѓето и, што е уште поважно, инфраструктурата стана сè повеќе зависна од комуникациите и меѓусебната поврзаност, ранливоста на напади и експлоатација соодветно се зголеми. Настаните кои го менуваа светот во последната година ги принудија организациите да се прилагодат и да го вклучат далечинскиот пристап за да обезбедат

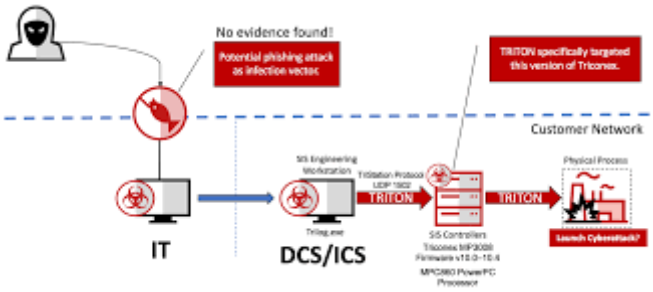
[129] Analysis of top 11 cyber attacks on critical infrastructure, 2021, достапно на: https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

континуитет. Тоа има своја цена, бидејќи повеќе од половина од индустрискиот персонал во САД верува дека индустриските мрежи немаат потребни безбедносни контроли за безбедно да работат. Уште повеќе, речиси три четвртини од персоналот за ИТ безбедност се позагрижени за нападите на критичната инфраструктура отколку за грешките во податоците на претпријатијата. Сосема очекувано, владите, регулаторите и другите јавни и приватни актери неодамна изврши притисок за зголемено финансирање и посветување внимание заради обезбедување на овие критични инфраструктурни сектори. Загриженоста е оправдана бидејќи истражувањето на персоналот во инфраструктурата покажа дека 90% од испитаниците имале еден безбедносен инцидент во последните 12 месеци, а половина имале најмалку два. Со оглед на тоа колку може да бидат катастрофални сајбер нападите врз критичната инфраструктура, вреди да се посочат нападите за да се научи како да се спречат во иднина.

За да се види колку овие напади се катастрофални, посочени се неколку примери за напад на критичната инфраструктура во светот.

10.6.1 Напад на малициозен софтвер Тритон 2017 година

Нападот на малициозен софтвер Тритон во 2017 година беше еден од потенцијално деструктивните и најопасните сајбер напади врз индустриските системи за контрола во последните неколку години. Овој државно спонзориран напад на малициозен софтвер беше откриен најпрво во саудиска петрохемиска фабрика, што им овозможи на хакерите да ги преземат системите за безбедност на фабриката. Овој злонамерен код можеше да доведе до експлозија или ослободување токсичен гас и беше прв таков напад што беше намерно дизајниран да предизвика загуби на живот. Истрагата заклучи дека фишингот бил првичниот вектор на напад што се користел за пристап до внатрешната мрежа на централата, иако други веруваат дека станува збор за погрешно конфигуриран заштитен sид. Фабриката можеше да го избегне нападот со постојано спроведување на безбедносни ревизии на нивната мрежа и обезбедување на нивните добавувачи да одржуваат ажуриран софтвер за нивните производи.



сл.4 Тритон малициозен сајбер напад[130]

10.6.2 Напад на Тајванската државна енергетска компанија

Државната енергетска компанија во Тајван, национално богатство задолжено за испорака на нафта и увоз на течен природен гас, беше цел на напад со откуп на софтвер. Иако производството на енергија остана неоштетено, хакирањето го уништи платниот систем на компанијата во хаос. Клиентите на бензинските пумпи не можеа да користат ВИП-картички за плаќање, а апликациите за плаќање беа некорисни, иако готовината и кредитот сè уште функционираше. Компромитиран флеш -уред е наводно непотврден виновник, а властите официјално не именуваа виновник, иако постои сомневање за хакерска група Виннти. Неколку мерки може да се воведат од страна на компанијата и другите даватели на енергетски сектори за да се спречат такви напади. Еден чекор е да се одделат Оперативните ИТ системи од мрежата и Оперативната технологија и да се стават оперативните технолошки процеси до степен што ги одделуваат критичните функции од останатите. Друго е да се ограничи пристапот до основните системи и контролорите на информатичките системи само на релевантни вработени.[131]

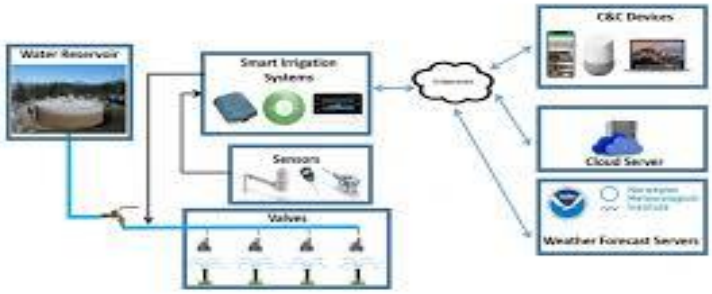
[130] KTH Royal Institute of Technology- достапно на: https://cnls.lanl.gov/External/GSSlides2021/Sandberg.pdf

[131] Information assurance, Semi- annual report 2020/1, Reporting and Analysis Centre for Information Assurance MELANI, 2020. Достапно на: https://www.newsd.admin.ch/newsd/message/attachments/63536.pdf

сл.5 Сајбер напад на државната енергетска компанија во Тајван

10.6.3 Израелски водни системи

Израелските водни системи беа цел на сајбер напади во голем број наврати кон средината на 2020 година. Нападите беа спроведени да ги компромитираат командните и контролните системи за пумпните станици во Израел, канализационите системи, постројките за отпадни води и земјоделските пумпи. Иако на крајот не успеаја, нападите имаа за цел да го зголемат хлорот и другите хемикалии во водата до штетни нивоа и да го нарушат снабдувањето со вода за време на топлотниот бран и „Ковид-19“. Групата ги искористи застарените системи кои сеуште се користат и несоодветни упатства за лозинка воспоставени во тие објекти. Редовното ажурирање на лозинките е навидум очигледно, но недоволно имплементирано решение за овие слабости, заедно со замена на застарената опрема и ажурирање на нивниот софтвер. Исто така, од суштинско значење е да се идентификуваат непознати уреди поврзани со мрежа и веднаш да се отстранат.



сл.6 Напад на израелските водни системи[132]

10.6.4 Напад на Нипон телеком

Оваа компанија, четврта по големина во светот, поддржува центри за податоци во повеќе од 20 земји во светот. Неодамна, тие имаа пробивање на податоците што беше потенцирано со големо планирање и повеќекратни фронтови за напад. Пробивањето на податоците опфатило податоци на 621 корпоративен клиент и хибриден по природа. Од Нипон телеком веруваат дека, вештачката интелигенција и машинското учење, заедно со алатките за напади на повеќе нивоа, биле имплементирани во пробивањето. Нападот бил лансиран од неколку надворешни, мрежно поврзани веб-локации, користејќи безбедносен пропуст во оперативниот сервер кој беше дел од серверот за управување со информации на компанијата. Вршењето рутински безбедносни проверки може да спречи напад од ваква природа, како и дополнителни безбедносни контроли. Овие поправки ќе го ограничат внесувањето на чувствителни податоци и од решенијата на компанијата и од вработените и ќе спречат ирелевантен пристап до податоци или системи.[133]

---

[132] Piping botnet – Israeli researchers warn of a potential distributed attack against urban water services that uses a botnet of smart irrigation systems that water simultaneously, Las Vegas, 2021, достапно: https://securityaffairs.co/wordpress/75389/hacking/piping-botnet-water-services.html

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

10.6.5 Напад на компанијата “Модерна“

Наводни хакери, поддржани од Кина ја испитуваа Модерна, компанија која е во првите редови на развојот на вакцината „Ковид-19“. Тие бараа пропусти на страниците и ги издвоија корисниците со проширено безбедносно овластување во мрежата во нивните обиди за хакерски напади. Примарниот начин на работа на хакерите беше искористување на софтверски пропусти во добро познат софтвер за развој на веб сајтот. Во овој случај, сепак, хакерите не беа во можност да украдат доверливи податоци и истражувања. Поголемиот проблем е што беше откриено дека хакерите тероризираат стотици претпријатија и владини агенции една деценија. Редовните безбедносни проценки, прегледи на кодови и надградби ќе ги направат побезбедни сличните компании и инфраструктурни објекти. Соработката со владините агенции може да помогне во ублажувањето на проблемите со безбедносна усогласеност и да понуди поддршка во зајакнувањето на безбедносните стандарди.

10.6.6 Неименуван американски оператор на природен гас

Оператор за природен гас во САД, кој остана неименуван, беше цел на хакерски напад што ги загрози ресурсите за комуникација и контрола. Сајбер-криминалецот прво користел тн. Spear Phishing Link за да добие пристап до информатичко технолошката мрежа пред да го употреби софтверот во мрежата. Компромитираните области вклучуваа интерфејси на човечки машини и складирање податоци. Централата никогаш не ја „изгуби контролата“ врз работењето, но тие беа принудени да затворат два дена додека не може да се набави и репрограмира опремата што е заменета. Недостатокот на сегментација помеѓу мрежите беше главната слаба точка на објектот.[134]

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

10.6.7 Напад на електричната мрежа во Украина

Украинскиот електроенергетски објект "Prykarpattya Oblenergo" во 2016 година беше уште еден пример на намерен, потенцијално смртоносен сајбер напад. Половина од населението (~ 700.000 поединци) во регионот на Ивано-Франковскиот во Украина, остана без струја во средината на декември поради напад на малициозен софтвер. Наводно од озлогласената руска хакерска група Sandworm, нападот користел опасен малициозен софтвер наречен „Black Energy 3". Сепак, овој напад не бил толку јасен. Хакерите, исто така, користеле убиец на хард дискови, Kill Disk, фишинг со копје, кражба на акредитиви, VPN, за далечински пристап, DoS телефонски напади и други тактики. Прво, за да се заштитат од такви повеќевекторски напади, мрежите мора да се сегментираат една од друга, а секој дел од мрежната опрема мора да има овозможено логирање каде што е достапно. Мониторингот на мрежата е исто така најважен во овој случај и задолжителен.[135]

10.6.8 Напад на железничкиот систем MUNI во Сан Франциско

Хакерите користеле софтвер наречен Mamba за да ја компромитираат градската железница (MUNI) во Сан Франциско во 2016 година, оневозможувајќи пристап до системот и шифрирање на преку 2000 канцелариски системи. Нападот ја принудил компанијата да ги затвори системите за издавање билети на четири дена, а на патниците им бил овозможен бесплатен превоз. Ниту еден патник или податок за трансакциите не бил загрозен во нападот, а "back up" му дозволиле на органот да ја врати функцијата на повеќето системи веднаш по откривањето на нападот. Периодичното надградување и извршување на безбедносни ревизии, констатирале дека ќе помогне да се откријат пропусти и заштита од евентуален повторен напад.[136]

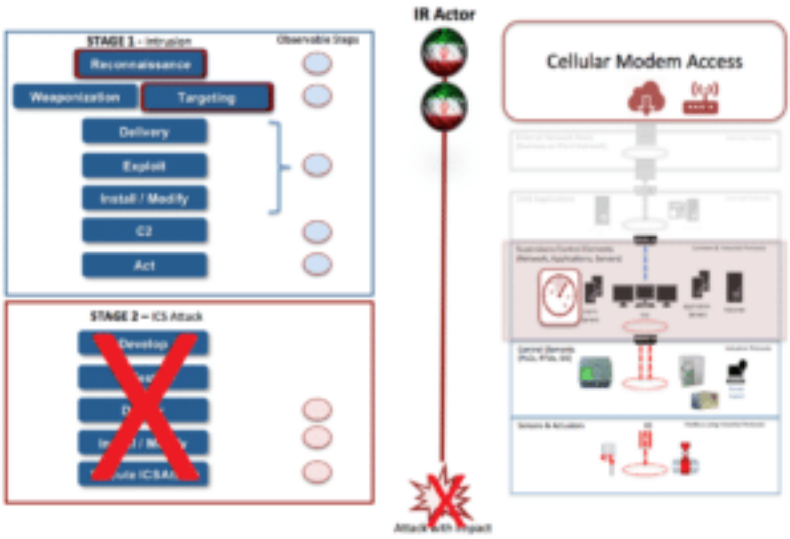
[135] Analysis of top 11 cyber attacks on critical infrastructure, 2021, достапно на:https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
[136] Analysis of top 11 cyber attacks on critical infrastructure, 2021, достапно на:https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

сл.7 Напад на железничкиот систем во Сан Франциско

10.6.9 Ирански сајбер напад на браната во Њујорк

Иранските хакери спонзорирани од државата, упаднале во системите за надзорна контрола и стекнување податоци (SCADA) на браната Бауман во Њујорк. Системот бил поврзан со мобилен модем, но бил одржуван за време на нападот.Хакерите ја искористиле незаштитената врска со модемот и недостатокот на безбедносни контроли за системите на браната. За среќа, хакерите пристапиле само до мала врата, но успеале стручно да изманипулираат со контролорите на SCADA. Нападот не бил сложен по природа, но се сметало дека е повеќе тест за да се испитаат слабостите.Критичните контролори за инфраструктура мора по секоја цена да се држат одделно од Интернет. Ако треба да се поврзани, мора да се спроведат соодветни безбедносни контроли и сегрегација, дури и за најмалите порти и цевки. Во овој случај, исто така, би требало операторите на браната да работат со општинската и државната влада за редовно да ја тестираат и подобруваат нивната безбедност.[137]

[137] Analysis of top 11 cyber attacks on critical infrastructure, 2021, Достапно на:https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/



сл.8 Сајбер напад на браната во Њујорк[138]

10.6.10 Напад на неименувана Американска институција за води

Хакери упаднале и ја презеле контролата врз мобилната мрежа на американската институвија за води, која останала анонимна. Сепак, нивните цели биле малку поинакви од некои други. Наместо да го нарушат снабдувањето со вода или да се обидат да ја отрујат водата, хакерите ги користеле мобилните рутери за да ги подигнат сметките за мобилни податоци за 15.000%, од 300 долари месечно на над 50.000 долари во период од два месеци. Слабата точка бил застарениот системски софтвер и фабрички инсталираната лозинка за рутерите на објектот. Подоцна истата година, била откриена ранливост во хард-кодираните ингеренции на рутерот, за што се верува дека е точката во која хакерите ги искористиле слабостите на мрежата.[139]

[138] Deconstructing the Reports of Iranian Activity Against the Power Grid and New York Dam, достапно на: https://www.sans.org/webcasts/deconstructing-reports-iranian-activity-power-grid-york-dam-101327/

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

10.6.11 Напад на колонијалниот нафтовод

На 7-ми Мај, 2021 година, еден од најразорните сајбер напади на инфраструктурата беше нападот на Колонијален нафтовод во САД. Најголемиот гасовод во САД и оној што снабдуваше повеќе од 45% од гасот, дизелот и авионското гориво на источниот брег беше принуден целосно да ги затвори своите мрежи и операции. Иако успеаја да ја вратат функцијата на системот, до 18-ти мај, речиси 11.000 бензински пумпи сè уште беа без бензин. Хакерската група Dark Side, исто така, украла повеќе од 100 GB податоци од серверите на компанијата пред нападот и ја предала контролата дури откако Colonial платила 5 милиони долари во криптовалута. Уште позначајно, просечната цена во САД за гас по галон се зголеми на национално ниво до највисоката цена во последните шест години. Векторот за напад сè уште е засега непознат.[140]

[140] Analysis of top 11 cyber attacks on critical infrastructure, 2021, Достапно на:https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

11. Национална стратегија за сајбер безбедност 2018-2022

Од описот на националните стратегии за заштита, се покажа дека и покрај нивните разлики, во сите стратегии може да се најдат клучни приоритетни области кои придонесуваат за ефективна холистичка стратегија за заштита на критичната инфраструктура. Овие области вклучуваат:

1. Визија/цели: Развојот на која било стратегија за заштита на критичната инфраструктура вклучува формулирање на стратешките цели (визија) кои се расчленети на индивидуалнимерливи цели.

2. Администрирање на безбедноста на критичната инфраструктура: Се однесува на административната/структурата на управување и назначување на надлежни и овластени тела за заштита на критичната инфраструктураа, дефинирање на улогите и одговорностите по тела, како и рамката за соработка помеѓу јавни и приватни тела.

3. Јавно-приватни партнерства: Секоја национална програма за заштита вклучува соработка на засегнатите страни (Комисија на ЕУ 2005), особено преку јавно-приватно партнерство (ЈПП), вклучувајќи ги јавните тела и сопствениците/оператори на критичната инфраструктура.

4. Размена на информации: Размената на информации се однесува на свесностаза закани/ранливости, за да се обезбеди рано предупредување за засегнатите страни, за споделување информации и соодветно знаење за ризиците и заканите.

5. Законодавно -регулаторна рамка: Донесувањето закони е важна алатка да се обезбеди, меѓу другото, дека јавните и приватните тела реагираат на нивните улоги и одговорности, како и почитување на специфичните безбедносни стандарди.

6. Идентификација и проценка на националната критична инфраструктура: Идентификација и проценкана националните критични средства (сектори, подсектори, услуги и специфични потсистеми) е предуслов за имплементација на

националните политики за заштита на КИ. Важен критериум за класификација на КИ е, меѓу другите, степенот и важноста на меѓусебните врски и меѓузависностите меѓу КИ.

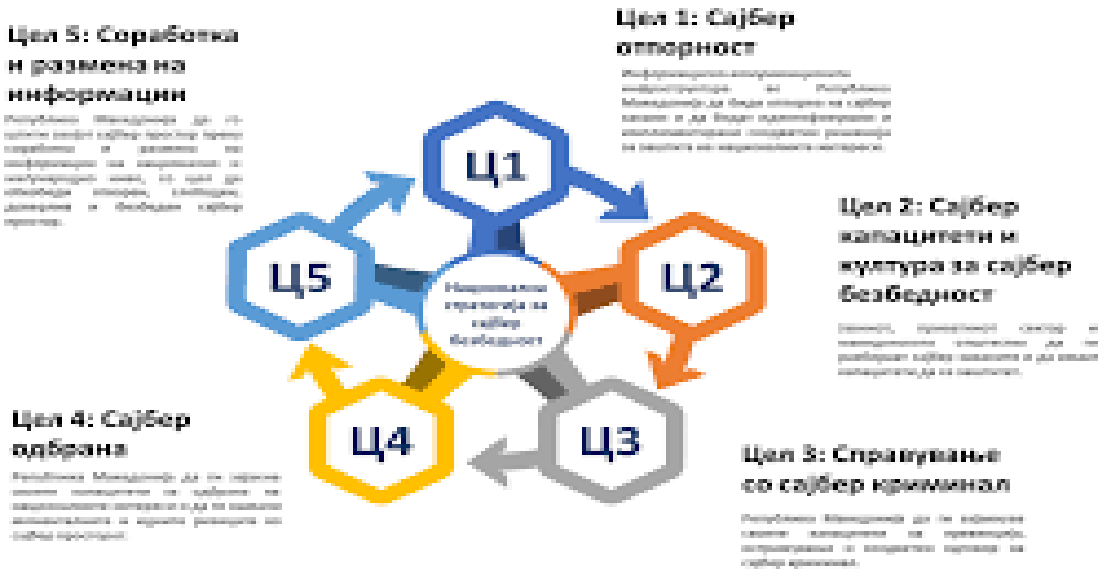
7. Проценка на ризик: Клучен елемент на стратегијата за заштита на критичната инфраструктура е методичката евалуација на заканите и проценка на безбедносните ризици што произлегуваат од националните критични инфраструктури.

8. Ризици и управување со кризи: Мерките за одговор при итни случаи обезбедуваат продолжена работа или брзо закрепнување на критичното средство.

Во развојот на македонското општество голем влијае има брзиот развој на информационата критична инфраструктура како основен двигател на глобализацијата воопшто. Зависноста од електронските услуги што го опфаќаат сајбер просторот, значи дека нефункционалните ИКТ системи и сериозните сајбер напади можат да имаат негативно влијание врз функционирањето на јавниот и приватниот сектор како и на целото општество.

Новите технологии и потребата од поголема застапеност во сајбер просторот е причината корисниците и институциите да ја зголемат свеста за значењето на интегритетот, автентичноста и доверливоста на податоците. Македонските комуникациски мрежи се дел од глобалните комуникациски мрежи, што подразбира дека сајбер безбедносните инциденти на друго место можат да влијаат врз македонскиот сајбер простор и услуги, и обратно.[141]

[141]Национална стратегија за сајбер безбедност на Република Македонија 2018-2022, Верзија 1,2, Министерство за информатичко општество и администрација, Министерство за внатрешни работи и Министерство за одбрана, јули 2018, стр. 4



сл.7 Цели на стратегијата за сајбер безбедност

Информационата критична инфраструктура во Македонија е неопходно да биде отпорна на сајбер закани и да бидат идентификувани и имплементирани соодветни решенија за заштита на националните интереси. 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.

Соработка и размена на информации

Македонија како членка на НАТО е потребно го заштитува својот сајбер простор преку соработка и размена на информации на национално и меѓународно ниво, со цел да обезбеди отворен, слободен, доверлив и безбеден сајбер простор. 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 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. Република Северна Македонија мора да ги преземе сите неопходни мерки да биде препознаена како држава која се грижи за безбедноста во сопствениот сајбер простор и дека сака активно да се вклучи воглобалната борба за справување со масовната злоупотреба на сајбер просторот одстрана на злонамерните корисници. Активното меѓународно учество во справување со глобалниот предизвик од сајбер заканите ќе придонесе за зголемување на државните капацитети за справување со сајбер ризиците.[142]

[142]Национална стратегија за сајбер безбедност на Република Македонија 2018-2022, Верзија 1,2, Министерство за информатичко општество и администрација, Министерство за внатрешни работи и Министерство за одбрана, јули 2018, стр. 31

12. Заклучок

Последните две децении беа обележани со експанзија во развојот на мрежна конекција. Развојот на интернетот го одбележа нагласувањето на интерперабилноста, ефикасноста и слободата, но и зголемената примена на интернетот не беше проследено во напорите да се сочува просторот од аспект на безбедноста. Ова повеќе се однесува на изворната цел на интернетот, содржана во размена на научни податоци, отколку на поддршката на целокупното глобално стопанство. Употребата и функционалноста ги надмина напорите да се реформира и обезбеди изворната инфраструктура.[143]

Сајбер безбедноста опфаќа предизвици кои ги надминуваат државните граници додека одговорите на нив остануваат претежно во национални рамки што се недоволни. Постојат огромни празнини во разбирање на проблемот како и во техничките и систематските специфичности на сајбер нападите. Покрај тоа, проблемите со демократичноста во управувањето, посебно кога станува збор за прашањата околу контролата, надзорот и транспарентноста кои се надвор од секаква дебата. Овие проблеми околу сајбер безбедноста ги прави поризични со големата улога во доменот на приватниот сектор. Имајќи го во предвид темпото со кои државите и приватните компании ја засилуваат сајбер безбедноста, подготвувајќи се за сајбер војна, многу е важно да се посвети внимание за прашањето на демократското управување со тие процеси.

Државите се посебно загрижени за националната безбедност и можноста на државните или недржавните актери или групи да украдат, променат, уништат или на друг начин компромитираат клучни информации и информациска инфраструктура. За националната безбедност е посебно значаен проблемот на попречување на телекомуникациите, електричната енергија, енергетските далноводи, финансиските мрежи, здравствените системи и другите есенцијални

[143]Lloyd's Emerging Risks Team, *Digital Risks: Views of a Changing Risk Landscape,* London: Lloyds, 2009.

служби.[144] Можно е навистина да зборуваме за сајбер војување како претходник на вториот бран на воената револуција што како главен инструмент на војување ќе ја замени кинетичката енергија. Сајбер војната покренува многу прашања поврзани со тоа што претставува критична инфраструктура, каков е нападот и каква улога може или треба да игра безбедносниот систем во одбрана или контранапад.

Сајбер војната ја замагли разликата помеѓу двете категории (цивилни и воени), како и категории на напаѓачи. Произлегува дилемата што во случај на сајбер војна, дали државите можат веродостојно и законски да се закануваат со дипломатски демарш, формален протест, економска одмазда, кривично гонење или воена интервенција.[145]

Уште понагласено од тоа е прашањето кои демократски процеси или законски стандарди треба да се почитуваат, кога се одлучува за можна реакција. Оваа последна точка е особено важна затоа што некои фактори драматично ја намалуваат транспарентноста на сајбер војната во однос на другите видови конфликти. За да се случи сајбер напад, потребно е техничко и високо специјализирано знаење, негово откривање, идентификување и одмазда, како и соработка на приватни актери. Ова во голема мера ја намалува транспарентноста. Поради високо техничката природа на проблемот, улогата на разузнавачките агенции е зголемена, што дополнително се намалува транспарентноста и можноста за надзор.

Денес, предизвици за националната безбедност и клучните државни инфраструктури (во поширока смисла) сè уште претставуваат само мал дел од обемот на заканата. Многу поголем проблем е прашањето како да се обезбеди демократски надзор над регулаторните тела, Интернетот и употреба на инфраструктура преку Интернет во напади врз поединци и други актери. Затоа, проблемот и не се однесува толку на сајбер војување или ранливоста преку Интернет на националната инфраструктура, колку што е прашањето за цензура,

[144]White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* Washington DC: White House, 2009.
[145]John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times,* 25 January 2010, World section.

надзор на коресподенцијата преку интернет без налог или собирање и чување на приватни податоци на ИТ компаниите (често во име на државите или соработката со нив).

Едно од посебните обележја на сајбер безбедноста е што често тешко може да се идентификуваат сторителите на нападите или дури и земјата на потекло. Затоа на поединците или групите им е релативно лесно да ги прикријат сопствената умешност или да да се вметнат во друг корисник.[146] Еден од клучните предизвици на сајбер безбедноста е фактот дека, иако владите, до одреден степен, се одговорни за информатичките и комуникациските мрежи, сопствениците на овие мрежи се претежно приватни актери.[147] Овие групи на актери имаат специфични интереси кои ја попречуваат ефикасноста и делувањето во областа на сајбер безбедноста, како и поткопување на обидите за заштита на јадрото на права и слободи.Овие потешкотии се уште поголеми како резултат на глобалната природа и на проблемот и на неговото решение. Ова е токму областа за улогата на меѓународните актери во развојот на глобални стандарди и идентификување на најдобрите практики. Такви актери, исто така, можат да учествуваат во поттикнување на усогласување на националните регулативи за истрага, гонење, заштита на податоци, безбедност, приватност, пристап до мрежна одбрана и одговор на напади. Покрај тоа, меѓународните актери можат да придонесат за идентификување на недостатоците во надзорот и да се посочат најдобрите практики за демократски надзор на актерите и партнерствата за безбедноста на Интернет. Оваа област заслужува многу поголемо внимание, имајќи во предвид дека моменталните обиди да се најдат најдобрите практики, повеќе се фокусирани на ефикасноста отколку на транспарентноста и надзорот, проблемите и сл. Овие последни акценти се посебно важни имајќи ги во предвид големите диспропорции што постојат во поглед на технолошките капацитети и правните рамки меѓу различните држави. Додека многу држави како САД и Велика Британија, на сајбер безбедност трошат милиони и забрзано го развиваат законодавството во таа област, останатите држави дури

[146] John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times,* 25 January 2010, World section.
[147]Jennifer Wood and Benoît Dupont, eds., *Democracy, Society and the Governance of Security,* Cambridge: Cambridge UniversityPress, 2006.

немаат основна ИТ инфраструктура, и немаат донесено стратегија за соочување со сајбер заканите што ја погодуваат или потекнуваат од нивна територија.[148]

Идентификацијата и проценката на критичните инфраструктури на национално ниво е една од главните приоритети, како што беше потврдено со голем број национални и меѓународни иницијативи. И меѓународната литература и реалноста покажаа дека поради меѓузависности меѓу КИ, појавата на закана или неуспех во КИ многу често води до каскадни влијанија врз други меѓусебно поврзани КИ, што доведува до кумулативни ефекти од големи размери. Ваквите појави може да се моделираат само систематски преку холистички пристап за заштита на КИ што се базира на добро дефинирани методологии и тестирани најдобри практики. Без разлика дали е управувано од држава или пристапот е управуван од операторот, првичната идентификација на националните КИ е предуслов за нивна последователна систематска проценка според секторски и/или критериуми за вкрстување.

Заштитата на критичната инфраструктура е голем сериозен предизвик за безбедноста во едно општество и претставува голема грижа за сите субјекти бидејќи таа е изложена на безбедносни закани. 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. 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.

[148]Benjamin S. Buckland, Fred Schrieier, Theodor H. Winkler, *Demokratsko Upravljanje izazovi sajber bezbednosti*, Geneva Security Forum, Beograd, 2010, str.13

Откривањето на упадите е сé уште нова категорија за заштита и безбедност на компјутерите, мрежните системи и се очекува со понатамошниот напредок и развој на интернетот и технологијата во рамките на сајбер криминалот. Се покажа дека добрата заштита на составот не може да се постигне само со една технологија туку треба повеќе технологии да се обединат. Системите за упад постојано се надоградуваат и секојдневно се имплементираат со нови правила за препознавање на упадите. Исто така, се развива систем за спречување на упад и се очекува негов поголем развој во иднина, не само што може да открие упади во системот, туку може да ги спречи истите. Операторите што управуваат со овие системи играат голема улога во безбедноста на системот и многу е важно тоатие добро ги познаваат и ги разбираат системите за заштита и ги интегрираат правилно во нивната мрежа. Системите за откривање на упад најдоа голема примена во организациите. За компаниите е многу важно да имаат добар безбедносен систем кој ќе ја заштити нивната мрежа од упад и ќе ги заштити нивните приватни податоци и спречи кражба на интелектуална сопственост.

Без оглед на донесените конвенции, нејзините потписници не можат да реагираат, бидејќи соработката е меѓудржавно ниво не е доволна, што го отежнува откривањето на сајбер нападите и спречува услугите да бидат поефикасни. Соработката е посебна комплицирана меѓу компании и корпорации со криминални групи и хакери во спроведување на индустриска шпионажа и саботажа. Заканите од хакерите, сајбер тероритите се потпомогнати со правните празнини, односно нерегулирањето со законски акти.

За превенција од напади на националната критична инфраструктура, било тоа да е физички или сајбер-напад, секоја држава треба да има стратегиски план за превенција, брз одговор и брзо отстранување на последиците и враќање во нормален работен тек на нападнатата критична инфраструктура, што опфаќа:проце на на слабостите што би довеле до физички или сајбер-напад; план за отстранување на значајните слабости; развивање системи за идентификување и спречување на обидите за напад; сигнализација за евентуален напад и отпор на нападот и обновување на работните способности на нападнатиот систем од критичната инфраструктура.

Борбата против сајбер нападите бара употреба на модерно техничко знаење, за превентивни цели и акција и превенција од хакери. Неопходно е да се синхронизира дејството, усогласување на законите меѓу државите, глобално дејствување со цел државите да имаат силен едукативен кадар во оваа област, со цел постапката на откривање, гонење подобро да настапи. Секоја активност во земјата треба да биде организирана така што ќе има соработка меѓу државните органи и истовременото работење на безбедносните служби (разузнавачки служби, полиција, воено разузнавање), како и јавно-приватна соработка.

Зајакнувањето на националните капацитети за превенција и заштита од сајбер напади, како и спроведување активности за подигнување на националната свест за сајбер безбедност ќе резултира во насока на безбедно и отпорно дигитално опкружување со цел заштита на критичната информациска структура.

Користена литература

1. Alisdair A. Gillespie. *Cybercrime: Key Issues and Debates Florence*, Kentucky (USA), 2015.
2. Austin Smith. *Presidential Policy Directive 21: Implementation: an interagency securitycommittee white paper*. Interagency Security Committee, 2017.
3. Analysis of top 11 cyber attacks on critical infrastructure, достапно на: https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
4. BKK Annual Report, Germany: federal office of civil protection and disasterassistance (BKK), 2015.ж
5. B.Simonović, *Kriminalistika*, Pravni fakultet u Kragujevcu, Kragujevac, 2004.
6. Buckland, B., Schreier, F. & Winkler, T. *Demokratsko upravljanje*: izazovi Sajber bezbednosti, Beograd: Forum za bezbednosti demokratiju, 2010.
7. CISA. Critical Infrastructure Sectors, достапно на: https://cset.inl.gov/Lists/Critical_Infrastructure_Sectors/DispForm.aspx?ID=1&Source=
8. Critical National Infrastructure. CPNI. https://www.cpni.gov.uk/critical-national-infrastructure-0
9. Critical Infrastructure Security and Resilience – PPD-21, Washington DC, 2013.
10. Critical infrastructure Protection. Science Direct, достапно на: https://www.sciencedirect.com/topics/computerscience/critical-infrastructure-protection
11. Connelly A et al. RESIN Glossary, Deliverable D1.2. EU H2020 Project RESIN, TheUniversity of Manchester, Manchester, United Kingdom, 2016.
12. D.Dimovski. *Kompjuterski kriminalitet*, Niš, 2010.
13. David Alberts, *Understanding informaton age warfare*, 2001, достапно на:http://www.dodccrp.org/files/Alberts_UIAW.pdf
14. Deconstructing the Reports of Iranian Activity Against the Power Grid and New York Dam достапно на: https://www.sans.org/webcasts/deconstructing-reports-iranian-activity-power-grid-york-dam-101327/

15. Donn B. Parker. *Fighting computer crime*, New York (USA), 1983.
16. D. Littlejohn Shinder, M. Cross. *Cybercrime*, Burlington, MA, United States, 2002.
17. EUROPOL. *The Interent Organised Crime Threat Assessment*, Hague, Netherlands, 2015.
18. *NBC News*. Critical Infrastructure Is Vulnerable to Cyberattacks, Says Eugene Kaspersky, 2015, достапно на: http://www.nbcnews.com/tech/security/critical-infrastructurevulnerable-cyberattacks-says-eugene-kaspersky-n379631.
19. European Commission, *European programme for critical infrastructure protection*, 2007.
20. EU Commission. *Review of the European Programme for Critical InfrastructureProtection* (EPCIP), 2012.
21. EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, BSA – the software alliance, 2015.
22. Executive Order 13010 - Critical Infrastructure Protection, Federal Register, Vol. 61, No. 138.
23. Explaining Distributed Denial of Service Attacks to Campus Leaders," May 3, 2005, http://www.uoregon.edu/~joe/ ddos-exec/ddos-exec.pdf
24. Federal Ministry of the Interior, Building and Community. Critical infrastructure Protection, достапно на: https://www.bmi.bund.de/EN/topics/civil-protection/critical-infrastructure-protection/critical-infrastructure-protection-node.html
25. Gregg, S., H.: Defining and Distinguishing Secular and Religious Terrorism. Perspectives on Terrorism. Vol 8, No. 2 2014.
26. Gullasch D, Bangerter E, Krenn S. Cache games–bringing access-based cache attackson AES to practice. In: *Security and Privacy (SP*), IEEE Symposium onIEEE, 2011.
27. Hower S., *Cyberterrorism,* Santa Barbara, CA: Greenwood, 2011.
28. Hybrid Conference: Critical Connections, Continuity and Supply – Assessing the Security of European Critical Infrastructure and Functions in a Hybrid Threat Context INTERPOL. *The protection of critical infrastructures against terrorist*

attacks: Compendium of good practices, United Nations Office of Counter-Terrorism, UN Counter Terrorism Centre, 2018.

29. Improving the Security of International Infrastructures. OSCE Secretariat, достапно на: https://www.osce.org/secretariat/107809
30. Information assurance, Semi- annual report 2020/1, Reporting and Analysis Centre for Information Assurance MELANI, 2020, достапно на :https://www.newsd.admin.ch/newsd/message/attachments/63536.pdf
31. Igor Ţ. Ţivkovski, Otkrivanje i razjašnjavanje kompjuterskog kriminaliteta, 2012.
32. I.Feješ, *Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti*, 2000.
33. Jennifer Wood and Benoît Dupont, eds., *Democracy, Society and the Governance of Security,* Cambridge: Cambridge UniversityPress, 2006.
34. Kissel R., (ed.). *Glossary of Key Information Security Terms*, 2011, достапно на https://www.newamerica.org/cyber-global/compilation-of-existingcybersecurity-and-information-security-related-definitions/
35. Konvencije o visokotehnološkom kriminalu, Savet Evrope, Budimpešta, 2001.
36. 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,
37. Kaspersky, Cyber threats to ICS Systems, 2014, достапно на: http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf.
38. Klaver M. *Good practices manual for CIP policies, for policy maker's inEurope*. Brussels: RECIPE, 2011.
39. KTH Royal Institute of Technology, достапно на: https://cnls.lanl.gov/External/GSSlides2021/Sandberg.pdf
40. La Porte, T.R. *Critical Infrastructure in the Face of a Predatory Future: Preparing for untoward surprise,* Vol. 15, No.1, 2007.
41. Lewis, T., *Infrastructure Protection in Homeland Security, Defending a Networked Nation*, Wile Interscience, 2006.

42. Li, H., et al, *Strategic Power Infrastructure Defense*, Proceedings of the IEEE, 2005. Lückerath D et al. *The RESIN Climate Change Adaptation Project and its Simple Modeling Approach for Risk-Oriented Vulnerability Assessment*. In: Workshop 2018 ASIM/GI-Fachgruppen (ASM 2018), Proceedings of ASIM workshop, Hochschule Heilbronn,Germany, March 8–9, 2018.
43. Luiijf E, Burger H, Klaver M, Marieke H. *Critical infrastructure protection in theNetherlands: a Quick-scan*. EICAR Denmark, Copenhagen, 2003.
44. Lloyd's Emerging Risks Team, *Digital Risks: Views of a Changing Risk Landscape,* London, 2009.
45. Mamić, D. D*ruštvene mreže kao omogućitelji društvene (ne) odgovornosti*, Zagreb, Fakultet elektronike i računarstva, 2012.
46. Mihaljević, B. Protection of Critical National Infrastrucutre: Challenges for the Private Security Sector. *Ann. Disaster Risk Sci.* 2018.
47. Moteff J. Parfomak P., *Critical Infrastructure and Key Assets: Definition and Identification, Congresional Research Service* - The Library of Congress, 2004.
48. Ментюкова, М. А. & М.М. Дубровина. Эволюцияуголовнойответственностизадоведениедосамоубийства с использованием сети Интернет. *Журнал Вопросысовременно й науки и практики,* (44), 2013
49. National Strategy for CIP. Federal Republic of Germany, 2009.National Security Strategy and Strategic Defence and Security Review, UK Government, 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
50. National Security Strategy and Strategic Defence and Security Review (2015) UK Government
51. Nickolov E., "Modern Trends in The CyberAttacks Against the Critical Information Infrastructure", ITU, Regional Cybersecurity Forum, Sofia, Bulgaria, 2008, достапнона: http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolovmodern-trends-sofia-oct-08.pdf.

52. Public Private Partnerships (PPP) – Cooperative models (2017) ENISA, достапно на ENISA: https://www.enisa.europa.eu/publications/public-private-partnerships-pppcooperative-models

53. Piping botnet – Israeli researchers warn of a potential distributed attack against urban water services that uses a botnet of smart irrigation systems that water simultaneously, Las Vegas, 2021, достапно на: https://securityaffairs.co/wordpress/75389/hacking/piping-botnet-water-services.html
54. Pursiainen C., *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6, 2009.
55. Rossella M, Cédric L-B. *Methodologies for the identification of critical informationi nfrastructure assets and services*. Guidelines for charting electronic data communicationnetworks, European Union agency for network and information security. ENISA, Heraklion, 2014.
56. Robert M. Clark, Simon Hakim*, Cyber-Phisical Security,* Springer*,* 2017.
57. Rinaldi, S., Peerenboom, J., Kelly, T., „Identifying, Understanding and AnalyzingCritical Infrastructure Interdependencies “, *IEEE Control Systems Magazine*, Vol. 21, No. 6, Dec 2001.
58. Rushkoff, D. *Media Virus*. New York: Ballantine Books, 1996.
59. San Francisko Metro System Hacked with Ransomware resulting in Free Rides, достапно на: https://thehackernews.com/2016/11/transit-system-hacked.html
60. S. V. N., Bhushan N. Critical Infrastructure: Defense Industrial Base Sector. In: Shapiro L., Maras MH. (eds) *Encyclopedia of Security and Emergency Management*. Springer, Cham, 2020.
61. S. Konstantinović-Vilić, V. Nikolić-Ristanović, *Kriminologija*, Niš, 2003.
62. Good Progress on Tackling Hybrid Threats. European Commission Press Release, 2003.
63. Slobodan R. Petrović, *Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije, "Bezbednost" -"Policajac”, Beograd, 2000.
64. Thomas A. Johnson (ed)., *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015.

65. Ţ.Aleksići M.Škulić, Kriminalistika, Beograd, 2007.
66. The Critical Infrastructure Protection in France. Paris: Secrétariatgénéral de la defenseet de la sécuriténationale (SGDSN), 2017, достапно на: Secrétariatgénéral de la défense et de lasécuriténationale: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf
67. Tripwire. Cyberterrorists Attack on Critical Infrastructure Could be Imminent, 2015, достапно на: http://www.tripwire.com/state-of-security/securitydata-protection/security-controls/cyberterrorists-attack-on-criticalinfrastructure-could-be-imminent/.
68. US Joint Publication 1-02., Department of defence dictonary of military and associated terms, November 2010, As Amended Through 15 January.
69. United States Government Accountability office, 2009.
70. Martin Charles Golumbic, Fighting terror online-The convergence of Security, Technology and the Law, 2008.
71. Vuletić, D. Napad na računarske sisteme, *Vojnotehnički glasnik*, Vol. 60, (1), 2012.
72. Wilson, C., Botnets, *Cybercrime and Cyberterrorism: Vulnerabilitiesand Policy Issues for Congress*, January, 2008
73. 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.
74. Бакрески О., Милошевска, Т. *Безбедноста на информациите и критичната инфраструктура*, Дирекција за безбедност на класифицирани информации, Скопје, 2021.
75. Бакрески, О, Милошевска, Т, Алчески Ѓ. *Заштита на критична инфраструктура*, Комора на Република Македонија за приватно обезбедување, Стеда-графика, Скопје, 2017.
76. Ген. Вотел, Јозеф Л. Разбирање на тероризмот денес и утре. *ЦТЦ Сентинел* 8. Издание 7, 2015.
77. Извештај на Групата на владини експерти за новитетите во полето на информации и телекомуникаци и контекстот на меѓународната безбедност, 24 јуни 2013 година, Генерално собрание на ОН. Резолуција А/68/98

78. Конвенција за компјутерски криминал. Совет на Европа. Договор бр. 185.
79. Ленц, Кристофер Е. Ленц. 2010.Обврска на државата да спречи и одговори на чинови на сајбер тероризам, *Чикаго журнал на меѓународно право*, 10 бр. 2.
80. Мишевски Д., Осигурување од сајбер ризици, *Осигурување*, Национално биро за осигурување-Македонија, бр.11, Скопје, 2017.
81. Милошевска, Т. *Глобален тероризам*, Универзитет Св. Кирил и Методиј, Филозофски факултет-Скопје, Мар-Саж, Скопје, 2018.
82. Национална стратегија за сајбер безбедност на Република Македонија 2018-2022, Верзија 1,2, Министерство за информатичко општество и администрација, Министерство за внатрешни работи и Министерство за одбрана, јули 2018.
83. Одлука на Советот за безбедност 1566 (2004) за Заканите по меѓународниот мир и безбедност предизвикани од чинови на тероризам. 8 октомври 2004. Совет за безбедност на Обединетите Нации. Резолуција S/RES/1566. Оп. став 3.
84. Попоска В., *Меѓународно правни аспекти за заштита на критичната инфраструктура од современи безбедносни закани*, Универзитет „ГоцеДелчев“, Штип, 2019.
85. Побивање на приказните на терористите. 2017. Совет за безбедност на Обединетите нации S /RES/2354 (2017). Преамбула став 12, и Забрана за наведување на терористички чинови. 2005.
86. Совет за безбедност на Обединетите нации S/RES/1624 (2005). Преамбула став 4 и оперативен став 1(а).
87. Правна рамка за обезбедување на критичната инфраструктура, Комора на Република Македонија за приватно обезбедување, Скопје, 2016
88. Стратешки документи. Министерство за одбрана на Република Северна Македонија, достапно на: http://www.mod.gov.mk/?page_id=39286&lang=mk
89. Употребата на интернетот за терористички цели. 2012. Канцеларија на Обединетите нации за дроги и криминал.

90. Хендисајд против Обединетото Кралство. 4 ноември 1976. Совет на Европа: Европски суд за човекови права. 5493/72
91. Џејкобсон, Мајкл. Јуни 2009. Финансирање на тероризмот преку интернет. ЦТЦ Сентинел 2. Издание 6
92. Службен весник на РМ“ бр. 166/2012, 164/2013, 148/2015, 193/2015, 55/2016
93. Закон за одбрана, „СлужбенвесникнаРМ “, бр. 185 од 30.12.2011 година
94. Службен весник на РМ бр.80/99,66/07,51/11
95. https://www.newamerica.org/cyber-global/compilation-of-existing cybersecurity- and-information-security-related-definitions/
96. https://op.europa.eu/webpub/eca/special-reports/ppp-9-2018/hr/
97. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/336/html
98. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN.
99. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/