МЕЃУНАРОДЕН СЛАВЈАНСКИ УНИВЕРЗИТЕТ

СВЕТИ НИКОЛЕ

РЕПУБЛИКА МАКЕДОНИЈА



ФАКУЛТЕТ ЗА ПРАВНИ НАУКИ

СТУДИСКА ПРОГРАМА: КАЗНЕНО ПРАВО

САЈБЕР ТЕРОРИЗАМ

МАГИСТЕРСКИ ТРУД

СТУДЕНТ: Митев Кристијан МЕНТОР: Проф. Др. Васко Стамевски

БРОЈ НА ИНДЕКС: М

Свети Николе, 2025

Абстракт

Sumary

Вовед

1.Тероризам – општи одредници

2. Класификација на тероризмот

2.1 Сајбер тероризам

2.1.2 Постоечки информации за сајбер тероризмот

2.2 Сајбер тероризам и сајбер криминал: разлики и превенција

2.3 Модели на толкување на сајбер тероризмот

2.4 Учесници и мети на сајбер тероризмот

2.5 Последици од сајбер тероризмот

2.6 Релација меѓу сајбер тероризмот и организираниот криминал

3. Технолошка еволуција како катализатор на криминалот

4. Меѓународна соработка и правни предизвици

4.1 Нови облици на соработка меѓу тероризмот и организираниот криминал

4.2 Безбедност во виртуелниот простор

4.3 Прилагодување на правниот систем на новите предизвици

4.4 Транснационалност на сајбер-криминалот

5. Злоупотреба на современите информациски и комуникациски технологии

5.1 Сајбер криминал

5.2 Сајбер криминал и сајбер тероризам

6.Фази на одбрана од сајбер тероризам

6. 1 Превенција

6.2 Одвраќање

6.2.1 Одвраќање со казна

6.2.2 Одвраќање со одбивање

6.3 Одговарање

6.4 Управување со инцидентот

6.5 Санирање на последиците

7. Мерки за одбрана од сајбер тероризмот

7.1 Активна одбрана од сајбер тероризмот

7.2 Пасивни мерки за одбрана од сајбер тероризмот

8. Нови стратегии за одбрана од сајбер тероризам

9.Меѓународна соработка во борбата против тероризамот

9.1 Меѓународна правна регулатива

9.2 Мултилатерална соработка

Заклучок

Користена литература

АБСТРАКТ

Тероризмот претставува глобален феномен со деструктивни последици врз поединците и заедниците. Неговата цел не е само физичка штета, туку и создавање психолошка паника и чувство на несигурност. Во услови на медиумска и дигитална поврзаност, ефектите на терористичките акти значително се засилуваат.

Иако постојат бројни дефиниции, тероризмот најчесто се третира како насилна, политички мотивирана и морално осудлива активност. Нападот врз САД на 11 септември 2001 година останува симбол на современиот тероризам, а Ал Каеда се смета за негов архетип. Сепак, јавната реторика често создава поедноставени слики за терористот, занемарувајќи ги комплексните социјални и психолошки корени на радикализацијата.

Технолошкиот развој внесе нови димензии: сајбер-тероризмот, дигитални напади врз критичната инфраструктура и користење криптирани платформи за координација. Радикализацијата и регрутацијата се префрлија во онлајн просторот, што ја зголеми транснационалната закана. Пандемијата Ковид-19 дополнително ја влоши ситуацијата, отворајќи простор за екстремни наративи и ерозија на довербата во институциите.

Современите трендови укажуваат на адаптибилност: манипулација со ранливи групи, експлоатација на нееднаквости и злоупотреба на жени и деца. Појавите како „сајбер-калифати“ бараат нови правни и безбедносни одговори.

Превенцијата се базира на комбинација на правосудни, безбедносни и социјални политики, чија ефективност зависи од адаптација кон новите предизвици и јакнење на општествената кохезија. Тероризмот е истовремено насилство и пропаганда, па неговото спречување бара координирани технолошки, правни и социјални стратегии.

Клучни зборови: тероризам, сајбер тероризам, превенција,општествен одговор кон тероризмот

ABSTRACT

Terrorism is a global phenomenon with destructive consequences for individuals and communities. Its aim is not only to inflict physical damage but also to create psychological panic and a pervasive sense of insecurity. In today's media and digital environment, the effects of terrorist acts are significantly amplified.

Although multiple definitions exist, terrorism is most often described as a violent, politically motivated, and morally reprehensible activity. The September 11, 2001 attacks on the United States remain a symbol of modern terrorism, with Al Qaeda regarded as its archetype. However, public rhetoric often produces oversimplified images of terrorists, obscuring the complex social and psychological roots of radicalization.

Technological progress has introduced new dimensions: cyberterrorism, digital attacks on critical infrastructure, and the use of encrypted platforms for coordination. Radicalization and recruitment have shifted to online spaces, intensifying the transnational nature of the threat. The Covid-19 pandemic further aggravated the situation, providing opportunities for extremist narratives and undermining trust in state institutions.

Contemporary trends indicate adaptability: manipulation of vulnerable groups, exploitation of inequalities, and the abuse of women and children. Phenomena such as "cyber-caliphates" highlight the need for new legal and security responses.

Prevention strategies rely on a combination of judicial, security, and social policies, whose effectiveness depends on their adaptability to emerging challenges and the strengthening of social cohesion. Terrorism is both violence and propaganda; therefore, its prevention requires coordinated technological, legal, and social strategies.

Keywords: terrorism, cyberterrorism, prevention, societal response to terrorism

Вовед

Тероризмот отсекогаш претставувал тема од посебен интерес за истражувачите, пред сè поради неговата деструктивна природа и глобалното влијание што го има преку терористичките акти. Неговата распространетост и непредвидливост го прават предмет на постојано истражување и анализа.

Постојат две главни причини поради кои тероризмот предизвикува длабока загриженост. Прво, терористичките напади, поради својата неселективност и често висока цена во човечки животи, предизвикуваат директен страв кај луѓето – и кај оние кои се присутни на местото на нападот, и кај оние што се идентификуваат со жртвите (роднини, пријатели, заедници). Ова претставува форма на **директен терор**. Второ, тероризмот не е насочен само кон физичко уништување или предизвикување жртви и материјална штета. Неговата поширока цел е да предизвика психолошки терор врз целото општество, односно да внесе чувство на несигурност и страв кај пошироката јавност. За да се постигне ова, пораката на терористичкиот акт мора да допре до што поширока публика – што денес се овозможува преку традиционалните медиуми, интернетот и социјалните мрежи. Така се остварува **индиректниот терор**, чија цел е општеството во целина.

И покрај бројните обиди, сè уште не постои единствено прифатена дефиниција за тероризмот. Сепак, општата согласност во академските кругови е дека тероризмот претставува **насилна, морално осудувачка и политички мотивирана активност**.

Иако делумно ќе се осврнеме на теоретските потешкотии при дефинирање на тероризмот, главната цел на овој труд не е да се формулира универзално прифатена дефиниција, туку да се анализира неговата **еволуција** – особено трансформацијата на методите и формите на делување на терористичките групи, односно неговиот променет *modus operandi*.

Кога ќе се спомне поимот „тероризам“, често првата асоцијација е нападот на САД на 11 септември 2001 година. Доколку размислуваме за сторителите на тој чин, веднаш се појавува името на Ал Каеда – како синоним за терористичка организација. А ако размислуваме за личност која го симболизира терористот, неретко се јавуваат стереотипи за злобен, бесчувствителен поединец – што го отвора прашањето за перцепцијата на тероризмот, не само како феномен, туку и како културна конструкција во јавната свеста

Овој поедноставен и често стереотипизиран приказ е резултат на влијанието на медиумите, политичкиот дискурс и културните репрезентации, кои ретко навлегуваат подлабоко во сложените психолошки, социолошки и политички аспекти на тероризмот.

Меѓутоа, современите облици на тероризам, особено со појавата на сајбер тероризмот, бараат поинаков, понијансиран пристап во неговото разбирање. Со промената на средствата, методите и целите, тероризмот денес не се манифестира само во физички напади, туку и преку дигитални напади врз витални инфраструктури, информациски системи и јавната свест. Овие промени бараат од научната заедница постојано следење, анализа и адаптација на концептите и стратегиите за справување со оваа закана.

Сепак, мора да појдеме од реалната констатација дека тероризмот не започна со нападите од 11 септември 2001 година, ниту пак Ал Каеда е неговиот најопасен застапник, а уште помалку Осама бин Ладен е неговиот најголем опонент. Тероризмот постои многу одамна, но развојот на технологијата придонесе тој да стане многу повидлив, со проширени можности за делување, особено преку радикализација, регрутација и транснационално присуство благодарение на онлајн платформите.

Современите терористи почнаа да ги учат слабостите на државните безбедносни системи – како што ќе видиме подолу во случајот со Едвард Сноуден – и од обични, следливи комуникациски методи преминаа кон користење на пософистицирани дигитални алатки. Тие користат апликации и платформи кои овозможуваат анонимна, криптирана комуникација, со цел нивните пораки да останат тајни и достапни само за внатрешниот круг.

За да се спречи понатамошна експанзија на тероризмот и насилниот екстремизам, државите и меѓународните институции започнаа со донесување стратешки документи

насочени кон справување со оваа закана. Прво беше развиена таканаречената „Контратерористичка стратегија“, но со оглед на новите безбедносни предизвици, беше воведена и нова, проширена стратегија – „Борба против насилниот екстремизам“. Оваа стратегија опфаќа политики, програми и интервенции со цел да се спречат поединци да се приклучат на насилни дејствија инспирирани од радикални политички, социјални, културни или религиозни идеологии и групи.

Пандемијата на Ковид-19 дополнително ја комплицираше состојбата. Терористичките организации ја искористија глобалната криза, рестрикциите, револтот и социјалното незадоволство како поволна основа за ширење на своите агенди. Тие успешно ги експлоатираа слабостите што произлегоа од ограничувањата, вклучително и чувството на обесправеност кај одредени групи во општеството.

Трендовите на тероризмот и насилниот екстремизам се преклопија низ повеќе региони, особено за време на пандемијата. Терористичките групи се обидоа да ги искористат социоекономските потреси и политичките тензии предизвикани од пандемијата – тензии кои беа дополнително влошени од рестриктивните мерки што често ги поткопуваа човековите права. Овие услови беа погодна основа за терористичките организации да го прошират своето влијание, да ги интензивираат напорите за регрутација и да ја еродираат довербата во државните институции.

Тероризмот не стагнира, туку постојано се адаптира и модернизира, прилагодувајќи се на новите глобални трендови. Тој манипулира со ранливите категории на луѓе – оние кои се социјално маргинализирани, економски обесправени, или кои се соочиле со трауматични искуства. Регрутацијата, радикализацијата и насилниот екстремизам станаа основни алатки за реализација на терористичките цели.

Во поново време, се забележува и тренд на вклучување на жените – како извор на финансии, но и како активни учеснички – како и злоупотреба на деца од најрана возраст во процесите на индоктринација и одржување на терористичката идеологија. Во овој контекст се зборува за постоење на „двоен калифат“ – еден „реален“, а другиот „сајбер-калифат“, кој егзистира во дигиталниот простор. Ова претставува сериозен предизвик за современото општество, кое мора да најде ефективен одговор.

Тероризмот денес не може да се анализира исклучиво низ призма на насилството. Еднакво важно е и прашањето на пропагандата – моќно оружје кое се шири со неверојатна брзина преку дигиталните медиуми, како што се социјалните мрежи, веб-страници, форуми, YouTube и слично. И насилството и пропагандата имаат иста крајна цел – да предизвикаат промена во однесувањето на јавноста. Насилството го прави тоа преку примена на физичка сила, често со екстремен, самоубиствен пристап, додека пропагандата се обидува да го постигне истото преку психолошко убедување.

Со оглед на тоа што државите почнаа да преземаат мерки за ограничување на пристапот до медиумите и онлајн просторите кои терористите ги користат за публицитет, терористичките мрежи почнаа да мигрираат кон нови, посигурни дигитални платформи. Тие избраа онлајн простори кои нудат поголема заштита на нивната комуникација, движење и анонимност, а кои им овозможуваат собирање финансиски средства, дистрибуција на пропаганден материјал, планирање напади и избегнување на детекција од страна на разузнавачките и безбедносните служби. Така, нивниот „нов дом“ стана темната страна на интернетот – т.н. дарк веб.

1.Тероризам – општи одредници

Современото општество се соочува со глобални предизвици како што се: таканаречениот „глобален тероризам“ (Шторп, 2009, 63), климатските промени, пандемијата со вирусот КОВИД-19, економската криза и енергетските промени. Последиците од глобалниот тероризам се од светски размери, а го карактеризираат мотиви кои главно се од етнонационалистичка и верска природа. Иако поминаа повеќе од две децении од терористичките напади врз САД од страна на Ал Каеда на 11 септември 2001 година, кога тероризмот преку „главната врата“ влезе на светската сцена, времето покажа дека тероризмот е проблем со долгорочен карактер.

Светската сцена е потресена од бројни глобални проблеми. Заканите и стравовите од тероризмот не стивнуваат, туку напротив, овие закани и стравови можат дополнително да се поттикнат од незадоволството предизвикано од новонастанатата состојба. Тероризмот несомнено претставува значаен предизвик за глобалната безбедност, а неговото разбирање и дефинирање е од суштинско значење за соодветно справување и борба со овој феномен. Утврдувањето на неговите клучни карактеристики се наметнува како една од основните цели на современите науки (општествени, правно-политички, безбедносни и други). Иако во литературата тероризмот најчесто се поврзува со

современото доба, факт е дека тероризмот не е појава од поново време. Историјата го потврдува постоењето на различни форми на тероризам. Затоа, поради неговата сложеност и за полесно разбирање, важно е да се земат предвид:

1. општествено-историските околности во кои се појавува тероризмот,
2. видот и квалитетот на општествено-политичките и економските односи во земјата и нејзиното опкружување,
3. актуелните политички ставови,
4. „климата“ во меѓународната заедница,
5. делувањето и однесувањето на другите држави и
6. постоењето или непостоењето на евентуални поттикнувачи за мешање во внатрешните односи и вршење на надворешни притисоци врз одредени суверени држави.

Тероризмот може да послужи како средство за индиректно влијание врз надворешната политика, преку загрозување на интегритетот на некоја држава, отежнување, забавување или оневозможување на нејзината интеграција во одредени меѓународни организации или институции. Исто така, тероризмот може да помогне во промоцијата на одредена влада на меѓународната сцена или пак да прикаже некоја влада како неподобна и неспособна да се справи со проблемите, дури и да ја прикаже како поддржувач на тероризмот. Справувањето со тероризмот без сомнеж бара повеќеслојна интервенција од страна на меѓународната заедница, што може да поттикне дезинтеграција и спроведување на одредени облици санкции. Поради можноста тероризмот да влијае врз надворешната политика, како и поради последиците што може да има врз националната безбедност, од големо значење е што се поголем број на научната заедница се вклучува во разбирањето на појавата тероризам и во донесувањето мерки за негово сузбивање и превенција

Толкувањето на претходната литература на тема тероризам укажува на тоа дека значењето на зборот „тероризам“ се менувало низ историјата. Дефинициите за тероризмот се претежно сложени и контроверзни, бидејќи овој термин означува употреба на насилство и застрашување. На пример, во текот на XIX век, овој термин се користел за да се означат анархистите, кои самите себеси така се нарекувале. Исто така, организацијата Лехи – борци за ослободување на Израел во 40-тите години на XX век – себеси се претставувале како еврејска терористичка група. Инаку, коренот на зборот тероризам потекнува од латинскиот јазик, каде што изразите „terror“, „terrere“ значат „ужас, голем страв, владеење преку застрашување, начин на владеење преку влевање

страв и насилство“ (Вујаклија, 1975, стр. 947). Како што наведува и Симеуновиќ: „теророт претежно е вршење на насилство во рамки на спроведувањето на моќта со цел задржување на власта, односно одржување или зголемување на моќта на владејачките – значи насилство од страна на власта“ (Симеуновиќ, 1989, стр. 144–145).

И покрај фактот што тероризмот е проблем од долгорочен карактер, поради неговата комплексност и големиот број различни појавни облици низ историјата, научната заедница сè уште нема постигнато согласност околу една општо прифатена дефиниција на тероризмот. Во англискиот речник тероризмот е определен како: „метод на владеење или спротивставување на некоја влада кој има за цел да предизвика страв“ (Wagner, 1987). Во италијанскиот речник овој поим е дефиниран како „средство на екстремно и незаконско насилство во политичката борба“ (Palazzi, 1965).

Терористите со текот на времето ја менувале и приспособувале својата методологија на делување според тековните историски процеси. Тоа е една од причините зошто тероризмот до ден-денес останал нерешен проблем. Го карактеризираат сложеноста и променливоста како негови основни обележја, поради што тероризмот треба да се толкува во општествено-политичкиот контекст во којшто настанал.

Симеуновиќ укажува на различните значења на овој термин низ историјата. Така, според неговите зборови, тероризмот најпрвин служел за да се означи насилното преземање на власта од страна на револуционери, додека „во текот на XIX век бил поврзан со насилното делување на анархистички и нихилистички организации. Во XX век, двапати терминот тероризам повторно бил поврзуван со насилството на власта – најпрво во врска со делувањето на режимите на стравовлада како што биле нацистичкиот и сталинистичкиот, а потоа и поради несогласувањето на западните големи сили со ослободителните движења на колонизираните народи, кои во својата борба за ослободување користеле и насилство. Понатаму, од седумдесеттите години па сè до денес повторно беше поврзуван со насилство против некоја власт или нечии властодршци, иако повремено и со насилството на одредени држави кои беа означувани како спонзори на тероризмот, „оски на злото“ и слично“ (Симеуновиќ, 2009, стр. 19).

Опасноста од тероризмот е постојана, никогаш не стивнува. „Современиот тероризам, како повеќедимензионален политички феномен, иако присутен од самиот почеток на класното општество во сите општествено-политички системи, добива толку опасни и широки размери што денес се смета за една од најголемите закани на планетата“ (Савиќ и Стајиќ, 2006, стр. 211–212). Многу автори се занимавале со толкување на тероризмот од аспект на различни научни дисциплини, што резултирало со голем број различни

дефиниции на тероризмот. Томашевски го објаснува тоа со фактот дека „под поимот тероризам се опфаќаат различни акти на насилство и загрозување на човековите права и човечки животи, како и јавни, односно заеднички и индивидуални добра. Во таа мноштвеност и разновидност на актите кои се подведуваат под поимот тероризам се наоѓа и дел од причината зошто не можела да се утврди една сеопфатна и општоприфатена дефиниција за тероризмот“ (Томашевски, 1983, стр. 13).

Сепак, и покрај големиот број различни дефиниции за тероризмот, анализата на содржината покажа дека постојните дефиниции во себе содржат сличности, односно основни карактеристики на тероризмот. Така, стравот и насилството се спомнуваат како негови основни одредници во речиси секоја дефиниција за тероризмот. Еве дело од тие дефиниции:

1. „Под општ поим тероризам се подразбира доктрина, метод и средство за предизвикување страв и несигурност кај граѓаните преку систематска употреба на насилство со цел остварување на одредени, пред сè политички цели“ (Скакавац, 2010, стр. 331).
2. Гајшновиќ ја гледа главната карактеристика на тероризмот во насилството и неговата употреба и смета дека тоа е: „организирана примена на насилство (или закана со насилство) од страна на политички мотивирани извршители, кои се решени преку предизвикување страв, загриженост, дефетизам и паника да ја наметнат својата волја на органите на власта и на граѓаните“ (Гајшновиќ, 1998, стр. 31). Тој исто така го гледа тероризмот како „продолжена рака на политиката, која се води со други (нелегални) средства“ (Гајшновиќ, 2011, стр. 18) за постигнување на своите цели.
3. Кегли (Kegley, 2003, стр. 13) предлага определување на тероризмот врз основа на негов опис. Според него, најпрво е потребно: да се утврдат неговите основни елементи, да се понуди објаснување на овој феномен преку причините кои ги мотивираат актерите да ги реализираат своите цели преку терористичко дејствување да се разгледаат досега постојните, предложени и применувани мерки, како превентивни, така и репресивни, за спречување на тероризмот на глобално ниво.
4. Шмид и Јонгман го дефинираат тероризмот преку насилството и во зависност од основната цел на тоа насилство, односно во зависност од пораката што терористите сакаат да ја испратат преку медиумите. Затоа тие наведуваат: „Тероризмот е со страв инспириран метод на повторување на насилни акции

извршени од страна на индивидуи, групи или државни актери поради криминални или политички причини, при што – за разлика од убиство – конкретната мета на насилството не е и клучната мета. Непосредните човечки жртви на насилството најчесто се избираат од целната популација – на случаен начин (мети според можноста) или селективно (претставници или симболични мети) – и служат како генератори на пораки.

Базиран на закана и насилство, процесот на комуникација меѓу терористите (организацијата), (загрозената) жртва и главната мета служи за манипулација со главната мета (јавноста – медиумите), претворајќи ја во мета преку терор, барања или привлекување внимание – зависно од тоа дали се во преден план застрашувањето, принудата или пропагандата“ (Schmid & Jongman, 2005, стр. 28).

5. Лемкин го дефинира тероризмот врз основа на основните мотиви на терористите, наведувајќи дека застрашувањето на луѓето е нивниот примарен мотив. Терористите користат различни форми на насилство за да создадат „danger coming“ (опасност што доаѓа) (Lemkin, 1933, стр. 900–901), односно една севкупна закана која претставува опасност за безбедноста и ги загрозува интересите на граѓаните, заедницата, а во некои случаи и интересите на одделни држави.

Тероризмот како повеќедимензионален феномен може да се појави во различни форми:

- манифестна форма (чија цел е да одекне во медиумите и да ја вознемири поширокатa јавност), или
- латентна форма на тероризам (камуфлирана, формално правно легална).

Без разлика на формата во која се појавува, тероризмот претставува „вид на индивидуално, нелегитимно и неинституционално насилство“ (Симеуновиќ, 1993, стр. 736) и како таков претставува закана за некое општество, држава или нејзините институции, па затоа „нема легитимна основа во релевантниот правен и етички кодекс на меѓународната заедница“ (Симеуновиќ, 1993, стр. 736).

2.Класификација на тероризмот

Во литературата за тероризмот се наведени различни примери на класификација на тероризмот во зависност од примарниот критериум на класификација. Мноштвото појавни облици и комплексноста на тематиката го усложнува и отежнува неговото исцрпно класифицирање, бидејќи одредени терористички организации истовремено се одликуваат со неколку различни облици на тероризам, кои според нивните

карактеристики не можат да се вметнат во една конкретна категорија. Токму поради тоа, различни автори предлагаат различни класификации на тероризмот.

Симеуновиќ предлага класификација на тероризмот според:

Програмско-целна ориентација:

1. Идеолошки мотивиран тероризам
2. Левичарски тероризам
3. Десничарски тероризам
4. Етно-сепаратистички тероризам
5. Верски фундиран тероризам
6. Тероризам на секти
7. Тероризам базиран на интерпретации на големите религии

Според средствата и методите:

1. **Класификација според средствата:**ж
   Класичен (конвенционален) тероризам
   Биохемиски тероризам
   Нуклеарен тероризам
2. **Класификација според методите:**
   Класичен (конвенционален) тероризам
   Самоубиствен тероризам
   Сајбер-тероризам (употреба на интернетот во терористички цели)
   Нарко-тероризам

Според типот на актери – субјекти на тероризмот:

1. Индивидуален тероризам
2. Тероризам на организации и илегални групи
3. Институционален тероризам (државен и сл.) (Симеуновиќ, 2009, стр. 82–85)

Милашиновиќ и Мијалковиќ предлагаат класификација на тероризмот според **начинот на извршување** на терористичкиот напад. Затоа тие спомнуваат: „т.н. промислен (го изведуваат терористи кои не сакаат да бидат фатени ниту убиени) и самоубиствен тероризам (го изведуваат политички, верски, националистички и други фанатици, користејќи конвенционални или импровизирани експлозивни направи, не грижејќи се за својот живот). Средишна, умерена тактика користи т.н. активен стрелец кој, користејќи огнено, поретко ладно оружје или друго средство погодно за напад, убива што повеќе невини луѓе околу себе, најчесто на јавно место (на улица, во училиште, во црква, во

јавен превоз во самопослуга, на спортски стадион и слично)“ (Милашиновиќ & Мијалковиќ, 2011, стр. 6).

Шикман, врз основа на следниве определби: „мотив за извршување, средство на извршување, начин на извршување, објект на напад или некој друг критериум“ (Шикман, 2011, стр. 46), дава класификација на тероризмот. Во текот на историјата се менувале мотивите кои ги поттикнувале терористите. Поранешните „традиционални“ терористи главно биле насочени против достигнувањата на современата демократска држава, нејзините структури на моќ, и настојувале бројот на жртви да биде што е можно поголем. Додека современиот тероризам главно е насочен против постојните економско-енергетски системи, како во национални, така и во меѓународни рамки — како што се, на пример, т.н. „енергетски тероризам“ или т.н. „рационален/пресметан тероризам“, кои ги споменуваат Милашиновиќ и Мијалковиќ (Милашиновиќ & Мијалковиќ, 2011, стр. 6). Тежнеењето на современите терористи е насочено кон предизвикување економска штета од што поголеми размери и прекинување на дотогашните финансиски текови, со цел да се загрози животниот стандард и да се промени моменталната економска состојба во нивна корист.

Тероризмот може да се класифицира според **средствата на извршување,** односно во зависност од оружјето кое се користи во терористичките активности: „нуклеарен, сајбер-тероризам, биолошки, хемиски или комбиниран тероризам“ (Милашиновиќ & Мијалковиќ, 2011, стр. 6). Современите терористи користат различни средства и оружја чија деструктивност е толку голема што можат да предизвикаат штета од огромни размери. Поради тоа, Милашиновиќ и Мијалковиќ предлагаат заеднички назив за овој вид тероризам — „постиндустриски тероризам“ или „супер (мега) тероризам“ (Милашиновиќ & Мијалковиќ, 2011, стр. 7).

Разни автори (Векман, 2006; Бовиќ, 2008, стр. 55–57; Геер, 2006; Лукнар, 2020а) наведуваат дека развојот и примената на технологијата изнедриле нови постмодерни, неконвенционални форми на тероризам, како и злоупотреба на високоразвиени технологии за реализирање на комуникација и организирање напади поради разните предности кои ги нуди интернетот (можност за анонимна комуникација и ниски трошоци). Дека новите информатички технологии значително го олеснуваат меѓународниот тероризам, укажува и практичниот пример на Исламската држава, која ги користеше социјалните мрежи за пропаганда и реализација на своите идеи.

Хармон зборува за посебен вид тероризам — т.н. „еколошки тероризам“ (Harmon, 2000, стр. 137–185). Овој облик на тероризам се карактеризира со употреба на насилство со

цел постигнување на јасно дефинирана цел — укажување на конкретни еколошки проблеми и зачувување на природата

Хармон зборува за посебен вид тероризам, т.н. „еколошки тероризам“ (Harmon, 2000, стр. 137–185). Овој облик на тероризам се карактеризира со употреба на насилство со цел постигнување на јасно дефинирана цел — укажување на конкретни еколошки проблеми (зачувување на природата, биодиверзитетот, водата, спречување на емисија на јаглерод диоксид, ефектот на стаклена градина и сл.), поради кои со насилство се врши притисок врз властите за тие да иницираат донесување на законски прописи со кои овие проблеми би се решиле.

Понатаму, тероризмот може да се разликува и според просторот каде што претежно се манифестира — т.н. „урбан“ или „рурален“ (Симеуновиќ, 2009, стр. 82), како и во зависност од тоа дали е присутен на територијата на една конкретна држава — „внатрешен“ или „надворешен“ — кога неговите последици ги надминуваат националните граници (Симеуновиќ, 2009, стр. 82).

2.1 Сајбер тероризам

2.1.1 Постоечки информации за сајбер тероризмот

Постојат обемни литературни извори кои даваат општи разгледи на тероризмот. Меѓутоа, литературата која се конкретно бави со сајбер тероризмот е осиромашена. Практично, нема литературни изданија во светот кои се посебно фокусирани на анализирањето на сајбер тероризмот од перспектива на специфични национални оквири, односно низ толкување на различни стратегии за борба против сајбер тероризмот. Имајќи го предвид континуираниот технолошки развој, особено развојот и примена на информациско-комуникациските технологии и интернетот, споменатата состојба укажува на сериозен недостаток во литературната понуда и потребата од итна реакција, најпрво од страна на научната заедница преку дебата, а потоа и на национален и глобален план преку предложени мерки, политики и стратегии. Сајбер тероризмот е форма на тероризам од поново време, која е недоволно истражена. Сè поголемото користење на интернетот и современите информациски и комуникациски технологии укажува на актуелноста на проблемот и потребата од толкување на можните закани и опасности во сајбер просторот. Сајбер тероризмот е специфична форма на тероризам, не само по средствата кои ги користат сајбер терористите, туку и затоа што се одвива во специфично опкружување — виртуелно, каде што постојат онлајн средства и принципи, каде што настаните и опасностите во сајбер просторот остануваат неприметени во

физичкиот свет, а нивните последици и причинетата штета можат директно да влијаат на секојдневниот живот на луѓето, медиумите, јавното мислење, инфраструктурата и безбедноста.

Научно-технолошката револуција произвела нови изуми и нови општестевни форми (виртуелни заедници, сајбер култура), нови начини на комуникација, но и нови проблеми. Додека пандемијата на КОВИД-19 вирусот ги стави на прво место напредните технологии и можностите за нивна примена во речиси сите области на човечката активност (е-управа, медицина и здравство, производство на храна, учење на далечина итн.), во современото општество техничко-технолошкиот фактор добил значителен значај, така што технолошката надмоќ на светската сцена денес значи многу. Затоа современите држави во светот се натпреваруваат во развојот на нови технологии и нивна примена. Ова доведува до тоа што инфраструктурата на современите држави, покрај традиционалните физички средства, во голема мера е составена од средства во онлајн (сајбер) просторот, а знаењето, особено во ИТ областа, станало еден од примарните ресурси во современото општество.

Најмоќните држави на светот издвојуваат големи количини финансиски средства за наоружување и технолошки развој, со што се енормно зголемуваат капацитетите за уништување на планетата и се нарушува глобалната безбедност. Актуелната друштвено-политичка ситуација е нарушена од негативните последици предизвикани од пандемијата на коронавирусот. Економската криза и новата прерасподела на моќта на глобалната сцена, заедно со технолошкиот развој, придонесуваат за зголемување на тензиите. На тој начин, опасноста од сајбер тероризам се наметнува како актуелен безбедносен проблем. Безбедноста на активностите на интернетот, заштита и превенција од сајбер напади и сајбер тероризам се наметнуваат како актуелни теми за разгледување од страна на стручњаците и теоретичарите од областа на безбедноста, правото, војската, информатиката, политиката и други науки.

Колин наведува дека терминот за сајбер тероризам е скован крајот на 20-тиот век (Collin, 1997, 15). Сепак, во научната заедница сè уште не постои општ консензус за прифатена дефиниција на поимот сајбер тероризам. Овој термин се користи најчесто за да означи безбедносни закани и различни криминални дела и саботажи што се извршени со помош на современите информациски и комуникациски технологии и интернетот, со цел политичко дејствување и создавање одредени политички ефекти и клима. Толкувањето и разбирањето на овој поим го отежнува големата „темна бројка“ на сајбер тероризмот, која настанува поради отежнатите околности за откривање на извршителите и

доказување на стореното дело. Додека предностите што сајбер тероризмот ги има во однос на традиционалните форми на тероризам ја прават оваа форма тероризам актуелна, особено во современото општество, споменатите предности произлегуваат од можностите што корисниците на ИКТ ги имаат, како што се:

1. **Анонимност** - можноста да креираат виртуелен (сајбер) идентитет,
2. **Можноста** да нанесат штета големи размери без големи физички напори и без конкретно оружје во реалниот (физички) свет, независно од реалната далечина помеѓу извршителот и метата,
3. **Релативно лесно извршување**, кое освен знаење од ИТ областа и технолошка опременост не бара дополнителни организации и ризици.

Во литературата што се бави со тумачење на сајбер тероризмот, се издвојуваат два основни правци на размислување. Првиот правец подразбира широко дефинирање на поимот така што, тој опфаќа политички мотивирани хакерски операции кои имаат за цел да предизвикаат сериозна штета, како што се губење на животи или големи економски штети. Значи, овој правец го дефинира сајбер тероризмот во однос на неговото разликување од обичните хакерски активности и компјутерски криминал, односно го дефинира како хактивизам кој е политички мотивиран. Значи, сајбер терористите се оние починители, хакери кои инсистираат дека се првенствено мотивирани од политиката, а не од некакви зли намери или желба за остварување финансиски добивка. Други, пошироки правци на размислување обично ги застапуваат владини функционери и лица од воената одбрана, според кои сајбер тероризам подразбира било кој напад во виртуелниот (сајбер) простор кој ја загрозува безбедноста. Овој правец на дефинирање на сајбер тероризам го поддржува и Шиндер, кој наведува: „Нападите на компјутерите и компјутерските мрежи може да се дефинираат како сајбер тероризам ако нивните ефекти се доволно деструктивни да предизвикаат страв кој е споредлив со физички терористички акт“ (Shinder, 2002, 19). Сајбер тероризам е современа форма на тероризам која се однесува на „незаконски напади и закани на напади врз компјутери, мрежи и информациите што се чуваат таму“, со цел „застрашување или присилување на влада или нејзините граѓани да работат на остварување политички или социјални цели“ (Manap, & Tehrani, 2012, 409) кои им одговараат на терористите. Левис истакнува дека сајбер тероризам претставува значителна закана, бидејќи подразбира „употреба на компјутерски мрежи и интернет алатки за нарушување на критичните национални инфраструктури (како што се енергија, јавен превоз, владини активности) или за

застрашување или присилување на влади на една земја или нејзините граѓани“ (Levis, 2002, 1).

Адекватното соочување со одреден проблем бара негово претходно прецизно дефинирање. Затоа се поставува прашањето: Која се тоа активности на интернетот што можеме да ги сметаме за терористички во вистинскиот смисол на зборот? Разни автори се обиделе да понудат одговор и да ги класификуваат тие активности. Вејмен предложил дека „сите активности на терористи на интернетот можат да се класифицираат во осум различни групи: 1) психолошка војна; 2) публицитет и пропаганда; 3) барање информации; 4) собирање фондови; 5) регрутирање и мобилизација; 6) умрежување; 7) споделување информации; 8) планирање и координација“ (Weimann 2004, 5-10). Мојра Конвеј предлага скала која активности на терористи на интернетот ги карактеризира како употреба, злоупотреба, офанзивна употреба и сајбер тероризам (Конвеј во: Дамњановић, 2009, 238). Елементите кои можат да послужат како основни одредници за прецизно дефинирање на сајбер тероризмот и јасно да го разликуваат од останатите онлајн злоупотреби на информациските и комуникациските технологии и интернетот (сајбер криминал, хакерски активности, па дури и сајбер екстремизмот и сајбер тероризмот

Сајбер екстремизмот се дефинира преку неколку клучни елементи. Овие елементи се:

- а) правен контекст (намери, завери, само закана или акт?)
- б) сајбер просторот служи како оружје или е целта?
- в) цел (и) злонамерни постапки кои содржат некоја форма на насилство со далекосежни психолошки ефекти на целната публика;
- г) намерите комбинирани со долгорочни цели (на пример, општествени или политички промени, влијание врз политичкото одлучување) кои ги следат терористите или терористичката група (Akhgar, Staniforth & Bosco 2014, 13).

Дамњановиќ издвојува неколку основни елементи за дефинирање на сајбер тероризмот, и тие се:

1. употреба на информациски/компјутерски технологии како оружје (а не само како логистичка поддршка, средство за комуникација или мета);
2. политичка мотивација;
3. ориентираност кон симболиката / спектакуларноста / публицитетот;
4. значителна материјална штета и/или човечки жртви, или закана за такви последици, што доведува до:
5. ширење на страв на поголеми размери (Дамјановиќ, 2009, 244).

Комплексноста на феноменот кој се истражува и разновидноста на формите во кои се изразува сајбер тероризмот имаат за последица бројни можности за негово дефинирање врз основа на различни критериуми. Една од најприфатените дефиниции на сајбер тероризмот е понудена од Денинг, која го дефинира како „политички мотивирани хакерски операции кои имаат за цел да предизвикаат сериозни штети, како што се загуба на животи или тешки економски штети“ (Denning 2001, 241).

Петровиќ го дефинира актот на сајбер тероризам прагматично како „користење на информациски ресурси во форма на закана или уцена со цел да се оствари одреден терористички цел“ (Петровиќ, 2000, 649). За постигнување на своите цели, сајбер терористите користат разни тактики (застрашување, мрежни упади и саботажи, онлајн терористички тренинзи и сл.), кои може да бидат се посложени и современи со растечките можности кои ИКТ ги нудат за корисниците.

Најчести покретачи на сајбер терористичките активности се политичката природа. Сајбер терористите, често се користат и со сајбер криминал, што најчесто не им е примарна цел, туку е само некој незаконски начин за прибирање на средства (финансиски и други), кои им помагаат во полесно остварување на нивната примарна цел. Сајбер тероризмот може да биде тесно поврзан со сајбер криминалот, но треба да се разликува од него, како и од информацискиот војна, сајбер шпионажата, бидејќи претставува посебен вид на сајбер закана.

Затоа, сајбер тероризмот подразбира организиран облик на криминално дејствување, што вклучува низ криминални мерки и процедури каде современите технологии се користат како средства или цели на нападите.

2.2 Сајбер тероризам и сајбер криминал: разлики и превенција

Сајбер тероризам не е исто што и сајбер криминал. Главната разлика помеѓу овие два феномени е во целта на нападот, бидејќи основниот мотив на сајбер криминалците е остварување економска добивка, додека основниот мотив на сајбер терористите е политичка или општествена промена. Успешното спречување на сајбер криминалот е една од основните функции на криминалната политика.

Сајбер нападите не само што наносят значителни материјални штети на финансиските институции, туку исто така може да имаат за цел да ја загрозат работата на националните одбранбени системи. За да се разбере потенцијалната опасност од сајбер тероризмот, важно е да се земат предвид два фактора: прво, дали постојат цели

кои се ранливи на напади кои можат да доведат до насилство или сериозна штета; и второ, дали постојат актери кои поседуваат способност и мотивација да ги извршат.

Со бројните штетни последици кои овие напади можат да ги предизвикаат, неопходно е да се преземат адекватни мерки за спречување на сајбер тероризмот. Како што наведува Дороти Денинг, сајбер тероризмот се однесува на незаконски напади и закани на напади на компјутери, мрежи и информации складирани во нив, со цел да се застраши или принуди владата или народот да ги промовираат политичките или општествените цели. Нападот мора да резултира со насилство против лица или имот или, најмалку, да нанесе доволно штета за да предизвика страв. (Денинг во: Дамјановиќ, 2009, 242-243)

Сајбер тероризмот несомнено е сложен и повеќедимензионален феномен, чија контрола бара организирани мерки за борба и превенција. Некои држави го препознаа овој проблем и формираа специјализирани тимови (како СЕКТ - Специјализиран тим за борба против сајбер закани) за итно реагирање и борба со онлајн заканите. Сепак, не постојат усогласени методи за справување со овој општествен проблем и различни држави применуваат различни методи.

САД и Велика Британија се добар пример за безбедносната политика за борба против сајбер тероризмот, бидејќи применуваат две врсти на методи за сајбер одбрана: активни и пасивни. Шиндер истакнува дека мерките за борба против сајбер тероризмот се значајни, но е потребно нивно точно дефинирање и соодветна едукација на оние кои ги применуваат овие мерки, со користење на одговарачка технологија.

Активните методи на одбрана вклучуваат директна одбрана и превенција, односно активности кои се насочени да ги спречат, ублажат или неутрализираат сајбер заканите што се упатени кон цивили и имот.

Додека пасивните методи на одбрана подразбираат различни безбедносни компјутерски техники и мерки на заштита (Стаубс & Бронс, 2015), како што се: криптографија (Танџонг & Шустер, 2006), користење антивирусен софтвер и фајерволи (Валснер, 1997), различни системи за откривање на пробивања и заштита на лозинки, енкрипциски клучеви (DES, 3DES и RSA) (Куљански, 2010, 65-77) и др.

Генерално гледано, терминот тероризам претставува комплексен општествен проблем. Имајќи предвид дека сајбер тероризмот е еден од неговите облици што се одвива во специфично опкружување — сајбер просторот — и дека оваа форма на тероризам бара познавање и примена на современи знаења и вештини, комплексноста на овој феномен

дополнително се усложнува и бара примена на мултидисциплинарен пристап за неговата анализа и толкување.

За потребите на истражувањето и подобро разбирање на овој феномен, авторот ги анализира прашањата што ги предлага Ешли за толкување на сајбер тероризмот:

1. Кои се извршителите на сајбер тероризмот (дали се поддржани од држава, дали државата ги отфрла, дали се паравоени формации, хакерски групи или лица на власт кои се занимаваат со шпионажа);
2. Кои алатки и техники ги користат во процесот на планирање и извршување на самиот напад;
3. Како ги применуваат техниките, тактиките и постапките за изведување сајбер напади (методи на социјален инженеринг, создавање и пуштање вируси, малициозни софтвери);
4. По извршување на нападот, кои се категориите на цели или потенцијални цели на терористичките сајбер напади (информатички и комуникациски мрежи, податоци, објекти во "реалниот" свет, енергетика, банкарство и финансии, витални услуги на една земја);
5. Зошто извршуваат напад, односно што ги мотивира за спроведување на сајбер терористички напади;
6. Кога нападот е извршен, кои се резултатите, предностите и слабостите на таквите акции. (Ашли, 2003)

2.3 Модели на толкување на сајбер тероризмот

Сајбер тероризмот претставува спој од седум клучни елементи:

1. човечки (индивидуални – поединец, терорист или групни – организации во чие име делуваат поединци);
2. ИКТ знаење (значаен ресурс на современото доба);
3. технолошки (ИКТ средства);
4. виртуелен (сајбер простор, онлајн идентитети и онлајн заедници);
5. насилство (насилен упад во мрежа, прибирање на податоци итн.);
6. страв;
7. политичка мотивираност за постигнување долгорочна цел.

Не може секој напад на компјутер или мрежен систем, сајбер закана или други инциденти и разни облици на вандализам што се случиле во сајбер просторот да се

сметаат за сајбер тероризам, доколку мотивот за нивното извршување не е идеолошки. Зашто, сајбер тероризмот и компјутерскиот (сајбер) криминал не се исто. Тоа се два различни поими кои треба да се разгледуваат одделно. Често се случува медиумите, поради недоволно разбирање на разликата меѓу овие два поими, одредени настани погрешно да ги прикажат како сајбер тероризам, иако суштински не се такви.
Пример за тоа е случајот од 2000 година, кога еден Австралијанец хакнал систем за управување со отпадни води и „испуштил“ милиони литри отпадни канализациони води во паркови, реки и индустриски погони (Смит, 2001). Овој случај претставува сајбер криминал, а не сајбер тероризам, бидејќи сторителот делувал исклучиво воден од лични мотиви, а не од желба да промовира одредена верска или политичка идеологија.

Тик и соработниците (Тик, Каска и Виланд, 2010, стр. 18) сметаат дека нападот во Естонија на 27 април 2007 година бил еден од првите примери на големи сајбер терористички напади, чии основни цели биле да ја загрозат националната безбедност, да го дестабилизираат финансискиот систем на земјата и да предизвикаат што е можно повеќе негативни последици врз функционирањето на јавната администрација и економијата.

Во научната јавност постојат несогласувања околу употребата на терминот сајбер тероризам. Едни автори сметаат дека употребата на овој поим е несоодветна и пренагласена, бидејќи нападите преку интернет и во сајбер просторот не можат да се карактеризираат како терор, туку повеќе како непријатност. Други автори, пак, укажуваат на непредвидливите ефекти од сајбер тероризмот, како и на неговите разорни последици по државната инфраструктура, но и на можноста да влијае врз надворешната политика, да го загрози кредибилитетот на некоја влада или да предизвика страв и несигурност со широки размери во меѓународната заедница.

За да можеме да го разликуваме сајбер тероризмот од класичниот сајбер напад, потребно е најпрво да ги разбереме двата поима. Сајбер нападот претставува конфликт што се одвива во виртуелниот (сајбер) простор и може да се изведува самостојно или како форма на поддршка во некој друг конфликт. Сајбер тероризмот, пак, можеме да го разгледуваме како посебен вид на сајбер напад, но истовремено и како посебен вид тероризам.

Условите потребни за успешно извршување на сајбер напад се следниве:

- познавање на целниот систем, вклучувајќи ги неговите функции, сервиси, конфигурации, политики и алатки за заштита и администрација;

- ефективно користење на програми што автоматски ги искористуваат ранливостите за да се пробие компјутерскиот систем (овие програми се познати како *exploits*);
- способноста на напаѓачот да ги прикрие своите траги со цел да избегне можност за детекција и следење;
- брзина на нападот, со што се намалува веројатноста од навремена реакција со заштитни мерки (Вулетиќ, 2011, стр. 22).

Значи, извршувањето на сајбер напад бара детална подготовка од страна на напаѓачот. Тоа значи собирање на што повеќе информации за метата, целните системи, можните „дупки“ во безбедноста и ранливостите (човечки, технички и организациски), како и запознавање со нивните механизми за заштита и нивоа на контрола.

Постоечката литература која го толкува поимот сајбер напади може да се подели во три поширок категории, зависно од аспектот од кој се разгледува:

1. Технолошки-центрични модели
2. Социјално-центрични модели
3. Ситуациски модел (Нара и Рајсстон, 2017, стр. 169–185).

Имајќи предвид дека дејствата на сајбер терористите претставуваат посебен вид на сајбер напади чии основни мотиви се политички, овие модели можат да се применат и за анализа на сајбер тероризмот.

Првиот модел технолошки-центричниот ги објаснува сајбер нападите првенствено од технолошки аспект. Многу автори посветуваат особено внимание на описот на различни алатки кои овозможуваат откривање на сајбер напади. На пример, Бишоп ги толкува сајбер нападите преку шест клучни карактеристики:

- суштинската природа на дефектот предизвикан од нападот,
- времето,
- добивката од експлоатацијата,
- областа/подрачјето на нападот,
- и изворот на идентификација на ранливоста предизвикана од нападот (Бишоп, 1995).

Коен, од аспект на технолошко-центричниот модел, ја толкува сајбер одбраната и го предлага т.н. **„модел на огледало“**, врз основа на следниов сет на карактеристики:

1. **Ортогонална неисполнетост** (*orthogonal incompleteness*),
2. **Корелација** (*correlation*),
3. **Хардверска неспецифичност** (*hardware nonspecificity*),

4. **Опис** (*description*),
5. **Применливост** (*applicability*),
6. **Непотполност** (*incompleteness*) (Коен, 1997, стр. 29–46).

Од друга страна, Хачинс и соработниците (Hutchins, Cloppert & Amin, 2011) предлагаат **„Cyber Kill Chain“** – технолошко-центричен модел применлив на сајбер нападите, кој ги вклучува следниве фази:

1. **Извидување** *(Reconnaissance)*
2. **Наоружување** *(Weaponization)*
3. **Испорака** *(Delivery)*
4. **Експлоатација** *(Exploitation)*
5. **Инсталација** *(Installation)*
6. **Команда и контрола** *(Command & Control – C2)*
7. **Активности кон целта** *(Actions on Objectives)*

- **Првата фаза – Извидување**: вклучува истражување и собирање што е можно повеќе информации, идентификување и избор на цел, прибирање на листи со е-пошта адреси, воспоставување социјални врски или собирање информации за специфични технологии.
- **Втората фаза – Наоружување**: значи прибавување средства за успешна испорака на автоматизиран алат (т.е. сајбер оружје) со цел постигнување на саканата експлоатација преку далечински пристап. Во пракса, сè почесто се злоупотребуваат податоци во познати екстензии како што се PDF или документи од MS Office.
- **Третата фаза – Испорака**: се однесува на начинот на кој се доставува алатот/сајбер оружјето, најчесто преку е-пошта прилози, веб-страници, преносливи USB мемории итн.
- **Четвртата фаза – Експлоатација**: започнува кога алатот се испорачува до домаќинот/жртвата и се активира код кој дозволува пробив во оперативниот систем или одредена апликација.
- **Петтата фаза – Инсталација**: обезбедува доследност и одржливост на нападот и покрај физичката оддалеченост меѓу напаѓачот и жртвата.
- **Шестата фаза – Команда и контрола (C2)**: овозможува активна вклученост на напаѓачот, кој рачно управува со системот – т.н. „раце на тастатурата“.
- **Седмата фаза – Активности кон целта**: се спроведува по успешно поминати претходните фази. Тогаш напаѓачот презема активности во согласност со целите:

рушење на интегритетот на жртвата, прибирање доверливи информации, шифрирање итн. (Hutchins, Cloppert & Amin, 2011).

Сајбер терористите користат различни методи за изведување на нападите. Оттука, се разликуваат три вида на напади:

1. **Класичен физички напад** – насочен е кон компјутерска опрема, објекти или далеководи со цел да се попречи или оневозможи нормалното функционирање и доверливоста на опремата. За овој тип напад, сајбер терористите најчесто користат конвенционално оружје (на пример, огнено оружје или експлозиви).
2. **Електронски напад** – подразбира употреба на електромагнетна енергија, односно електромагнетен пулс насочен против компјутерска опрема со цел да се оневозможи, попречи или загрози преносот и интегритетот на податоците (прегревање на струја или нарушување на комуникацијата).
3. **Напад на компјутерски мрежи (CNA – Computer Network Attack)** – претставува сајбер напад насочен кон процесниот код на компјутерот, неговата логика и инструкции или податоците. Таквиот напад генерира штетни мрежни пакети со цел да се нарушат податоците или логиката на системот, користејќи слабости во софтверот и безбедносни пропусти во системите на организацијата која е цел на нападот (Weimann, 2006, стр. 155–156).

Активностите на сајбер терористите се комплексни, и терористите можат да ги применат сите претходно наведени методи и типови на напади (физички, електронски и сајбер напади насочени кон специфични компјутерски објекти и системи) со цел остварување на нивните политички намери.

Најдеструктивните видови на сајбер напади се: напади врз **SCADA системи**, напади врз **бот мрежи**, **DDoS напади** и **STAKT / STOR напади**, кои се одвиваат по следниов редослед: **SCADA, STOR и STAKT** (Табела 4). Единствено со постојан и систематски надзор може да се постигне ефикасна одбрана и безбедност од овие типови на сајбер напади.

Вториот модел, **социјално-центричниот модел**, се обидува да го толкува, разбере и предвиди сајбер напад преку **човечкиот (социјален) фактор** . Овој пристап подразбира идентификација на поединци кои не уживаат целосна доверба и кои би можеле да претставуваат значителен ризик за сајбер безбедноста.

Истакнати автори (Greitzer & Frincke, 2013, стр. 90–97; Kazimierz и соработници, 2013, стр. 261–266; Slayton и др., 2014, стр. 119–131) кои се залагаат за примена на овој модел, предлагаат методи и метрики за проценка и предвидување на таканаречените **инсајдерски закани**. За идентификација и мапирање на потенцијални проблеми и случаи на нарушување на сајбер безбедноста / доверливоста, неопходно е во анализата да се вклучи **човечкото однесување** и интеракцијата со корисничкиот интерфејс, односно **сите односи меѓу корисниците, нивните цели и околината** (Akbanov, Sillitti & Vosco, 2014, стр. 51).

Застапниците на третиот модел, ситуациониот модел, при толкувањето и разбирањето на сајбер нападите, предност даваат на ситуационите елементи, односно факторите од околината. Сепак, соодветното толкување на сајбер нападите суштински бара примена на сите три модели што претходно беа наведени.

Евалуацијата на извршен сајбер терористички напад може да се врши преку следниве критериуми, според кои нападот се оценува квалитативно:

1. **Јачина** – се одредува според обемот, траењето и интензитетот на последиците од сајбер нападот.
2. **Непосредност** – се однесува на брзината со која последиците се манифестираат.
3. **Директност** – се анализира ланецот на причинско-последични врски.
4. **Инвазивност** – степен до кој операциите во сајбер просторот претставуваат целни упади врз државата или нејзините мрежни системи кои ги загрозуваат нејзините интереси.
5. **Мерливост на ефектите** – Колку повеќе последици можат да се квантифицираат и идентификуваат, толку полесно државата може да ја процени сериозноста на применетата сила.
6. **Воен карактер** – веројатност за поврзаност меѓу сајбер операцијата и воени интервенции.
7. **Вклученост на државата**.
8. **Меѓународно право** – степенот на негово кршење (Prugoš и др., 2018, стр. 376).

Се поставува прашањето: **Како да се разликува обичен (или комбиниран) сајбер напад од оној извршен од терорист?** Искуството покажало дека терористите користат разни криминални дејства на патот кон постигнување на својата примарна цел, која речиси секогаш е **идеолошка**.

Akhgar **и соработниците** (Akhgar, Staniforth & Bosco 2014) предлагаат четири елементи кои можат да послужат како **одредници на сајбер нападите** и за подобро разбирање на **сајбер тероризмот**:

1. **Интегритет на информациите** – Најчесто се однесува на неовластено бришење или менување информации, што доведува до **губење доверба во ИКТ и општеството**. Цели на сајбер терористите се **бази на податоци** што се клучни за функционирањето на општеството: лични документи, регистрација на возила, имотни евиденции, финансиски податоци и слично.
2. **Доверливост на информациите** – Повредата на доверливоста во широк обем, како на пример **објавување на чувствителни лични податоци**, може да доведе до **општествени потреси**. На пример, јавно објавување на здравствена евиденција на ХИВ-позитивни лица во една нација може да предизвика масовна вознемиреност и дури и самоубиства.

Достапност на ИКТ услуги (сервиси) – Се однесува на **отежнување или оневозможување на пристапот до услуги** што ги нудат информационите и комуникационите технологии, што води кон **колапс од широки размери**. На пример, оневозможување на услугите во подолг временски период, неовластено прекинување на работата на одредени системи или мрежи, или физички и електромагнетни напади на дата-центри и критични компоненти на **ИКТ системите**.

Четвртиот елемент, „процеси засновани на ИКТ кои контролираат физички процеси во реалниот свет“, подразбира насоченост на сајбер терористите кон нарушување на работата на нуклеарни електрани, рафинерии, сообраќајни возила и други видови транспорт, системи за здравствен мониторинг и контрола, инфраструктура на „паметни мрежи“ и „паметни градови“, односно сите системи што се круцијални за секојдневното функционирање на општеството (Аккдаг, Стајнѓорнли и Воco, 2014, стр. 14).

Ролинс и Вилсон наведуваат **два клучни елемента** што мора да бидат исполнети за еден чин да се класифицира како **сајбер тероризам**:

1. **Ефектот** – Кога нападот врз компјутерски систем предизвикува **страв, како што е случајот кај традиционалните терористички напади**.
2. **Намерата** – **Постигнување на политички цели** (Rollins & Wilson, 2007, стр. 3).

Оттука, единствено политички мотивирана употреба на компјутери како оружје или како цел, од страна на поднационални групи или тајни агенти, со намера насилно да

влијаат врз јавноста или владата за да ја сменат нејзината политика, може да се смета за сајбер тероризам (Wilson, 2003, стр. 4).

На глобално ниво, стравот и незнаењето се тесно поврзани со толкувањето на овој поим. Поради тоа, Обединетите Нации во 2008 година (United Nations, 2008) сумираа меѓународни инструменти што се однесуваат на превенција и сузбивање на тероризмот. Меѓутоа, не беа понудени прецизни критериуми со кои може да се утврди кога еден акт претставува „употреба на сила“ или „оружен напад“, односно кои мерки може да се преземат и до кој степен, за да се зачува или обнови меѓународниот мир и безбедност.

Постои дури и поделба меѓу оние што се занимаваат со сајбер тероризмот:

- „Believers“ – оние што веруваат дека сајбер нападите веке се случиле,
- „Non-believers“ – оние што сметаат дека таков вид напади сè уште не се случиле (Bipp-Sawyer, 2008).

Меѓународна група експерти, во студијата Tallinn Manual, ги разгледала можностите за примена на меѓународното право при толкување на сајбер конфликтите и сајбер војните.

Оваа група предложи категоризација на сите сајбер активности врз основа на два критериума:

1. Интензитетот на предизвиканата штета,
2. Степенот на прекршување на меѓународното право (Schmitt, 2013).

Според ова, тие предлагаат четири степени на сајбер напади:

- Првиот степен – напади со најнизок степен на загрозеност, чии последици не надминуваат ниво на незначителна непријатност во функционирањето на државата.
- Вториот степен – напади со поголем интензитет категоризација на сајбер напади, која се однесува на употреба на сила (како што е дефинирано во член 2 (4) на Повелбата на ОН), има важна улога во правното толкување и примената на меѓународно ниво. Повелбата на ОН, како што се наведува, подразбира дека сите членки се обврзани да се воздржат од закани или употреба на сила, која ќе биде насочена против територијалниот интегритет или политичката независност на било која држава или било кој друг начин кој не е во согласност со целите на Обединетите Нации. Овој член е клучен за разликување помеѓу сајбер напади кои претставуваат терористички акции и оние кои се повеќе политички мотивирани и претставуваат активна агресија.

- Следната категорија се однесува на сајбер напади кои припаѓаат на третиот степен на интензитет. Овие напади угрожуваат меѓународниот поредок и претставуваат закана за меѓународниот мир и стабилност. За овие напади е потребна активна инволвираност на Советот за безбедност на ОН и, во некои случаи, повикување на Резолуцијата на Советот за безбедност за да се утврди обемот на заканата или причинетата штета. Овие напади може да подразбираат агресија или кршење на мирот, поради што се бараат привремени мерки (како што се економски санкции, трговски санкции) или Советот за безбедност да овласти мировни сили да употребат сила. Ова е важен чекор за заштита на глобалната безбедност.
- Четвртата категорија се однесува на сајбер напади четврти степен на интензитет, кои се мерливи со оружен напад. Овие напади имаат највисок интензитет и можат да доведат до целосно дејство на државата или меѓународната безбедност. Во овие случаи, постои неопходно право на самоодбрана според поглавје VII на Повелбата на ОН. Ова право на самоодбрана е оправдано кога нападот има такви последици што државата мора да реагира со оружје за да се заштити од потенцијално разнишување или уништување.

Адекватна одбрана и превенција бараат добро разбирање и познавање на сите облици на сајбер напади кои ги користат сајбер тероритите. Некои автори наведуваат постоење на три основни видови на сајбер напади: едноставно-структурирани, напредно-структурирани и сложено-координирани .

1. **Едноставно-структурирани сајбер напади** се оние кои не бараат комплексни алати или напредни вештини за извршување. Овие напади припаѓаат на најниските ниво според интензитетот. Најчест пример за оваа врста на напади е бришење или отстранување на податоци, каде напаѓачот користи основни алати и вештини, често преземени од други.
2. **Напредно-структурирани сајбер напади** подразбираат дека напаѓачот поседува одредени вештини потребни за извршување на посложени напади. Оваа врста на напади бара активности на повеќе системи и мрежи истовремено, како и способност да се модификуваат или креираат основни хакерски алати. Најчест пример за оваа врста на напади се **онлајн пљачки на банкарски сметки**.

3. **Сложено-координирани сајбер напади** се најкомплексни, бидејќи бараат висок ниво на подготовка и организација. Овие напади користат софистицирани хакерски алати и напредни знаења за извршување на масовни нарушувања со помош на компјутери. Примери за оваа врста на напади се иницирање на авионски несреќи, колапс во сообраќајот, нестанок на струја и колапс на телекомуникации.

Акгар и соработниците истакнуваат дека сајбер тероризмот против земјата и нејзините граѓани може да се случува на различни нивоа на софистицираност, а секое ниво бара одредени технолошки способности и инвестиции од страна на напаѓачот. Штетата што се нанесува е директно пропорционална на нивото на вложени ресурси (Akhgar Staniforth& Bosco 2014, 168)

Натаму, тие разликуваат три основни категории на сајбер напади според **скалата на нанесена штета**:

1. **Напад на пристапната мрежа на организацијата** – напад кој се фокусира на мрежната инфраструктура и пристап.
2. **Напад на информационите системи на организацијата** – напад насочен кон податоците и информациите што ги чува организацијата.
3. **Напад на основните оперативни системи** – напад на критични системи кои поддржуваат функционирање на организацијата.

Во зависност од обемот на штетата, разликуваме три нивоа на сајбер тероризам. Во **првото ниво**, сајбер терористите користат најосновни и наједноставни видови напади.

1. **Желени напади** подразбираат директни упади на интернет страници и го онеможуваат пристапот на веб страниците, го ометуваат нивниот работен процес така што манипулираат со информациите и податоците, додека причинетата штета е краткотрајна и брзо решлива.
2. **Оснос напади** претставуваат дистрибуирано порекнување на услуги. Најчесто мети на нападите се банки, мобилни оператори, провајдери на кабелска и сателитска телевизија, разни берзански услуги, медиуми и други.
3. **Напади на DNS (Domain Name System)** сервери служат за да го насочат протокот на информации преку интернет, обезбедувајќи одредени локации и информации на кои напаѓачите сакаат да го насочат интернет сообраќајот. Ова се постига така што барањето на корисникот се пренасочува од неговиот компјутер на локацијата на напаѓачот, а не на вистинската локација што

корисникот ја избрал за пребарување или работа на интернет. Покрај одземањето на услугите на клиентите, најчеста штета е кражбата на информации, што го доведува во прашање функционирањето и репутацијата на сервисот. Исто така, терористите се служат со пропаганда на своите активности и цели, па оваа врста на напади служи за да го пренасочат интернет сообраќајот на соодветни страници и содржини кои ги промовираат.

Другиот ниво на скалата на причинета штета во сајбер просторот подразбира среден ниво на сајбер тероризам. Овде спаѓаат различни напади на информациски и компјутерски системи каде што се складираат и обработуваат податоци (сервери, бази на податоци). За спроведување на оваа врста на напади потребни се покомплицирани технолошки средства и вештини, но и пристап до компјутери од внатре, односно учество на вработени лица во организацијата која се обидува да претрпи штета и да се спречи обезбедувањето услуги. Најчесто мети на нападите се банки, мобилни оператори и интернет провајдери. Јасна разлика помеѓу оваа врста напади на сајбер терористи и третото, најсофистицирано ниво на сајбер тероризам е тоа што овие напади не резултираат со физички оштетувања, но сепак се ослонуваат на виртуелни услуги и пристап до нив, и може да предизвикаат значителна штета. Како пример може да послужи нападот на компјутерите на нафтната компанија во Саудиска Арабија познат како **Агатсо**, кој се случи во август 2012 година. Напаѓачите користеле компјутерски вирус **Скатооп**, кој ги онеспособил 30.000 компјутери. Иако нападот не влијаел на основните оперативни системи на компанијата, го загрозил нејзиниот работен процес така што многу податоци од организацијата биле избришани од компјутерите, што значително ја отежнало и успорило понатамошната работа на компанијата за подолг период. Тоа подоцна значително се одразило на нафтената индустрија и нарушило тогашната рамнотежа на моќта на нафтените компании во таа земја.

Третата врста сајбертерористички напад припаѓа на третиот ниво според интензитетот на причинета штета, бидејќи подразбира напад на критичната инфраструктура, односно основните оперативни системи кои ја поддржуваат секојдневната работа и живот. Оваа врста на сајбертерористички напад е најсложена, подразбира користење на различни технолошки средства и може да се одвива на неколку различни нивоа. Исто така, сајбертерористички напад на третиот ниво бара напаѓачот да поседува напредни способности и вештини за ракување со опрема за изведување на сајбер напади, додека причинетата штета е директно соразмерна со нивоата на инвестиции. Најчести примери за оваа врста напади се напади врз системи кои

управуваат и контролираат индустриските сектори на некоја земја (гориво и гас, водоснабдување, струја, јавен транспорт, системи за банкарски платен промет итн.). Овие врсти на сајбертерористички напади се најсофистицирани, бидејќи вклучуваат момент кога причинената штета преминува од сајбер просторот во реалноста (физичкиот свет), каде што предизвикува штета на големи размери, чији ефекти можат да бидат значајно деструктивни за одредена држава и нејзината нација.

Целел утврди „пет главни типови на сајбертерористички напади":

1. упад (hacking)
2. уништување (destruction)
3. дезинформација (misinformation)
4. одбивање на услуга (denial of service)
5. дискредитација на сајтови (website defacement) (Џолел, 2003, 8).

Наведените напади се разликуваат според тежината на причинената штета и целите.

2.4 Учесници и мети на сајбер тероризмот

Главни учесници во терористичките активности се терористи (изведувачи и организатори на терористички активности) и жртви (цивили или целни политички функционери). Занимавањето со тероризмот и неговите различни форми подразбира и разбирање на поимот терорист. Така на пример, „Обединетите нации сметаат дека терорист е секоја личност која, дејствувајќи независно од знаењето на некоја земја, или како поединец, или како член на група која не е призната како официјално тело или дел од некоја нација, дејствува на тој начин што уништува или оштетува имот на цивилното население или влада за да постигне некој политички цел" (Гаћиновић, 2011, 23).

Интензивниот технолошки развој и глобалното поврзување создале нов облик на тероризам, кој произлегува од интеграцијата човек-компјутер (социјална фузија и фисија). Социјалната фузија која произлегува од таа релација се однесува на бројните предности кои компјутерите ги даваат на луѓето (побрза и полесна комуникација, бази на податоци, пребарување и др.). Оттука настанува **IoT** — **Internet of Things** (Интернет на нештата), актуелната системска парадигма која подразбира испреплетена мрежа на перцепции, онлајн интеракции, социјални односи и когнитивно размислување.

Социјалната фисија пак подразбира користење на тие предности на деструктивен начин, било авто-деструктивно (социјална изолација) или деструктивно за поширокаата заедница (сајбер терористички напад и слично). Бидејќи „интернетот и социјалните

мрежи се идеално место за спроведување на терористички активности и операции, бидејќи овозможуваат географски неограничени акции и нивно брзо спроведување" , новата генерација терористи е насочена кон користење на овие предности при изведување на своите операции.

На тој начин, примената, развојот и сè поголемата достапност на технолошки алати, особено информациските и комуникациските технологии во рацете на терористите, ги комплицираат потенцијалните закани од оваа современа форма на тероризам — сајбер тероризам.

Сајбер тероризмот претставува спој на човечкиот и технолошкиот елемент. Сајбер просторот обезбедува предности кои им овозможуваат на терористите да останат анонимни и да формираат лажни IP профили и адреси. Поради комплексноста и напредните карактеристики на ИКТ, овој вид тероризам станува сè повозбудлив и поприсутен.

Потребни се исклучителни напори, напредно технолошко знаење, како и оспособеност со најсавремени технологии и вештини за да се утврди идентитетот на починителот на сајбер тероризмот, неговата намера или евентуалната политичка и финансиска поддршка што терористот како извршител ја имал. Адекватната одбрана од сајбер терористите најпрво подразбира адекватно соочување, односно идентификација и способност да ги препознаеме клучните карактеристики на оваа врста на тероризам. Потенцијалниот сајбер терорист може да биде секој кој има непријателски намери, добро знаење од областа на информационите и комуникационите технологии и пристап до доверливи ИТ информации. Односно, за да го разбереме тероризмот, важно е да го разбереме умот, односно психата на терористот, како и да ги имаме на ум неговите генерални карактеристики како што се правдољубивост и мотивираност по идеологии, политика, религии, освета, било поединечно или во комбинација. Нашата представа за терористите како психички нарушени луѓе е погрешна. „Според расположливите научни докази за поврзаноста помеѓу насилството и менталните болести во популацијата, насилството не е предизвикано од големи психијатриски проблеми како што се шизофренија, биполарни пореметувања или депресија" (Степсон, 2012).

Истражувањата покажале полни, старосни и класни обележја на терористите. Главно се работи за мажи. Меѓутоа, жените и децата често се манипулирани да им се приклучат на терористичките организации. Затоа тие често се појавуваат како починители на терористички дела, како што се деца војници (Сладер, 2006, 373-384), осмогодишни бомбаши во Пакистан (Мист, 2013), и терористички дејства на Шри Ланка

- Тамилски Тигрови (Мштату, 2010). Класната анализа на повеќе од 150 терористи од Ал-Каида покажала дека тоа се високообразовани, ожењени мажи од средна и висока средна класа (Василетоски, 2007, 13-18). Сент Клер, како актер на сајбер тероризмот, ги спомнува: „терористичките организации, нивните симпатизери и ловци на сензации" (Сат-Сладер, 2011).

Клучни актери на тероризмот се терористичките организации (групи). Иако материјалите на терористичките групи се транспарентни и лесно може да се најдат на интернет, терористичките организации се релативно „затворени“ групи на терористи, базирани на доверба и во тајност ги чуваат своите методи на напади и поуздани учесници. Меѓутоа, терористичките групи се достапни на интернет и нивните учесници комуницираат преку различни (проверени) канали за комуникација, на пример, преку Скајп платформи, скајп и други.

Терористички организации чии активности е меѓу најголемите на интернет се:

1. **Ал-Каида (А1-Каида)** - Многи припадници Ал-Каиде имаат добро образование во областа на инженерството и технологијата. По организираниот напад во Авганистан во ноември 2001 година, кога американските сили неочекувано напаѓаат активисти на Ал-Каида, многу од нив биле принудени да побегнат од Кабул. Тогаш биле пронајдени многу чувствителни информации и документи кои оперативците на Ал-Каида ги оставиле зад себе, кои потврдуваат профил на терористите како добро образовани и обучени за работа на компјутери и оперативни системи: „Технички скици на арапски, англиски и германски јазик, студентски бележници на арапски, турски, курдски и руски јазик покажале доследност во интересувањето и широко познавање на електрично и хемиско инженерство, атомска физика, балистика, компјутери и радио станици" (Балиќ, 2002).
2. **ИСИС** - Американската компанија за сајбер безбедност „Рѓже Еѓе" јавно изјавила дека ИСИС користи тамната мрежа (dark web) за терористички цели. На овој начин, ИСИС може да извршува трговија со сајбер оружје / алатки на едноставен начин, без потреба од ангажирање на сложени средства и стручност (Антоета, 2015, 82).
3. **ИРА (Ирска Републиканска Армија)** - По економските санкции кои САД и европските земји ги воведоа против Иран, ИРА го спонзорирала групата терористи за извршување сајбер напади како одговор на оваа ситуација.

4. **Тамилски тигрови** (Tamil Tigers) - Најсмртоносната терористичка група во Шри Ланка, основана 1976 година, забранета во повеќе од тридесет земји низ светот. Оваа терористичка група беше главниот причина за граѓанската војна во Шри Ланка. ЕТТЕ (Експлозивни Тамилски Тигрови) се специјализирана фракција на Тамилските тигрови чиј главен циљ беше да ја наштетат владата на Шри Ланка преку сајбер терористички операции.

Популарни радикални групи од меѓународно значење, како шиитските групи во Либан (Сехат ли-Шиитс Голабс) и Исламската држава. **Хезболах** од Либан користи интернет-сајтови за различни цели: за објавување на статии или најави за предстоечки настани, за објавување на ново-снимени видео-снимки итн. (Вешчек, 1996).

Покрај терористичките организации, како актери на сајбер тероризмот можат да се јават и симпатизери кои имаат слична идеологија како терористичките групации, иако не се активно вклучени во онлајн терористички дејности. Третата категорија актери ги сочинуваат **барателиначувства** (sensation seekers). Тоа се напаѓачи кои не се идеолошки поврзани со одредена терористичка групација, односно нивниот примарен мотив не е политички или идеолошки, туку се водат од желбата да стекнат слава. Најчесто тоа се хакери кои сакаат да го прослават своето име (псевдоним) со изведување на одредени сајбер напади кои бараат врвни ИТ вештини, што им носи слава во виртуелната заедница.

Сајбер безбедноста ја загрозуваат: хакери (професионалци и аматери), незадоволни вработени, сајбер криминалци, сајбер терористички групи и други. Спроус и Бајерс (Спроус & Бајерс, 1998) спровеле истражување на примерок од 100.000 хакери и покажале процентуалниот удел на хакерите во сајбер тероризму: хакери-аматери се одговорни за околу 90% од сите терористички активности на интернету, 9,9% чине потенцијално професионални хакери и 0,1% меѓународно светски познати сајбер криминалци .

Терористите најчесто регрутираат нови членови преку пропагирање на своите идеи терористите ги промовираат повикувајќи се на наводна потреба за заштита на ранливи и загрозени општествени групи, потпирајќи се на чувство на неправда, отуѓеност и понижување. Односно, тие главно ја применуваат т.н. „патерналистичка“ метода која подразбира тесен избор на целна субпопулација и насочување на пропагандата кон нејзините специфични демографски карактеристики (како што се возраста или полот), општествени или економски околности (Weltman, 2008). На пример, за регрутирање малолетници преку интернет, терористите користат пропаганда

прилагодена на детската возраст – во форма на детски приказни, карикатури, популарни музички видеа или компјутерски игри и друг материјал што содржи пораки со кои се промовираат и слават терористички дела или самоубиствени напади. Некои терористички организации отишле и подалеку, финансирајќи и/или дизајнирајќи „онлајн“ видео игри што служат како средство за регрутација, вработување и обука на членови преку промоција на употреба на насилство.

Во научната јавност преовладува разбирањето дека целите на терористите се првенствено политички (верски, националистички или сепаратистички). Сепак, познато е дека мотивите и целите се променливи категории и дека терористите може да ги приспособат своите цели според интересите на своите финансиери. Различни причини и мотиви можат да го наведат поединецот да се занимава со тероризам – политички, етнички, верски, идеолошки, економски (криза, сиромаштија, несигурност), социјални (аномија, социјална изолација), психолошки (карактерни црти, фрустрации, акумулиран стрес, незадоволство од постојната животна состојба), идеолошки, геополитички, територијални (етносепаратистички, националистички) и комбинирани.

Терористите несомнено се карактеризираат со употреба на насилство при остварување на своите цели – како во реалниот простор (физичко насилство), така и во сајбер-просторот (дигитално насилство) кое се рефлектира со нанесување штета во физичкиот свет. Токму оваа примена на насилство дополнително ги модифицира нивните првични мотиви и ја распламтува нивната намера на насилен, нелегитимен начин да се обидат да ја променат постојната општествено-политичка реалност, да предизвикаат рушење на конкретна државна власт или да изнудат одредени политички отстапки.

Она што ги карактеризира извршителите на терористички сајбер-напади е нивната јасна насоченост кон метата, добра организираност и концентрирани напади кои, кога се спроведуваат здружено, имаат поголеми шанси да предизвикаат сериозна штета на целта.

2.5 Последици од сајбер тероризмот

Насоката на технолошкиот развој предупредува дека сајбер тероризмот има голема веројатност да стане сè попопуларна закана во иднина. Посебно сме сведоци на брзиот напредок и зголемување на бројот на високо квалификувани стручњаци во областа на информациските и комуникациските технологии, како и на постојано растечката потреба за кадар од оваа област. Истовремено, погодностите што ги нудат

современите технологии – со релативно ниски трошоци и едноставност на извршување – го прават овој вид напади најлесната и најпрактична опција за делување од страна на терористите во модерното општество.

Факт е дека современите држави во голема мера го засноваат функционирањето на клучните (витални) структури на модерни технологии и компјутерски системи. Затоа, најголем предизвик за сајбер терористите претставува насочувањето кон ИКТ-технологиите што ја поддржуваат работата на клучните/критични инфраструктури. Што подразбираме под „критична инфраструктура“? – „Сет на мрежи, ентитети, системи и структури кои можат да ја нарушат одржливоста на општествениот поредок или јавните услуги доколку делумно или целосно престанат да ги извршуваат своите функции“ (Väyrynen & Bell, 2014, стр. 911).

Критични инфраструктури се: „фабрики за преработка на храна, фармацевтски постројки, постројки за електрична енергија и природен гас, железнички раскрсници и системи за сообраќајна контрола, идната генерација на контрола на воздушен сообраќај, целокупната модерна воена опрема, воените и јавнобезбедносните комуникации, како и цивилните комуникации“ (Дамјановиќ, 2009, стр. 245). Иако критичната национална инфраструктура е генерално добро заштитена во повеќето држави, секогаш постои потреба за подобрување на нивото на безбедност и зајакнување на отпорот против дејствата на сајбер тероризмот. Зашто, без разлика на формата на манифестирање на сајбер тероризмот, кога мета на напад е критичната инфраструктура – последиците можат да бидат катастрофални.

Вилке (Wilke, 1999) укажува на сериозноста на заканата од сајбер терористички напади, потсетувајќи дека некои од тие напади можат да предизвикаат последици од катастрофални размери – било во форма на еден масовен напад врз критичната национална инфраструктура, или преку серија координирани, наизглед независни напади.

Нујен исто така укажува на сериозноста на последиците од сајбер-терористички напад, наведувајќи дека: „Толкувањето на последиците од сајбер тероризмот е предизвик и речиси невозможно без да се земат предвид неговите следни карактеристики:

1. обем на ефекти (Scope of Effects);
2. непредвидливост (Unpredictability);
3. реверзибилност на штетата (Reversible Damage);

4. анонимност и проблем со припишување одговорност или вина за причинетата штета (Anonymity and the Problem of Attribution)" (Tsguyen, 2013, стр. 1098–1106).

Сајбер напаѓачите најчесто, покрај директната цел — како напад на одреден сервер, систем или уред, бришење или модификација на кодот на кој функционира системот, или измена на зачувани податоци — имаат и индиректна цел што сакаат да ја постигнат. Таа крајна цел се однесува на ефектите што ги произведува извршениот сајбер-напад, односно на начинот на кој нападот може да влијае врз носењето човечки одлуки преку пласирани и обработени информации од страна на сајбер терористите.
Општо гледано, секој сајбер-терористички напад произведува индиректни ефекти кон кои се стремат напаѓачите. Бидејќи по извршувањето на нападот, се создава ланец на последици кои во некои случаи може значително да потсетуваат на вооружен напад, па дури и да предизвикаат смрт. Сепак, сајбер нападите се суштински различни од традиционалните воени напади. Пред сè, затоа што вклучуваат пософистицирана употреба на алатки и оружја (ИКТ, компјутерски системи), додека традиционалниот напад користи физичко оружје кое предизвикува директна штета, со што постои ризик од повреда за напаѓачот поради незнаење, невнимание или несреќа.

Сајбер нападот, напротив, може да се изведе „од фотеља“, далеку од целната мета — и просторно и временски — и не претставува физичка закана по извршителот, а истовремено може да нанесе огромна штета. На пример, само еден злонамерен код може автоматски да ја реплицира штетата, брзо да инфицира други системи и да избрише цели сетови информации од компјутерот.

Споменатите карактеристики — голема неизвесност на последиците, потенцијално широк опсег на прекин во работењето на оперативните системи и оштетувања, како и висок ризик од колатерална штета — го прават сајбер тероризмот најактуелна форма на тероризам во современото време. На пример, компјутерскиот црв „Sapphire worm“ го оневозможи работењето на сервери во Јужна Кореја, создаде проблеми во интернет услугите во Тајланд, Јапонија, Филипини, Малезија, Индија, го прекина итниот 911 сервис и предизвика проблеми во работењето на 13.000 банкомати во САД (Schneier, 2003), тоа доведе до одложување на канадските национални избори и авионски летови во 2003 година. Во мај 2021 година, гасоводот *Colonial Pipeline* беше мета на хакерски напад, а неколку месеци претходно, во февруари 2021 година, еден хакер успеа да навлезе во системот за водоснабдување на еден град во Флорида и се обиде да внесе опасна количина на хемиско средство во водата (Tisdall, 2021). На ист

начин, можно е сајбер напад да биде насочен и кон воени ресурси, со што лесно може да прерасне во напад врз цивилното население.

Ворен наведува „четири главни цели на сајбер нападите што ги извршуваат терористите:

1. оневозможување на оперативните способности на непријателот;
2. уништување на репутацијата или намерно искривување на сликата за одредена организација, нација или сојуз;
3. убедување на нападнатите да ја променат својата припадност;
4. демонстрирање на способност пред следбениците дека можат да нанесат значителна штета на своите цели“ (Warren, 2002).

Најчеста цел на сајбер терористите е да ја загрозат и/или оневозможат оперативната способност на непријателот. Затоа, тие применуваат видови на напади кои можат сериозно да го нарушат или уништат функционирањето на противничките системи и да предизвикаат сериозна штета на цела нација, да доведат до економски колапс или општествена криза.

Во современото општество, маркетингот и угледот се витални елементи врз кои се засноваат активностите на модерните организации. Затоа, втората најчеста цел на сајбер терористите е да нанесат штета преку уништување на репутацијата или искривено претставување на одредена организација, нација или сојуз. Терористите најчесто го постигнуваат ова преку ширење лажни гласини преку електронски медиуми (е-пошта, веб-страници итн.).

Со оглед на тоа што медиумите играат клучна улога во секојдневниот живот, терористите често хакуваат електронски медиуми за да ја пренесат сликата за своите напади, цели и мотиви низ целиот свет. На тој начин им покажуваат на своите следбеници и пошироката јавност дека се способни да предизвикаат сериозна штета на своите цели, дека претставуваат вистинска закана и ширум сеат страв.

Некои дела на сајбер тероризмот имаат за цел да ги нарушат постојните партнерства и сојузи, и да ги натераат нападнатите да ја променат „страната“ на која дотогаш ѝ биле лојални.

Последиците од тероризмот можат да бидат различни, а неговите ефекти се „исклучително сложени, латентни и често претставуваат стратешки ризик за безбедноста на државата и граѓаните поради следниве причини:

1. загрозување на човечки животи, односно повреди и смрт како последица на терористички напади;

2. загрозување на здравствената безбедност на луѓето;
3. загрозување на животната средина, растителниот и животинскиот свет;
4. дестабилизација на економијата и на економските инвестиции;
5. загрозување на енергетската безбедност на државата;
6. загрозување на социјалната безбедност;
7. загрозување на финансиската стабилност на државата;
8. демографска дестабилизација на државата;
9. пораст на национализам и верски тензии;
10. експанзија на т.н. медиумски криминал;
11. поврзување на тероризмот со други видови криминал, од кои најопасно е соработката со организираниот криминал и субверзивните активности на разузнавачки служби на непријателски настроени држави;
12. пораст на корупцијата во јавниот сектор;
13. загрозување на функционалноста на одделни државни институции;
14. создавање недоверба на граѓаните во државата и нејзините органи;
15. создавање недоверба меѓу граѓаните и државата во меѓународните органи и институции;
16. нарушување на меѓународните односи и угледот на земјата на меѓународната сцена“ (Милашиновиќ и Мијалковиќ, 2011, стр. 9–10).

Шиндер смета дека најчестите акти на компјутерски тероризам се:
а) електронска комуникација со цел спроведување на одредени терористички активности или регрутирање нови членови на терористички организации;
б) саботажа на воздушниот сообраќај, со цел предизвикување авионска несреќа, или саботажа на електронски системи за прочистување вода со цел загадување на водата за пиење;
в) пробивање на болнички и здравствени системи за да се избришат или изменат бази на податоци за пациенти и пропишани терапии или напади врз енергетска инфраструктура, што може да предизвика смрт кај лица приклучени на респиратори итн. (Schinder, 2002, стр. 19).

Вајмен смета дека најштетните ефекти на сајбер тероризмот се постигнуваат преку напади врз „бот мрежи“ и „SCADA системи“ (Duckenapp, 2015, стр. 157).

Ботнети или бот мрежи претставуваат голем број компромитирани компјутери кои се заразени со злонамерен код и може да се контролираат од далечина преку интернет-команди. Стотици или илјадници заразени компјутери дејствуваат заедно со

цел да го нарушат или блокираат интернет-сообраќајот на целната жртва. Ботнетите може да се користат за DDoS напади, кражба и злоупотреба на податоци, дистрибуција на малициозен софтвер и други организирани криминални терористички активности. Исто така, тие може да се користат за прибирање доверливи информации или за напади на клучна инфраструктура која во голем дел се потпира на интернетот, како и како средство во пропагандни или психолошки кампањи со цел ширење страв, заплашување или јавна дискредитација.

Ботнетите несомнено стануваат главна закана и оружје на современите сајбер терористи, главно затоа што можат да се дизајнираат така што ќе го нарушат функционирањето на целните компјутерски системи на различни и ефикасни начини, а терористите дури можат и да ги изнајмат за свои потреби, доколку не поседуваат доволно технички вештини за нивен дизајн (Duckenapp, 2015, стр. 156).

SCADA – Supervisory Control and Data Acquisition (системи за супервизорска контрола и прибирање податоци) се вид компјутерски систем што го следи и контролира функционирањето на клучните (критични) инфраструктурни системи, како приватни така и јавни. Овие системи со примена на различни алатки, како што се: програмски логички контролери, далечински терминални единици и други уреди за следење и автоматизација, управуваат со:

– пречистување и дистрибуција на вода,

– собирање и третман на отпадни води,

– работа на нафтоводи и гасоводи,

– пренос и дистрибуција на електрична енергија,

– ветерни електрани,

– системи за цивилна заштита,

– работа на сирени,

– следење и контрола на системите за греење, вентилација и климатизација,

– потрошувачка на енергија во згради, аеродроми, бродови и вселенски станици (Duckenapp, 2015, стр. 157).

SCADA системите постојат од 1960-тите години, но тогаш не биле добро мрежно поврзани. Експоненцијалниот раст на мрежите и поврзувањето на информациските системи што ги обединуваат деловните, административните и оперативните системи, доведе до тоа пристапот до SCADA системите да стане еден од најатрактивните цели за сајбер терористите. Секоја промена на податоците што се користат за оперативни одлуки или за функционирањето на овие програми може да има катастрофални последици.

Генерално, тероризмот често е замислен како форма на психолошка војна. Целта на речиси секој терористички напад, вклучително и на сајбер тероризмот, е да ја дестабилизира и вознемири јавноста. Психолошките последици од сајбер тероризмот за жртвите и поширокаta јавност се значајни, без оглед на тоа дали нападот предизвикал човечки жртви или економска штета.

Директните жртви на насилството не се примарна цел на терористичкото делување – насилството служи како средство за пренесување пораки. „Комуникацијата меѓу терористите (организацијата), жртвите (загрозените) и главната публика (јавноста), која се темели на закани и насилство, се користи за манипулација со главната публика – претворајќи ја во цел на теророт, цел на барањата или цел на вниманието – во зависност од тоа дали целта е заплашување, присила или пропаганда“ (Sauter & Jonathan, 2005, стр. 28).

Според тоа:

„Сајбер тероризмот се вклопува во целите на терористите преку внесување страв во животите на нивните непријатели. Тој може да се случи без какво било предупредување, а обичните цивили не можат да направат многу за да се заштитат од вакви напади. Оваа неизвесност и недостатокот на контрола врз сопствениот свет го прави сајбер тероризмот застрашувачка опција во очите на јавноста“ (Duckenapp, 2015, стр. 153).

2.6 Релација меѓу сајбер тероризмот и организираниот криминал

Примарната безбедносна закана за една држава во минатото доаѓала од спротивставени држави, воени потенцијали и коалиции. Меѓутоа, промените на глобалната сцена донесоа изменети околности. Различни недржавни актери станаа закана за националната безбедност. Организираниот криминал претставува комплексна криминолошка појава која постои во различни облици ширум светот. Тој претставува постојана опасност што се толкува различно во националните законодавства, тешко се препознава и соодветно се третира.

Одредени криминални организации со текот на времето значајно ги профилираат своите активности, се поврзуваат и воспоставуваат поблиска соработка со слични организации кои исто така се занимаваат со инкриминирани активности на државно и меѓународно ниво. На тој начин настанува организираниот криминал, односно таа сложена криминална форма што наликува на мрежа. Оттука, Абадински предлага дека за разбирање на организираниот криминал неопходно е да се разберат „организацијата

на групата и нејзиното делување, кои според него претставуваат суштински делови на овој современ феномен, па така наведува дека организацијата е подготвена да користи насилство или поткуп за да ги постигне своите цели или да обезбеди дисциплина“ (Abadinsky во: Шкуљиќ, 2003, стр. 38–39).

Делувањето на организираниот криминал негативно влијае врз функционирањето на економскиот систем на државата, нејзината сфера на економско-политички односи и безбедносниот сектор.

„Организираниот криминал претставува добро организирана криминална структура, со строга хиерархија, дисциплина, одговорност, лојалност и поделба на задачи, чија цел е остварување што поголем профит и легализација на незаконски стекнат имот, благодарение на постигнатиот степен на општествен углед – било преку продор во структури на власта или преку воспоставени врски со државни органи, легални бизнис субјекти и влијателни политички партии и групации“ (Бошковиќ, 1998, стр. 9).

Шкуљиќ наведува општи услови што мора да бидат исполнети за постоење на организирана криминална група:

1) број на членови – групата мора да се состои од најмалку три лица;
2) соодветна временска континуираност – групата мора да постои одредено време;
3) криминална целна насоченост – групата мора да дејствува по договор со цел извршување на едно или повеќе кривични дела за кои е пропишана затворска казна од четири години или потешка казна;
4) општа цел на криминалното дејствување – групата извршува кривични дела со цел:

а) непосредно или посредно стекнување финансиска или друга корист или
б) остварување и задржување влијание врз економски или други значајни државни структури“ (Шкуљиќ, 2014, стр. 2–3).

Клучните обележја на организираниот криминал се: мрежна структура со јасно утврдени надлежности и хиерархија, насилна природа, конспиративност во дејствувањето, лојалност на членовите на групата, релативна трајност (континуитет во дејствувањето), адаптибилност.

Павлиневиќ додава и други карактеристики: „специјализирана поделба на трудот меѓу членовите; спроведување на дисциплински мерки;употреба на насилство или слични средства за заплашување;користење на комерцијални или други слични деловни структури;учество во перење пари;транснационален карактер и влијание преку легитимни социјални институции – државни органи (министерства за правда, внатрешни работи) или економски институции“ (Павлиневиќ, 2017, стр. 36–37).

Организираниот криминал постои во различни форми. Хејген ги наведува четирите типа организиран криминал според мотивот на инкриминираната активност:

1. Политичко-социјален организиран криминал;
2. Наемнички или предаторски организиран криминал;
3. Групно ориентиран организиран криминал;
4. Синдикален или гангстерски организиран криминал (Hagan, 2010, стр. 298–299).

Некои автори организираниот криминал го гледаат како специфична „нова форма на геополитика“ (Galeotti & Tzankova, 2010, стр. 393).

Дејствувањата на организираниот криминал и терористичките групи сè повеќе се преплетуваат. Сè до појавата на наркотероризмот, поимите организиран криминал и тероризам се толкувани одвоено.

Шели и Мелцер, преку две студии на случај за шверц на цигари, наведуваат заеднички карактеристики на тероризмот и организираниот криминал: „незаконско финансирање, слична организациска структура, користење на корупција, организирање на бизнис модели во области со слаба државна контрола, користење на современа технологија, исти техники за перење и трансфер на пари, па дури и исти извршители“ (Shelley & Melzer, 2008).

Шмид исто така наведува неколку сличности меѓу тероризмот и организираниот криминал: „рационално оправдување, примена на техники за заплашување, закани со физичко насилство и употреба на слични тактики“ (Schmid, 1996).

Иако постојат сличности помеѓу тероризмот и организираниот криминал, овие два облика на криминално делување се јасно и недвосмислено разликуваат. Она што ги

разликува организираните криминални групи од терористичките е пред сè: неидеолошкиот карактер, ексклузивното членство со строга специјализација и поделба на трудот, како и постоењето на строги внатрешни правила.

Иако меѓународниот тероризам исто така се карактеризира со: меѓународен карактер, мрежна структура, насилна природа и лојалност на членовите на групата, суштинската разлика во однос на организираниот криминал е неговиот идеолошко-политички карактер. Примарната цел на организираниот криминал е „стекнување на профит и моќ индивидуално или во целина“ (Savona, Adamoli, Di Nicola & Zoffi, 1998, стр. 6), односно стекнување корист на незаконит начин.

Кога станува збор за организираниот криминал, „најголемата добивка се остварува преку трговија со дрога, перење пари, трговија со оружје или организирани кражби“ (Петровиќ, 1998, стр. 37–39).

Дури и кога организираниот криминал содржи политичко-социјална компонента (на пример, дејствување во соработка со терористички групи, герилски организации, соработка со различни општествено-воени движења), тој не подразбира криминални активности со примарна политичко-идеолошка цел, туку е насочен кон прибавување моментална корист или интерес за организираната криминална група (перење пари, организирање трговија со луѓе, киднапирања, производство и дистрибуција на различни видови дрога, формирање лоби групи итн.).

Како што забележува Абадински, „организираниот криминал е неидеолошко здружение на одреден број лица, кои меѓусебно остваруваат блиски општествени интеракции, организирани на хиерархиска основа од најмалку три нивоа – ранга, со цел обезбедување профит и моќ, благодарение на учеството во незаконски и законски активности“ (Abadinsky, 1994, стр. 38).

Криминалните групи што припаѓаат на организираниот криминал спроведуваат активности со кои се кршат меѓународните регулативи, но поради различните толкувања на поимот организиран криминал во различни држави, значително е отежната надворешната контрола и откривањето на тие активности од страна на безбедносните служби.

Помеѓу организираниот криминал и тероризмот постојат заемни релации што се манифестираат на неколку начини: коегзистираат, соработуваат или се конвергираат (Pinzoni & Kostell, 2020). Заедничката точка помеѓу тероризмот и организираниот криминал, како што наведуваат Мијалковиќ и Бошковиќ (Мијалковиќ & Бошковиќ, 2009), е финансирањето на тероризмот, односно „валканите пари“.

Терористичките организациии тесно соработуваат со останатите криминални актери за да обезбедат материјални ресурси кои се неопходни за спроведување на нивните терористички активности. За да опстане, криминалната организација мора да користи насилство или други средства, како што се застрашувањето, и да воспостави поврзаност со државни, политички, економски и финансиски субјекти преку корупцију, уцену, изнуда или други методи (Бошковиќ, 1998, стр. 53).

Терористи често извршуваат тешки кривични дела, како што се рекетирање, кријумчарење на луѓе и дрога, за да обезбедат корист за себе или за организацијата. Овие активности нанесуваат штета на поединци и правни лица, како што се банки, компании, менувачници, пошти, златари и други.

Што го карактеризира овој облик на меѓународен организиран криминал е неговиот политички карактер. Тероризмот често е поврзан со некоја држава или ужива заштита од политички партии кои се стремат да се дојдат на власт или да ја задржат на власт, а кои имаат интереси засновани на иредентистички и сепаратистички цели.

Со оглед на зголемената употреба на дигитални уреди и експоненцијалниот раст на технологијата, евидентно е дека многу од идните криминални дејства ќе вклучуваат сајбер компонента.

Трансформацијата која ја носат современите информатичко-комуникациски технологии (ИКТ) поставува значајни предизвици во областа на етиката, јавните политики и безбедноста. Традиционалните кривични дела се јасно дефинирани во кривичните закони на национално ниво, додека сајбер-криминалот често не се вклопува лесно во таа регулатива, што го прави неговото правно третирање и борба против него предизвик. Како што наведуваат авторите Согела и Вотспоп (1999), XXI век означува почеток на нова ера во решавањето на овие проблеми, бидејќи правните системи мора да се прилагодат на брзите технолошки промени.

Покрај тоа, постојат повеќе причини кои го отежнуваат откривањето на сајбер-криминалот:

1. **Црна бројка** – голем дел од сајбер-престапите не се пријавуваат или не се евидентираат кај надлежните органи, што значи дека вистинскиот обем на овие кривични дела останува непознат.
2. **Недоволна информираност** – многу луѓе и организации не се доволно запознаени со овој облик на криминал.
3. **Нов поим** – сајбер-криминалот е релативно нов концепт во правниот и општествениот контекст.
4. **Развојот на ИКТ не е еднаков во сите држави** – развиените земји имаат подобар пристап до новите технологии, што им овозможува подобро да го контролираат сајбер-криминалот.
5. **Транснационалност** – сајбер-криминалот не е врзан за одредена територија, што го прави потешко контролиран и процесуиран.
6. **Просторна прикриеност** – сајбер-криминалот се одвива во дигиталниот простор и ги надминува географските граници, што ја отежнува неговата следливост и идентификација на сторителите.
7. **Временска прикриеност** – брзото извршување на сајбер-престапите и можноста да не постои временска дистанца меѓу извршувањето и последиците го прави тешко за откривање.
8. **Мотиви за прикривање** – компаниите кои се занимаваат со електронско банкарство и интернет трговија често имаат мотив да ги прикријат сајбер-престапите за да ја заштитат својата репутација.

Современите ИКТ, од друга страна, значајно го олеснија функционирањето и одржувањето на сложени криминални системи како што се организираниот криминал и тероризмот. Тие претставуваат не само средство за извршување, туку и за откривање на кривичните дела. Како што се наведува, сè поголемиот број на сајбер-криминални дела и нивната поврзаност со организираниот криминал и тероризмот може да се очекува и во иднина, бидејќи технологиите истовремено претставуваат средство за ефикасна извршна и оперативна акција, но и за нивно прикривање.

Овој развој ја нагласува потребата за промена и адаптација на законодавството и безбедносните структури кои ќе можат да се справат со новите облици на криминал кои се појавуваат во дигиталното доба.

Конкретни аспекти кои се однесуваат на врската меѓу сајбер-криминалот и организираниот криминал вклучуваат различни предизвици поврзани со:

- заштита на безбедноста,
- откривање и процесуирање на овие дела,
- како и меѓународната соработка.

3. Технолошка еволуција како катализатор на криминалот

Со развојот на ИКТ, организираниот криминал и тероризмот ги усвоија новите технологии како средство за извршување на кривични дела. Ова опфаќа:

- **Користење на криптовалути и анонимни платформи:** Платформи како Tor и криптовалутите им овозможуваат на криминалците анонимно да спроведуваат незаконити трансакции и да избегнат откривање.
- **Социјален инженеринг и фишинг напади:** Криминалните организации ги користат овие техники за да манипулираат поединци и компании со цел кражба на информации и пристап до чувствителни податоци.
- **Хакирање и уцени:** Сајбер-нападите во форма на уцена (ransomware) сè почесто се користат како начин на монетарна експлоатација, при што напаѓачите ги „киднапираат“ податоците на компании или државни органи и бараат откуп.

4. Меѓународна соработка и правни предизвици

Сајбер-криминалот често ги надминува националните граници, што создава сериозни проблеми за правосудните системи. Тука е важно да се разгледаат:

- **Неусогласеност на законите:** Законодавствата на различни држави во однос на сајбер-криминал не се усогласени, што ја отежнува меѓународната соработка. Ова значи дека извршителите на сајбер-престапи можат да дејствуваат без страв од процесуирање.

- **Барања за екстрадиција:** Сајбер-престапниците кои дејствуваат во држави со слаби правни системи можат да ги искористат овие слабости за да ја избегнат правдата, што бара меѓународна соработка и правни договори за екстрадиција.

4.1 Нови облици на соработка меѓу тероризмот и организираниот криминал

Терористичките организации сè почесто користат средства и структури карактеристични за организираниот криминал. Ова вклучува:

- **Финансирање на тероризмот:** Сајбер-криминалците можат да им помогнат на терористите да ги финансираат своите активности преку перење пари, сајбер-напади на банки или кражба на податоци за издавање лажни кредити.
- **Шверц и трговија со оружје:** Терористичките групи користат мрежи на организиран криминал за набавка и дистрибуција на оружје и други нелегални супстанци. ИКТ игра клучна улога во комуникацијата и логистиката на овие активности.

4.2 Безбедност во виртуелниот простор

Виртуелниот простор стана зона во која криминалците можат да се кријат и манипулираат без физичко присуство. Конкретните аспекти вклучуваат:

- **Напади врз критичната инфраструктура:** Сајбер-напади на електрични мрежи, водоснабдување, болници и други делови од критичната инфраструктура стануваат сè почести. Овие напади можат да имаат сериозни последици врз јавната и националната безбедност.
- **Шпионажа и кражба на податоци:** Сајбер-криминалци кои се дел од организирани криминални групи можат да користат напредни техники како што се хакирање на софтвер и кражба на интелектуална сопственост, што има долгорочни економски последици.

4.3 Прилагодување на правниот систем на новите предизвици

Правните системи мора да се прилагодат на овие нови реалности:

- **Едукација и обука на правосудните органи:** Органите за спроведување на законот треба да бидат обучени за користење на технологии за следење и откривање на сајбер-престапи. Ова вклучува совладување на техники на дигитална форензика, анализа на податоци и меѓународни правни процедури.
- **Реформа на правните и безбедносните институции:** Потребно е создавање и реформа на закони кои ќе се фокусираат на сајбер-просторот, со цел овозможување соодветно процесуирање и превенција на сајбер-престапи.

4.4 Транснационалност на сајбер-криминалот

Сајбер-криминалот не е врзан за територија како традиционалните облици на криминал, што претставува сериозен предизвик за правото и безбедноста. Напаѓачите можат да бидат на една страна од светот, а жртвите на друга, што бара координирана меѓународна акција и соработка. Тука е важно:

- **Размена на информации меѓу државите и меѓународните организации**, како што се Интерпол и Европол.
- **Потреба од глобална координација и меѓународни договори за борба против сајбер-криминалот**, кои ќе овозможат полесно следење и сузбивање на овие криминални активности.

Овие аспекти укажуваат на сè поголема потреба од меѓународна соработка и иновации во правниот и технолошкиот систем, кои ќе овозможат подобро следење, спречување и санкционирање на сајбер-криминалот, кој често вклучува елементи на организиран криминал и тероризам.

5. Злоупотреба на современите информациски и комуникациски технологии

Научно-технолошката револуција произведе современи револуционерни технолошки изуми кои значително го промениле човештвото во скоро сите области на човечкото постоење. Интернетот претставува најефикасна современа метода на комуникација, бидејќи овозможува брзо и едноставно манипулирање со податоци од различен тип (аудио и видео) и нуди широк спектар на идеи и информации. Вајмен како „основни предности на интернетот ги наведува: едноставен пристап, малку или воопшто нема регулација, цензура или други форми на контрола од страна на властите,

потенцијално огромна публика која е распрсната низ светот, анонимност на комуникацијата, брз проток на информации, евтин развој и одржување на присуство на мрежата, мултимедијално опкружување (можност да се комбинира текст, слика, аудио и видео и да им се дозволи на корисниците да „симнуваат" филмови, песни, книги, постери и така натаму), можност да се обликува известување во традиционалните масовни медиуми, кои сè повеќе користат интернет како извор на своите информации" (Вајтапу: Дамњановиќ, 2009, 238-239). Користењето на интернетот и современите ИКТ стана неизбежен дел од секојдневието. Поради бројните предности што интернетот и ИКТ ги нудат, расте и нивната примена, додека истовремено расте и потенцијалот за нивни различни злоупотреби. Брзиот проток на информации на интернетот овозможува брзо ширење на компјутерски вируси, црви, тројанци и други злонамерни софтвери, што, во комбинација со генералното незнаење на корисниците на интернетот за постоечките мерки за заштита, го прави интернетот извор на многу проблеми и предизвици. Корисниците на интернетот генерално немаат доволно знаење за безбедно користење на бројните услуги што интернетот ги нуди. Понатаму, „корисниците на интернетот обично не се доволно запознаени со функционирањето на компјутерите, и многу често не се подготвени и спремни да преземат мерки за заштита за кои сметаат дека се премногу скапи, премногу технички барани или дека е потребно да се потроши премногу време за нивно користење" (Авгатс, Росел и Јајосна, 1995, 117). Примената на теоријата на социјална контрола и едукацијата за правилното / забрането однесување, како и заканите во сајбер просторот може значително да помогне во спречувањето или барем намалувањето на малициозните активности на интернет. Теоријата на социјална контрола има потенцијал да обезбеди и / или прошири знаење и свест за сајбер криминалот и другите злоупотреби на интернетот . Бидејќи, ако злоупотребите на интернетот избегаат од кривично- прекршочната процесуирање, тоа може да има последица во зголемувањето на насилното однесување во сајбер просторот.

Интернет сам по себи не е причинител на криминал, но е едноставно моќно средство за комуникација кое има потенцијал да го зголеми и забрза криминалот (Натс, 2008). Научно-технолошката револуција овозможила голем број луѓе да добијат пристап до информации, што влијаело на криминогената средина така што ја трансформирало и создало нова форма на криминал во сајбер просторот . Повеќето измами на интернет всушност се само усовршени верзии на претходните, класични измами и криминални дела во кои интернетот внел новини. „Нивната девијантност, поддржана од моќната

технологија, може да има многу сериозни и обемни последици за општеството. Така, без разлика дали ќе им се допадне на некого или не, тие стануваат респектабилни членови на клубот на криминалци со бела крагна. Расте нова елита наречена сајбер елита. Она што не смее да се занемари е висока веројатност за обединување и заедничко делување на оваа новонастаната елита со девијантниот дел од класичната моќна елита" (Петровиќ & Стојановиќ, 2016, 13).

Најчести облици на злоупотреба на интернетот се:

1. хакирање,
2. незаконско собирање податоци,
3. кривично дело пресретнување податоци,
4. ометување податоци,
5. интернет рекетирање,
6. фалсификување,
7. перење пари,
8. интернет инвестиционни измами и
9. прекршоци на интернетот поврзани со содржината.

Хакирањето е активност на интернетот која може да се тумачи двојно. Тоа истовремено може да биде кривично дело што се извршува преку интернет и подразбира нелегален упад во компјутерски системи, но може да биде и позитивно дејство, особено во областа на заштита од познатите рањивости и најчести напади, со цел подобрување на безбедноста на компјутерските системи и податоци. Значи, има различни цели и мотивации, а за неговото извршување се потребни подготвителни активности, пристап до заштитени (тајни) податоци, лозинки или користење на специјално предвидени хардвери или софтвери.

Друг често настануван облик на злоупотреба на интернетот е незаконското собирање податоци. Овде спаѓаат нападите на бази на податоци од веб апликации, при што се прибираат доверливи информации, како што се социјалните сигнали и други лични податоци и лични податоци од веб-страници . Следниот вид злоупотреба е кривичното дело пресретнување податоци, кое се однесува на ометање на трансферот на податоци, информации и нивно снимање, без разлика дали комуникацијата се врши

преку интернет, бежични или мобилни мрежи (е -tach, Skype и слично), или фиксни линии.

Мета напада е комуникациската инфраструктура. Исто така, во малициозни активности на интернетот спаѓа и ометување податоци, што означува вид напад, најчесто насочен кон ометување и бришење на податоци што се чуваат во компјутерските системи. Најчесто се изведува со помош на вируси, црви и други злонамерни софтвери. Потоа следи интернет рекетирањето, односно ометување на работата на системите. Напаѓачите заканууваат со напад (DDos attac) и уценуваат компании што своето работење го остваруваат електронски, како што се: електронско банкарство и е-продавници, пружатели на е-услуги и интернет коцкање и др. Најчесто со вируси и програмирани мрежи од компјутери, организирани DDos напади го ометуваат работењето на овие компании, напаѓаат веб-сајтови и ги онемогуќуваат нивните услуги, напаѓаат сервери или компјутерски системи.

Интернетот и компјутерските алатки како сечи (cut), лепи (paste) или копирај (copy), овозможуваат да се изврши сечење или копирање на делови од текстови или документи и да се залепат на лажни документи. Некогашното кривично дело фалсификување е модернизирано со употребата на интернет и други технологии. Што е поголема сериозноста на фалсификатот, толку повеќе е потребна вештина и познавање на различни компјутерски програми. Современите информациски технологии и глобалните финансиски пазари овозможиле потешко следење на тековите на парите и полесно злоупотребување. Преку интернет исто така се спроведува и перење пари, односно „нелегално прикривање на незаконски профит од страна на поединци, мали претпријатија, корпорации, криминални синдикати, корумпирани официјални лица, па дури и корумпирани влади" (Britz 2013, 106). Правната регулатива во врска со банкарските операции не е усогласена насекаде во светот. Така, во некои земји банките со закон ги заштитиле своите операции со т.н. банкарска тајна, додека во други земји банките се обврзани да поднесуваат редовни извештаи за своето работење. Оваа ситуација отвора простор за поединци да перат пари така што ги депонираат анонимно во земја со поволна правна регулатива, а потоа го префрлаат парите и без проблеми ги користат во друга земја.

Ниту инвеститорите не останале имуни на предностите кои интернетот ги нуди. Лесниот и брз пристап до различни инвестициони извори, како и неверојатно лесната

трговија со хартии од вредност, направиле интернет да биде прифатен како важен алат за инвеститорите. Сепак, инвестирањето носи одреден степен на ризик, кој со примена на интернет во оваа област се зголемил. Тоа го потврдува големиот број и разновидност на инвестиционите измами (е-инвестициони билтени, инвестициони веб-сајтови со лажни фондови, и слично).

Еден вид злоупотреба на интернетот се прекршувањата поврзани со содржината, кои се однесуваат на промовирање содржини кои се забранети со закон во поголемиот дел од земјите. То се однесува на: детска порнографија, содржини што поттикнуваат ксенофобија и навредување на етничка, расна, верска или половна основа и слично.

Злоупотребите на интернетот може да се појават во различни форми. Може да ги систематизираме во две главни категории: „упад во системи и DDoS напади" . „Упад" подразбира напад на компјутерски системи кои се базираат на пропусти, односно „рупи" во системот што напаѓачите ги користат како можност за упад во одреден систем за да имаат пристап до неговите ресурси и да испорачаат желена алатка (вирус или малвер). Малвер е „код или софтвер што е специјално дизајниран да оштети, наруши, украде или нанесе штета или нелегитимно влијае на податоци, хостови или мрежи. Напаѓачите применуваат DDoS напади за да го оневозможат пружањето на услугите одреден систем.

Терористите исто така го користат интернетот за различни цели. Вајмен наведува дека „активностите на терористите на интернетот можат да се класификуваат во осум групи: 1. психолошки војна, 2. јавност и пропаганда, 3. барање информации, 4. собирање средства, 5. регрутирање и мобилизација, 6. умрежување, 7. споделување информации, 8. планирање и координација" (Дамјановиќ, 2009, 239). На интернетот може да се најдат различни содржини поврзани со терористи: терористички веб-сајтови, снимки од терористички напади, па дури и е-обуки за терористи и слично.

5.1 Сајбер криминал

Експанзијата на автоматизираните информациско-технолошки системи создава постојани предизвици и безбедносни ризици. Традиционалните кривични дела како што се различни видови измами, фалсификати, проневери на пари и кражби во сајбер просторот добиваат нов облик и начин на извршување. Употребата на компјутерски технологии за извршување на кривични дела бара создавање нова регулатива и мерки за

санкционирање на таквото противправно однесување. Затоа, на поимот општ криминалитет неопходно е да му се додаде и „компјутерски криминал како обележје на прогресивен криминалитет“ (Ђокић и Живановиќ, 2005, стр. 305–318).

Во литературата се среќаваат различни поими: „сајбер криминал“ (Clay, 2007, стр. 4), „компјутерски криминалитет“ (Derksen, 2012, стр. 11), „високотехнолошки криминал“ (Закон за организација и надлежност на државните органи за борба против високотехнолошки криминал, „Службен гласник на РС“ бр. 61/05, 104/09), како и термини како „computer abuse – злоупотреба на компјутери“, „cyber delicts – деликти со помош на компјутери“, „computer fraud – компјутерска измама“, информатички криминалитет, сајбер криминалитет, технокриминалитет (Јовашевиќ, 2011, стр. 639), за да се означи посебен вид криминални дејства за чие извршување се користат ИКТ и интернетот.

Сајбер криминалот ја загрозува безбедноста на сајбер просторот во целина или на негови поединечни делови. Извршителите на сајбер криминал користат различни средства во рамките на компјутерските системи за да стекнат противправна корист за себе или да предизвикаат штета на физичко или правно лице. Сајбер криминалот опфаќа: „кражба на интелектуална сопственост, повреда на права од заштита на патенти, трговски тајни, повреда на авторски права, напади на компјутери со намера да се влијае на обработката на податоци“ (Clay, 2007, CJS – 4). Можностите за злоупотреба на информациските технологии се големи: „Компјутер или уред може да биде средство за извршување на злосторство, помошно средство или цел на злосторството; злосторството може да се случи на самиот компјутер или на некоја невиртуелна локација“ (Solomon & Poole, 2006, стр. 14). Терминот сајбер криминал се користи за да се означи широк спектар на криминални постапки, односно не опфаќа само напади што можат да се извршат со употреба на телекомуникациски мрежи, туку и напади на самите информациски системи, компјутери, како што се: шпионажа, откривање и пресретнување на тајни податоци и нивно неовластено копирање, попречување на обработката на податоци, кражба на интелектуална сопственост, авторски права или патенти, дистрибуција **различна содржина** (вируси, детска порнографија и сл.), измами преку интернет и електронска пошта, мешање во онлајн финансиски услуги и многу други. Токму поради тоа произлегоа и голем број дефиниции за сајбер криминалот.

Многу автори се обиделе да дадат одговор на прашањето што претставува сајбер криминал. На Конгресот на Обединетите нации беше предложена следнава дефиниција на сајбер криминалот: „Криминал што се однесува на кој било облик на криминално дејство што може да се изврши преку компјутерски системи и мрежи, во компјутерски системи и мрежи или против компјутерски системи и мрежи“ (Derksen, 2012, стр. 11–12).

Оваа дефиниција нуди сеопфатна определба на сајбер криминалот, односно го дефинира како компјутерски криминал со кој се загрозува безбедноста на компјутерските системи и податоци, а воедно ги опфаќа и сите криминални дејствија што се извршени со употреба на компјутери (компјутерски системи), вклучувајќи и нелегална дистрибуција на информации и друга содржина.

Според Извештајот на Советот на Европа за организиран криминал, следните категории дела се евидентирани како сајбер криминал:

1. **Кривични дела против доверливоста**, интегритетот и достапноста на податоци и компјутерски системи;
2. **Традиционални кривични дела извршени со помош на компјутер**;
3. **Кривични дела поврзани со содржина**, како што се детска порнографија, расизам и ксенофобија;
4. **Кривични дела поврзани со повреда на авторски и сродни права** (Council of Europe, 2005, стр. 40).

Кривичните дела против доверливоста подразбираат незаконски пристап до компјутерски системи, хакерски напади, прислушкување, интернет измами (на пример: шпионажа, кражба на лозинки, „фишинг“), компјутерска шпионажа (вклучувајќи употреба на тројански коњи и други техники), компјутерска саботажа и уцени (на пример: вируси и „црви“, напади од типот „одбивање на услуга“ – DoS, спам или „бомбардирање“ со електронска пошта).

Традиционалните кривични дела извршени со помош на компјутер опфаќаат широк спектар на класични измами, како што се: манипулации со сметки или биланси на компании, општи манипулации, измами на аукции и нарачки, незаконска употреба на

банкомати, злоупотреба на кредитни картички, фалсификати и други форми на измами и манипулации.

Кривичните дела поврзани со содржина, како што се на пример: детска порнографија, расизам и ксенофобија, подразбираат барање, поттикнување и давање упатства за однесување што е казниво и што поттикнува различни злосторства — од убиство, силување, мачење, саботажа до тероризам. Оваа категорија вклучува и сајбер вознемирување, клевета и ширење лажни информации преку интернет и интернет коцкање. Кривични дела поврзани со прекршување на авторските и сродните права подразбираат неовластено репродуцирање и користење на компјутерски програми, аудио/видео и други форми на дигитални дела, или податоци од бази и книги.

Сајбер-криминалот од аспект на правните науки подразбира деликти кои се инкриминирани со законите. Тоа е специфична форма на криминалитет што е многу поврзана со компјутерските мрежи. Она што одреден криминален акт го дефинира како сајбер-криминал е фактот што е „извршен со користење на сајбер-технологија во сајбер-домен“ (Таваш, 2003, 103). Фишер предлага употреба на поширокиот поим „сајбер закани“ (Pfleeger, 2005), за да се опфатат и инкриминираните дејства, како и оние кои сè уште не се прогласени за кривични дела според важечките кривични закони. Тој ги дефинира сајбер заканите како „злонамерна употреба на технологии што припаѓаат на сајбер-просторот, кои се јавуваат како инструмент на закана, но и како цели од страна на голем број актери – криминалци, терористи, организации и држави“ (Pfleeger, 2005, 6).

Овој вид криминалитет се одликува со тесна поврзаност со технологијата, од која произлегува и неговата динамичност и разновидност на појавни форми. Иако сајбер-криминалот се јавува во различни облици, сепак можеме да издвоиме седум основни карактеристики:

1. Првата карактеристика на сајбер-криминалот е тоа што ја нарушува заштитата и безбедноста на компјутерските податоци на одреден информациски систем во целина или на еден негов сегмент.
2. Втората карактеристика произлегува од специфичниот карактер и природата на противправните дејства.

3. Третата карактеристика е дека овој вид криминални дејства бара посебни знаења од сторителот, специјализирани за извршување на кривични дела.
4. Четвртата карактеристика е злоупотребата на компјутерот како средство за противправно остварување на целта.
5. Петтата карактеристика е намерата на сторителот да обезбеди корист за себе или за друго лице, или да предизвика штета на друго физичко или правно лице.
6. Шестата карактеристика е тоа што физички контакт помеѓу сторителот и жртвата не е потребен.
7. Седмата карактеристика се однесува на сторителите на сајбер-криминалот. Тоа најчесто се лица кои имаат физички пристап до информацискатa технологија, поседуваат стручни знаења и практични вештини од областа на компјутерските технологии, главно се ненасилни и не се деликвентни, и затоа избираат сајбер-форма на криминални активности.

Сè се одвива во виртуелниот простор – сајбер-просторот (cyberspace). Тоа е „вештачка творба која бара висока техничка опременост, добра информациска инфраструктура што е ничија и сечија сопственост, во која паралелно коегзистираат виртуелното и реалното, и каде што комуникацијата е колективна“ (Malczewski – Ostajewski, 2014, стр. 279–298).

Значи, специфичноста на компјутерските кривични дела произлегува и од самата фактичност дека се извршуваат во рамките на виртуелниот (сајбер) простор, на прикриен начин, под таен (виртуелен) идентитет, често со временска разлика меѓу моментот на извршување на кривичното дело и времето кога се појавуваат последиците од таквото противправно дејствување.

Сајбер-криминалот се манифестира во различни форми, а зависи од следните елементи:

1. **Основната мета (цел) на сајбер-нападите** – зависно од тоа дали е насочен кон физичко или правно лице, дали целта е да се нанесе штета на мрежата во целина или на одреден нејзин сегмент, дали е примарна намера да се нарушат специфични функции, да се изврши упад и сл.;

2. **Алатките** кои сајбер-криминалците ги користат за постигнување на своите цели;
3. **Околината** во која се реализираат сајбер-нападите;
4. **Доказите**, односно употребените технолошки средства и интернетот за нивно извршување – што помага во класификацијата на делото како сајбер-криминал и олеснува негово откривање и докажување;
5. **Тежината на последиците** и **висината на причинетата штета**.

Фактот дека сајбер-криминалот е растечки проблем кој бара сè поголемо внимание во иднина, го потврдува и современата ситуација. Пандемијата на вирусот COVID-19 негативно влијаеше врз сајбер-безбедноста. Во вториот извештај на Европската комисија за 2021 година се наведува следново во однос на влијанието на пандемијата врз сајбер-криминалот:

„Криминалците брзо ги искористија промените донесени од работа од далечина и зголемената употреба на онлајн услуги... Бројот на сајбер измами и измами поврзани со пандемијата, користење на малициозен софтвер (malware), ransomware и phishing напади, се зголеми за време на пандемијата, таргетирајќи поединци, компании и особено здравствениот сектор.“ (European Commission, 2021, стр. 8)

Во услови на пандемија, се зголеми бројот на лажни веб-продавници кои рекламираат и продаваат непостоечка стока, здравствена заштитна опрема, тест-комплети, лажни понуди за вакцини против COVID-19 и слично.

5.2 Сајбер криминал и сајбер тероризам

Сајбер криминал и сајбер тероризам се разликуваат според примарната цел (мотивација) на извршените активности во сајбер-простор. Како што забележува Фишер, „сајбер криминал обично се однесува на злосторства што се извршени со употреба на информациски технологии, особено интернетот, за остварување лична корист, додека сајбер тероризмот се однесува на злосторства што вклучуваат употреба на информациски технологии за политички цели“ (Pfleeger, 2005, стр. 5-10).

Една од најзабележливите разлики меѓу сајбер криминалот и сајбер тероризмот е тоа што починителите на сајбер криминал обично се обидуваат да останат анонимни и

неоткриени, додека сајбер терористите, како и терористите, најчесто сакаат да добијат публицитет и да предизвикаат страв на што поголеми размери. „Начините на кои терористите се обидуваат да постигнат желениот ниво на публицитет вклучуваат: 1) планирање на акции кои треба да имаат големо значење во вестите; 2) спроведување активности што треба да ја засилат нивната пропаганда и регрутирање; 3) избор на најпогодно време и локација за привлекување публицитет при спроведување на акциите; 4) издавање прогласи; 5) одржување контакти со медиумите и давање изјави; 6) признавање одговорност за одредени акции; 7) испраќање пораки преку значењето и симболиката на целите или актите“ (Raleigh & Scktm, 1992, стр. 32).

Во рамките на сајбер просторот се случуваат бројни сајбер активности кои, иако се извршуваат со слични операции, се разликуваат по својата суштина (Слика 4). Клучната разлика помеѓу сајбер вандализмот, сајбер криминалот и сајбер тероризмот е мотивот. „Сајбер заканите, сајбер инцидентите и сајбер вандализмот, како оштетување на сајтови, не се тероризам. Сама загриженоста за сајбер тероризмот потекнува од комбинација на страв, незнаење или од фактот што на глобално ниво не се дефинирани, таксативно набројани актите што можат да се окарактеризираат како такви“ (Јонев & Бериша, 2016, стр. 2). Може да се каже дека сајбер вандализмот често нема некој посебен мотив, освен што починителите уживаат во неовластеното пробивање на информациски системи кои се добро заштитени.

Додека класичните сајбер криминалци се водат од лични мотиви, односно желбата да остварат корист (имовинска или неимовинска) за себе или некој друг, или да нанесат штета на друго лице или институција поради лични причини, сајбер терористите се водат од политичко-идеолошки мотиви.

Јазив наведува „три видови мотивации кои го одредуваат дејствувањето на одредени терористички групи: 1) **Рационална мотивација** одредува однесувањето на терористите во смисла на тоа дека првенствено размислуваат за своите цели и можностите, анализирајќи ги преку призма на „цената“ што треба да ја платат и можниот добиток. 2) **Психолошка мотивација** за спроведување на терористички акции произлегува од личната незадоволност на терористот со својот живот и постигнувања. 3) **Културна мотивација** во рамките на терористичките групи силно влијае на единството и обликувањето на целите и вредностите во овие групи. Културата ги

обликува вредностите и ги мотивира луѓето од определени заедници на начин кој изгледа неразумно за набљудувачите од страна“ (Јазив, 2010, стр. 122–123).

Иако најголемиот број на извршени терористички акти бил во знакот на верски фанатизам, „основната цел на повеќето терористички групи е независност и држава“ (Јазив, 2010, стр. 115). Не е непознато дека одредени терористички движења уживаат поддршка од некои држави поради филозофските ставови кои ги застапуваат и кои одговараат на интересите на тие држави. Често државите финансираат терористички операции „за остварување на свои надворешнополитички цели или, на внатрешен план, за зајакнување на сопствената политика“ (Григ & Вепс, 2004, стр. 14–16). Тогаш зборуваме за државен тероризам, односно сајбер-војна (Шутев, 2006), кога терористите ги применуваат современите информациски технологии за да постигнат повисоки цели кои влијаат на надворешнополитичкото или внатрешнодржавното состојба.

„Сајбер терористите обично имаат намера да деморализираат цивилното население, што ги разликува од сајбер војната, која не е директно насочена против цивилите“ (Вепегер, 2007, стр. 388).

Сајбер војна е дејствување на државни учесници кое подразбира примена на информациски и комуникациски технологии, било како средства или цели на напад, а кое е насочено против сајбер инфраструктурата на непријателот.

Во последните децении, технологијата се развиваше со неверојатна брзина, што не само што ја трансформираше нашата секојдневна комуникација и работни процеси, туку и ја променија природата на војните. Сајбер војната, како нова форма на глобален конфликт, ја постави прашањето дали војните на иднината ќе се водат во виртуелниот простор. Овој нов вид на војна не се води на теренот, туку во дигиталните и комуникациските мрежи. Нападите се изведуваат преку хакерски напади, вируси, малвери и други дигитални средства кои ја користат инфраструктурата на противникот. Сајбер војната претставува нова, непозната форма на агресија која има потенцијал да создаде деструктивни последици на глобално ниво.

Сајбер војната се однесува на користење на информациски и комуникациски технологии како средства на напад и одбрана во конфликтни ситуации. За разлика од традиционалната војна, која се води со оружје и во физички простор, сајбер војната се

води во виртуелниот простор. Нападите се насочени на дигиталната инфраструктура на противникот, вклучувајќи го електричниот систем, комуникациските мрежи, финансиските институции и други критични делови од инфраструктурата. Со помош на вируси, малвер и други софистицирани напади, напаѓачите можат да ја парализираат земјата-цел и да го оштетат економскиот и политичкиот систем.

Една од најголемите разлики помеѓу традиционалната војна и сајбер војната е анонимноста. Нападите во виртуелниот простор можат да се изведат без физички контакт, што го прави многу потешко да се идентификува напаѓачот. Најчесто, напаѓачите се државни или нелегални актери кои остануваат анонимни. Ова создава сериозни предизвици за правдата и меѓународниот правен систем, бидејќи не постојат јасни и брзи методи за идентификација на напаѓачите.

Една од главните цели на сајбер војната е нападот на критичната инфраструктура на противникот. Сајбер напади може да бидат насочени кон електрични мрежи, водоснабдување, болници, банки и други клучни делови од инфраструктурата кои обезбедуваат функционирање на една држава. Нападите врз овие системи можат да создадат хаос и да имаат долгорочни последици за економијата и благосостојбата на населението.

Пример за таков напад е „Stuxnet“, вирус кој беше дизајниран да уништи иранските нуклеарни објекти во Натанц. Овој напад беше првиот познат пример на сајбер војна, бидејќи беше насочен кон физички објект со помош на дигитални средства. Овој тип на напад покажува како сајбер војната може да биде ефикасна за нарушување на безбедноста на еден државен апарат без потреба од физички напад.

Дигиталната технологија овозможува нови форми на манипулација и дезинформации. Сајбер војната не се однесува само на директни напади на инфраструктурата, туку и на контрола на информациите. Манипулирањето со информациите преку интернет и социјални мрежи може да има деструктивни последици на политички и социјални планови. Лажни вести, пропагандни кампањи и дезинформации можат да доведат до паника и да влијаат на јавното мислење, што ја прави сајбер војната комплексна и многу опасна.

Пример за тоа е употребата на социјалните мрежи за ширење на лажни информации и дезинформации кои влијаат на избори и политички процеси. Во 2016 година, на пример, беше откриено дека Русија користела сајбер напади за да влијае на изборите во САД, ширејќи лажни информации преку социјалните мрежи.

Сајбер војната не е ограничена само на директни конфликти помеѓу две земји. Таа може да вклучува и непрекидна геополитичка манипулација, каде што една земја користи сајбер напади за да ги дестабилизира политичките структури на друга земја. Ова ја прави сајбер војната слична на традиционалните војни, но со нови средства и стратегии.

Пример за ова е сајбер нападот на Украина во 2015 и 2016 година, кога Русија изврши напади врз украинската енергетска мрежа и други инфраструктурни објекти. Овие напади имаа за цел да ја дестабилизираат Украина и да ја ослабат нејзината економска и политичка моќ.

Сајбер војната претставува ново поле на глобален конфликт кое значително го менува традиционалниот концепт на војна. Со развојот на технологијата, сајбер војната ќе продолжи да расте во важност и ќе стане клучен елемент на глобалната безбедност. Државите мораат да се подготват за ова ново време на конфликти, што подразбира развој на нови стратегии за одбрана и контранапад во виртуелниот простор. Сајбер војната не само што претставува директна закана за националната безбедност, туку и за глобалниот мир и стабилност.

6.Фази на одбрана од сајбер тероризам

Безбедност и одбрана на компјутерските системи се прашања од приоритетно значење, имајќи предвид дека современото општество во голема мера се потпира на работата и поддршката на информациските и комуникациските инфраструктури. Прашањето за сајбер безбедност најчесто подразбира заштита на ресурси (материјални и/или нематеријални) од потенцијални опасности (Kizza, 2009, 45-46; Solange, 2009, 3). Меѓутоа, ова прашање се однесува и на зачувување на животот на луѓето и одржување на меѓународниот мир, бидејќи негативните последици од нападите изведени во сајбер просторот лесно можат да се пренесат во реалниот живот и да имаат директно влијание како на животите на луѓето, така и на состојбата во одредени држави и меѓународните

односи. Размерите на потенцијалната штета се разликуваат од: краткотрајно прекинување на секојдневните активности, причинување значителни економски штети, колапс (во сообраќајот, трговијата, на берзата) па до катастрофи со голем број на жртви. Причинената штета зависи од неколку фактори: напаѓачот, односно неговите цели и мотивација, способностите и ресурсите (знаење, алатки) што ги има на располагање, постојниот систем на одбрана и метата на нападот. Имајќи предвид дека не можеме да влијаеме на карактеристиките на напаѓачот, она што е клучно е силната и ефикасна одбрана. Сепак, Гудмен даде кратка проценка на нашите вкупни способности да се бориме со терористи кои користат сајбер простор и заклучи: „дека сме технолошки и процедурно слаби во сите три фази на сајбер одбрана против квалификувани, трпеливи и постојани напаѓачи, кои веројатно нема да биде лесно да се запрат“. Затоа, современите директиви за постигнување на сајбер безбедност имаат широк опсег и ги покриваат „десяти основни сектори: транспорт, енергетика, банкарство, инфраструктура на финансискиот пазар, здравство, вода за пиење, отпадни води, дигитални инфраструктури, инфраструктури на јавната управа и простор“ (European Commision 2021, 3).

Имајќи во предвид дека технологијата се развива и применува со голема брзина, службите за сајбер заштита и одбрана се соочуваат со тежок задач да ги следат и одржат истиот темпо на развој. Кога станува збор за одбраната од сајбер тероризмот, Гудмен предлага „три фази на одбрана: 1) превенција; 2) управување со инцидентот, ублажување на нападот, ограничување на штетата; 3) управување со последиците“ (Goodman 2007, 46.

Корисниците се меѓусобно поврзуваат во рамките на компјутерските системи поради најразлични потреби и мотиви. Одбраната од сајбер тероризам не е едноставна. Следењето на активностите во сајбер просторот се отежнува со големиот број на корисници. Прашањето за заштита на компјутерските мрежи исто така е проблематично, бидејќи заштитните мерки и средства тешко можат да ја следат динамиката на развојот на иновациите на напаѓачите. Напаѓачите се главно фокусирани на откривање на ранливости, односно на пронаоѓање на „рупи во системот“ и инсајдери, односно соучесници кои можат да им помогнат во криминалните активности и да им овозможат пристап до системот. Проблемите со сајбер одбраната се усложнуваат со внатрешната мобилност на организациите и соработката со надворешни партнери, што значително го

отежнува следењето на активностите и потенцијалните злоупотреби во овој сегмент. Отежнувачка околност е и тоа што терористите во сајбер просторот делуваат преку лажни онлајн профили, криејќи го својот вистински идентитет. Благодарение на тоа, тие имаат можност да се инфилтрираат меѓу другите сè до моментот на извршување на нападот. Извршените дела на сајбер криминал остануваат во голема мера непријавени поради незнаење, недостаток на средства за решавање на потенцијалните сајбер закани и проблеми, како и поради тешкотиите во прибавувањето на валидни докази. Потребно е да се работи на развој на нови мерки за одбрана од сајбер тероризам.

6.1 Превенција

Превенцијата е првиот, особено важен, чекор (фаза) на одбраната од сајбер тероризмот. Различни држави, институции и организации не се дигитализирани во ист степен. Со тоа, не е подеднаква ниту веројатноста за заканите од сајбер терористички напади, ниту разорноста на последиците од можен акт на сајбер тероризам во различни земји. Големите компании се значително дигитализирани, бидејќи за своето секојдневно работење користат големи компјутерски мрежи и како такви се често мети на напади. Колку е системот покомплексен, толку е потенцијално подложен на ранливости. Многу информациско-технолошки системи се дизајнирани да обезбедат што поефикасно сервисирање на корисниците, но нивната сајбер заштита не е доволно истакната.

Сајбер тероризмот, за разлика од другите форми на сајбер криминал, има за цел да предизвика штета што е можно поголема. Сајбер одбраната е проблематична. Практично е невозможно да се следи динамиката на развојот на современите технолошки иновации и да се одржи чекор со нив за да се обезбедат адекватни заштитни мерки. Затоа, авторите посебно се фокусираат на превенцијата и откривањето на најдобри методи за предвидување на сајбер напади и предлагаат клучни податоци кои може да послужат во таа насока: „1) мотивација, што овозможува предвидување на најверојатната цел на сајбер нападот; 2) можност за извршување, што овозможува одредување на најверојатната врста на сајбер напад; 3) време, што овозможува предвидување на точниот момент кога може да се случи сајбер напад“ (Munkhdorj, & Yuji, 2017, 110). Дејвис исто така смета дека „превенцијата и свеста се клучни елементи во намалувањето на преваленцијата на девијантни акти, особено во борбата против компјутерскиот криминал“ (Davis, 2012, 278). Клајн предлага „холистичка стратегија на превенција“ (Klein, 2018) која вклучува сите средства, односно интегрира воени и не-

воени пристапи. Оваа сеопфатна стратегија на превенција подразбира спроведување на воени и не-воени активности заедно во целите на превенцијата на сајбер тероризмот „одвраќање и одговарање“ на потенцијалниот противник да изврши акт на сајбер тероризам (Klein 2018, 29).

6.2 Одвраќање

„Иако постојат ограничувања во влијаењето на одлуките на потенцијалните напаѓачи и нивните лидери, одвраќањето останува одржлив концепт за превенција на сајбер тероризмот“ (Klein, 2018, 30). Сè додека се внимателно разгледуваат принципите на воена потреба и законска регулатива, и воените и не-воените одговори се одржливи опции. Успехот на стратегијата за одвраќање многу зависи од перцепцијата на потенцијалниот непријател. Одвраќањето е посилно ако постои веродостојна закана од сила и неприфатливи последици за напаѓачите кои ќе им следат по секој вид на сајбер напад. Претпоставка за добра превенција е одржување на постојани и агресивни операции против дела на сајбер тероризам. На пример, ако Исламска држава или раководството на Ал-Каида чврсто веруваат дека по актот на тероризам ќе бидат изложени на систематски воени или не-воени интервенции кои ќе го загрозат нивниот опстанок, таквата перцепција може да ги одврати од сајбер напади кои претставуваат закана за животот.

Во основа, стратегијата на одвраќање од сајбер тероризам е влијание на непријателот и уверување на истиот дека штетноста на последиците по извршувањето на сајбер нападот ја надминува потенцијалните користи. Во текот на времето се користат различни видови одвраќање. Иако постојат бројни подврсти, се издвојуваат две главни стратегији на одвраќање: „одвраќање со казна и одвраќање со одбивање“ (Iasiello, 2018, 36).

6.2.1 Одвраќање со казна

Подразбира уверување на напаѓачот за значењето на казната и одмаздата за извршен напад. Оваа стратегија на одмазда не се ограничува на специфични акциите, туку вклучува и други средства како што се кинетички и економски санкции. Добар пример за ова е доктрина на Студената војна, каде заканата со употреба на нуклеарно оружје го спречила противникот да употреби слично оружје. Овој принцип на одвраќање

со казна може да се примени и во сајбер просторот, каде одмаздата може да се изврши преку дигитални акции како што се сајбер напади против потенцијалните сторители на сајбер тероризам, или предизвикување колапс на мрежата на непријателот. Се верува дека САД стоеле зад нападот со вирусот Stuxnet, кој бил насочен против иранските нуклеарни програми поврзани со истражувањето на ураниум, што предизвикало големи застои во работата и развојот на овие програми. Овој случај е добар пример за „стратегијата на одвраќање со казна“ во случајот на САД против Иран.

6.2.2 Одвраќање со одбивање

Претставува помалку конфликтна стратегија која се заснива на обидите да се потенцијални напаѓачи убедат дека, без оглед на вложените напори, ќе останат лишени од очекуваните користи од нападот. Оваа стратегија претставува традиционална дефанзивна форма која, кога се применува во сајбер просторот, подразбира обесхрабрување или фрустрирање на непријателот преку користење робусни, проактивни и скапи одбранбени мерки, така што односот на вложеното и добиеното за напаѓачот има негативен биланс. Примената на оваа стратегија бара силна фокусираност и посветеност на владата, големи материјални инвестиции и соработка со приватниот сектор за да се обезбедат системите и мрежите и да се стават под нејзина контрола. Користењето на напредни безбедносни практики и усвојување на поуздани компоненти на хардвер и софтвер бараат големи инвестиции и континуирано следење на технолошкиот развој.

Успехот на стратегијата за одвраќање од сајбер тероризам зависи од неколку фактори: „комуникација, сигнализација, приписивање и пропорционалност“ (Iasiello, 2018, 37–41). Ако некој од овие фактори не е исполнет, постои ризик од ескалација на непријателството во државен сукоб поради недоразбирање или погрешно толкување.

Ефикасната комуникација со меѓународната заедница, а особено со противниците, е еден од предусловите за успех и прашање на кредибилитет на една држава-нација, која мора да ги познава границите, односно „црвените линии“ кои не се преминуваат, како и кога е потребно тие да се прегази. Значи, ефективната комуникација бара постоење консензус за оперативните норми на однесување во сајбер просторот, што бара голем напор. Соединетите Американски Држави и Кина не успеаја да најдат заеднички јазик во стратешкиот и економскиот дијалог во јули 2013 година. САД, со

фокус на технологиите и мрежите на автоматизирани машини, преферираат употреба на терминот сајбер безбедност, додека земји како Кина и Русија претпочитаат поширок поим, информациона безбедност, која вклучува технологии и информации што се разменуваат на мрежата, за да ја зголемат контролата над содржините и информациите на кои нивното население има пристап, додека САД поддржуваат политика на слободен интернет. Без заеднички јазик, двете страни остануваат во несогласување и не успеваат да постигнат консензус за тоа како интернетот треба да се користи на најбезбеден начин. Слабостите во комуникацијата го отежнуваат испраќањето на јасни пораки во сајбер просторот, што може да ги зголеми тензиите.

Сигнализација се применува долго време во областите на меѓународната политика, преговорите во војни, кризи и меѓународните економски преговори. Без разлика кога се применува, во мир или војна, клучен елемент на која било стратегија за сајбер одвраќање е способноста правилно да се прикажат и испратат намерите до посакуваните приматели. Без можност за сигнализирање, се зголемува ризикот од погрешно разбирање или толкување, што може да ја направи стратегијата „одвраќање казном“ неефикасна.

На пример, пред да се примени стратегијата „одвраќање со казна“, државата која се брани мора јасно да ја сигнализира својата незадоволство на агресорот така што тој правилно ќе ја разбере и толкува, со цел потенцијалните трошоци од извршување на одреден сајбер напад да го надминат потенцијалниот бенефит. За сигнализацијата да биде ефикасна, државата мора да има установено работно тело кое ќе ја спроведе успешната и деструктивната сајбер одмазду. Ако противникот не верува во кредибилитетот на државата, сигнализацијата не може да биде успешна. Како и комуникацијата, сигнализацијата во сајбер просторот може лесно да се погрешно интерпретира, игнорира или дури и да не се забележи од агресорот. Сигнализацијата може да се спроведе јавно, тајно или преку дипломатски, економски или воени канали.

Припишувањето на одговорност во сајбер просторот е исклучително тешко, бидејќи сајбер просторот им овозможува на корисниците да делуваат тајно. „Спектар на одговорност на државата - Преглед на спектарот на сајбер нападите“ (Hea1ey, 2012) е специјално дизајнирана алатка која помага аналитичарите да припишат одговорност за одреден сајбер напад со прецизност и транспарентност, базирано на десет категории, каде секоја е обележана со различен степен на одговорност.

За да се идентификуваат агресорите во сајбер просторот, техничка анализа не е доволна, бидејќи многу непријателски актери користат исти тактики, техники и процедури, користат исти алати или се занимаваат со слични операции за спроведување на злонамерни активности. Иако техничките податоци се корисни за утврдување на нивото на вештини и ТТП (технолошки тактики, техники и процедури) на сајбер напаѓачите, тие не се целосно ефикасни за приписување, бидејќи не ги земаат предвид однесувањето, карактеристиките, намерите, мотивациите или желбите на актерите, ниту пружаат предвидување за идни напади и цели (Iasiello, 2012, 5).

Постојат ограничувања на техниките за приписување на дела на сајбер тероризмот: „припишување со задоцнување, неуспешно припишување и отсутство на припишување“ (Iasiello, 2012, 5-6). „Припишување со задоцнување“ - Техничката анализа бара време. Потребно е да се утврди дали инцидентот бил навистина злонамерен, потоа да се идентификува компјутерот од кој потекнува злонамерната активност (познато е дека починителите користат ботнети - мрежи на компромитирани компјутери што ги контролира починителот). Овој процес трае и се одложува за да се соберат сите податоци, што му остава простор на напаѓачот да избега, односно да исчезне пред да му се припише злосторството. Неуспешно приписување може да се случи поради ограничените способности на техничката опрема и човечката анализа грешките или стручноста на извршителите, техничката анализа не е секогаш во можност да обезбеди успешна идентификација на извршителот. Отсуството на припишување може да се случи од бројни причини кои понатаму можат да доведат до погрешна идентификација на локацијата или идентитетот на извршителот: неисправен софтвер, неисправни податоци, нејасни или погрешно толкувани податоци (Iasiello, 2012, 5-6).

Пропорционалноста во сајбер просторот подразбира дека штетата предизвикана од сајбертеристички напад треба да биде соразмерна со казната која следува. Практично, ова е тешко да се постигне поради различни причини. Кога национална држава дејствува независно, без вклучување на меѓународна организација како што се Обединетите нации, се ризикува да се загрозат дипломатските и економските односи. Затоа, пред да донесе одлука за одмазда (сајбер или не-сајбер одмазда), државата треба добро да ја процени последиците и потенцијалната штета, како и да размисли за реакцијата на меѓународната заедница.

6.3 Одговарање

Покрај одвраќањето, значаен дел од холистичката стратегија за превенција. Тоа е „намера да се влијае на водството на потенцијалните непријатели така што ќе се обесхрабрат иницијативите за воени конкуренции“ (Klein, 2018, 30). Постапката за одговарање е најделотворна пред да се манифестира заканата. Одговарањето вклучува „активности за обликување“, кои обично се не-војни по обем и се спроведуваат во мир, односно само надвор од потенцијалната опасност од војна. Стратегијата која вклучува одвраќање е насочена на покажување на сајбер нападите како бескорисни, што ќе го обесхрабри потенцијалниот агресор да спроведе такви акции.

Бослер и Холт спровеле истражување за да ја прикажат перцепцијата на полицијата за нивната моментална способност да одговорат на дела сајбер криминал и ги изнесле следните предлози за подобрување на социјалниот одговор на сајбер криминалот: 1) „корисниците на интернет треба да бидат попретпазливи кога користат интернет, 2) посурови казни за сајбер криминалците, 3) потешки кривични гонења за сајбер криминалците, 4) појасни закони против сајбер криминалот ќе ја зголемат успешноста на гонењето и истрагите, 5) специјализирани форензички алати и технологии, 6) зголемување на средствата за обука на агенциите во службата на законот, 7) создавање подобра соработка меѓу државата и нејзините сојузници за прашања на сајбер криминал, 8) работа со провајдери (на пример, АОГ) за следење на интернетот, 9) подобра едукација на јавноста во врска со сајбер криминалот, 10) соработка со деловната заедница за подобрување на известувањето и истражувањето на криминалот, 11) наменски структурирани локални единици за сајбер криминал, 12) подобри методи за откривање на сајбер криминал, 13) повеќе компјутерски обуки за службеници, 14) зголемување на менаџментот за да се развие следење на регионално ниво, 15) работа со граѓаните" (Boss1er & Ho11, 2012, 175).

Поменатите предлози се применливи и кога станува збор за превенција на сајбер тероризам. Тоа значи дека јавниот и приватниот сектор треба да се ангажираат заедно и да соработуваат на остварување на сајбер безбедноста, применувајќи различни методи на одбрана. Тоа значи дека компаниите од приватниот сектор кои тесно соработуваат со државни витални структури, како што се приватни безбедносни агенции, фондации за остварување на граѓански права и други, треба да се вклучат и да информираат за заканите од сајбер тероризам, како и за другите видови на сајбер криминал.

Добрата превенција подразбира: 1) усогласување на прописи и казнување на дела од сајбер тероризам на меѓународно ниво, 2) развој на истражувачки единици за сајбер криминал на локално ниво, 3) добра координација помеѓу приватниот и јавниот сектор, 4) примена на одредени стандарди, процедури и процедури за подобра безбедност на системите, 5) преземање на одредени мерки на заштита (редизајнирање на постоечките системи, физичко или сајбер пресретнување на напади, прислушување, поставување на сензори и други), 6) примена на различни техники како филтри за корисници кои имаат дозвола за пристап, тајни или јавни клучеви за енкрипција, различни системи за откривање на упади и други), 7) планирање (финансиски, истражувачки проекти за развој на нови технологии за одбрана и заштита), 8) подигнување на свеста за евентуална закана од сајбер тероризам, 9) свесна употреба и имплементација на современи ИКТ, 10) едукација.

6.4 Управување со инцидентот

Компјутерските системи функционираат автоматизирано, така што правилно поставената функција ги активира или доведува до оштетување или внесување неисправен код за „лошо“ функционирање. За да информациските и комуникациските структури функционираат, потребни се два клучни елемента: физички – опрема (машина) и човечки елемент – кој спроведува неколку технолошки постапки и дадени наредби што се испишуваат со програмски јазик, користејќи соодветни програмерски алатки.

За да се намали опасноста за компјутерските системи, најпрво е неопходно да се создаде заштита, односно некој вид бариера, со која ќе се ограничи или онемогуќи пристапот на „спољни“ неовластени корисници кои сакаат да манипулираат со податоците и изведуваат малверзации. Тоа најчесто се постигнува со поставување на одреден систем на лозинки, кои го ограничуваат пристапот на овластени корисници. Исто така, од голема важност е поставувањето сензори кои служат за навремено детектирање на напад и предупредување кога нападот е започнат. Некои автори (Janczewski & Colarik, 2008, 274 - 276) сметаат дека поради големата количина податоци е невозможно да се контролира целиот проток на информации, па затоа е многу важно да се постават системи за надгледување на соодветни места. Овие системи, кои го следат интернет сообраќајот, можат да извршуваат различни функции (собирање податоци, снимање, филтрирање на информации и алармирање во случај на напад).

Сајбер нападот најчесто се открива со методи кои ги следат сигналите и детектираат аномалии. Одбраната, односно примената на одредени системи за противмери во овие случаи, се применува само по откривањето на сајбер нападот. Техниките за откривање на сајбер нападите и контрамерите се усовршуваат во согласност со досега познатите или откриени методи за изведување на сајбер напади. Постои ограничување на системите, кои поради нивните недостатоци не се во можност да откријат сите сајбер напади со висок степен на прецизност и точност. Затоа, во многу случаи администраторите на системи можеби не ни забележуваат дека биле изложени на напад или обид за напад. Односно, сајбер нападот станува откриен само кога ќе се направи значителна штета која не може да помине незабележано. Токму поради тоа, системите за одбрана не се доволно подготвени за претстојните напади од страна на сајбер терористи.

Многu автори предлагаат употреба на методи за предвидување можни сајбер напади или одредена врста напада - овие можат да бидат добар извор за собирање информации за сајбер напади. Болен и соработниците претпоставуваат дека некои промени што се насочени против жртвата во сајбер просторот се случуваат непосредно пред извршувањето на самиот напад. Оттаму, тие предлагаат следните постапки за негово предвидување:

1. Прибирање архиве на сајбер инциденти кои се случиле во минатото,
2. Собирање извори на ранливости кои биле искористени во инцидентите. Собирање на социјални извори (членови, вести, твитови) кои се однесуваат на секоја жртва во архивата.
3. Детектирање на образци кои се повторуваат, разгледувани од аспект на угроженост. Откривање на образецот преку споредба на социјалните извори со жртвата, објавени непосредно пред нападот и оние објавени во други периоди.
4. Обучување модел за учење на машини на примерокот откриен во претходниот чекор.
5. Внесување дневни социјални содржини во обучениот модел и проверка дали се појавува шаблон во дневните извори. Откриениот образец во петтиот чекор треба да биде резултат на предвидување.

За предвидување на сајбер напади може да послужи и потенцијалната мотивација за негово извршување (Munkhdorj, B. & Yuji, 2017). За постигнување на безбедност, администраторите на мрежата треба да автоматизираат анализа на дневниците за да ги препознаат напади кои се во тек или трендови кои укажуваат на обиди за упад. На пример, низата неуспешних обиди за пријавување може да укаже на тоа дека некој се обидува да погоди лозинка и да добие неовластен пристап до мрежата. Администраторите на мрежите се одговорни за нивната безбедност и повеќето од нив се добро информирани за ризиците. Тие преземаат разни мерки за да спречат напади на нивните мрежи и компјутери.

Гудмен (Goodman, 2007, 49) смета дека организациите треба да креираат сопствени безбедносни политики и планови за одбрана кои покриваат широк спектар на одбрана од можни сајбер напади кои претставуваат потенцијален ризик за одреден тип организација. Тој исто така смета дека практичните вежби се многу корисни, но тие обично се избегнуваат од организациите бидејќи се скапи и нарушувачки, бидејќи многу информациони системи се деликатни, па нивните сопственици се плашат дека нешто може да тргне наопако.

6.5 Санирање на последиците

Соочување со сајбертерористички напади не подразбира само превентивни заштитни мерки и откривање напада, туку и управување со последиците од нападите, така што се тие: што е можно повеќе ублажат и ограничат, причинета штета да се сведе на минимум, ресурси и информации да се заштитат, да се врати што е можно повеќе податоци (раскир, гесоуергу функциите) и да се соберат што е можно повеќе информации за извршениот напад (ревизорски функции), за да се откријат извршителите и да се превенираат напади од таков вид во иднина.

По сајбертерористички напад, во оваа фаза на одбрана постојат две примарни процедури за одбрана. Тоа се: „опоравок (recovery) и одговор (response)" (Goodman 2007, 50). Следните постапки се вклучени во опоравок:

1. Отстранување или затворање на непријателски ентитети;
2. Проценка на штетата, што е скршено или изменето, а што не е;

3. Автоматски процеси за проценка и брза и ефикасна рационализација на она што останало;
4. Утврдување на приоритетни функции кои треба да се реконструираат;
5. Враќање на системот на состојба пред нападот без уништување на доказите.

Добро планираните и внимателно извршени напади, како што се корумпирање на податоци или злонамерен код, претставуваат најголем предизвик за опоравок. Ова е така, бидејќи организацијата може подолго време да биде изложена на маскиран напад, што значително го отежнува откривањето на соодветни резервни копии на податоци и откривање на сите штетни трансакции. Опоравокот е пасивен облик на одбрана, бидејќи подразбира реконструкција на оштетениот ИТ систем по нападот за да се врати организацијата на нормално функционирање што е можно побрзо.

Одговорот (response), пак, подразбира активен облик на одбрана, бидејќи се однесува на идентификување и казнување на извршителите на сајбертерористичкиот напад, како и на целосно информирање за опасностите на базата на претходно искуство со цел ефикасна одбрана и заштита од слични напади во иднина. Одговорот (response) вклучува следниве постапки:

1. Ппонаоѓање на вистинскиот виновник: прецизни траги и форензички алатки, нека врста на „отисок на прстите“;
2. Измерена одмазда: правни принципи и пропорционална одмазда;
3. Асиметрија: што да се прави со напаѓачите кои имаат ограничени ИТ средства или ранливости?;
4. Ескалација: проценка на штетата за да се одлучи дали треба да се испрати силна порака.

7. Мерки за одбрана од сајбер тероризмот

Сајбер тероризмот треба да се истражува како и било кој друг случај што вклучува дигитални докази. За да бидат собраните дигитални докази прифатливи на суд, тие мора да ги исполнуваат одредените форензички стандарди и протоколи кои се применуваат за идентификација, набавка, располагање и испитување на електронски докази, како на национално, така и на меѓународно ниво. Ова е особено важно затоа што истражувањето и решавањето на случаите на сајбер тероризам подразбира покрај

вклучување на државни (национални) судови, исто така и ангажирање на трибунали и меѓународни судови и институции.

Сајбер терористите користат различни техники за да го маскираат својот идентитет и да останат анонимни. Со помош на прокси сервери ги сокриваат ИП адресите, како и чекорите со кои е извршен нападот, користејќи фалсификувани ИП адреси. Овие активности им обезбедуваат повисоки нивоа на анонимност, што го отежнува пронаоѓањето на починителите на сајбер тероризмот. Нивоата на вештини на починителите не може лесно да се проценат, бидејќи тие главно избираат фајлови врз основа на нивната ранливост, кои не бараат употреба на сложени хакерски вештини и алатки за нивно искористување. Техничката анализа има свои ограничувања и не може да навлезе подлабоко за да даде одговори на прашањата како: зошто напаѓачот го избрал специфичниот компјутер; кој е нивото на ризик што го претпоставил пред да го изврши нападот и слично.

Процесот на аналитичка хијерархија (AHP) претставува структурирана техника која се користи за донесување сложени одлуки. Сепак, методологијата е премногу статична и бара варирање на алтернативи во фиксна, пондерисана хијерархија. Сајбер сценариите се подинамични и не можат лесно да се вклопат во систем на рангирање. AHP се фокусира на "ефектите" од сајбер активностите анализирајќи хипотези за тоа што е веројатно да се случи, но не се фокусира на мотивите за извршување на сајбер активностите.

Анализата на конкурентни хипотези (ACH) се базира на идентификација и анализа на алтернативни хипотези, а не само на еден "најверојатен" заклучок. Меѓутоа, како и процесот на аналитичка хијерархија, оваа анализа не може да ја земе предвид динамичната природа на сајбер просторот и сите настани во него, па затоа останува недоволно прецизна. Основната структура на анализата на конкурентни хипотези не ја зема во предвид она што се крие "зад" доказите на извршениот сајбер напад, туку служи само за наоѓање докази.

За да биде сојбер одбраната што е можно поприфатлива, Бериша и Баршљи сметаат дека е неопходно да се формира еден централен авторитет кој ќе го координира одговорот на национално ниво. Националниот тим за одговор на инциденти се состои од експерти за информациска безбедност кои ги проучуваат ранливостите на

компјутерските системи. Во одбраната од сајбер тероризмот, неизбежна е употребата на компјутери, но исто така потребно е да се воведат длабоки механизми на одбрана, како што се: системски пристап кон проблемот, едукација, создавање политика која широко го покрива проблемот со сајбер тероризмот, интеграција на меѓународни и национални мерки за одбрана и стандарди. Потребно е да се посвети поголемо внимание на "пораките" кои се емитуваат онлајн.

Активната сајбер одбрана подразбира проактивни мерки за сузбивање на непосредните ефекти од сајбер инцидентот, додека пасивната одбрана е насочена на производство на сајбер средства кои обезбедуваат ефикасен отпор на сајбер нападите.

7.1 Активна одбрана од сајбер тероризмот

Активна сајбер одбрана подразбира вклучување на човечки елемент во процесот, односно аналитичари кои спроведуваат различни активности со основен цел да обезбедат одбрана од сајбер напади. Розенцвајг ја дефинира активната сајбер одбрана како „синхронизирана и навремена способност да се откриваат, анализираат и намалуваат заканите. Активната сајбер одбрана функционира на брзината на мрежата, користејќи сензори, софтвер и интелигенција за да открие и запре штетни активности пред да стигнат до мрежи и системи". Со цел да се спроведе активна сајбер одбрана, аналитичарите се ангажираат за различни активности како што се: следење и примена на знаење во рамките на мрежата, наоѓање адекватни одговори, постојано усовршување за што поефикасно справување со заканите од сајбер тероризмот, како и следење на дневниците на активности кои автоматски собираат информации помагајќи им да откријат напади или обиди за упади во системот. Аналитичарите за сајбер безбедност најчесто се специјализирани за одредени области или домени (тестирање, следење на инциденти и реагирање, анализа на малвери, управување со ризик и собирање информации за заканите, итн.). Генерално, активната сајбер одбрана вклучува: „1) експлоатација; 2) контранапад; 3) предухитрувачки напад; 4) превентивен напад.

Првиот процес на активната сајбер одбрана вклучува експлоатација на компјутерските системи кои се мета на сајбер напади. Пасивни мерки за одбрана можат да откријат ИП адреси од кои е започнат нападот по време на или по извршувањето на нападот. Меѓутоа, напаѓачите се се повеќе усовршуваат во своите техники. Современите напади се се пософистицирани и произлегуваат како резултат на ланцените реакции на

поврзани хакнати компјутери, што значително ги отежнува можностите за откривање на вистинскиот извор на нападот и пратиме на првичниот извор на нападот. Затоа некои автори предлагаат IP (Belenky, A. & Ansari 2003, 162). Меѓутоа, оваа техника сè уште не е широко примена поради: неекономичноста, бидејќи треба да се имплементира на што повеќе ИП-адреси за да резултатите бидат што поконкретни и точни. Исто така, има проблеми со компатибилноста и перформансите. Ревизијата на сајбер нападите го враќа целиот процес назад додека не се открие последната ИП адреса на компјутерот од кој е извршен нападот. Потоа, форензичарите го идентификуваат сопственикот на компјутерот, истражувајќи документи на компјутерот, веб-историја, кеш-фајлови, е-пошта итн. (Keith, Bejtlich & Rose, 2008, 205 - 300). Значи, експлоатацијата подразбира детален преглед на сајбер нападите.

Контранапад е вид на активна сајбер одбрана кој подразбира одговор на напаѓачот со еквивалентен сајбер напад. Ова не само што ја одбива моменталната закана, туку ја спречува понатамошната активност на напаѓачот.

Предухитрувачкиот напад, како и контранападот, се класифицираат како „Hack Back активности" (Boebert, 2010, 48 - 49). Предухитрувачкиот напад е „предузимање сила против напад за кој се верува дека е неизбежен, врз основа на докази дека непријателската акција е започната или наскоро ќе започне". Оваа форма на активна одбрана подразбира реакција врз претпоставен сценарио, односно „спроведување напад на мрежата или системот во очекување дека тој ќе изврши напад врз вашиот систем." Целта на предухитрувачкиот напад е да го ослабне и неутрализира непријателот, така што тој нема да може да спроведе планираната офанзива. „Свесноста на потенцијалните напаѓачи за таквото „сајбер патролирање" само по себе делува како одвраќање" (Boebert 2010, 49), бидејќи тие се изложени на дополнителни безбедносни предизвици и неизвесност во поглед на степенот до кој се сами изложени на закана.

Превентивниот напад е сличен на предухитрувачкиот напад, но се разликува по тоа што подразбира „употреба на сила против очекуван напад, кој се базира на процена на постоечките или потенцијални средства кои напаѓачот може да ги користи за напад во иднина или за предизвикување на друга штета" (Sofaer, 2010, 9).

Технички, активната сајбер одбрана се заснова на веќе позната и валидна технологија која ја користат и самите напаѓачи, и затоа нема значајни технички бариери

за нејзино спроведување. Сепак, можат да се јават законски и политички пречки. На пример, правото на сопственост над нападнатите/оштетените машини е дискутабилно. Може да се тврди дека правото над машината која постои на интернет го има сопственикот на физичкиот хардвер, но сајбер терористите можат да користат украдени машини за да извршат злочин.

Ограничувањата на овие мерки за активна сајбер одбрана се многу контроверзни, бидејќи нивното спроведување може да ги прекрши одредени меѓународни закони. Денинг наведува „етичките и легални принципи за спроведување активна сајбер одбрана: 1. власт; 2. имунитет на трета страна; 3. нужност; 4. пропорционалност; 5. човечко учество; 6. граѓански слободи" (Bryant 2014, 111).

Четирите карактеристики на активната сајбер одбрана се: обем на ефекти, степен на соработка, врсти на ефекти и степен на автоматизација (Bryant 2014, 109).

Циклусот на активна сајбер одбрана се состои од четири фази кои го формираат основниот оквир за реагирање на закани и заштита на мрежите и системите:

1. **Закана**: Оваа фаза вклучува собирање на разузнавачки информации за потенцијалните закани. Заканите можат да се идентификуваат преку локално или оддалечено собирање информации. Локалното собирање се спроведува внатре во организацијата, додека оддалеченото вклучува соработка со други организации и собирање на информации надвор од границите на организацијата. Целта на оваа фаза е да се препознаат реалните опасности.
2. **Идентификација на промените**: Во оваа фаза, компанијата или организацијата ги анализира промените во околината и на мрежата кои покажуваат на сериозноста на заканата. Одговорот на оваа фаза е важен затоа што овозможува брзо реагирање и проценка дали заканата е реална и до кој степен е опасна.
3. **Реагирање на инцидент**: Третата фаза е насочена кон брзо и ефективно реагирање на инцидентот, зависно од неговата сериозност. Ова вклучува преземање мерки за отстранување или намалување на последиците од нападот, како и следење на ефективноста на применетите мерки.
4. **Закана и ракување со околината**: Последната фаза е фокусирана на подобрување на мрежата и системите, за да бидат попотпорни на идните

закани. Оваа фаза вклучува анализа на инцидентот и оптимизација на безбедносните мерки, што ја прави мрежата поинаку сигурна и отпорна на идни напади.

Циклусот на активна сајбер одбрана им овозможува на организациите брзо да реагираат на безбедносни инциденти и да ги минимизираат потенцијалните штетни последици по нивните системи и податоци.

7.2 Пасивни мерки за одбрана од сајбер тероризмот

Сите корисници интернет, било да се работи за поединец или организација, треба да применуваат пасивни мерки одбрани (сет на одбранбени системи), бидејќи тие обезбедуваат континуирана заштита или увид во заканите од сајбер тероризам преку алатки со минимални барања за постојан надзор и интервенција на луѓето. Ова се системи кои бараат периодично одржување и поправање, како што се: заштитни ѕидови и различни системи за заштита кои служат за откривање (IDS) или спречување на напади (IPS), спречување на процури на податоци (DLP), антивирусен софтвер, системи за детекција на напади, филтри за спам и други.

Што подразбира пасивната сајбер одбрана? „Пасивната сајбер одбрана вклучува криптографија и стеганографија (аналогно на употребата на камуфлажа и прикривање на авиони), безбедносен инжењеринг и верификација, конфигурација на мониторинг и управување, проценка на ранливости и ублажување, проценка на ризици, резервно копирање и опоравување на изгубени податоци, едукација и обука на корисниците“ .Тоа вклучува: основни принципи за сајбер „хигиена“ која тренира и едуцира работната сила како да се заштити од грешки или прекршоци кои можат да доведат до сајбер напади, сензорска технологија која служи за детекција на „копија“ или мамци кои служат за дистракција и управување со ризиците на сајбер просторот преку колективна одбрана, паметни партнерства, информатичка обука, зголемена свесност за ситуацијата и формирање на сигурни и отпорни мрежни околини. Ова покажува дека пасивната сајбер одбрана вклучува сложени механизми на одбрана. Сепак, бројни механизми кои ги вклучува пасивната одбрана се суштински пасивни, но стануваат активни кога вклучуваат елементи за оневозможување на откриените закани. Пасивната сајбер одбрана долго време се применува од страна на организации кои се грижат за безбедноста на нивното работење.

8. Нови стратегии за одбрана од сајбер тероризам

Сајбер нападите сè повеќе стануваат сериозни и сложени, а последиците се се позначајни, па затоа зависноста од постојните системи на одбрана станува недоволна за континуирано следење и анализа на системите и податоците. За одбраната од сајбер тероризмот да биде ефикасна, потребно е постојано усовршување на постоечките системи и барање нови стратегии и идеи. Во потрагата по нови идеи, Ајасиело истражувал можности за примена на досегашните модели на државна одбрана во сајбер доменот. Тој истражувал: „стратегијата за нуклеарно одвраќање, стратегијата за одвраќање од тероризам, стратегијата за одвраќање од заканите на непријателски држави , (Iasiello, 2018, 41-45).

Нуклеарно одвраќање - Во основа, оваа стратегија има цел да го спречи користењето на нуклеарно оружје, а се применува само на држави кои располагаат со нуклеарно оружје. На почетокот на седумдесеттите години, за време на Студената војна помеѓу САД и Советскиот Сојуз, оваа стратегија се покажа како многу успешна. Стратегијата за нуклеарно одвраќање се базира на теоријата „тишање на оружјето" (Payne, & Walton, 2002, 169), што значи сигурно взаимно уништување на земјите кои ќе се осмелат да користат нуклеарно оружје. Затоа ниту една од овие земји, без разлика на многуте несогласувања и влошени односи, не се одлучила да го користи нуклеарното оружје, избегнувајќи го почетокот на нуклеарна војна која би имала разорни глобални последици.

Милвенон и Ретреј забележуваат сличности помеѓу сајбер и нуклеарен конфликт: „1. И двата дејствуваат на сите три нивоа на воени операции: стратешки, оперативен и тактички, и нивните ефекти можат да бидат од мали до глобални размери. 2. И два можат да создадат големи, па дури и егзистенцијално деструктивни ефекти. 3. И два се можни да се спроведат помеѓу национални држави, помеѓу нација-држави и недржавни актери, или помеѓу хибриди кои вклучуваат национални држави и недржавни застапници. 4. Нуклеарен и сајбер конфликт може да доведе до одлучувачки пораз на непријателот, преку негирање на потребата за конвенционално војување. 5. И два можат намерно или ненамерно да предизвикаат каскадни ефекти надвор од почетниот цел на нападот“ (Milvenon**,** Rattray**,** 2012, 18).

Покрај сличностите, постојат и разлики помеѓу сајбер и нуклеарни конфликти: „1. Националните држави генерално не ја преземаат одговорноста за непријателските акции во сајбер просторот. 2. Нема застрашување во смисла што може да направи сајбер напад; инциденти како сајбер нападот каде малвер уништил 30.000 хард дискови

нафтената компанија во Саудиска Арабија, предизвикал значајни нарушувања, но не бил доволен да има сериозно влијание врз операциите во нуклеарната централа или нафтената компанија. 3. Извонредно тешко е да се идентификува извршителот во сајбер просторот; што не би било случај при покретање на нуклеарно оружје и, 4. Развојот на нуклеарното оружје може да се следи, но за разлика од него, не постои слична транспарентност за производството на сајбер оружје во државата, ниту постои надзорна меѓународна агенција која ќе го следи таквиот развој“ (Iasiello, 2013, 398). Споменатите разлики помеѓу сајбер и нуклеарните конфликти укажуваат дека стратегијата за нуклеарно одвраќање не е применлива во сајбер просторот (Iasiello 2018, 42).

„Стратегија за одвраќање од тероризмот - Оваа стратегија се покажала успешна во неколку случаи. На пример, кога терористичката организација презема атрибути на национална држава, односно кога поседува имот што може да биде оштетен како одмазда, тогаш може да се влијае на водството на терористите за да ја ограничи својата политика и активности во корист на зачувување на ресурсите кои организацијата ги поседува. Убиството на највисок терористички лидер може исто така да биде ефикасно во одвраќање на терористите од нивните планирани активности, но само за одредено време додека не се организираат повторно. За стратегијата за одвраќање да биде успешна, противничката страна „мора да ја разбере (имплицитно или експлицитно) заканата и да донесе одлуки кои се резултат на калкулацијата на трошоците и користите“. Неуспешните обиди за спречување на упорен противник укажуваат дека има многу повеќе пречки отколку корист од оваа стратегија. Кога ќе се примени на сајбер просторот, кој не е нужно поврзан со една иста локација, се поставува прашањето: Како да се делува на поединец или група терористи во сајбер просторот без поуздани информации за тоа кои тие всушност се или каде живеат? Дополнителен фактор кој ја комплицира примената на оваа стратегија во сајбер просторот е мотивацијата. Може да се каже дека терористот кој делува во сајбер просторот го цени својот живот, бидејќи користи сајбер оружје и виртуелен идентитет. Така, тој не е директно загрозен. За разлика од тоа, терористите кои делуваат оперативно во реалниот/физичкиот свет се компромитираат и се подготвени да го изгубат својот живот заради остварување на целите на организацијата.

„Стратегија за одвраќање од заканите на непријателски држави се применува за зачувување на националната безбедност. САД ја применуваат оваа стратегија за одбрана

во однос на Сирија и Северна Кореја. За да биде стратегијата за одвраќање што поефикасна, развиена е нејзината посебна форма - „прилагодена одвраќање. Тоа се специјално дизајнирани стратегии за одвраќање кои се базираат на разузнавачки информации за секоја држава или ситуација, чии цели се да дејствуваат на психолошките профили на лидерите и нивните одлуки. Примената на оваа стратегија во сајбер просторот не е погодна, поради сложеноста и разновидноста на учесниците во сајбер нападите. Терористите не функционираат како непријателски настроени држави чија крајна цел е стабилноста на сопствениот режим и зачувување на лидерството.

Либицки наведува дека основната цел на сајбер одбраната е да го намали „ризикот од сајбер напади на прифатлив ниво за прифатливи цени“ (Либицки, 2009, 32). Во врска со стратегијата за одвраќање преку казни, потребно е националната држава пред било какви одмазди да не заговара агресивни акции, туку внимателно избрани мерки во одбранбени цели. Ајасиело смета дека успешната стратегија за одвраќање преку казни се заснова на „три основни аксиоми: 1. Припишување; 2. повторливост 3. успех (Success)” (Iasiello 2018, 46). Пред да се покрене било каков контраудар, неопходно е да се знаат: идентитетот на извршителот, неговата намера, мотивација, методот на извршување на нападот, целта на нападот и конечната цел. Со други зборови, за приписувањето да биде што попрецизно, потребно е да се одговори на многу прашања: „Дали сајбер терористот е поврзан со национална држава? Дали дејствува самостојно или добил наредби одгоре? Дали одмаздата соодветно одговара на причинетата штета? Дали конечната цел на нападот е национална држава или нешто друго? Дали намерите на напаѓачот беа да: уништи, деградира, оспори или нешто друго? Дали нападот имал друга цел освен она што е видливо на површината?“ (Iasiello, 2018, 47). Дополнително, не може да се применува една иста стратегија за одбрана од различни видови напади, напаѓачи и цели во сајбер просторот. Успехот зависи од применетата тактика. Различни тактики за казнување треба да се применуваат пред, за време или по одреден сајбер напад.

Бидејќи „доменот на сајбер просторот е инхерентно нестабилен“ , Здружението за испитување на сајбер конфликти предлага пет нивоа на одбрана: „1. стратегија, 2. војска и оперативa, 3. недржавни актери во сајбер просторот, 4. домашно и меѓународно право, 5. пристапи за ублажување на сајбер конфликти“. Бегс и Батлер ја анализираат

сајбер одбраната на девет нивоа, односно девет точки. Тие наведуваат дека ефикасната борба против сајбер напади се базира на многу детализирани стратегије и пристапи.

9. Меѓународна соработка во борбата против тероризамот

9.1 Меѓународна правна регулатива

Проблематиката на сајбер безбедноста ја комплицира постоењето на три суштински проблеми (технички, политички и правни) кои постојат од самото појавување на информациските и комуникациските технологии. **Првиот проблем** е од техничка природа. „Основниот технички проблем се наоѓа во срцето на сајбер просторот, бидејќи неговата основна архитектура никогаш не била дизајнирана со безбедноста на ум; уште повеќе, првичните дизајнери никогаш не замислиле дека мрежата ќе се користи за злонамерни цели“ (Milenop & Kahalu, 2012, 1). Приоритетите на првите дизајнери биле функционалноста и лесното поврзување на корисниците (конекција), како и технолошките иновации кои го олеснуваат животот. **Вториот проблем** е од политичка природа, бидејќи „еволуцијата на технолошката архитектура далеку ги надминала соодветните концепциски, доктринарни, организациски и правни структури, што резултира во реактивна и назадна политичка динамика, каде што сегашните идеи и организации често се занимаваат со вчерашните проблеми, без доволна флексибилност за справување со идните предизвици што ги носат најавените технолошки иновации“ (Milenop & Kahlahu, 2012, 1). **Третиот проблем** е од правна природа. Примената на законите на интернет и регулирањето на неговите бројни можности претставува дилема за правниците ширум светот. Ставање на дигиталното под правна рамка, како и примената на „аналоги“ територијални закони врз нејасните дигитални граници на бесконечната глобална комуникациска мрежа, „се чини дека е премногу за нашите конвенционални правни системи“ (Aquilina, Shviliov & Bosco, 2014, 3).

Ранливоста на сајбер просторот отвора можности за извршување на сајбер тероризам, па затоа е неопходно да се регулираат сите активности што се спроведуваат во или во врска со сајбер просторот. За таа цел, Коутим (Coutim, 2010) предлага пет јурисдикциски теории и пристапи:

1. **„Територијална теорија“** – Местото каде што е извршено кривичното дело, целосно или делумно, ја определува јурисдикцијата. Недостатокот на овој

пристап лежи во тоа што се базира на претпоставката дека државата има неспорен суверенитет над територијата што е предмет на спор, што не е лесно да се потврди поради флуидните граници на сајбер просторот. Инаку, оваа теорија ги има своите корени во моделот на државен суверенитет воспоставен со Вестфалските мировни договори (Beaulac, 2004, 181).

2. **„Теорија на националност (или активна личност)“** – Заснована е пред сè на националноста на сторителот на кривичното дело.
3. **„Теорија на пасивна личност“** – Додека „теоријата на националноста“ се занимава со националноста на сторителот, „пасивната теорија на личноста“ се занимава со националноста на жртвата. Коутим ова го нарекува „област на сајбер криминологија“ и како добар пример го наведува случајот кога руски државјанин бил осуден на суд во Хартфорд, Конектикат, за хакирање на компјутери во САД.
4. **„Теорија на заштита“** (позната и како „принцип на безбедност“ и „теорија за повредени форуми“) – Се занимава со повредените национални или меѓународни интереси и доделување на надлежност на државата која има интерес, било национален или меѓународен, во ситуација предизвикана од напад. Коутим наведува дека оваа теорија ретко се применува, и тоа главно во случаи на фалсификување на пари и хартии од вредност.
5. **„Теорија на универзалност“** – Се заснова на принципот на универзалност, кој произлегува од меѓународниот карактер на кривичното дело и му овозможува на секоја држава да бара надлежност за извршени кривични дела, дури и ако тие дела немаат директно влијание врз таа држава. Иако изгледа дека оваа теорија има најголем потенцијал за примена во сајбер просторот, Коутим укажува на две нејзини клучни ограничувања. Прво, државата мора да го има обвинетиот во притвор кога бара надлежност, под претпоставка дека е извршено кривично дело. Второ, делото мора да биде „особено навредливо за меѓународната заедница“. Постојат значајни практични потешкотии во дефинирањето на параметрите на принципот на универзалност и во можноста за проширување на овој принцип на областа на сајбер просторот и активностите во него. Теоријата на универзалност најчесто се применува кај кривични дела како пиратерија и нелегална трговија со стоки.

Сајбертерористичките дела по својата природа можат, но и не мораат да предизвикаат вооружен конфликт, во зависност од конкретните околности. Кога станува збор за толкувањето и примената на законите на една конкретна држава надвор од нејзините административни граници на надлежност, справувањето со сајбер тероризмот е дискутабилно, бидејќи линијата што ја раздвојува употребата на сила и меѓународното хуманитарно право е замаглена. Затоа, Шмит наведува четири клучни прашања поврзани со регулирањето на сајбер операциите низ призмата на меѓународното право:

1. Кога една сајбер операција претставува недозволена употреба на сила со која се прекршува Повелбата на Обединетите нации, член 2(4) и меѓународното обичајно право?
2. Кога една сајбер операција претставува закана и прекршување на мирот или акт на агресија, така што Советот за безбедност може да дозволи преземање дејствија како одговор на тоа?
3. Кога една сајбер операција претставува оружен напад, така што државата-жртва може да се брани, дури и со кинетички средства, во согласност со правото на самоодбрана според член 51 од Повелбата на ОН и обичајното меѓународно право?
4. Кога една сајбер операција достигнува ниво на оружен конфликт, така што истата се регулира од страна на меѓународното хуманитарно право како воени активности? (Schmitt, 2010, 152).

Шмит (Schmitt, 1999, 18) идентификува низа фактори преку кои економската и политичката присила можат да се разликуваат од употребата на оружена сила. Примената на овие фактори во сајбер доменот може да влијае врз проценката на една држава дали одредена сајбер операција претставува употреба на сила:

1. **„Тежина на последиците“** – Проценка на сериозноста на штетата во зависност од обемот, размерот и времетраењето на последиците. Дали нанесената штета претставува само помала непријатност или провокација за поединец и/или имот? Или е екстремна и влијае на критичните национални интереси?
2. **„Моменталност“** – Во зависност од временскиот аспект, односно појавувањето на штетните последици: дали се манифестираат веднаш или

доцна и со бавно штетно дејство. Кога последиците се јавуваат веднаш, државата е приморана брзо да реагира.

3. **„Директност“** – Се однесува на причинско-последичната врска. Колку што е таа врска послаба помеѓу почетниот акт и последиците, толку е помала веројатноста државата да го смета актерот одговорен за кршење на забраната за употреба на сила. На пример, последиците од економска криза најчесто се резултат на пазарни сили и пристап до пазари, што значи дека причинската врска е индиректна. За разлика од тоа, експлозијата има јасна и директна врска меѓу причина и последица.
4. **„Инвазивност“** – Колку е посигурен таргетираниот систем, толку е поголема загриженоста за пробивањето во него. Конкретен пример е сајбер шпионажата, која иако е високо инвазивна, не се смета за употреба на сила или оружен напад, туку според меѓународното право се третира како недозволено физичко пробивање на територијата на целната држава – како во случајот кога воен брод или авион собира разузнавачки информации од територијалното море или воздушен простор.
5. **„Мерливост“** – Во интерес на државата е што попрецизно да ја измери нанесената штета. Разгледано од аспект на меѓународното право, економската присила може да предизвика значителни страдања, но не се смета за употреба на сила. Од друга страна, воен напад се класифицира врз основа на измерен степен на разурнување. Тешко е да се идентификува или квантитативно да се процени штетата во сајбер просторот.
6. **„Претпоставен легитимитет“** – Меѓународното право експлицитно забранува одредени дејствија, а за оние кои не се забранети се претпоставува дека се легитимни. Било во домашното или меѓународното право, примената на насилство се смета за нелегитимна, освен во случај на самоодбрана.

7. **„Одговорност“** – Законот уредува кога една држава може да се смета за одговорна за сајбер операции. Колку е посилна врската помеѓу одредена држава и операцијата во сајбер просторот, толку е поголема веројатноста другите држави да го протолкуваат тоа како употреба на сила, што ја доведува во прашање меѓународната стабилност (Schmitt, 2010, 916). Затоа е потребно особено внимание да се насочи кон воената политика, која, според тврдењата на Carr, „треба да биде насочена кон воспоставување на меѓународни правни механизми

кои би овозможиле спречување на потенцијалните агресори да користат сајбер оружје неконтролирано и тајно“ (Carr, 2010, 168). Технолошкиот развој создаде нови форми на сајбер алатки/оружје чии последици можат да бидат подеднакво деструктивни како и при употреба на класично оружје. Затоа бројни аналитичари (Wheeler, 2013; Kanuck, 2013) укажуваат дека постојното воено право станало неадекватно и предлагаат зголемена регулација на сајбер просторот.

Сајбер тероризмот претставува посебна форма на тероризам. Речиси и да не постои регион во светот во кој не се разгледува борбата против тероризмот. Меѓутоа, и покрај тоа што многу земји се потписнички на бројни конвенции и протоколи од областа на тероризмот и неговите различни појавни облици, практичната примена не е нималку едноставна. Како што забележуваат Комлен Николиќ и соработниците, основните пречки за сузбивање на сајбер криминалот на меѓународно ниво се:

- правна неусогласеност околу дефинирање на дејствијата и формите на извршување на одредени кривични дела;
- недоволна обученост на лицата задолжени за постапување во предмети од сајбер криминал (полиција, обвинители и судии);
- неусогласеност на правилата за истрага на сајбер криминалните дела;
- неусогласеност или отсуство на механизми за правна помош и договори за екстрадиција на меѓународно ниво (Комлен Николиќ и др., 2010, 31).

Со оглед на постојаниот раст на заканите од сајбер тероризмот, неопходно е меѓународната заедница да пристапи кон пообемна и посистематска регулација на сајбер просторот. Тоа вклучува и унапредување на постојното меѓународно право, воспоставување на нови механизми за одговорност и заштита, како и зголемена соработка и обука на надлежните органи на национално и меѓународно ниво.

9.2 Мултилатерална соработка

Регулативите што се однесуваат на справување со тероризмот индиректно се однесуваат и на проблемот на сајбер-тероризмот, кој претставува негова посебна форма. Обединетите нации исто така го препознаа сајбер-тероризмот како една од најзначајните закани што му се заканувааат на современото човештво. Обединетите нации дале голем придонес во областа на безбедноста и одбраната од тероризмот, и се донесувачи на

бројни меѓународни документи, резолуции и други акти уште од 30-тите години на XIX век. По атентатот на 9 октомври 1934 година во Марсеј, беше донесена резолуција со која се забранува „било какво мешање во политичкиот живот на друга држава“ (Slansky, 1935: 405). Во периодот од 1 до 16 ноември 1937 година во Женева беше одржана меѓународна конференција посветена на тероризмот. Од првата половина на XIX век до денес се донесени бројни документи, резултат на состаноци, седници и конференции. Како што тероризмот станувал посложен со текот на времето, така и ОН донесувале нови документи и формирале тела за справување со тероризмот. По терористичкиот напад во Њујорк и Вашингтон, Обединетите нации донесоа одлука во 2001 година да се основа Комитет за борба против тероризмот.

Кофи Анан, како вршител на должноста генерален секретар на ОН, предложи светските лидери да прифатат заедничка дефиниција за тероризмот и да се договорат за условите под кои меѓународната заедница може да користи сила за заштита на мирот и безбедноста. Исто така, ОН се донесувачи на Глобалната антитерористичка стратегија (UN Global Counter-Terrorism Strategy), која претставува уникатен инструмент за справување со тероризмот на меѓународно ниво. Оваа стратегија се ревидира на секои две години, за да ги следи трендовите во развојот на тероризмот и се базира на четири основни столба:

1. Идентификација на условите кои придонесуваат за ширење на тероризмот,
2. Превенција и сузбивање на тероризмот,
3. Изградба на капацитетите на државите и зајакнување на улогата на ОН,
4. Обезбедување владеење на правото и почитување на човековите права (UN Global Counter-Terrorism Strategy, 2006).

Обединетите нации активно се занимаваат со проблемот на тероризмот. Во јуни и јули 2021 година беше одржана двонеделна конференција на тема борба против тероризмот, на која учествуваа раководители на агенции од земјите-членки. Главната цел на конференцијата беше градење нови партнерства и зајакнување на мултилатералната соработка во борбата против тероризмот (United Nations, 2021). На таа конференција беа идентификувани нови и постоечки прашања, се продлабочи разбирањето на проблемите и предизвиците, и беа истражени можности за наоѓање поефикасни одговори во борбата против тероризмот. ОН се стремат да обезбедат антитерористичка платформа за експерти од различни географски, мултикултурни и

родови средини за посветена размена на знаења со цел унапредување на глобалниот и мултидимензионален пристап, кој е неопходен за борба против тероризмот и насилниот екстремизам. Обединетите нации се една од водечките меѓународни организации која сериозно и континуирано вложува напори за справување со овој проблем.

НАТО, политичко-воената евроатлантска алијанса, веќе подолго време е свесна за заканите од новите форми на војување – сајбер војување, како и другите закани што произлегуваат од сајбер просторот. Во ноември 2002 година, на самитот во Прага, лидерите на НАТО одлучија да ги зајакнат своите капацитети за одбрана од сајбер-напади. Таа одлука поттикна посистематски пристап и бројни иницијативи и програми за справување со тероризмот во рамките на НАТО. Тогаш беа формирани различни тела на НАТО со надлежности во областа на заштита и одбрана од сајбер инциденти:

а) Агенцијата на НАТО за комуникациски и информациски системи (NCIA – NATO Communications and Information Systems Services Agency), која се смета за прва линија на одбрана од сајбер-тероризмот;

б) Техничкиот центар на НАТО NCIRC (NATO NCIRC Technical Center), одговорен за компјутерска и комуникациска безбедност;

в) Оперативниот центар за информации на НАТО (NIAOC – NATO Information Assurance Operations Centre), кој има надлежности за управување и координација на криптографската опрема што се користи за реагирање на сајбер-напади насочени кон НАТО;

г) Центарот на НАТО за реагирање на компјутерски инциденти (NCIRC – NATO Computer Incident Response Capability), чија главна задача е заштита на шифрираната комуникација внатре во системите на НАТО.

NCIRC претставува главен извор на техничка и оперативна експертиза и капацитети на НАТО во областа на сајбер-одбраната и служи за заштита на субјектите на НАТО (на пр. администрацијата на НАТО) и мисиите; исто така се користи за справување со заканите по сајбер-безбедноста на информациските системи на НАТО (2002).

НАТО започна да се фокусира поинтензивно на сајбер одбраната по нападот врз Естонија во 2007 година, кога оваа држава стана жртва на координиран сајбер-напад. Повеќе од три недели беа напаѓани владини и парламентарни веб-страници, министерства, новински куќи, интернет провајдери, големи банки и мали претпријатија

во Естонија преку DDoS напади. Овие напади се совпаднаа со одлуката на естонската влада да го отстрани споменикот на Бронзениот војник од центарот на Талин — споменик посветен на загинатите во Втората светска војна.

Естонија се прогласи себеси за прва жртва на меѓународен сајбер-напад. Во 2008 година, министрите на НАТО се состанаа во Нордвејк и се договорија за „концепт на сајбер одбрана“, со што беше објавен Талинскиот прирачник и започна развојот на сајбер-одбранбената политика на НАТО, која во 2010 година стана дел од „Стратешкиот концепт“ (Bogdanovski & Petreski, 2016).

НАТО и Европската унија (ЕУ) соработуваат преку технички договор за сајбер одбрана, кој беше потпишан во февруари 2016 година. Во светло на заедничките предизвици, НАТО и ЕУ ја зајакнуваат соработката во областа на сајбер одбраната, особено во деловите на размена на информации, обуки, истражување и вежби. На самитот во Брисел во 2021 година (NATO, 2021), сојузниците ја поддржаа новата сеопфатна политика за сајбер одбрана, која ги поддржува клучните задачи на НАТО и севкупното одвраќање и одбрана, со цел понатамошно подобрување на отпорноста на Алијансата.

НАТО го гледа сајбер тероризмот како сериозна закана која во иднина може значително да ја наруши безбедноста и стабилноста, поради што одржува добра соработка со меѓународни организации кои исто така се занимаваат со прашања на меѓународната безбедност, како што се Обединетите нации (ОН), ОБСЕ и други.

Советот на Европа (CoE – Council of Europe) даде значаен придонес во областа на борбата против сајбер криминалот. На предлог на Советот на Европа, во 1997 година беше формиран Комитетот на експерти за криминал во сајбер просторот (Committee of Experts on Crime in Cyber-space), кој работеше на изработка на „Конвенцијата за сајбер криминал“ (Convention on Cybercrime). Конвенцијата беше завршена во јуни 2001 година и претставува првиот меѓународен договор на тема сајбер криминал.

Во ноември истата година, конвенцијата беше потпишана во Будимпешта од 34 држави, а шест од нив ја ратификуваа (Естонија, Литванија, Унгарија, Романија, Албанија и Хрватска). Конвенцијата содржи: список на кривични дела кои секоја потписничка држава мора да ги внесе и криминализира во своето законодавство,

процедурални механизми и стандарди кои треба да се имплементираат во националните закони, како и обврска за меѓусебна соработка и спроведување на најшироки меѓународни истражни мерки во врска со компјутерски системи, податоци или електронски докази поврзани со кривични дела. Конвенцијата има голем меѓународен авторитет и е отворена за сите држави, не само за земјите-членки на Советот на Европа. До ноември 2021 година, кон неа пристапиле 66 држави.

Комитетот на министри на Советот на Европа на 17 ноември 2021 година усвои Втор протокол на Конвенцијата за сајбер криминал, кој се однесува на подобрување на соработката и откривање на електронски докази (Council of Europe, 2021). Со ова се прошири правната регулатива во сајбер просторот, се овозможи подобра заштита на интернет-корисниците и се даде поддршка во остварување на правда за жртвите на кривични дела.

ОБСЕ (OSCE – Organization for Security and Co-operation in Europe) започна поинтензивно да се занимава со сајбер безбедноста по одлуката на Советот на министри во 2004 година да ги следи активностите и злоупотребата на интернетот од страна на терористи, како што се финансирање, пропаганда и регрутација (Bogdanovski & Petreski, 2016, стр. 68). ОБСЕ игра важна улога во јакнење на сајбер безбедноста. Форумот за безбедносна соработка на ОБСЕ беше основан со цел следење на вооружувањето, за да се спречат ризици и да се обезбеди воена стабилност во Европа.

Покрај основните политичко-воени договори меѓу државите-членки, ОБСЕ сè повеќе ги вклучува прашањата поврзани со сајбер безбедноста, предизвиците во сајбер просторот и заканата од сајбер оружје. Одделението за транснационални закани (TNTD – Transnational Threats Department) го препознава сајбер тероризмот како сериозна закана и работи на размена на знаење и искуства во оваа област.

На 22 и 23 јуни 2021 година, во Виена беше организирана третата меѓурегионална конференција за сајбер безбедност, на која учествуваа 280 владини и невладини претставници (OSCE, 2021). Целта на конференцијата беше да обезбеди отворена платформа за дијалог меѓу државните институции, бизнис секторот, експертите и младите за актуелни теми поврзани со заштитата од сајбер закани.

Интернет сообраќајот е тешко да се следи поради огромната количина на информации што постојано циркулираат. Електронскиот надзор на телекомуникациите вклучува прислушување на телефонски разговори и следење на други облици на комуникација, што во суштина претставува судир со политиката на почитување на приватноста. Овој вид надзор се спроведува првенствено за собирање релевантни докази во судски постапки, откривање на мрежи на членови на терористички организации, утврдување на хиерархијата и криминалните активности на организацијата. Такви мерки може да ги применуваат само законски овластени лица и тоа строго во согласност со утврдени принципи и процедури.

Примената на овие мерки се дозволува кога истрагата со претходно применетите методи не дала резултати. Барањето за прислушување мора да биде прецизно образложено, со наведени факти и околности под кои другите методи не биле успешни, како и причините поради кои се смета дека прислушувањето би било ефикасно. Во барањето се наведува и времетраењето на надзорот, кој според закон може да трае до триесет дена, врз основа на наредба од надлежен судија. Надзорот може да се продолжува за уште триесет дена во неколку наврати, секогаш со нова судска наредба (Weaver, Augustine & Bastian, 2007, стр. 564).

Во случаи каде што терористичката активност тоа особено го наложува, може да се примени и таен надзор на лица чиишто идентитети не се целосно утврдени, но кои се поврзани со најтешки кривични дела. Еден од методите што понекогаш се користи е прикриениот истражител. Овој метод се применува поретко поради сè уште недоволно прецизираната правна рамка, како и бројните практични потешкотии што произлегуваат од неговата реализација. Членовите на терористичките групи најчесто се крајно недоверливи кон новодојденци, што дополнително го отежнува инфилтрирањето.

Ситуацијата се комплицира уште повеќе кога прикриениот истражител треба да учествува во криминално дело. За вакво нешто е потребно посебно одобрение од Одборот за водење тајни истраги во итни случаи – со цел прибирање информации корисни за кривичната постапка, зачувување на неговиот кредибилитет или заштита од смртна опасност или тешки телесни повреди (Јович, 2001, стр. 181).

Од сето наведено може да се заклучи дека меѓународната заедница е целосно свесна за ризиците што произлегуваат од употребата на современите информатички и

комуникациски технологии, а безбедноста на сајбер просторот е актуелна тема што постојано се дискутира. Сепак, бројот на документи и интензитетот на мултилатералната соработка не претставуваат гаранција за ефективна превенција и одбрана, доколку усвоените решенија останат само на хартија. Неопходна е нивна практична примена и ефективна оперативна изведба.

Заклучок

Сајбер тероризмот денес претставува една од најголемите закани за современото општество, заедно со климатските промени, пандемиите и економските кризи. Со појавата на дигиталната ера, тероризмот доби нова димензија – сајбер просторот, каде што физичките бариери и традиционалните безбедносни механизми се покажуваат како недоволни. Сајбер тероризмот се развива со исклучителна брзина, користејќи ги предностите на глобалната поврзаност, а притоа ги надминува конвенционалните форми на насилство. Наместо експлозиви и оружје, денешните терористи сè почесто користат тастатури, софистицирани софтверски алатки и деструктивни компјутерски програми како што се вируси, тројанци и малвери. Ова ги прави сајбер нападите подмолни, тешко детектибилни и со потенцијал да предизвикаат катастрофални последици во реалниот свет.

Нападите врз критичната инфраструктура, како што се енергетските системи, болниците, банкарските мрежи, телекомуникациите и државните институции, веќе не се теоретска претпоставка, туку се реалност која светот ја гледа сè почесто. Сајбер тероризмот не е само напад врз компјутерските системи; тој е напад врз стабилноста на државата, врз довербата во институциите, врз економијата и врз социјалната кохезија. Со неколку клика може да се парализираат цели системи, да се предизвика паника, економска загуба, па дури и загрозување на човечки животи.

Во еден ваков контекст, неопходно е да се сфати дека сајбер тероризмот не е само проблем на ИТ експертите или безбедносните служби. Тој претставува мултидимензионален предизвик кој бара синергичен пристап на државата, академската заедница, приватниот сектор, невладиниот сектор, медиумите и меѓународната заедница. Безбедноста не може да се обезбеди со изолирани напори. Потребно е

воспоставување на национални и меѓународни механизми за превенција, заштита, одговор и обновување по сајбер напад.

Посебен акцент треба да се стави на едукацијата и подигнување на свеста кај населението. Голем дел од сајбер нападите се успешни поради човечка грешка – некористење на безбедносни протоколи, неажурирани системи, слаби лозинки, па дури и непознавање на основните правила за дигитална безбедност. Затоа, едукацијата мора да започне од најмладите, преку образовниот систем, но и преку медиумите и јавните кампањи за информирање на сите граѓани.

Истовремено, неопходно е државата да ги зајакне капацитетите за следење, откривање и спречување на сајбер напади. Треба да се инвестира во обука на стручни кадри, во модерни технолошки алатки за мониторинг, како и во развој на национални стратегии за сајбер безбедност. Потребни се и јасни законски регулативи кои ќе го дефинираат сајбер тероризмот и ќе овозможат брза и ефикасна реакција на институциите. Во тој контекст, неопходна е постојана меѓународна соработка, бидејќи сајбер просторот е глобален и заканите не познаваат граници.

Македонија, иако мала држава, е дел од глобалниот дигитален екосистем. Како таква, подеднакво е изложена на ризиците од сајбер тероризам. Свесна за овие закани, државата презема активности за нивно регулирање преку усвојување на меѓународни конвенции, создавање на законски рамки и развој на институционални капацитети. Националниот систем за спречување на тероризмот, вклучувајќи ја и сајбер безбедноста, е поставен, но треба да се надградува, адаптира и постојано да се унапредува. Особено важно е континуираното следење на трендовите, развојот на нови методи за заштита и вклучување во меѓународни иницијативи за размена на информации и најдобри практики.

Покрај државниот сектор, клучна е улогата на приватните компании, особено оние од ИТ индустријата. Тие често располагаат со технолошки знаења и ресурси кои се неопходни за ефикасна заштита од сајбер закани. Затоа, соработката меѓу јавниот и приватниот сектор треба да биде стратешки приоритет. Истото важи и за медиумите, кои треба да бидат партнери во борбата против дезинформации, манипулации и онлајн пропаганда – алатки кои терористичките организации ги користат за регрутација и радикализација.

Неопходно е да се признае дека технолошкиот развој никогаш нема да може целосно да се спречи или контролира, ниту пак е тоа пожелно. Наместо тоа, треба да се стремиме кон развој на етички и безбедносни стандарди кои ќе ги минимизираат ризиците, а ќе ги максимизираат придобивките од технологијата. Ова подразбира континуирана евалуација на заканите, развој на стратегии за сајбер одбрана, и градење на дигитална култура базирана на безбедност, свесност и одговорност.

На крајот, сајбер тероризмот не е само технолошки проблем – тоа е предизвик кој го засега секој аспект од современото живеење. Безбедноста во сајбер просторот е предуслов за економски развој, заштита на човековите права, демократски процеси и национална стабилност. Само со заеднички напори, глобална соработка, постојана едукација и проактивен пристап ќе можеме да изградиме отпорно општество кое ќе се соочи со предизвиците на дигиталната ера.

КОРИСТЕНА ЛИТЕРАТУРА

1. Abadinsky у: Шкулић, М. (2003). Организовани криминалитет. Појам и кривично процесни аспекти, Београд: Досије. Abadinsky, H. (1994). Organized Crime, Chicago: Nelson- Hall Publishers.
2. Abrahamson, P. (1995). Social Exclusion in Europe: Old Wine in New Bottles? Družboslovne razprave 11(19–20), 119–136.
3. Abrams, M., Podell H., Jajodia S. (1995). Information Security: An Integrated Collection of Essays, Los Alamitos, CA USA: Computer Society Press, 117
4. Akhgar, B., Staniforth A. & Bosco F. (2014). Cyber Crime and Cyber Terrorism Investigator’s Handbook, USA: Elsevier Inc.
5. Albrow, M. (1996). The Global Age: State and Society Beyond Modernity. Cambridge: Polity Press.

6. Alqahtani, S. H. (2016). Latest Trends and Future Directions of Cyber Security Information Systems. Journal of Information Engineering and Applications 6 (11), 9-14.
7. Appadurai, A. (2000). Grassroots Globalization and the Research Imagination. Public Culture 12 (1), 1-19 .
8. Arnett, J.J. (2002). The psychology of globalization. American Psychologist, Vol. 57, 774-783.
9. Ashley, K. B. (2003). Anatomy of cyber terrorism: Is America vulnerable? USA: Air University, Maxwell AFB, AL.
10. Auwema, N.M. (2015). The Discourse of Cyberterrorism:Exceptional measures call for the framing of exceptional times, Thesis MSc Political Science.
11. Бабић, В. (2009). Компјутерски криминал, Сарајево: Рабиц. Басан, М., Кофман, В. & Жоа, Д. (2005). „Десет теза за социолошку теорију урбане динамике“. У: Вујовић, С. & Петровић М. (прир.) (2005). Урбана социологија (229-238). Београд: Завод за уџбенике и наставна средства.
12. Bamberg, M. (2011). Who am I? Narration and its contribution to self and identity. Theory and Psychology 21(1), 3-24.
13. Baruch, Y. (2000). Teleworking: Benefits and Pitfalls as Perceived by Professionals and Managers. New Technology, Work and Employment, Vol. 15, 34–49.
14. Бауман, З.(2003). „Туристи и вагабунди“. У: Вулетић, В. (ур.) (2003). Глобализација – мит или стварност (251-273). Београд: Завод за уџбенике и наставна средства.
15. Bauman, Z. (1998). Globalization: the human consequences. New York, Columbia University Press.
16. Beaulac, S. (2004). The Westphalian model in defining international law: challenging the myth. Australian Journal of Legal History Vol. 7, 181–213.
17. Beggs, C & Butler, M. (2004). Developing New Strategies to Combat Cyber-Terrorism, Idea Group Publishing.
18. Бериша, Х. & Баришић, (2016). Безбедносни изазови - Кибернетски простор и информационо ратовање. У: С. Петровић (ур.). Злоупотреба информационих технологија и заштита, Београд: ИТ вештак.
19. Belenky, A. & Ansari, N. (2003). IP Traceback with Deterministic Packet Marking. IEEE Communications Letters, Vol. 7, No. 4.

20. Bianchi, A. (2011). Terrorism and Armed Conflict: Insights from a Law & Literature Perspective. Leiden Journal of International Law 24 (1), 1–21.
21. Bishop, M. (1995). A taxonomy of UNIX system and network vulnerabilities. Technical report CSE 95/10. University of California at Davis: Department of Computer Science.
22. Божиловић, Н. (2004). Рок култура. Ниш: Студенстски културни центар.
23. Бошковић, М. (1998). Организовани криминалитет, Београд: Полицијска академија.
24. Бошковић, М. (1998). Организовани криминалитет, Београд: Полицијска академија.
25. Bobbitt, P. (2008). Terror and Consent: The Wars for the Twenty-First Century. New York: Anchor Books.
26. Boebert, W. E. (2010). A Survey of Challenges in Attribution. Proceedings of a workshop on Deterring CyberAttacks, Informing Strategies and Developing Options for U.S. Policy, Washington DC: National Academy of Sciences.
27. Bollen, J., Mao H. & Zeng, X. (2011). Twitter mood predicts the stock market. Journal of Computational Science 2 (1), 1–8.
28. Boon, S. & Sinclair, C. (2009). A world I don't inhabit: disquiet and identity in Second Life and Facebook. Educational Media International 46 (2), 99–110.
29. Bossler, A.M. & Holt, T.J. (2012). Patrol officers' perceived role in responding to cybercrime. Policing: An International Journal of Police Strategies & Management 35 (1), 165-181.
30. Brenner, S. W. (2007). At Light Speed, The Journal of Criminal Law and Criminology, Vol. 97, No. 2, 379-475.
31. Britz, M. T. (2013). Computer Forensics and Cyber Crime – An Introduction, Prentice Hal, 3th edition.
32. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime, Policing: An International Journal of Police Strategies and Management 2, 408-433.
33. Bryant R. & Stephens, P. (2014). Policing Digital Crime: the International and Organisational Context. In: Bryant R.& Bryant S. (eds.)(2014). Policing Digital Crime (111-123).
34. Surrey: Ashgate Publishing Limited. Burrows, M. & Engelke P. (2020). What World POST-COVID-19? Three Scenarios, Atlantic Council: Scowcroft Center for Strategy and Security.

35. Carr J. (2010). Inside Cyber Warfare, Sebastopol: Reilly Media. Carter, D., Schwartz, N.& Norris, F. (2008, 6. oktobar). Financial crises spread in Europe, New York Times.
36. Chak, K. & Leung, L. (2004) Shyness and locus of control as predictors of internet addiction and internet use. CyberPsychology & Behavior 5, 559-570.
37. Chandan, K. S. (1935). Le terrorisme devant la Societe des Nations, Paris.
38. Cheng, Y. Y. (2010). Social psychology of globalization: Joint activation of cultures and reactions to foreign cultural influence. University of Illinois at Urbana-Champaign: PhD Dissertation.
39. Chiu, C.Y., Gries, P., Torelli, C. J. & Cheng, S. Y.Y. (2011). Toward a social psychology of globalization. Journal of Social Issues 67, 663–676.
40. Clarke R. & Knake R. (2010). Cyber War – The next treat to National Security and What to do about it, Harper Collins Publisher.
41. Cohen, F. (1997). Information system attacks: a preliminary classification scheme. Computer & Security 16 (1), 29-46.
42. Collin, B. (1997).The Future of Cyberterrorism, Crime and Justice International 13(2),15-18.
43. Condorelli, L. & Naqvi, Y. (2004). The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of" Date? In: Bianchi A. & Naqvi Y. (eds.) (2004) Enforcing International Law Norms Against Terrorism (25-37). Oxford ; Portland, Or. : Hart.
44. Correia, M. & Bowling, C. (1999). Veering toward digital disorder: computer-related crime and law enforcement preparedness. Police Quarterly 2 (2), 225-244.
45. Cottim, A. (2010). Cibercrime, cyberterrorism and jurisdiction: an analysisof article 22 of the COE convention of cybercrime. European Journal of Legal Studies 2 (3), European University
46. Cronin A.C. (2009). Behind the Curve, Globalization and International Terrorism. In: Howard, D. R., Sawyer, L.R & Bajema, E.N. (eds.), Terrorism and Counter Terrorism, Readings and Interpretations (30-58). Boston: Higher education.
47. Davis, T. J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component, Policing: An International Journal of Police Strategies & Management 35 (2), 272-284.
48. Deardorff, A. & Stern, R. (2001). What you should know about globalization and the world trade organization? Review of International Economics, 403-427.

49. Della Porta D. (2012). Communication in movement: Social movements as agents of participatory democracy. In: Loader B. & Mercea D. (eds) Social Media and Democracy: Innovations in Participatory 221 Сајбер тероризам Politics (39–55). London: Routledge.
50. Denning, D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy. In: Arquilla, J. & Ronfeldt, D. (eds.) (2001) Networks and Netwars. The Future of Terror, Crime, and Militancy (239-288).
51. RAND Corporation. Denning, D. (2014). Framework and Principles for Active Cyber Defense. Computers & Security, Vol. 40, 108-113.
52. Dogrul, M., Aslan A. & Celik E. (2011). Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, Turkey: Turkish Air War College Istranbul.
53. Dollar, D. & Kraay, A. (2001). Trade, Growth and Poverty. Washington: The World Bank, Development Research Group.
54. Dreher, A., Gassebner M. & Siemers, L. H. (2010). Does Terrorism Threaten Human Rights? The Journal of Law & Economics 53 (1), 88.
55. Duggan, P. (2015). Harnessing cyber-technology's human potential, Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School, Vol. 28, Iss. 4, p. 15.
56. Dunn-Cavelty, M. (2008). Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age. New York: Routledge, Print.
57. Ериксон, Е. (2008). Идентитет и животни циклус. Београд: Завод за уџбенике.
58. Everett, A. (2004). On cyberfeminisms and cyberwomanism: High-tech mediations of feminism's discontents. Signs: Journal of Women in Culture and Society 30(1), 1278–1285.
59. Farwell, J.P. & Rohozinski, R. (2012). The New Reality of Cyber War,Survival 54 (4), 107–120.
60. Ferreira, F. (1999). Inequality and Economic Performance. Washington: World Bank.
61. Fidler, P. D, Pregent, R & Vandurme, A. (2013). Nato, Cyber Defense, and International Law, ST. John's Journal of International & Law 4 (1), 1-25.
62. Flaxner S. B. (1987). The Random Hause Dictionary of the English language, New York: Random House.
63. Frances, S. (2004). Development and security, Conflict, Security and Development 4(3), 261-288.

64. Friedman, T. L. (1999). The Lexus and the Olive Tree, US: Farrar, Straus and Giroux.
65. Fu, H.-Y., & Chiu, C. -Y. (2007). Local culture's responses to globalization: Exemplary persons and their attendant values. Journal of CrossCultural Psychology, Vol. 38, 636–653.
66. Geer, E. Daniel Jr. (2006). The Physics of Digital Law: Searching for Counterintuitive Analogies. In: Balkin, J. M., Grimmelmann J.,
67. Katz E., Kozlovski N.,Wagman S., Zarsky T., (Eds.), Cybercrime: Digital Cops in a Networked Environment (13-36). New York University Press.
68. Gilpin R. (2001). Global Political Economy: Understanding the International Economic Order, Princeton University Press.
69. Giraldo, J. & Trinkunas, H. (2010). Terrorism Financing and State Responses: A Comparative Perspective. Redwood: Stanford University Press.
70. Goodman, M. (2001). Making computer crime count. FBI Law Enforcement Bulletin, 70 (8), 10-17.
71. Гаћиновић, Р. (1998). Савремени тероризам, Београд: Графомарк.
72. Гаћиновић, Р. (2011). Тероризам – Изазов науке и политике. У: Шикман, М., Амиџић Г. (ур.) СупростављањетероризмуМеђународни стандарди и правна регулатива. Бања Лука: Висока школа унутрашњих послова.
73. Goodman, S. E. (2007). Cyberterrorism and Security Measures. In: National Academy of Sciences, R. Narasimha, A. Kumar, S. P. Cohen & R. Guenther (Eds.), Science and Technology to CounterTerrorism. The Proceedingsof an Indo – U.S Workshop (43-54), Washington DC: The National Academy Press.
74. Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology 2 (1), 13–20.
75. Гиденс, Е. (1998) Последице модерности, Београд: Филип Вишњић. Гиденс, Е. (2003). Социологија, Београд: Економски факултет.
76. Giddens, A. (2005). Odbjegli svijet – kako globalizacija oblikuje naše živote? Zagreb: Klub studenata sociologije Diskrepancija i Naklada Jesenski i Turk.
77. Grabosky, P. (2007). Electronic Crime, New Jersey: Pearson Prentice Hall.
78. Gray, J. (1998). False Dawn. The Delusions of Global Capitalism, New York Press.
79. Greitzer F.L. & Ferrymann T.A. (2013). Methods and metrics for evaluating analytic insider treat tools. In: Proccedings of the 2013 IEE security and privacy workshops (SPW'13), (90-97).

80. California, USA: IEE. Hafner, K. (1998). Where Wizards Stay Up Late: The Origins of the Internet, New York: Simon & Schuster.
81. Hagan, E. F. (2010). Crime Types and Criminals. Thousand Oaks, California: SAGE Publications.
82. Halfond, W., Viegas, J, Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures, IEEE International Symposium on Secure Software Engineering, The Institute of Electrical and Electronics Engineers.
83. Hapa, J. and Fairclough, G. (2017). „A Model to Facilitate Discussions about Cyber Attacks“. In: M. Taddeo, L. Glorioso (eds.), Ethics and Policies for Cyber Operations. Philosophical Studies Series 124, Springer International Publishing Switzerland, 169-185.
84. Harmon, C.C. (2000). Terorrism today, London; Portland, OR: Frank Cass.
85. Hathaway, A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue W., Spiegel, J. (2012). The Law of Cyber-Attack. California Law Review 100 (4), 817-885.
86. Hengsbach, F. (1997). Ein neuer Gesellschaftsvertrag in Zeiten der Globalisierung. In: Fricke, W. (Ed.), Jahrbuch Arbeit und Technik (182–195), Dietz: Bonn.
87. Holm, H., Ekstedt, M &Andersson, D. (2012). Empirical analysis of system-level vulnerability metrics through actual attacks, Transactions on Dependable and Secure Computing 9 (6), 825– 837.
88. Iasiello, E. (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy, Tallinn: NATO CCD COE Publications.
89. Janczewski L. & Colarik, A. (2008). Cyber Warfare and Cyber Terrorism, Hersey (USA): IGI Global.
90. Јазић, А. (2010). Терористичка пропаганда и улога медија, Међународни проблеми, Вол. 62, Бр.1, 113-135.
91. Јовашевић, Д. (2011). Лексикон кривичног права. Београд: Службени 231 Сајбер тероризам гласник. Јовић, В. (2001). Прикриверни иследник, Београд: Сезам.
92. Јонев, К. & Бериша, Х. (2016). Опасност од кибертероризма. У: С. Петровић (ур.). Злоупотреба информационих технологија и заштита- ЗИТЕХ16, Београд: ИТ вештак Кастелс, М. (2000). Информацијско доба : економија, друштво и култура. Књ. 1, Успон умреженог друштва. Загреб : Голден маркетинг.
93. Jones, A. L. & Howard- Hassmann, R. E. (2005). Under Strain: Human Rights and International Law in the Post 9/11 Era, Journal of Human Rights, Vol. 4, 61–71.

94. Kacerguis, M. & Adams, G. (1979). Erickson stage resolution: The relationship between identity and intimacy. Journal of Youth and Adolescence 9(2), 117-126.
95. Kahn R. & Kellner, D. (2004). New media and internet activism: From the Battle of Seattle to blogging. New Media and Society 6(1), 87–94.
96. Kandias, M., Stavrou V, Božović N., Mitrou L., Gritzalis, D. (2013). Predicting the insider threat via social media: the YouTube case, In: Proccedings of the 12th ACM Workshop on privacy in the electronic society (261-266), Berlin: ACM Press.
97. Katz, C. (2004). Growing up global: economic restructuring and children's everyday lives. Minneapolis, MN: University of Minnesota Press.
98. Kaul, I. (1994). Human security: The need for a new security council. Roundtable on Global Change. Change: Social Conflict or Harmony? United Nations Development Programme (UNDP), Stockholm, Sweden. Participant Paper no. 32 (22–24 July).
99. Kegley, C. W. Jr. (2003). The New Global Terrorism: Characteristics, Cause, Control, New Jersey: Prentice Hall.
100. Комлен Николић Л, Гвозденовић Р., Радуловић, С., Милосављевић, А., Јерковић, Р, Живковић, В. Живановић, С, Рељановић, М, Алексић, И. (2010). Сузбијање високотехнолошког криминала, Београд: Удружење јавних тужилаца и заменика јавних тужилаца Србије. Куљански Р. С. (2010). РСА алгоритам и његова практична примена. Војнотехнички гласник: стручни и научни часопис Југословенске народне армије 58 (3), 65-77.
101. Keith, J, Bejtlich, R. & Rose, C. (2008). Real Digital Forensics, New Jersey: AddisonWesley.
102. Khamis, S. (2015). Gendering the Arab Spring: Arab women journalists/ activists, cyber-feminism and the socio-political revolution. In: Carter C, Steiner L and McLaughlin L (Eds.) The Routledge Companion to Media and Gender (565–575), London: Routledge.
103. Kizza J. (2009). Guide to Computer Network Security, London: Springer.
104. Лукнар, И. (2022а). „Прошлост као инструмент геополитике". У: З. Милошевић (ур.), Историја као инструмент геополитике (141-161). Београд: Институт за политичке студије.
105. Љајић, С., Мета, М. & Младеновић, Ж. (2016). Глобализација економски и психолошки аспекти, Економски сигнали: пословни магазин 11 (1), 39-62.
106. Lechner, J. F. & Boli, J. (2003). The Globalization Reader. Maiden: Mass.

107. Lemkin, R. (1933). Faut il un nouveau délit de droit gens nomme terrorisme, Revue de droit penal et criminologie, Belge, no. 13, 900–901.
108. Li, H., Squire, L. & Zou, H. (1998). Explaining International and Intertemporal Variations in Income Inequality. The Economic Journal Vol. 108, 26-43.
109. Li, Q. (2005). Does democracy promote or reduce transnational terrorist incidents? Journal of Conflict Resolution 49 (2), p. 278 - 97.
110. Liem, A., C. Wang, Y. Wariyanti, C.A. Latkin & B.J. Hall (2020). The neglected health of international migrant workers in the COVID-19 epidemic. The Lancet Psychiatry 7 (4). doi: 10.1016/S2215- 0366(20)30076-6
111. Luknar, I. (2018). Terrorism and human rights. In: M Gjurovski (Ed.), Security System Reforms as Precondition for Euro-Atlantic Integrations. Vol. 2. International scientific conference Ohrid (p. 94-99). Skopje: Faculty of security.
112. Luknar, I. (2020a). Cyber Terrorism Threat and the Pandemic. In: Cane T. Mojanoski (Ed. in chief), The Euro-Atlantic values in the Balkan countries, Vol. 3 (p. 29-38). Bitola: University "St. Kliment Ohridski", Skopje: Faculty of Security.
113. Luknar, I. (2020b). Cybercrime – Emerging Issue. In: S. Jaćimovski (ed.), Archibald Reiss Days. Vol. 10. International scientific conference (621-628). Beograd: Kriminalističko-policijski univerzitet.
114. Luknar, I. (2021). „Social implications of the Internet in new reality due to COVID-19", Српска политичка мисао, Вол. 72, Бр. 2, 225-235.
115. Luknar, I. (2022b). Social control theory and cibercrime issue. Национални интерес, Бр.1,
116. Lundberg, M. & Squire, L. (2000). The Simultaneous Evolution of Growth and Inequality. World Bank Working Paper.
117. Lutz M. J. & Brenda J. L. (2004).
118. Global Terrorism, Routledge. Mahoney, J. (2000). Path Dependence in Historical Sociology. Theory and Society, 29(4), 507-548.
119. Manap., N.A., & Tehrani, P. M. (2012). Cyber Terrorism: Issues in Its Interpretation and Enforcement. International Journal of Information and Electronics Engineering, 2(3), 409-413.
120. Мандер, Џ. (2003). „Правила корпорацијског понашања". У: Џ. Мандер и Е. Голдсмит, Т. Живић, М. Марковић, И. Чорбић (Прир.). Глобализација – аргументи против, Београд: Clio. Марић, Р. (1998). Поткултурни стил као поље симболичке акције. Социологија 40(2), 159-190.

121. Мијалковић, С. & Бошковић, Г. (2009). Прање новца и финансирање тероризма. У: Матијевић, М. (ур.). Корупција и прање новца – узроци, откривање, превенција (293–302). Сарајево: Интернационална асоцијација криминалиста.
122. Милашиновић, Р. & Мијалковић, С. (2011). Тероризам као савремена безбедносна претња. У: Шикман, М., Амицић Г. (ур.) Супростављање тероризму-Међународни стандарди и правна регулатива. Бања Лука: Висока школа унутрашњих послова.
123. Matijašević-Obradović, J. (2014). The Significance and modalities of internet abuse as the primary global communicat. computer networks in cyberspace. Megatrend revija 11(1), 279-298.
124. Mattdort, J. H. & Whitman, E.M. (2011). Roadmap to Information Security, USA, Boston: Course Technology.
125. Merton, R.K. (1957). Social theory and social structure, Glencoe, Ill. : Free Press. 225
126. Miller, C., Matusitz, J., O'Hair, D., & Eckstein, J. (2008). The complexity of terrorism: Groups, semiotics, and the media. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), Terrorism: Communication and retorical perspectives. Cresskill, NJ: Hampton Press.
127. Mittelman, H. J. (2000). The Globalization Syndrome: Transformation and Resistance, Princeton University Press. Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet, Global Politics and Strategy, Vol.58, No.1, 7-38. Morris, M. W., Mok, A. & Mor, S. (2011). Cultural identity threat: The role of cultural identifications in moderating closure responses to foreign cultural inflow. Journal of Social Issues, Vol. 67, 760–773.
128. Munkhdorj, B. & Yuji S. (2017). Cyber attack prediction using social data analysis, Journal of High Speed Networks 23 (2), 109–135.
129. Murthy, D. (2012). Towards a Sociological Understanding of Social Media: Theorizing Twitter, Sociology 46(6), 1059 –1073.
130. Nagar, R, Lawson, V, Mc Dowell & Hanson, S. (2002). Locating globalization: feminist (re)readings of the subjects and spaces of globalization. Economic Geography, 78 (3), 257–284.
131. Neeraj (2001). Globalisation or Recolonisation, ELGAR: Pune. Nguyen, R. (2013). „Jus Ad Bellum" in the Age of Cyber Warfare,
132. Nicholas N. (2007). The Black Swon – The Impact of the Highly Improbable, New York : Random House.

133. Ning, H., Liu, H., Ma, J., Yang, T. L. & Huang, R. (2016). Cybermatics: Cyber-physical-social-thinking hyperspace based science and technology. Future Generation Computer Systems Vol. 56, 504- 522.
134. Norasakkunkit, V. & Uchida, Y. (2011). Psychological consequences of postindustrial anomie on self and motivation among Japanese youth. Journal of Social Issues Vol. 67, 774–786.
135. Norris, P. (2011). Democratic Deficit. Critical Citizens Revisited. Cambridge: Cambridge University Press.
136. O'Harrow, R. Jr. (2005). No Place to Hide, New York: Free Press.
137. Olsen, M. (1969). Two Categories of Political Alienation. Social Forces Vol. 47, 288-299.
138. Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective, IEEE Security & Privacy 1 (5), 35-43. Palazzi, E. (1965). Dizionario della lingua italiana, Milano: Garzanti.
139. Paletz, L. D. & Schmid P. A. (1992). Terrorism and the Media, Sage Publications: Newbury Park.
140. Pauwels, T. (2014). Populism in Western Europe: Comparing Belgium, Germany and the Netherlands. London: Routledge.
141. Payne B. K., & Walton, C. D. (2002). Deterrence in the Post-Cold War World. In: John Baylis, James Wirtz, Eliot Cohen, and Gray Colin (Eds.), Strategy in the Contemporary World, An Introduction to Strategic Studies, Oxford: Oxford University Press.
142. Павлићевић, П. (2017). Тероризам и организовани криминал: анализа и процена ризика. Национална безбедност 4 (6), 34–56.
143. Пејановић, Љ. & Бејатовић, М. (2009). Авиотероризам, Нови Сад: АБМ економик. Пејановић, Љ. (2003). Тероризам и противтерористичка дејства у ваздушном саобраћају, Београд: ВИЗ-ЈАТ.
144. Петровић, Д. (1998). Организовани криминалитет између визије и реалности. У: Д. Стојановић (ур.) Србија и европско право III (30-48), Крагујевац: Правни факултет Универзитета: Институт за правне и друштвене науке.
145. Петровић, Р.С. & Стојановић Р. М. (2016). Информациона технологија у функцији криминала беле-крагне. У: С. Петровић (ур.). Злоупотреба информационих технологија и заштита, Београд: ИТ вештак, 13-26.
146. Piazza, J.A. & Walsh, J.I. (2010). Terrorism and Human Rights: Editors' Introduction. Political Science and Politics 43 (3), 407-409.

147. Piketty, T. (2015). Kapital u dvadesetprvom veku, Sarajevo: Buybook.
148. Pipyros K., Thraskias C., Mitrou L., Gritzalis D., Apostolopoulos T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, Computers & Security Vol. 74, 371-383.
149. Robertson, R. (1992). Globalization: Social theory and global culture. London: Sage Publications Ltd.
150. Sassen, S. (2002). Towards a sociology of information technology. Current Sociology 50(3), 365–385.
151. Савић, А. & Стајић Љ. (2006). Основи цивилне безбедности, Нови Сад: Факултет за правне и пословне студије.
152. Симеуновић, Д. (1989). Политичко насиље, Београд: Радничка штампа.
153. Симеуновић, Д. (1993). Насиље. Енциклопедија политичке културе, Београд: Савремена администрација.
154. Симеуновић, Д. (2009). Тероризам: општи део, Београд: Правни факултет Универзитета у Београду.
155. Скакавац, З. (2010). Тероризам - савремени феноменолошки облици испољавања и карактеристике. У: М, Крећа (ур.). Међународни научни скуп Тероризам и људске слободе, Вол. ИХ. (331-345), Београд: Удружење за међународно кривично право.
156. Savona, E.U., Adamoli, S., Di Nicola A. & Zoffi, P. (1998). Organized Crime Around the World, No. 31, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI).
157. Schjolberg, S. (2014). The History of Cybercrime: 1976-2014, Koln.
158. Schmid, A. (1996). The links between transnational organized crime and terrorist crimes. Transnational Organized Crime 2(4), 40-82.
159. Schmid, A., Jongman A. (2005). Political Terrorism. Piscataway, NJ: Transaction Publishers.
160. Schmitt, N. M. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press.
161. Schuster, J. (2013). Invisible feminists? Social media and young women's political participation. Political Science 65(1), 8–24.
162. Selley, L. (2003). Organized Crime, Terrorism and Cybercrime. In: Alan Bryden, Philipp Fluri (eds.) Security Sector Reform: Institutions, Society and Good Governance (303-312). Nomos Verlagsgesellschaft: Baden-Baden.

163. Sennett, R. (1998). The Corrosion of Character. The Personal Consequences of Work in the New Capitalism. W. W. Norton & Company, New York/London.
164. Shelley, L. I. & Melzer, S., A. (2008). The Nexus of Organized Crime and Terrorism: Two Case Studies in Cigarette Smuggling, International Journal of Comparative and Applied Criminal Justice 32 (1), 1-21.
165. Shinder, L. D. (2002). Scene of the Cybercrime: Computer Forensics Handbook. USA; Rockland, MA: Syngress Publishing Inc.
166. Sieber, U. (1994). Information Technology Crime – National Legislations and International Initiatives, Köln: Carl Heymanns Verlag.
167. Silvey, R. (2009). Development and geography: anxious times, anemic geographies and migration, Progress in Human Geography, 33(4), 507–515.
168. Sinai, J. (2011). Terrorism on the Internet and Effective Countermeasures, The Intelligencer: Journal of U.S. Intelligence Studies Vol. 18, 21–24.
169. Sklair, L. (2013). Globalization. Capitalism and its Alternatives. Oxford University Press.
170. Sofaer, A. D. (2010). The Best Defense? Legitimacy and Preventive Force, Stanford, CA: Hoover Institution Press.
171. Solange G.H. (2009). Cybersecurity Guide for Developing Countries, Geneva: International Telecommunication Unione.
172. Sommestad, T. (2012). A framework and theory for cyber security assessments. Doctoral dissertation, Stockholm, Sweden: KTH, Royal Institute of Technology.
173. Stallings, W. & Brown L. (2015). Computer security : principles and practice, Harlow : Pearson Education Limited.
174. Stavrou V, Kandias, M., Karoulas G., Gritzalis, D. (2014). Business process modeling for insider threat monitoring and handling. In: Proccedings of the 11th international conference on trust, privacy &security in digital business (119-131). Germany: Springer.
175. Stoll, C. (2005). The Cuckoo's Egg, New York: Gallery Books.
176. Stytz, M. (2006). Cyberwarfare Distributed Training, Military Technology (MILTECH) Vol. 11, 95-96.
177. Тасић, В. & Бауер И. (2003). Речник компјутерских термина, Београд: Микро књига. Томашевски, К. (1983). Изазов тероризма, Београд: НИРО Младост.
178. Talbot, J. & Welsh D. (2006). Complexity and Cryptography: an introduction, Cambridge: Cambridge University Press.

179. Tavani H. T. (2003). Ethics and Technology: Ethical Issues in an Age of Information and Communications Technology, Hoboken, John Wiley & Sons Inc.
180. Todd, E. (2003). After the Empire: The Breakdown of the American Order, New York: Columbia University Press. Tomlinson, John (1999): Globalization and Culture, Cambridge: Polity Press.
181. Tong, Y. -Y., Hui, P. P. -Z., Kwan, L. & Peng, S. (2011). National feelings or rational dealings? The role of procedural priming on the perceptions of cross-border acquisitions. Journal of Social Issues 67, 743–759.
182. Tonhauser, M. & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level, Transportation Research Procedia 40, 1591–1596. https://doi.org/10.1016/j. trpro.2019.07.
183. Townsend, P. (1979). Poverty in the United Kingdom. Harmondsworth: Penguin Books.
184. Townsend, P. (1987). Deprivation. Journal of Social Policy, 16(2), 125–146.
185. Trager F. R & Zagorcheva, P. D. (2005-2006). Deterring Terrorism, International Security 30 (3), 87-123.
186. Tsakloglou, P. & Papadopoulos, F. (2002). Aggregate Level and Determining Factors of Social Exclusion u Twelve European Countries, Journal of European Social Policy 12(3), 211–225.
187. Урошевић, В. (2009). „Нигеријска превара“ у Републици Србији, Безбедност Вол.3, 1-12 Хантингтон, С. (2000). Сукоб цивилизација, Подгорица: ЦИД Хелд, Д. (2003). Дебате о глобализацији. У: В. Вулетић (ур.), Глобализација – мит или стварност (48-60). Београд: Завод за уџбенике и наставна средства.
188. United Nations Environment Programme (2021). Emissions Gap Report 2021: The Heat Is On – A World of Climate Promises Not Yet Delivered. Nairobi.
189. Vandemoortele, J. (2002). Are we really reducing global poverty. New York: UNDP. Vernotte, A., Dadeau, F., Lebeau, F., Legeard, B., Peureux, F. & Piat, F. (2014). Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities, 10th International Conference on Information Security Systems, Indija: ICISS 2014.
190. Vidanage, H. R. (2006). Apparition of the predator. The Lanka Academic, 6 (281), p. 3.
191. Wagner, R. Abraham (2005). Terrorism and the Internet: Use and Abuse. In: Fighting Terror in Cyberspace, Terrorism and the internet; (Eds.) Mark Last, Abraham Kandel, World Scientific.

192. Wagner-Pacifici, R. & Hall, M. (2012). Resolution of Social Conflict. Annual Review of Sociology Vol. 38, 181-199.
193. Walsh E. L. (1997). Firewall : the Iran-contra conspiracy and cover-up, New York: W. W. Norton & Company.
194. Walsh, J. I. (2007). Do States Play Signaling Games? Cooperation and Conflict: Journal of the Nordic International Studies Association 42 (4), 441.
195. Weaver, L.R., Abramson, W.L. & Bacigal, R. (2007). Criminal Procedure, cases, Problem and Exercises, USA: Gale Cengage.
196. Weimann, G. (2006). Terror on the Internet: Tne New Arena, The New Challenges, Washington: United States Institute of Peace Press.
197. Weimann, G. (2015). Terrorism in Cyberspace. The Next Generation, New York: Columbia University Press.
198. Weinstock N. N. (2000). Cyberspace self-Governance, California Law 229 Сајбер тероризам Review Vol. 88.
199. Wenger, E., McDermott, R., & Snyder, W. M. (2002). Cultivating communities of practice. Boston: Harvard Business School Press.
200. Williams, K. (2008). Using Tittle's control balance theory to understand computer crime and deviance, International Review of Law Computers & Technology 22 (1-2), 145-155.
201. Wong, P. T (2011). Active cyber defense: enhancing national cyber defense, Calhoun: The NPS Institutional.
202. Yang, D. Y-J., Chen, X., Cheng, S. Y. Y., Kwan, L., Tam, K. -P., & Yeh, K. -H.(2011). The lay psychology of globalization and its social impact. Journal of Social Issues Vol. 67, 677–695.
203. Yeates, N. (2001). Globalization and Social Policy, London: SAGE Publications.
204. Yergin, D. & Stanislaw, J. (2002). The Commanding Heights: The Battle for the World Economy,